Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

TS-03109-5

Testspezifikation zur Technischen Richtlinie TR-03109-5

Version 1.1.1

Datum 11.06.2024

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: smartmeter@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Einleitung

1.1 Zielsetzung

Die Technische Richtlinie [TR-03109-5] beschreibt Mindestanforderungen an CLS-Kommunikationsadapter im Home-Area-Network (HAN) eines Smart-Meter-Gateways (SMGW).

Das vorliegende Dokument ist die Testspezifikation für die [TR-03109-5]. Diese beschreibt zum einen die vorläufigen Testfälle, die durchgeführt werden müssen, um die Korrektheit der Implementierung der funktionalen Anforderungen aus der [TR-03109-5] bewerten zu können. Zum anderen werden die Mitwirkungspflichten eines Geräteherstellers dargestellt, die für eine Bewertung durch eine unabhängige Prüfstelle erfüllt werden müssen. Die Testspezifikation ist die Grundlage für eine TR-Zertifizierung, über die der Nachweis der Konformität zur [TR-03109-5] erbracht werden kann.

Die aktuelle Version der Testspezifikation ermöglicht den Nachweis einer Mindestinteroperabilität für die [TR-03109-5], sowie der zugehörigen Detailspezifikation [DS] und der mitgeltenden [TR-03109-3]

1.2 Zielgruppe

Die Testspezifikation ist primär für den folgenden Adressatenkreis vorgesehen:

- Hersteller von CLS-Kommunikationsadaptern, welche die Konformität ihres Produkts zu den Anforderungen der [TR-03109-5] überprüfen möchten.
- Prüfstellen, welche die Konformität eines Gerätes zu den Anforderungen der [TR-03109-5] unabhängig bewerten und in einem Prüfbericht dokumentieren sollen.
- Zertifizierungsstellen, welche auf Basis von Prüfberichten im Fall einer bestandenen Prüfung ein TR-Zertifikat erteilen können.

1.3 Konformitätsprüfung und Zertifizierung

Die Testspezifikation ist Grundlage für Zertifizierungen nach [TR-03109-5]. Allgemeine Informationen zu Zertifizierungen gemäß Technischen Richtlinien des BSI können auf [TRZertWeb] eingesehen werden.

1.4 Aufbau der Testspezifikation

In ▸Kapitel 2 wird die Notation festgelegt, die bei der Beschreibung der Testfälle Anwendung findet und zum Verständnis der Testfälle beitragen soll.

In ▸Kapitel 3 wird anschließend der Testaufbau und die Testumgebung beschrieben. Dabei werden auch die notwendigen technischen Akteure beschrieben, die in der Testumgebung benötigt werden.

In ▸Kapitel 4 werden die Testfälle beschrieben, die für eine Konformitätsbewertung nach [TR-03109-5] durchgeführt und bestanden werden müssen.

1.5 Versionshistorie

Version	Datum	Beschreibung
1.0	06.12.2023	Initiale Version 1.0
1.1	07.06.2024	Release Version 1.1
1.1.1	11.06.2024	TC.CLS.TLS.MustAbortHandshakeWithExpiredServerCertificate entfällt
		TC.CLS.ZEIT.MustGetSystemTime entfällt
		TC.CLS.TLS.MustNotAcceptEarlyData entfällt

Tabelle 1.1 Versionshistorie

2 Testfallnotation

Die Testfälle, welche in ▸Kapitel 4 als Unterkapitel hinterlegt sind, enthalten jeweils die folgenden Informationen:

Überschrift Die Kapitelüberschrift eines Testfallkapitels beinhaltet die Testfall-ID. Die Testfall-ID ist ein eindeutiger Bezeichner für den Testfall in der Form TC.<Kategorie>.<Unter-Kategorie>.<Sprechender Name>.

Version Die Versionsnummer des Testfalls in der Form <Major>.<Minor>.<Patch> [1].

Zweck Kurze textuelle Beschreibung, die das Ziel des Testfalls angibt.

Kurzbeschreibung Kurze textuelle Beschreibung, die den Ablauf des Testfalls angibt.

Abgedeckte Anforderungen Die Anforderungen aus der [TR-03109-5], deren korrekte Umsetzung im Testfall überprüft wird.

Relevante Implementation-Conformance-Statements (ICS) Die Implementation-Conformance-Statements (ICS) aus der [TR-03109-5], die für die Durchführung des Testfalls relevant sind.

Ein Testfall ist nur dann auszuführen, wenn alle binär (Ja bzw. Nein) zu beantwortenden ICS als zutreffend beantwortet wurden.

Der Hersteller hat die in den ICS geforderten Informationen bereitzustellen.

Vorbedingungen Die Tabelle **Status** enthält Vorbedingungen, die der Testfall als gegeben voraussetzt.

Bei Testfällen, die Interaktionen mit dem Prüfgegenstand vorsehen, wird hier beispielsweise Betriebszustände genannt, in denen sich der Prüfgegenstand befinden muss. Weitere Vorbedingungen sind z.B. Festlegungen, welche Konfigurationsprofile vor der Durchführung des Testfalls eingespielt werden müssen.

Hinweis: Der Aufbau von Kommunikationsverbindungen ist eine implizite Vorbedingung, es sei denn der Verbindungsaufbau befindet sich im Fokus des Testfalls. Gleiches gilt für die erfolgreiche Authentifizierung eines Akteurs vor Durchführung von Aktivitäten.

Weitere allgemeine technisch notwendige Vorbedingungen sind in ▸Kapitel 3 zu finden.

Vorbereitende Testschritte Vorbereitende Testschritte sind die Testschritte des Testfalls, die vor Durchführung des eigentlichen Testablaufs abgearbeitet werden müssen, z.B. um den Prüfgegenstand für die Durchführung des Testfalls vorzubereiten.

Testschritte Testschritte sind die Testschritte des Testfalls, welche den eigentlichen Testablauf beinhalten, um das Ziel des Testfalls zu erreichen. Diese Testschritte des Testfalls werden jeweils mit folgenden Informationen beschrieben:

- **Nr.** Die laufende Nummer des Testschritts.
- **Beschreibung** Eine ausführliche Beschreibung des Testschritts.
- **Erwartetes Ergebnis** Die Liste der erwarteten Ergebnisse nach der Durchführung des Testschritts.

Nachbereitende Testschritte Nachbereitende Testschritte sind die Testschritte des Testfalls, die nach Durchführung des eigentlichen Testablaufs abgearbeitet werden müssen, z.B. um den Prüfgegenstand wieder in einen definierten Status, wie den Ausgangsstatus, zurückzusetzen.

[1] Die Bedeutung der Versionsnummer entspricht Semantic Versioning gemäß https://semver.org.

3 Testaufbau und Testumgebung

Das folgende Kapitel beinhaltet einerseits Anforderungen, die an eine Implementierung der Testfälle gestellt werden. Dies betrifft insbesondere Anforderungen, wenn für die Durchführung der Testfälle nicht die durch das BSI bereitgestellte Smart-Metering-Testplattform verwendet wird.

Andererseits enthält dieses Kapitel ebenfalls Anforderungen an Dokumentation und Nachweisführung, sofern die ausgeführten Testfälle zur Zertifizierung des Prüfgegenstandes herangezogen werden sollen. Üblicherweise sind diese Dokumentationen und Nachweisführungen von einer Prüfstelle einem abschließenden Prüfbericht hinzuzufügen.

3.1 Allgemeine Anforderungen an die Testumgebung

Der wesentliche Teil der Testfälle in ▸Kapitel 4 benötigt einen einheitlichen Testaufbau für die Testdurchführung. Neben dem CLS-Kommunikationsadapter als Prüfgegenstand wird für den Testaufbau eine Testumgebung benötigt, welche die Funktionen eines Externen Marktteilnehmers (EMT) und eines SMGW an dessen HAN-Schnitttstelle simuliert.

Für die Prüfung des Prüfgegenstands muss dieser mit der HAN-Schnittstelle (s. Kap. 2.2 in [TR-03109-1]) des SMGW der Testumgebung verbunden werden. Darüber hinaus müssen abhängig vom Prüfgegenstand ggf. weitere physische Schnittstellen (vgl. Kap. 2.4.1.1 in [TR-03109-5]) mit den für sie vorgesehenen Netzwerken verbunden werden. Die die Prüfung betreffenden technischen Akteure sind in ▸Tabelle 3.1 aufgeführt.

Technischer Akteur	Beschreibung
SMGW	Für jeden Testfall wird, sofern in den Testfallparametern oder -hinweisen nicht anders angegeben, genau ein SMGW benötigt. Auf dem SMGW müssen die notwendigen Profile für den Prüfgegenstand sowie benötigte Externe Marktteilnehmer (EMT) installiert werden, um eine Proxyverbindung zwischen dem Prüfgegenstand und dem EMT zu erlauben.
EMT	Es wird ein EMT benötigt, der in der Lage ist, Daten mit dem Prüfgegenstand auszutauschen. Soweit der Prüfgegenstand das Network Time Protocol (NTP) implementiert, muss der EMT auch dies unterstützen.
Weitere Akteure	Abhängig von der Ausprägung des Prüfgegenstands können weitere Akteure am Testgeschehen teilnehmen. Der Grund für die Notwendigkeit weiterer Akteure und deren Einwirken auf den Prüfgegenstand ist für jeden Testfall zu dokumentieren. Akteure, die lediglich dazu dienen, die Funktionsweise von Geräten, die nicht der Prüfgegenstand sind, zu gewährleisten und nicht mit dem Prüfgegenstand interagieren (z.B. ein SMGW-Administrator), müssen nicht dokumentiert werden.

Tabelle 3.1 Technische Akteure in der Testumgebung

Der Testaufbau stellt sicher, dass

- Netzwerkverbindungen zwischen SMGW, EMT sowie Prüfgegenstand funktionieren und
- notwendige Adressen für die technischen Akteure eingerichtet wurden (z.B. IP, DHCP).

Es ist grundsätzlich unerheblich, ob die benötigten technischen Akteure als separate physische Komponenten betrieben oder ob mehrere Akteure durch eine Komponente simuliert werden, sofern die jeweils notwendigen Kommunikationsszenarien entsprechend korrekt angewendet werden.

Die technischen Akteure unterstützen insbesondere auch bei der Erzeugung der Evidenzen, die gemäß der Testfallbeschreibungen in ▸Kapitel 4 zusammengetragen werden müssen (siehe auch ▸Abschnitt 3.2).

Testfälle, die zur Zertifizierung vorgelegt werden sollen, werden grundsätzlich unter Verwendung derselben, zu zertifizierenden Software-Version durchgeführt.

3.2 Nachweise

Für jeden auszuführenden Testfall müssen für den Zeitraum zwischen den Testschritten, die das Tracing starten und beenden, die Nachweise aus ▸Tabelle 3.2 bereitgestellt werden.

Nachweistyp	Beschreibung
Netzwerkmitschnitt	Ein Mitschnitt aller eingehenden und ausgehenden Daten an einer benannten Schnittstelle des Prüfgegenstands zwischen dem Starten des Tracings bis zum Beenden bzw. Stoppen des Tracings. Der Mitschnitt muss eine Inspektion der Daten auf allen Netzwerkschichten erlauben, diese aber nicht entschlüsseln oder Schlüsselmaterial bereitstellen. Ein Beispiel für einen Netzwerkmitschnitt wäre eine von Wireshark erzeugte Datei im packet capture (pcap)-Format.
Anfrage-Antwort-Protokoll	An den Prüfgegenstand oder externe Systeme (z.B. ein EMT) gesendete oder empfangene Nachrichten auf Inhaltsdatenebene im jeweiligen Testschritt. Die Daten müssen dabei grundsätzlich entschlüsselt, d.h. ohne Transportverschlüsselung, vorliegen. Wird eine Inhaltsdatenverschlüsselung vorgenommen, muss diese nicht entschlüsselt werden. Ein Beispiel für ein Anfrage-Antwort-Protokoll wäre ein textuell protokollierter HTTP-Request-Response-Dialog einschließlich HTTP-Methode, Pfad, Parameter, Header, Body und Statuscode. Findet in dem Testfall keine Verschlüsselung statt (z.B. bei MDNS) ist kein Anfrage-Antwort-Protokoll erforderlich, da die Inhalte bereits im Netzwerkmitschnitt enthalten sind.

Tabelle 3.2 Nachweistypen

3.3 CLS-Testplattform

Für die Durchführung kann die vom BSI zur Verfügung gestellte Implemetierung der nachfolgenenden Testfälle auf der Smart-Metering-Testplattform genutzt werden. Dazu muss der Hersteller eine [CLS-Api] bereitstellen. Diese wird benutzt, um im Prüfgegenstand Fachanwendungsfälle und weitere Vorgänge auszulösen, deren Umsetzung in der [TR-03109-5] nicht spezifiziert ist und somit dem Hersteller frei steht.

Alternativ kann die Prüfstelle oder der Hersteller die Testfälle selbst implementieren. In diesem Fall muss der Hersteller bzw. die Prüfstelle eine Testdokumentation über folgende Sachverhalte beibringen:

- die Funktionsweise der konkret verwendeten Testumgebung, insb. im Bezug darauf, wie die einzelnen technischen Akteure ausgestaltet sind,
- die Art und Weise, wie Nachweise innerhalb dieser Testumgebung generiert werden und
- sofern das Format der Nachweise von dem hier definierten abweicht, wie diese zu interpretieren sind.

4 Testfälle

4.1 TC.CLS.DNS.CanUseDnsSd

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, den Port eines Dienstes mittels DNS-SD zu bestimmen.

Kurzbeschreibung

Es wird geprüft, ob der Prüfgegenstand den Port eines Diensts über DNS-SD auflöst.

Abgedeckte Anforderungen

- REQ.IOP.HKS.DNSDISCOVERY.50

Relevante Implementation-Conformance-Statements (ICS)

- ICS.HKS.DNSDISCOVERY.20
- ICS.HKS.DNSDISCOVERY.30

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.1 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface.
2	Starten eines virtuellen SMGW mit generierter Geräte-ID.

Tabelle 4.2 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Abwarten und Beantworten der mDNS-SD-Query.	• Innerhalb des Timeouts wird eine Nachricht empfangen, welche den Querytype "SRV" hat. • Die empfangene Nachricht ist eine Query. Somit ist das Query/Response-Bit "false". • Der OPCODE der Query ist "0". • Das Authoritative-Answer-Bit der Query ist "false". • Das Recursion-Desired-Bit der Query ist "false". Da dies nach RFC6762 eine SOLL-Anforderung ist, liefert diese Assertion ggf. ein falsch negatives Ergebnis. • Das Recursion-Available-Bit der Query ist "false". • Das Zero-Bit der Query ist "false".

Nr.	Beschreibung	Erwartetes Ergebnis
		• Das Authentic-Data-Bit der Query ist "false". • Das Checking-Disabled-Bit der Query ist "false". • Der Response-Code der Nachricht ist 0.

Tabelle 4.3 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Stoppen des virtuellen SMGW.
2	Stoppen des gestarteten Tracings.

Tabelle 4.4 Ablaufbeschreibung

4.2 TC.CLS.DNS.MustUseMulticastDns

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, die IP4-Adresse des SMGW mittels mDBS zu bestimmen.

Kurzbeschreibung

Es wird gewartet, ob der Prüfgegenstand die Auflösung der IPv4-Adresse eines SMGW mittels mDNS abfragt. Der Prüfgegenstand darf dazu die QNames "smgw.local. oder "<SMGW-ID>.local." verwenden.

Abgedeckte Anforderungen

- REQ.FA.DiscoverSmgwAddress.10
- REQ.FAKAT.SmgwAssociation.10
- REQ.HKS.DNSDISCOVERY.10
- REQ.HKS.DNSDISCOVERY.30
- REQ.HKS.DNSDISCOVERY.40

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.5 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface.

Nr.	Beschreibung
2	Starten eines virtuellen SMGW mit generierter Geräte-ID.

Tabelle 4.6 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Abwarten und Beantworten der mDNS-Query.	• Innerhalb des Timeouts wird eine Nachricht empfangen, welche den Querytype "A" hat. • Die empfangene Nachricht fragt nach einer Auflösung von "smgw.local." oder "<SMGW-ID>.local.". • Die empfangene Nachricht ist eine Query. Somit ist das Query/Response-Bit "false". • Der OPCODE der Query ist "0". • Das Authoritative-Answer-Bit der Query ist "false". • Das Recursion-Desired-Bit der Query ist "false". Da dies nach RFC6762 eine SOLL-Anforderung ist, liefert diese Assertion ggf. ein falsch negatives Ergebnis. • Das Recursion-Available-Bit der Query ist "false". • Das Zero-Bit der Query ist "false". • Das Authentic-Data-Bit der Query ist "false". • Das Checking-Disabled-Bit der Query ist "false". • Der Response-Code der Nachricht ist 0.

Tabelle 4.7 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Stoppen des virtuellen SMGW.
2	Stoppen des gestarteten Tracings.

Tabelle 4.8 Ablaufbeschreibung

4.3 TC.CLS.DOCUMENTS.MustHaveFixedTimeCyberSecurityCertification

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand eine Beschleunigte Sicherheitszeritifizierung (BSZ) durchlaufen hat.

Kurzbeschreibung

Der Testfall prüft, ob der Prüfgegenstand eine Beschleunigte Sicherheitszeritifizierung (BSZ) durchlaufen hat.

Abgedeckte Anforderungen

- REQ.GEN.Schnittstellen.10

Relevante Implementation-Conformance-Statements (ICS)

- ICS.GEN.Schnittstellen.20

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Der Hersteller legt einen BSZ-Zertifizierungsreport und ein BSZ-Zertifikat für den Prüfgegenstand vor.	• Es liegt eine erfolgreich durchlaufene BSZ für den Prüfgegenstand in der vorliegenden Hard- und Softwareversion vor.

Tabelle 4.9 Ablaufbeschreibung

4.4 TC.CLS.MGMT.MustDoFactoryResetClsAsClient

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand dazu in der Lage ist, einen Reset auf Werkseinstellungen durchzuführen.

Kurzbeschreibung

Zu Beginn wird ein Pairing zwischen SMGW und CLS-Gerät durchgeführt, welches durch das Abwarten eines Verbindungsaufbaus verifiziert wird. Anschließend wird über die Hersteller-API ein Werksreset durchgeführt und das nun zu verwendende Schlüsselmaterial abgefragt. Daraufhin muss das CLS-Gerät beim erneuten Verbindungsaufbau das von der Hersteller-API gelieferte zertifikat präsentieren.

Abgedeckte Anforderungen

- REQ.FA.RestoreDefaults.20

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.10 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.
4	Warten auf den Verbindungsaufbau durch den Prüfgegenstand.
5	Schließen der Verbindung.
6	Aufruf des FA.CreateClsKeyPairAndCert über die Hersteller-API

Tabelle 4.11 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Durchführen des Werksresets über die Hersteller-API.	• Innerhalb des Timeouts wird eine Antwort der API empfangen. • Der HTTP-Rückgabe-Code der Hersteller-API entspricht dem Code OK (200).
2	Abrufen des nun verwendeten CLS_HAN_TLS_CRT über die Hersteller-API.	• Innerhalb des Timeouts wird eine Antwort der API empfangen. • Der HTTP-Rückgabe-Code der Hersteller-API entspricht dem Code OK (200). • Es wird ein Zertifikat von der Hersteller-API empfangen.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.	• Innerhalb des Timeouts wird eine Antwort der API empfangen. • Der HTTP-Rückgabe-Code der Hersteller-API auf die Route zum Zertifikatspinning entspricht dem Code OK (200).
4	Warten auf einen Verbindungsaufbau durch den Prüfgegenstand.	• Das vom Prüfgegenstand päsentierte Zertifikat entspricht dem, welches die Hersteller-API zurückgegeben hat.

Tabelle 4.12 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.13 Ablaufbeschreibung

4.5 TC.CLS.MGMT.MustDoFactoryResetClsAsServer

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand dazu in der Lage ist, einen Reset auf Werkseinstellungen durchzuführen.

Kurzbeschreibung

Zu Beginn wird ein Pairing zwischen SMGW und CLS-Gerät durchgeführt, welches durch einen Verbindungsaufbau verifiziert wird. Anschließend wird über die Hersteller-API ein Werksreset durchgeführt und das nun zu verwendende Schlüsselmaterial abgefragt. Daraufhin muss das CLS-Gerät beim erneuten Verbindungsaufbau das von der Hersteller-API gelieferte zertifikat präsentieren.

Abgedeckte Anforderungen

- REQ.FA.RestoreDefaults.20

Relevante Implementation-Conformance-Statements (ICS)

- ICS.FA.PinSmgwCertificate.10
- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.14 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.
4	Aufbau einer Verbindung zum Prüfgegenstand.
5	Schließen der Verbindung.
6	Aufruf des FA.CreateClsKeyPairAndCert über die Hersteller-API

Tabelle 4.15 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Durchführen des Werksresets über die Hersteller-API.	• Innerhalb des Timeouts wird eine Antwort der API empfangen. • Der HTTP-Rückgabe-Code der Hersteller-API entspricht dem Code OK (200).
2	Abrufen des nun verwendeten CLS_HAN_TLS_CRT über die Hersteller-API.	• Innerhalb des Timeouts wird eine Antwort der API empfangen. • Der HTTP-Rückgabe-Code der Hersteller-API entspricht dem Code OK (200). • Es wird ein Zertifikat von der Hersteller-API empfangen.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.	• Innerhalb des Timeouts wird eine Antwort der API empfangen. • Der HTTP-Rückgabe-Code der Hersteller-API auf die Route zum Zertifikatspinning entspricht dem Code OK (200).
4	Aufbau einer Verbindung zum Prüfgegenstand.	• Das vom Prüfgegenstand päsentierte Zertifikat entspricht dem, welches die Hersteller-API zurückgegeben hat.

Tabelle 4.16 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.17 Ablaufbeschreibung

4.6 TC.CLS.MGMT.MustUpdateFirmware

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand dazu in der Lage ist, ein Firmware-Update durchzuführen.

Kurzbeschreibung

Zunächst wird der aktuelle Stand der Firmware (FW) abgefragt. Daraufhin wird das FW-Update ausgeführt und der Stand erneut abgefragt. Die jeweils zurückgegebenen FW-Stände müssen sich unterscheiden. Der zweite abgefragte FW-Stand muss dem des eingespielten Updates entsprechen.

Abgedeckte Anforderungen

- REQ.FA.FwInstallation.10
- REQ.FA.FwInstallation.40
- REQ.FAKAT.FwUpdate.10

Relevante Implementation-Conformance-Statements (ICS)

- ICS.FA.FwInstallation.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.18 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.19 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Auslesen der aktuellen FW des Prüfgegenstandes via Hersteller-API.	• Innerhalb des Timeouts wird eine Antwort der API empfangen. • Der HTTP-Rückgabe-Code der Hersteller-API auf die Route zum Zertifikatspinning entspricht dem Code OK (200).
2	Abfrage der neuen FW von der Hersteller-API.	• Innerhalb des Timeouts wird eine Antwort der API empfangen.

Nr.	Beschreibung	Erwartetes Ergebnis
		• Der HTTP-Rückgabe-Code der Hersteller-API auf die Route zum Zertifikatspinning entspricht dem Code OK (200).
3	Überprüfen der beiden gelesenen Firmwareversionen.	• Die FW-Version der Hersteller-API ist neuer als die FW-Version des Prüfgegenstandes.
4	Einspielen der neuen FW über die Hersteller-API in den Prüfgegenstand.	• Innerhalb des Timeouts wird eine Antwort der API empfangen. • Der HTTP-Rückgabe-Code der Hersteller-API auf die Route zum Zertifikatspinning entspricht dem Code OK (200).
5	Erneutes Auslesen der aktuellen FW-Version des Prüfgegenstandes.	• Innerhalb des Timeouts wird eine Antwort der API empfangen. • Der HTT-Rückgabe-Code der Hersteller-API auf die Route zum Zertifikatspinning entspricht dem Code OK (200). • Die ausgelesene FW-Version entspricht der zuvor eingespielten FW-Version.

Tabelle 4.20 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Stoppen des virtuellen SMGW.
3	Stoppen des gestarteten Tracings.

Tabelle 4.21 Ablaufbeschreibung

4.7 TC.CLS.PAIRING.MustImportClsKeyPairAndCertClsAsClient

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand ein neues Zertifikat beim SMGW anfragen und verwenden kann.

Kurzbeschreibung

Zu Beginn wird ein Pairing zwischen SMGW und CLS-Gerät durchgeführt. Anschließend wird das CLS-Gerät mittels der Hersteller-API aufgefordert, ein neues CLS_HAN_TLS_CRT zu importieren. Daraufhin lauscht das SMGW auf eine entsprechende Anfrage und beantwortet diese. Im Anschluss wird eine Verbindung zum CLS-Gerät aufgebaut, bei dessen Handshake das CLS-Gerät das neu generierte Zertifikat verwenden muss.

Abgedeckte Anforderungen

- REQ.FA.ImportClsKeyPairAndCert.40
- REQ.FA.ImportClsKeyPairAndCert.50
- REQ.FAKAT.SmgwAssociation.60

Relevante Implementation-Conformance-Statements (ICS)

- ICS.FA.ImportClsKeyPairAndCert.10
- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.22 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Erstellen eines CLS_HAN_TLS_CRT für den Prüfgegenstand.
4	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.23 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufruf des FA.ImportClsKeyPairAndCert über die Hersteller-API.	• Innerhalb des Timeouts wird eine Nachricht von der Hersteller-API empfangen. • Der HTTP-Rückgabe-Code der Hersteller-API entspricht dem Code OK (200).
2	Abwarten einer Anfrage zur Schlüsselgenerierung an die API des virtuellen SMGW.	• Es muss eine Anfrage zur Schlüsselgenerierung beim SMGW eingehen.
3	Warten auf den Verbindungsaufbau durch den Prüfgegenstand.	• Der TLS-Verbindungsaufbau ist erfolgreich. • Das vom CLS-Gerät verwendete Zertifikat entspricht dem vom SMGW generierten Zertifikat.

Tabelle 4.24 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.25 Ablaufbeschreibung

4.8 TC.CLS.PAIRING.MustImportClsKeyPairAndCertClsAsServer

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand ein neues Zertifikat beim SMGW anfragen und verwenden kann.

Kurzbeschreibung

Zu Beginn wird ein Pairing zwischen SMGW und CLS-Gerät durchgeführt. Anschließend wird das CLS-Gerät mittels der Hersteller-API aufgefordert, ein neues CLS_HAN_TLS_CRT zu importieren. Daraufhin lauscht das SMGW auf eine entsprechende Anfrage und beantwortet diese. Im Anschluss wird eine Verbindung zum CLS-Gerät aufgebaut, bei dessen Handshake das CLS-Gerät das neu generierte Zertifikat verwenden muss.

Abgedeckte Anforderungen

- REQ.FA.ImportClsKeyPairAndCert.40
- REQ.FA.ImportClsKeyPairAndCert.50
- REQ.FAKAT.SmgwAssociation.60

Relevante Implementation-Conformance-Statements (ICS)

- ICS.FA.ImportClsKeyPairAndCert.10
- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.26 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Erstellen eines CLS_HAN_TLS_CRT für den Prüfgegenstand.
4	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.27 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufruf des FA.ImportClsKeyPairAndCert über die Hersteller-API.	• Innerhalb des Timeouts wird eine Nachricht von der Hersteller-API empfangen. • Der HTTP-Rückgabe-Code der Hersteller-API entspricht dem Code OK (200).
2	Abwarten einer Anfrage zur Schlüsselgenerierung an die API des virtuellen SMGW.	• Es muss eine Anfrage zur Schlüsselgenerierung beim SMGW eingehen.
3	Aufbau einer Verbindung zum Prüfgegenstand.	• Der TLS-Verbindungsaufbau ist erfolgreich. • Das vom CLS-Gerät verwendete Zertifikat entspricht dem vom SMGW generierten Zertifikat.

Tabelle 4.28 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.29 Ablaufbeschreibung

4.9 TC.CLS.PAIRING.MustNotCommunicateWithOtherSmgwClsAsClient

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand nach erfolgtem Zertifikatspinning keine Verbindungen auf Basis anderer Zertifikate mehr zulässt.

Kurzbeschreibung

Über die Hersteller-API wird zunächst der FA.PinSmgwCertificate aufgerufen. Danach wird ein Verbindungsaufbau abgewartet, bei dem das Zertifikatspinning stattfinden soll. Diese Verbindung muss erfolgreich sein. Im Anschluss wird ein weiterer Verbindungsaufbau abgewartet, bei dem ein falsches Zertifikat verwendet wird. Die zweite Verbindung muss fehlschlagen.

Abgedeckte Anforderungen

- REQ.FA.PinSmgwCertificate.20
- REQ.FA.PinSmgwCertificate.30
- REQ.IOP.KS.HAN.10

Relevante Implementation-Conformance-Statements (ICS)

- ICS.FA.PinSmgwCertificate.10
- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.30 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-TLS-Port des aktuellen SMGW.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.
4	Warten auf den Verbindungsaufbau durch den Prüfgegenstand.

Nr.	Beschreibung
5	Trennen der Verbindung zum Prüfgegenstand.
6	Neustarten des SMGW mit einem anderen GW_HAN_TLS_CRT, Abwarten eines Verbindungsaufbaus und Trennen dieser Verbindung, um den Pinningzustand sicher zu beenden.

Tabelle 4.31 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Neustarten des SMGW mit einem weiteren, bisher noch nicht präsentierten GW_HAN_TLS_CRT.	-
2	Warten auf den Verbindungsaufbau durch den Prüfgegenstand.	• Der TLS-Verbindungsaufbau schlägt fehl.

Tabelle 4.32 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Schließen der Verbindung zum Prüfgegenstand.
2	Starten eines SMGW mit validem Zertifikat und deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.33 Ablaufbeschreibung

4.10 TC.CLS.PAIRING.MustNotCommunicateWithOtherSmgwClsAsServer

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand nach erfolgtem Zertifikatspinning keine Verbindungen auf Basis anderer Zertifikate mehr zulässt.

Kurzbeschreibung

Über die Hersteller-API wird zunächst der FA.PinSmgwCertificate aufgerufen. Danach wird ein Verbindungsaufbau initiiert, bei dem das Zertifikatspinning stattfinden soll. Diese Verbindung muss erfolgreich sein. Im Anschluss wird ein weiterer Verbindungsaufbau initiiert, bei dem ein falsches Zertifikat verwendet wird. Die zweite Verbindung muss fehlschlagen.

Abgedeckte Anforderungen

- REQ.FA.PinSmgwCertificate.20
- REQ.FA.PinSmgwCertificate.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.FA.PinSmgwCertificate.10
- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.34 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-TLS-Port des aktuellen SMGW.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.
4	Aufbau einer Verbindung zum Prüfgegenstand.
5	Trennen der Verbindung zum Prüfgegenstand.
6	Neustarten des SMGW mit einem anderen GW_HAN_TLS_CRT, Aufbauen und Trennen einer Verbindung, um den Pinningzustand sicher zu beenden.

Tabelle 4.35 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Austausch des GW_HAN_TLS_CRT im virtuellen SMGW.	-
2	Aufbau einer Verbindung zum Prüfgegenstand.	• Der TLS-Verbindungsaufbau schlägt fehl.

Tabelle 4.36 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Schließen der Verbindung zum Prüfgegenstand.
2	Starten eines SMGW mit validem Zertifikat und deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.37 Ablaufbeschreibung

4.11 TC.CLS.PAIRING.MustNotCommunicateWithSmgwWith-DeactivatedCertificateClsAsClient

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand einen Verbindungsaufbau mit einem SMGW, das ein deaktiviertes Zertifikat präsentiert, abbricht.

Kurzbeschreibung

Zu Beginn werden zwei unterschiedliche SMGW-Zertifikate GW_HAN_TLS_CRT_1 und _2 gepinnt. Um zu prüfen, dass dieses erfolgreich war, wird ein Verbindungsaufbau initiiert, bei dem vom SMGW das GW_HAN_TLS_CRT_2 präsentiert wird. Dieser muss erfolgreich sein. Daraufhin wird das Zertifikat des SMGW über die Hersteller-API deaktiviert. Im Anschluss wird ein weiterer Verbindungsaufbau initiiert, der fehlschla-

gen muss. Je nach Implementierung kann der Testfall bei trust-on-first-use ein falsch-negatives Ergebnis liefern.

Abgedeckte Anforderungen

- REQ.FA.DeactivateSmgwTrustAnchor.10
- REQ.FA.DeactivateSmgwTrustAnchor.20
- REQ.FAKAT.SmgwAssociation.50
- REQ.IOP.KS.HAN.10

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.38 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Starten eines virtuellen SMGW mit GW_HAN_TLS_CRT_1.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API für GW_HAN_TLS_CRT_1.
4	Aufruf des FA.PinSmgwCertificate über die Hersteller-API für GW_HAN_TLS_CRT_2.
5	Neustarten des SMGW mit GW_HAN_TLS_CRT_2.

Tabelle 4.39 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand und Verbindung anschließend wieder abbauen.	• Der TLS-Verbindungsaufbau ist erfolgreich.
2	Deaktivieren von GW_HAN_TLS_CRT_2.	• Die Hersteller API kann innerhalb der angegeben Zeit erreicht werden. • Der HTTP-Rückgabe-Code der Hersteller-API auf die Route zum Pairing entspricht dem Code OK (200).
3	Verbindungsaufbau durch den Prüfgegenstand abwarten.	• Der TLS-Verbindungsaufbau schlägt fehl.

Tabelle 4.40 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Neustarten des SMGW mit GW_HAN_TLS_CRT_1 und deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Stoppen des virtuellen SMGW.
3	Stoppen des gestarteten Tracings.

Tabelle 4.41 Ablaufbeschreibung

4.12 TC.CLS.PAIRING.MustNotCommunicateWithSmgwWith-DeactivatedCertificateClsAsServer

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand einen Verbindungsaufbau mit einem SMGW, das ein deaktiviertes Zertifikat präsentiert, abbricht.

Kurzbeschreibung

Zu Beginn werden zwei unterschiedliche SMGW-Zertifikate GW_HAN_TLS_CRT_1 und _2 gepinnt. Um zu prüfen, dass dieses erfolgreich war, wird ein Verbindungsaufbau abgewartet, bei dem vom SMGW das GW_HAN_TLS_CRT_2 präsentiert wird. Dieser muss erfolgreich sein. Daraufhin wird das Zertifikat des SMGW über die Hersteller-API deaktiviert. Im Anschluss wird ein weiterer Verbindungsaufbau abgewartet, der fehlschlagen muss. Je nach Implementierung kann der Testfall bei trust-on-first-use ein falsch-negatives Ergebnis liefern.

Abgedeckte Anforderungen

- REQ.FA.DeactivateSmgwTrustAnchor.10
- REQ.FA.DeactivateSmgwTrustAnchor.20
- REQ.FAKAT.SmgwAssociation.50
- REQ.IOP.KS.HAN.10

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.42 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Starten eines virtuellen SMGW mit GW_HAN_TLS_CRT_1.

Nr.	Beschreibung
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API für GW_HAN_TLS_CRT_1.
4	Aufruf des FA.PinSmgwCertificate über die Hersteller-API für GW_HAN_TLS_CRT_2.
5	Neustarten des SMGW mit GW_HAN_TLS_CRT_2.

Tabelle 4.43 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau und anschließender Abbau einer Verbindung zum Prüfgegenstand.	• Der TLS-Verbindungsaufbau ist erfolgreich.
2	Deaktivieren von GW_HAN_TLS_CRT_2.	• Die Hersteller-API kann innerhalb der angegeben Zeit erreicht werden. • Der HTTP-Rückgabe-Code der Hersteller-API auf die Route zum Pairing entspricht dem Code OK (200).
3	Aufbau einer Verbindung zum Prüfgegenstand.	• Der TLS-Verbindungsaufbau schlägt fehl.

Tabelle 4.44 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Neustarten des SMGW mit GW_HAN_TLS_CRT_1 und deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Stoppen des virtuellen SMGW.
3	Stoppen des gestarteten Tracings.

Tabelle 4.45 Ablaufbeschreibung

4.13 TC.CLS.PAIRING.MustNotCommunicateWithSmgwWithDeactivatedTrustAnchorClsAsClient

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand einen Verbindungsaufbau mit einem SMGW abbricht, das ein Zertifikat mit einer "Chain of Trust" zu einem deaktivierten Vertrauensanker präsentiert.

Kurzbeschreibung

Zu Beginn werden die jeweiligen Root- und Sub-CA-Zertifikate für ein GW_HAN_TLS_CRT_1 und _2 importiert. Es wird ein Verbindungsaufbau abgewartet, bei dem das SMGW GW_HAN_TLS_CRT_2 präsentiert. Der Verbindungsaufbau muss erfolgreich sein. Danach wird der Vertrauensanker für GW_HAN_TLS_CRT_2 deaktiviert. Anschließend wird auf einen erneuten Verbindungsaufbau unter Verwendung von GW_HAN_TLS_CRT_2 gewartet. Dieser Verbindungsaufbau muss fehlschlagen.

Abgedeckte Anforderungen

- REQ.FA.DeactivateSmgwTrustAnchor.20
- REQ.FAKAT.SmgwAssociation.50
- REQ.IOP.KS.HAN.10

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.46 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-TLS-Port des aktuellen SMGW.
2	Start eines virtuellen SMGW mit GW_HAN_TLS_CRT aus der ersten PKI.
3	Import des ersten Root-CA-Zertifikats als Vertrauensanker über die Hersteller-API.
4	Import des ersten Sub-CA-Zertifikats als Vertrauensanker über die Hersteller-API.
5	Import des zweiten Root-CA-Zertifikats als Vertrauensanker über die Hersteller-API.
6	Import des zweiten Sub-CA-Zertifikats als Vertrauensanker über die Hersteller-API.
7	Neustarten des virtuellen SMGW mit einem GW_HAT_TLS_CRT mit "Chain of Trust" zum zweiten Vertrauensanker.

Tabelle 4.47 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand und anschließendes Abbauen der Verbindung.	• Der TLS-Verbindungsaufbau ist erfolgreich.
2	Neustarten des virtuellen SMGW mit einem GW_HAT_TLS_CRT mit "Chain of Trust" zum ersten Vertrauensanker.	-
3	Deaktivieren des zweiten Root- und Sub-CA-Zertifikats.	• Die Hersteller-API kann innerhalb der angegeben Zeit erreicht werden. • Der HTTP-Rückgabe-Code der Hersteller-API auf die Route zum Zertifikatspinning entspricht dem Code OK (200). • Die Hersteller-API kann innerhalb der angegeben Zeit erreicht werden. • Der HTTP-Rückgabe-Code der Hersteller-API auf die Route zum Zertifikatspinning entspricht dem Code OK (200).
4	Neustarten des virtuellen SMGW mit einem GW_HAN_TLS_CRT mit "Chain of Trust" zum zweiten Vertrauensanker.	-
5	Warten auf den Verbindungsaufbau durch den Prüfgegenstand.	• Der TLS-Verbindungsaufbau schlägt fehl.

Tabelle 4.48 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Neustarten des virtuellen SMGW mit einem GW_HAN_TLS_CRT mit "Chain of Trust" zum ersten Vertrauensanker.
2	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.49 Ablaufbeschreibung

4.14 TC.CLS.PAIRING.MustNotCommunicateWithSmgwWith-DeactivatedTrustAnchorClsAsServer

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand einen Verbindungsaufbau mit einem SMGW abbricht, das ein Zertifikat mit einer "Chain of Trust" zu einem deaktivierten Vertrauensanker präsentiert.

Kurzbeschreibung

Zu Beginn werden die jeweiligen Root- und Sub-CA-Zertifikate für ein GW_HAN_TLS_CRT_1 und _2 importiert. Es wird ein Verbindungsaufbau initiiert, bei dem das SMGW GW_HAN_TLS_CRT_2 präsentiert. Der Verbindungsaufbau muss erfolgreich sein. Danach wird der Vertrauensanker für GW_HAN_TLS_CRT_2 deaktiviert. Anschließend wird auferneut ein Verbindungsaufbau unter Verwendung von GW_HAN_TLS_CRT_2 initiiert. Dieser Verbindungsaufbau muss fehlschlagen.

Abgedeckte Anforderungen

- REQ.FA.DeactivateSmgwTrustAnchor.20
- REQ.FAKAT.SmgwAssociation.50
- REQ.IOP.KS.HAN.10

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.50 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-TLS-Port des aktuellen SMGW.
2	Start eines virtuellen SMGW mit GW_HAN_TLS_CRT aus der ersten PKI.
3	Import des ersten Root-CA-Zertifikats als Vertrauensanker über die Hersteller-API.
4	Import des ersten Sub-CA-Zertifikats als Vertrauensanker über die Hersteller-API.

Nr.	Beschreibung
5	Import des zweiten Root-CA-Zertifikats als Vertrauensanker über die Hersteller-API.
6	Import des zweiten Sub-CA-Zertifikats als Vertrauensanker über die Hersteller-API.
7	Neustarten des virtuellen SMGW mit einem GW_HAT_TLS_CRT mit "Chain of Trust" zum zweiten Vertrauensanker.

Tabelle 4.51 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau und anschließender Abbau einer Verbindung zum Prüfgegenstand.	• Der TLS-Verbindungsaufbau ist erfolgreich.
2	Neustarten des virtuellen SMGW mit einem GW_HAT_TLS_CRT mit "Chain of Trust" zum ersten Vertrauensanker.	-
3	Deaktivieren des zweiten Root- und Sub-CA-Zertifikats.	• Die Hersteller-API kann innerhalb der angegeben Zeit erreicht werden. • Der HTTP-Rückgabe-Code der Hersteller-API auf die Route zum Zertifikatspinning entspricht dem Code OK (200). • Die Hersteller-API kann innerhalb der angegeben Zeit erreicht werden. • Der HTTP-Rückgabe-Code der Hersteller-API auf die Route zum Zertifikatspinning entspricht dem Code OK (200).
4	Neustarten des virtuellen SMGW mit einem GW_HAT_TLS_CRT mit "Chain of Trust" zum zweiten Vertrauensanker.	-
5	Aufbau einer Verbindung zum Prüfgegenstand, wobei der neue Vertrauensanker verwendet wird.	• Der TLS-Verbindungsaufbau schlägt fehl.

Tabelle 4.52 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Neustarten des virtuellen SMGW mit einem GW_HAN_TLS_CRT mit "Chain of Trust" zum ersten Vertrauensanker.
2	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.53 Ablaufbeschreibung

4.15 TC.CLS.PAIRING.MustSupportDirectTrustWithPkiCertClsAsClient

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, ein Direct-Trust-Verhälnis auf ein nicht selbstsigniertes Zertifikat aufzubauen.

Kurzbeschreibung

Es wird ein Zertifikatspinning mit einem Zertifikat durchgeführt, welches aus einer PKI stammt. Anschließend wird abgewartet, ob das CLS-Gerät einen Kanal aufbaut. Dabei wird vom SMGW das initial gepinnte Zertifikat präsentiert. Der Verbindungsaufbau muss erfolgreich sein. Der Testfall kann zu einem falsch negativen Ergebnis führen, wenn das Produkt aufgrund organisatorischer Maßnahmen niemals ohne Vertrauensanker

ausgeliefert wird und technisch nicht in einen Zusand versetzt werden kann, in dem kein Vertrauensanker vorliegt.

Abgedeckte Anforderungen

- REQ.Implementierungshinweis01

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.54 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-TLS-Port des aktuellen SMGW.
2	Starten eines virtuellen SMGW mit GW_HAN_TLS_CRT aus einer PKI.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.55 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand.	• Der TLS-Verbindungsaufbau ist erfolgreich.

Tabelle 4.56 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Zurücksetzen des Prüfgegenstands.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.57 Ablaufbeschreibung

4.16 TC.CLS.PAIRING.MustSupportDirectTrustWithPkiCertClsAsServer

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, ein Direct-Trust-Verhälnis auf ein nicht selbstsigniertes Zertifikat aufzubauen.

Kurzbeschreibung

Es wird ein Zertifikatspinning mit einem Zertifikat durchgeführt, welches aus einer PKI stammt. Anschließend wird eine Verbindung zum CLS-Gerät aufgebaut. Dabei wird vom SMGW das initial gepinnte Zertifikat präsentiert. Der Verbindungsaufbau muss erfolgreich sein. Der Testfall kann zu einem falsch negativen Ergebnis führen, wenn das Produkt aufgrund organisatorischer Maßnahmen niemals ohne Vertrauensanker ausgeliefert wird und technisch nicht in einen Zusand versetzt werden kann, in dem kein Vertrauensanker vorliegt.

Abgedeckte Anforderungen

- REQ.Implementierungshinweis01

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.58 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-TLS-Port des aktuellen SMGW.
2	Starten eines virtuellen SMGW mit GW_HAN_TLS_CRT aus einer PKI.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.59 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand.	• Der TLS-Verbindungsaufbau ist erfolgreich.

Tabelle 4.60 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Zurücksetzen des Prüfgegenstands.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.61 Ablaufbeschreibung

4.17 TC.CLS.PAIRING.MustSupportTwoConcurrentTrustAnchorsClsAsClient

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, zwei Vertrauensanker gleichzeitig zu unterstützen.

Kurzbeschreibung

Zu Beginn werden jeweils voneinander unterschiedliche Root- und Sub-CA-Zertifikate für zwei SMGW-Zertifikate GW_HAN_TLS_CRT_1 und _2 importiert, die für das gleiche SMGW (identischer CN) ausgestellt sind. Daraufhin wird auf einen Verbindungsaufbau mit einem SMGW gewartet, welches GW_HAN_TLS_CRT_1 präsentiert. Der Verbindungsaufruf muss erfolgreich sein. Anschließend wird erneut ein Verbindungsaufbau abgewartet, bei dem das Zertifikat mit anderem Vertrauensanker GW_HAN_TLS_CRT_2 präsentiert wird. Dieser Verbindungsaufbau muss ebenfalls erfolgreich sein.

Abgedeckte Anforderungen

- REQ.FA.ImportSmgwTrustAnchor.20
- REQ.FA.ImportSmgwTrustAnchor.30
- REQ.FA.ImportSmgwTrustAnchor.40
- REQ.FAKAT.SmgwAssociation.40

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.62 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-TLS-Port des aktuellen SMGW.
2	Starten eines virtuellen SMGW mit GW_HAN_TLS_CRT mit "Chain of Trust" zum ersten Vertrauensanker.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.
4	Import des ersten Vertrauensankers.
5	Import des ersten Sub-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
6	Deaktivieren des "Direct Trust" für das initial gepinnte Zertifikat.

Tabelle 4.63 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Import des zweiten Vertrauensankers.	• Die Hersteller-API kann innerhalb der angegeben Zeit erreicht werden. • Der HTTP-Rückgabe-Code der Hersteller-API auf die Route zum Zertifikatspinning entspricht dem Code OK (200).
2	Import des zweiten Sub-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.	• Innerhalb des Timeouts wird eine Antwort der API empfangen. • Der HTTP-Rückgabe-Code der Hersteller-API auf die Route zum Zertifikatspinning entspricht dem Code OK (200).
3	Warten auf den Verbindungsaufbau durch den Prüfgegenstand unter Verwendung des alten Vertrauensankers und anschließender Abbau der Verbindung.	• Der TLS-Verbindungsaufbau ist erfolgreich.
4	Neustart des SMGW mit GW_HAN_TLS_CRT mit "Chain of Trust" zum neuen Vertrauensanker.	-
5	Warten auf den Verbindungsaufbau durch den Prüfgegenstand unter Verwendung des neuen Vertrauensankers und anschließender Abbau der Verbindung.	• Der TLS-Verbindungsaufbau ist erfolgreich.

Tabelle 4.64 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Stoppen des virtuellen SMGW.
3	Stoppen des gestarteten Tracings.

Tabelle 4.65 Ablaufbeschreibung

4.18 TC.CLS.PAIRING.MustSupportTwoConcurrentTrustAnchorsClsAsServer

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, zwei Vertrauensanker gleichzeitig zu unterstützen.

Kurzbeschreibung

Zu Beginn werden jeweils voneinander unterschiedliche Root- und Sub-CA-Zertifikate für zwei SMGW-Zertifikate GW_HAN_TLS_CRT_1 und _2 importiert, die für das gleiche SMGW (identischer CN) ausgestellt sind. Daraufhin wird ein Verbindungsaufbau mit einem SMGW initiiert, welches GW_HAN_TLS_CRT_1 präsentiert. Der Verbindungsaufruf muss erfolgreich sein. Anschließend wird erneut ein Verbindungsaufbau initiiert, bei dem das Zertifikat mit anderem Vertrauensanker GW_HAN_TLS_CRT_2 präsentiert wird. Dieser Verbindungsaufbau muss ebenfalls erfolgreich sein.

Abgedeckte Anforderungen

- REQ.FA.ImportSmgwTrustAnchor.20
- REQ.FA.ImportSmgwTrustAnchor.30
- REQ.FA.ImportSmgwTrustAnchor.40
- REQ.FAKAT.SmgwAssociation.40

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.66 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-TLS-Port des aktuellen SMGW.
2	Starten eines virtuellen SMGW mit GW_HAN_TLS_CRT mit "Chain of Trust" zum ersten Vertrauensanker.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.
4	Import des ersten Vertrauensankers.
5	Import des ersten Sub-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
6	Deaktivieren des "Direct Trust" für das initial gepinnte Zertifikat.

Tabelle 4.67 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Import des zweiten Vertrauensankers.	• Die Hersteller-API kann innerhalb der angegeben Zeit erreicht werden. • Der HTTP-Rückgabe-Code der Hersteller-API auf die Route zum Zertifikatspinning entspricht dem Code OK (200).
2	Import des zweiten Sub-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.	• Innerhalb des Timeouts wird eine Antwort der API empfangen. • Der HTTP-Rückgabe-Code der Hersteller-API auf die Route zum Zertifikatspinning entspricht dem Code OK (200).
3	Aufbauen einer Verbindung zum Prüfgegenstand unter Verwendung des alten Vertrauensankers und anschließender Abbau der Verbindung.	• Der TLS-Verbindungsaufbau ist erfolgreich.
4	Neustart des SMGW mit GW_HAN_TLS_CRT mit "Chain of Trust" zum neuen Vertrauensanker.	-
5	Aufbau einer Verbindung zum Prüfgegenstand unter Verwendung des neuen Vertrauensankers und anschließender Abbau der Verbindung.	• Der TLS-Verbindungsaufbau ist erfolgreich.

Tabelle 4.68 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Stoppen des virtuellen SMGW.

Nr.	Beschreibung
3	Stoppen des gestarteten Tracings.

Tabelle 4.69 Ablaufbeschreibung

4.19 TC.CLS.TLS.MustAbortHandshakeWithClientThatSendsNoCert

Version: 1.0.0

Zweck

Der Testfall prüft, dass der Prüfgegenstand einen TLS-Handshake mit einem SMGW abbricht, das kein Zertifikat präsentiert.

Kurzbeschreibung

Zunächst wird ein Verbindungsaufbau initiiert. Dabei wird vom Client nach Anforderung durch den Server kein Zertifikat gesendet. Der Prüfgegenstand muss einen "handshake_failure"- oder "close_notify"-Alert senden und den Verbindungsaufbau abbrechen.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.30
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.20

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.70 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.71 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand, wobei der Client auf Anforderung des Servers kein Client-Zertifikat sendet.	• Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Server aus.

Nr.	Beschreibung	Erwartetes Ergebnis
		• Der TLS-Server sendet "handshake_failure" oder "close_notify" als TLS-Alert.

Tabelle 4.72 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Beenden der Verbindung zum CLS Gerät.
2	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.73 Ablaufbeschreibung

4.20 TC.CLS.TLS.MustAbortHandshakeWithCorruptServerCertificate

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand mit einem SMGW kommunziert, das ein korruptes Zertifikat präsentiert.

Kurzbeschreibung

Zunächst wird ein Verbindungsaufbau abgewartet. Dabei wird vom Server ein korruptes Zertifikat präsentiert. Der Prüfgegenstand muss den Verbindungsaufbau abbrechen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.20

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.74 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Starten eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.
4	Neustarten des virtuellen SMGW mit korruptem GW_HAN_TLS_CRT.

Tabelle 4.75 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "bad_certificate" oder "decode_error" als TLS-Alert.

Tabelle 4.76 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Schließen der Verbindung zum Prüfgegenstand.
2	Starten eines SMGW mit validem Zertifikat und deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.77 Ablaufbeschreibung

4.21 TC.CLS.TLS.MustAbortHandshakeWithIllegalSigAlgoExtensionInClientHello

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, einen TLS-Handshake durchzuführen, wenn das SMGW ein Client-Hello sendet, in dem die signature_algorithms_cert-Extension verwendet wird.

Kurzbeschreibung

Zunächst wird ein Verbindungsaufbau initiiert. Dabei wird vom Client die signature_algorithms_cert gesendet, in der ausschließlich nicht von der TR-03116-3 erlaubte Verfahren aufgeführt werden. Der Prüfgegenstand muss den Verbindungsaufbau abweisen. Da RFC 8446 die Interpretation der signature_algorithms_cert für TLS 1.2 nur als SOLL-Anforderung nennt, kann dieser Testfall falsch negative Ergebnisse liefern.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10
- ICS.TA.TLS.HanHandshake.40

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.78 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface.
2	Starten eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.79 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand, wobei im Client-Hello nur unzulässige Signaturalgorithmen angeboten werden.	• Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Server aus. • Der TLS-Client sendet "handshake_failure" als TLS-Alert.

Tabelle 4.80 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Beenden der Verbindung zum CLS-Gerät.
2	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.81 Ablaufbeschreibung

4.22 TC.CLS.TLS.MustAbortHandshakeWithImproperCipherSuitePinningModeDirectTrustClsAsClient01

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Verwendung nicht erlaubter Cipher-Suites unterbindet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello die Cipher-Suite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 verhandelt wird unabhängig davon, ob diese im Client-Hello angeboten wurde. Diese Cipher-Suite wird nicht von der TR-03116-3 erlaubt. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.82 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.83 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die unzulässige Cipher-Suite forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "illegal_parameter" oder "handshake_failure" als TLS-Alert.

Tabelle 4.84 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.85 Ablaufbeschreibung

4.23 TC.CLS.TLS.MustAbortHandshakeWithImproperCipherSuitePinning-ModeDirectTrustClsAsClient02

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Verwendung nicht erlaubter Cipher-Suites unterbindet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello die Cipher-Suite TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 verhandelt wird unabhängig davon, ob diese im Client-Hello angeboten wurde. Diese Cipher-Suite wird nicht von der TR-03116-3 erlaubt. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.86 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.87 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die unzulässige Cipher-Suite forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl.

Nr.	Beschreibung	Erwartetes Ergebnis
		• Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "illegal_parameter" oder "handshake_failure" als TLS-Alert.

Tabelle 4.88 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.89 Ablaufbeschreibung

4.24 TC.CLS.TLS.MustAbortHandshakeWithImproperCipherSuitePinning-ModeDirectTrustClsAsClient03

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Verwendung nicht erlaubter Cipher-Suites unterbindet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello die Cipher-Suite TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 verhandelt wird unabhängig davon, ob diese im Client-Hello angeboten wurde. Diese Cipher-Suite wird nicht von der TR-03116-3 erlaubt. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.90 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.

- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.91 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die unzulässige Cipher-Suite forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "illegal_parameter" oder "handshake_failure" als TLS-Alert.

Tabelle 4.92 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.93 Ablaufbeschreibung

4.25 TC.CLS.TLS.MustAbortHandshakeWithImproperCipherSuitePinning-ModeDirectTrustClsAsClient04

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Verwendung nicht erlaubter Cipher-Suites unterbindet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello die Cipher-Suite TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 verhandelt wird unabhängig davon, ob diese im Client-Hello angeboten wurde. Diese Cipher-Suite wird nicht von der TR-03116-3 erlaubt. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10

- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.94 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.95 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die unzulässige Cipher-Suite forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "illegal_parameter" oder "handshake_failure" als TLS-Alert.

Tabelle 4.96 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.97 Ablaufbeschreibung

4.26 TC.CLS.TLS.MustAbortHandshakeWithImproperCipherSuitePinningModeDirectTrustClsAsClient05

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Verwendung nicht erlaubter Cipher-Suites unterbindet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello die Cipher-Suite TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 verhandelt wird unabhängig davon, ob diese im Client-Hello angeboten wurde. Diese Cipher-Suite wird nicht von der TR-03116-3 erlaubt. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.98 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.99 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die unzulässige Cipher-Suite forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus.

Nr.	Beschreibung	Erwartetes Ergebnis
		• Der TLS-Client sendet "illegal_parameter" oder "handshake_failure" als TLS-Alert.

Tabelle 4.100 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.101 Ablaufbeschreibung

4.27 TC.CLS.TLS.MustAbortHandshakeWithImproperCipherSuitePinningModeDirectTrustClsAsClient07

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Verwendung nicht erlaubter Cipher-Suites unterbindet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello die Cipher-Suite TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 verhandelt wird unabhängig davon, ob diese im Client-Hello angeboten wurde. Diese Cipher-Suite wird nicht von der TR-03116-3 erlaubt. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.102 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.103 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die unzulässige Cipher-Suite forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "illegal_parameter" oder "handshake_failure" als TLS-Alert.

Tabelle 4.104 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.105 Ablaufbeschreibung

4.28 TC.CLS.TLS.MustAbortHandshakeWithImproperCipherSuitePinningModeDirectTrustClsAsClient08

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Verwendung nicht erlaubter Cipher-Suites unterbindet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello die Cipher-Suite TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 verhandelt wird unabhängig davon, ob diese im Client-Hello angeboten wurde. Diese Cipher-Suite wird nicht von der TR-03116-3 erlaubt. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.106 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.107 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die unzulässige Cipher-Suite forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "illegal_parameter" oder "handshake_failure" als TLS-Alert.

Tabelle 4.108 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.109 Ablaufbeschreibung

4.29 TC.CLS.TLS.MustAbortHandshakeWithImproperCipherSuitePinningModeDirectTrustClsAsClient09

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Verwendung nicht erlaubter Cipher-Suites unterbindet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello die Cipher-Suite TLS_DHE_RSA_WITH_AES_128_CBC_SHA verhandelt wird unabhängig davon, ob diese im Client-Hello angeboten wurde. Diese Cipher-Suite wird nicht von der TR-03116-3 erlaubt. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.110 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.111 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die unzulässige Cipher-Suite forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "illegal_parameter" oder "handshake_failure" als TLS-Alert.

Tabelle 4.112 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.113 Ablaufbeschreibung

4.30 TC.CLS.TLS.MustAbortHandshakeWithImproperCipherSuitePinning-ModeDirectTrustClsAsClient10

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Verwendung nicht erlaubter Cipher-Suites unterbindet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello die Cipher-Suite TLS_DHE_RSA_WITH_AES_256_CBC_SHA verhandelt wird unabhängig davon, ob diese im Client-Hello angeboten wurde. Diese Cipher-Suite wird nicht von der TR-03116-3 erlaubt. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.114 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.

Nr.	Beschreibung
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.115 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die unzulässige Cipher-Suite forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "illegal_parameter" oder "handshake_failure" als TLS-Alert.

Tabelle 4.116 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.117 Ablaufbeschreibung

4.31 TC.CLS.TLS.MustAbortHandshakeWithImproperCipherSuitePinningModeDirectTrustClsAsClient11

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Verwendung nicht erlaubter Cipher-Suites unterbindet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello die Cipher-Suite TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 verhandelt wird unabhängig davon, ob diese im Client-Hello angeboten wurde. Diese Cipher-Suite wird nicht von der TR-03116-3 erlaubt. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.118 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.119 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die unzulässige Cipher-Suite forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "illegal_parameter" oder "handshake_failure" als TLS-Alert.

Tabelle 4.120 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.121 Ablaufbeschreibung

4.32 TC.CLS.TLS.MustAbortHandshakeWithImproperCipherSuitePinningModeDirectTrustClsAsClient12

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Verwendung nicht erlaubter Cipher-Suites unterbindet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello die Cipher-Suite TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 verhandelt wird unab-

hängig davon, ob diese im Client-Hello angeboten wurde. Diese Cipher-Suite wird nicht von der TR-03116-3 erlaubt. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.122 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.123 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die unzulässige Cipher-Suite forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "illegal_parameter" oder "handshake_failure" als TLS-Alert.

Tabelle 4.124 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.

Nr.	Beschreibung
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.125 Ablaufbeschreibung

4.33 TC.CLS.TLS.MustAbortHandshakeWithImproperCipherSuitePinning-ModeDirectTrustClsAsClient13

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Verwendung nicht erlaubter Cipher-Suites unterbindet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello die Cipher-Suite TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 verhandelt wird unabhängig davon, ob diese im Client-Hello angeboten wurde. Diese Cipher-Suite wird nicht von der TR-03116-3 erlaubt. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.126 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.

Nr.	Beschreibung
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.127 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die unzulässige Cipher-Suite forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "illegal_parameter" oder "handshake_failure" als TLS-Alert.

Tabelle 4.128 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.129 Ablaufbeschreibung

4.34 TC.CLS.TLS.MustAbortHandshakeWithImproperCipherSuitePinningModeDirectTrustClsAsClient14

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Verwendung nicht erlaubter Cipher-Suites unterbindet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello die Cipher-Suite TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305 verhandelt wird unabhängig davon, ob diese im Client-Hello angeboten wurde. Diese Cipher-Suite wird nicht von der TR-03116-3 erlaubt. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.130 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.131 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die unzulässige Cipher-Suite forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "illegal_parameter" oder "handshake_failure" als TLS-Alert.

Tabelle 4.132 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.133 Ablaufbeschreibung

4.35 TC.CLS.TLS.MustAbortHandshakeWithImproperCipherSuitePinning-ModeDirectTrustClsAsClient15

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Verwendung nicht erlaubter Cipher-Suites unterbindet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello die Cipher-Suite TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 verhandelt

wird unabhängig davon, ob diese im Client-Hello angeboten wurde. Diese Cipher-Suite wird nicht von der TR-03116-3 erlaubt. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.134 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.135 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die unzulässige Cipher-Suite forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "illegal_parameter" oder "handshake_failure" als TLS-Alert.

Tabelle 4.136 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.

Nr.	Beschreibung
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.137 Ablaufbeschreibung

4.36 TC.CLS.TLS.MustAbortHandshakeWithImproperCipherSuitePinning-ModeDirectTrustClsAsClient16

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Verwendung nicht erlaubter Cipher-Suites unterbindet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello die Cipher-Suite TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305 verhandelt wird unabhängig davon, ob diese im Client-Hello angeboten wurde. Diese Cipher-Suite wird nicht von der TR-03116-3 erlaubt. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.138 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.

Nr.	Beschreibung
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.139 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die unzulässige Cipher-Suite forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "illegal_parameter" oder "handshake_failure" als TLS-Alert.

Tabelle 4.140 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.141 Ablaufbeschreibung

4.37 TC.CLS.TLS.MustAbortHandshakeWithImproperCipherSuitePinningModeDirectTrustClsAsClient16a

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Verwendung nicht erlaubter Cipher-Suites unterbindet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello die Cipher-Suite TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256 verhandelt wird unabhängig davon, ob diese im Client-Hello angeboten wurde. Diese Cipher-Suite wird nicht von der TR-03116-3 erlaubt. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.142 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.143 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die unzulässige Cipher-Suite forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "illegal_parameter" oder "handshake_failure" als TLS-Alert.

Tabelle 4.144 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.145 Ablaufbeschreibung

4.38 TC.CLS.TLS.MustAbortHandshakeWithImproperCipherSuitePinningModeDirectTrustClsAsClient16b

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Verwendung nicht erlaubter Cipher-Suites unterbindet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello die Cipher-Suite TLS_PSK_WITH_AES_128_CBC_SHA256 verhandelt wird unabhängig

davon, ob diese im Client-Hello angeboten wurde. Diese Cipher-Suite wird nicht von der TR-03116-3 erlaubt. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.146 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.147 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die unzulässige Cipher-Suite forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "illegal_parameter" oder "handshake_failure" als TLS-Alert.

Tabelle 4.148 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.

Nr.	Beschreibung
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.149 Ablaufbeschreibung

4.39 TC.CLS.TLS.MustAbortHandshakeWithImproperCipherSuitePinning-ModeDirectTrustClsAsClient17

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Verwendung nicht erlaubter Cipher-Suites unterbindet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello die Cipher-Suite TLS_CHACHA20_POLY1305_SHA256 verhandelt wird unabhängig davon, ob diese im Client-Hello angeboten wurde. Diese Cipher-Suite wird nicht von der TR-03116-3 erlaubt. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20
- ICS.TA.TLS.HanHandshake.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.150 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.

Nr.	Beschreibung
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.151 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die unzulässige Cipher-Suite forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "illegal_parameter" als TLS-Alert.

Tabelle 4.152 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.153 Ablaufbeschreibung

4.40 TC.CLS.TLS.MustAbortHandshakeWithImproperCipherSuitePinning-ModeDirectTrustClsAsClient18

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Verwendung nicht erlaubter Cipher-Suites unterbindet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello die Cipher-Suite TLS_AES_128_CCM_8_SHA256 verhandelt wird unabhängig davon, ob diese im Client-Hello angeboten wurde. Diese Cipher-Suite wird nicht von der TR-03116-3 erlaubt. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20
- ICS.TA.TLS.HanHandshake.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.154 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.155 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die unzulässige Cipher-Suite forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "illegal_parameter" als TLS-Alert.

Tabelle 4.156 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.157 Ablaufbeschreibung

4.41 TC.CLS.TLS.MustAbortHandshakeWithImproperCipherSuitePinning-ModeDirectTrustClsAsServer

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Verwendung nicht erlaubter Cipher-Suites unterbindet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Client-Hello ausschließlich Cipher-Suiten angeboten werden, die nicht von der TR-03116-3 erlaubt sind. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.158 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.159 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand, wobei im Client-Hello nur unzulässige Cipher-Suites angeboten werden.	• Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Server aus. • Der TLS-Server sendet "illegal_parameter" oder "handshake_failure" als TLS-Alert.

Tabelle 4.160 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.161 Ablaufbeschreibung

4.42 TC.CLS.TLS.MustAbortHandshakeWithImproperEllipticCurve-PinningModeDirectTrustClsAsClient01

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand mit einem SMGW kommuniziert, das nicht erlaubte elliptische Kurven verwendet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau abgewartet, bei dem die elliptische Kurve Secp521r1 (IANA 25) verhandelt wird (unabhängig davon, ob diese vom Client angeboten wurde), die nicht von der TR-03116-3 erlaubt ist. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30
- REQ.TA.TLS.Handshake.50

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.162 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start des virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.163 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die unzulässige elliptische Kurve Secp521r1 forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "illegal_parameter", "unexpected_message" oder "handshake_failure" als TLS-Alert.

Tabelle 4.164 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.165 Ablaufbeschreibung

4.43 TC.CLS.TLS.MustAbortHandshakeWithImproperEllipticCurve-PinningModeDirectTrustClsAsClient02

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand mit einem SMGW kommuniziert, das nicht erlaubte elliptische Kurven verwendet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau abgewartet, bei dem die elliptische Kurve X25519 (IANA 29) verhandelt wird (unabhängig davon, ob diese vom Client angeboten wurde), die nicht von der TR-03116-3 erlaubt ist. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30
- REQ.TA.TLS.Handshake.50

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.166 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start des virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.167 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die unzulässige elliptische Kurve X25519 forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "illegal_parameter", "unexpected_message" oder "handshake_failure" als TLS-Alert.

Tabelle 4.168 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.169 Ablaufbeschreibung

4.44 TC.CLS.TLS.MustAbortHandshakeWithImproperEllipticCurve-PinningModeDirectTrustClsAsClient03

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand mit einem SMGW kommuniziert, das nicht erlaubte elliptische Kurven verwendet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau abgewartet, bei dem die elliptische Kurve X448 (IANA 30) verhandelt wird (unabhängig davon, ob diese vom Client angeboten wurde), die nicht von der TR-03116-3 erlaubt ist. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30

- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30
- REQ.TA.TLS.Handshake.50

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.170 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start des virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.171 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die unzulässige elliptische Kurve X448 forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "illegal_parameter", "unexpected_message" oder "handshake_failure" als TLS-Alert.

Tabelle 4.172 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.173 Ablaufbeschreibung

4.45 TC.CLS.TLS.MustAbortHandshakeWithImproperEllipticCurve-PinningModeDirectTrustClsAsClient04

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand mit einem SMGW kommuniziert, das nicht erlaubte elliptische Kurven verwendet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau abgewartet, bei dem die elliptische Kurve GC256A (IANA 34) verhandelt wird (unabhängig davon, ob diese vom Client angeboten wurde), die nicht von der TR-03116-3 erlaubt ist. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30
- REQ.TA.TLS.Handshake.50

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.174 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start des virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.175 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die unzulässige elliptische Kurve GC256A forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "illegal_parameter", "unexpected_message" oder "handshake_failure" als TLS-Alert.

Tabelle 4.176 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.177 Ablaufbeschreibung

4.46 TC.CLS.TLS.MustAbortHandshakeWithImproperEllipticCurve-PinningModeDirectTrustClsAsServer

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand mit einem SMGW kommuniziert, das nicht erlaubte elliptische Kurven verwendet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem die elliptische Kurven Secp521r1 (IANA 25), X25519 (IANA 29), X448 (IANA 30) und GC256A (IANA 34) angeboten werden, die nicht von der TR-03116-3 erlaubt sind. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.30
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.30
- REQ.TA.TLS.Handshake.50

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.178 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.

- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start des virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.179 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand, wobei im Client-Hello nur unzulässige elliptische Kurven angeboten werden.	• Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der Client muss einen "handshake_failure"- oder "insufficient_security"-Alert senden.

Tabelle 4.180 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.181 Ablaufbeschreibung

4.47 TC.CLS.TLS.MustAbortHandshakeWithImproperTlsVersionPinning-ModeDirectTrustClsAsClient01

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand mit einem SMGW kommuniziert, das eine nicht zugelassene TLS-Version verwendet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello SSL 1.0 verhandelt wird (unabhängig davon, ob diese Version im Client-Hello angeboten wurde), die nicht von der TR-03116-3 erlaubt ist. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.OpenHanSessionAsClient.10

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.182 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Starten eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.183 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello SSL 1.0 als Version forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "protocol_version" als TLS-Alert.

Tabelle 4.184 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.185 Ablaufbeschreibung

4.48 TC.CLS.TLS.MustAbortHandshakeWithImproperTlsVersionPinning-ModeDirectTrustClsAsClient02

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand mit einem SMGW kommuniziert, das eine nicht zugelassene TLS-Version verwendet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello SSL 2.0 verhandelt wird (unabhängig davon, ob diese Version im Client-Hello angeboten wurde), die nicht von der TR-03116-3 erlaubt ist. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.OpenHanSessionAsClient.10

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.186 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Starten eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.187 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello SSL 2.0 als Version forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "protocol_version" als TLS-Alert.

Tabelle 4.188 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.

Nr.	Beschreibung
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.189 Ablaufbeschreibung

4.49 TC.CLS.TLS.MustAbortHandshakeWithImproperTlsVersionPinning-ModeDirectTrustClsAsClient03

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand mit einem SMGW kommuniziert, das eine nicht zugelassene TLS-Version verwendet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello SSL 3.0 verhandelt wird (unabhängig davon, ob diese Version im Client-Hello angeboten wurde), die nicht von der TR-03116-3 erlaubt ist. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.OpenHanSessionAsClient.10

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.190 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Starten eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.191 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello SSL 3.0 als Version forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "protocol_version" als TLS-Alert.

Tabelle 4.192 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.193 Ablaufbeschreibung

4.50 TC.CLS.TLS.MustAbortHandshakeWithImproperTlsVersionPinning-ModeDirectTrustClsAsClient04

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand mit einem SMGW kommuniziert, das eine nicht zugelassene TLS-Version verwendet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello TLS 1.0 verhandelt wird (unabhängig davon, ob diese Version im Client-Hello angeboten wurde), die nicht von der TR-03116-3 erlaubt ist. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.OpenHanSessionAsClient.10

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.194 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Starten eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.195 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello TLS 1.0 als Version forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "protocol_version" als TLS-Alert.

Tabelle 4.196 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.197 Ablaufbeschreibung

4.51 TC.CLS.TLS.MustAbortHandshakeWithImproperTlsVersionPinning-ModeDirectTrustClsAsClient05

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand mit einem SMGW kommuniziert, das eine nicht zugelassene TLS-Version verwendet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Server-Hello TLS 1.1 verhandelt wird (unabhängig davon, ob diese Version im Client-Hello angeboten wurde), die nicht von der TR-03116-3 erlaubt ist. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30

- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.OpenHanSessionAsClient.10

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.198 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Starten eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.199 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello TLS 1.1 als Version forciert wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "protocol_version" als TLS-Alert.

Tabelle 4.200 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.201 Ablaufbeschreibung

4.52 TC.CLS.TLS.MustAbortHandshakeWithImproperTlsVersionPinning-ModeDirectTrustClsAsServer

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand mit einem SMGW kommuniziert, das eine nicht zugelassene TLS-Version verwendet.

Kurzbeschreibung

Zunächst wird der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein TLS-Kanalaufbau gestartet, bei dem im Client-Hello ausschließlich SSL 1.0 bis TLS 1.1 angeboten wird, die nicht von der TR-03116-3 erlaubt sind. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.OpenHanSessionAsClient.10

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.202 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Starten eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.203 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand, wobei im Client-Hello nur unzulässige SSL/TLS-Versionen angeboten werden.	• Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Server aus. • Der TLS-Server sendet "protocol_version" als TLS-Alert.

Tabelle 4.204 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.

Nr.	Beschreibung
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.205 Ablaufbeschreibung

4.53 TC.CLS.TLS.MustAbortHandshakeWithInvalidClientCertificate-Signature

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand als Server eine TLS-Verbindung zu einem SMGW ablehnt, welches ein Zertifikat mit einer nicht validen Signatur präsentiert.

Kurzbeschreibung

Zunächst wird ein Verbindungsaufbau initiiert. Dabei wird vom Client ein Zertifikat präsentiert, welches eine fehlerhafte Signatur aufweist. Der Prüfgegenstand muss den Verbindungsaufbau abbrechen.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.30
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.20

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.206 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-TLS-Port des aktuellen SMGW.
2	Starten eines virtuellen SMGW mit einem GW_HAN_TLS_CRT, dessen Signatur durch die zufällige Bitfolge gleicher Länge ersetzt wurde.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.207 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand.	• Der TLS-Verbindungsaufbau schlägt fehl.

Nr.	Beschreibung	Erwartetes Ergebnis
		• Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Server aus. • Der TLS-Server sendet "bad_certificate" oder "close_notify" oder "unknown_ca" als TLS-Alert. Es ist möglich, dass in zukünftigen Versionen dieses Testfalls die Möglichkeit, den Verbindungsaufbau mit "close_notify" oder "unknown_ca" abzubrechen, entfällt.

Tabelle 4.208 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Schließen der Verbindung zum Prüfgegenstand.
2	Starten eines SMGW mit validem Zertifikat und deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.209 Ablaufbeschreibung

4.54 TC.CLS.TLS.MustAbortHandshakeWithInvalidServerCertificate-Signature

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand als Client eine TLS-Verbindung zu einem SMGW ablehnt, welches ein Zertifikat mit einer nicht validen Signatur präsentiert.

Kurzbeschreibung

Zunächst wird ein Verbindungsaufbau abgewartet. Dabei wird vom Server ein Zertifikat präsentiert, welches eine fehlerhafte Signatur aufweist. Der Prüfgegenstand muss den Verbindungsaufbau abbrechen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.20

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.210 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.

- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten eines virtuellen SMGW mit Zertifikat aus der SM-PKI.
2	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.
3	Import des Root-CA-Zertifikats als Vertrauensanker über die Hersteller-API.
4	Import des Sub-CA-Zertifikats als Vertrauensanker über die Hersteller-API.
5	Neustarten des virtuellen SMGW mit einem GW_HAN_TLS_CRT, dessen Signatur durch die zufällige Bitfolge ersetzt wurde.
6	Starten des Tracings auf dem HAN-TLS-Port des aktuellen SMGW.

Tabelle 4.211 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Abwarten des Verbindungsaufbau durch den Prüfgegenstand.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "bad_certificate", "close_notify", oder "decrypt_error" als TLS-Alert. Es ist möglich, dass in zukünftigen Versionen dieses Testfalls die Möglichkeit, den Verbindungsaufbau mit "decrypt_error" abzubrechen, entfällt.

Tabelle 4.212 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Schließen der Verbindung zum Prüfgegenstand.
2	Starten eines SMGW mit validem Zertifikat und deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.213 Ablaufbeschreibung

4.55 TC.CLS.TLSPROXY.MustDoHandshakeWithLegalSigAlgoInPinning-ModeChainOfTrustClsAsClient01

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, einen TLS-Handshake durchzuführen, wenn das SMGW zur Signierung des Handshakes einen erlaubten Signaturalgorithmus verwendet.

Kurzbeschreibung

Zunächst wird ein Verbindungsaufbau abgewartet. Dabei wird der Handshake vom Server mit ECDSA / SHA-256 signiert. Darüber hinaus muss der Client in der Client-Hello-Extension exakt durch die TR-03109-3

erlaubten Algorithmen aufführen. Der Prüfgegenstand muss den Verbindungsaufbau erfolgreich durchführen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.214 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface.
2	Starten eines virtuellen SMGW mit GW_HAN_TLS_CRT aus der SM-PKI.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.
4	Import des Root-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
5	Import des Sub-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
6	Deaktivieren des "Direct Trust" für das initial gepinnte Zertifikat.

Tabelle 4.215 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Handshake der zulässige Signaturalgorithmus ECDSA-SHA256 verwendet wird.	• Der TLS-Verbindungsaufbau ist erfolgreich. • Der Client bietet ECDSA-SHA256 als Signaturverfahren an. • Der Client bietet ECDSA-SHA384 als Signaturverfahren an. • Der Client bietet ECDSA-SHA512 als Signaturverfahren an.

Tabelle 4.216 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Beenden der Verbindung zum CLS-Gerät.

Nr.	Beschreibung
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.217 Ablaufbeschreibung

4.56 TC.CLS.TLSPROXY.MustDoHandshakeWithLegalSigAlgoInPinning-ModeChainOfTrustClsAsClient02

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, einen TLS-Handshake durchzuführen, wenn das SMGW zur Signierung des Handshakes einen erlaubten Signaturalgorithmus verwendet.

Kurzbeschreibung

Zunächst wird ein Verbindungsaufbau abgewartet. Dabei wird der Handshake vom Server mit ECDSA / SHA-384 signiert. Darüber hinaus muss der Client in der Client-Hello-Extension exakt durch die TR-03109-3 erlaubten Algorithmen aufführen. Der Prüfgegenstand muss den Verbindungsaufbau erfolgreich durchführen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.218 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface.
2	Starten eines virtuellen SMGW mit GW_HAN_TLS_CRT aus der SM-PKI.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.
4	Import des Root-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
5	Import des Sub-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
6	Deaktivieren des "Direct Trust" für das initial gepinnte Zertifikat.

Tabelle 4.219 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Handshake der zulässige Signaturalgorithmus ECDSA-SHA384 verwendet wird.	• Der TLS-Verbindungsaufbau ist erfolgreich. • Der Client bietet ECDSA-SHA256 als Signaturverfahren an. • Der Client bietet ECDSA-SHA384 als Signaturverfahren an. • Der Client bietet ECDSA-SHA512 als Signaturverfahren an.

Tabelle 4.220 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Beenden der Verbindung zum CLS-Gerät.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.221 Ablaufbeschreibung

4.57 TC.CLS.TLSPROXY.MustDoHandshakeWithLegalSigAlgoInPinning-ModeChainOfTrustClsAsClient03

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, einen TLS-Handshake durchzuführen, wenn das SMGW zur Signierung des Handshakes einen erlaubten Signaturalgorithmus verwendet.

Kurzbeschreibung

Zunächst wird ein Verbindungsaufbau abgewartet. Dabei wird der Handshake vom Server mit ECDSA / SHA-512 signiert. Darüber hinaus muss der Client in der Client-Hello-Extension exakt durch die TR-03109-3 erlaubten Algorithmen aufführen. Der Prüfgegenstand muss den Verbindungsaufbau erfolgreich durchführen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.222 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.

- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface.
2	Starten eines virtuellen SMGW mit GW_HAN_TLS_CRT aus der SM-PKI.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.
4	Import des Root-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
5	Import des Sub-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
6	Deaktivieren des "Direct Trust" für das initial gepinnte Zertifikat.

Tabelle 4.223 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Handshake der zulässige Signaturalgorithmus ECDSA-SHA512 verwendet wird.	• Der TLS-Verbindungsaufbau ist erfolgreich. • Der Client bietet ECDSA-SHA256 als Signaturverfahren an. • Der Client bietet ECDSA-SHA384 als Signaturverfahren an. • Der Client bietet ECDSA-SHA512 als Signaturverfahren an.

Tabelle 4.224 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Beenden der Verbindung zum CLS-Gerät.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.225 Ablaufbeschreibung

4.58 TC.CLS.TLSPROXY.MustDoHandshakeWithLegalSigAlgoInPinningModeChainOfTrustClsAsServer01

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, einen TLS-Handshake durchzuführen, wenn das SMGW zur Signierung des Handshakes einen erlaubten Signaturalgorithmus verwendet.

Kurzbeschreibung

Zunächst wird ein Verbindungsaufbau abgewartet. Dabei wird der Handshake vom Server mit ECDSA / SHA-256 signiert. Darüber hinaus muss der Client in der Client-Hello-Extension exakt durch die TR-03109-3 erlaubten Algorithmen aufführen. Der Prüfgegenstand muss den Verbindungsaufbau erfolgreich durchführen.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.226 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface.
2	Starten eines virtuellen SMGW mit GW_HAN_TLS_CRT aus der SM-PKI.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.
4	Import des Root-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
5	Import des Sub-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
6	Deaktivieren des "Direct Trust" für das initial gepinnte Zertifikat.

Tabelle 4.227 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand, wobei im Client-Hello nur einer der zulässigen Signaturalgorithmen (ECDSA-SHA256) angeboten wird.	• Der TLS-Verbindungsaufbau ist erfolgreich. • Der Server verwendet ECDSA-SHA256, um den Handshake zu signieren.

Tabelle 4.228 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Beenden der Verbindung zum CLS-Gerät.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.229 Ablaufbeschreibung

4.59 TC.CLS.TLSPROXY.MustDoHandshakeWithLegalSigAlgoInPinningModeChainOfTrustClsAsServer02

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, einen TLS-Handshake durchzuführen, wenn das SMGW zur Signierung des Handshakes einen erlaubten Signaturalgorithmus verwendet.

Kurzbeschreibung

Zunächst wird ein Verbindungsaufbau abgewartet. Dabei wird der Handshake vom Server mit ECDSA / SHA-384 signiert. Darüber hinaus muss der Client in der Client-Hello-Extension exakt durch die TR-03109-3 erlaubten Algorithmen aufführen. Der Prüfgegenstand muss den Verbindungsaufbau erfolgreich durchführen.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.230 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface.
2	Starten eines virtuellen SMGW mit GW_HAN_TLS_CRT aus der SM-PKI.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.
4	Import des Root-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
5	Import des Sub-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
6	Deaktivieren des "Direct Trust" für das initial gepinnte Zertifikat.

Tabelle 4.231 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand, wobei im Client-Hello nur einer der zulässigen Signaturalgorithmen (ECDSA-SHA384) angeboten wird.	• Der TLS-Verbindungsaufbau ist erfolgreich. • Der Server verwendet ECDSA-SHA384, um den Handshake zu signieren.

Tabelle 4.232 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Beenden der Verbindung zum CLS-Gerät.

Nr.	Beschreibung
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.233 Ablaufbeschreibung

4.60 TC.CLS.TLSPROXY.MustDoHandshakeWithLegalSigAlgoInPinning-ModeChainOfTrustClsAsServer03

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, einen TLS-Handshake durchzuführen, wenn das SMGW zur Signierung des Handshakes einen erlaubten Signaturalgorithmus verwendet.

Kurzbeschreibung

Zunächst wird ein Verbindungsaufbau abgewartet. Dabei wird der Handshake vom Server mit ECDSA / SHA-512 signiert. Darüber hinaus muss der Client in der Client-Hello-Extension exakt durch die TR-03109-3 erlaubten Algorithmen aufführen. Der Prüfgegenstand muss den Verbindungsaufbau erfolgreich durchführen.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.234 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface.
2	Starten eines virtuellen SMGW mit GW_HAN_TLS_CRT aus der SM-PKI.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.
4	Import des Root-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
5	Import des Sub-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
6	Deaktivieren des "Direct Trust" für das initial gepinnte Zertifikat.

Tabelle 4.235 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand, wobei im Client-Hello nur einer der zulässigen Signaturalgorithmen (ECDSA-SHA512) angeboten wird.	• Der TLS-Verbindungsaufbau ist erfolgreich. • Der Server verwendet ECDSA-SHA512, um den Handshake zu signieren.

Tabelle 4.236 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Beenden der Verbindung zum CLS-Gerät.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.237 Ablaufbeschreibung

4.61 TC.CLS.TLS.MustDoHandshakeWithLegalVersionAndCipherSuite01

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, eine TLS-Verbindung aufzubauen, bei der ausschließlich TLS1.2 mit der Cipher-Suite TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 angeboten wird.

Kurzbeschreibung

Es wird ein Verbindungsaufbau initiiert, bei dem ausschließlich TLS1.2 / TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 angeboten wird. Der Verbindungsaufbau muss erfolgreich sein.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.238 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.

Nr.	Beschreibung
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.239 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand, wobei im Client-Hello nur eine der zulässigen Cipher-Suites angeboten wird.	• Der TLS-Verbindungsaufbau ist erfolgreich.

Tabelle 4.240 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.241 Ablaufbeschreibung

4.62 TC.CLS.TLS.MustDoHandshakeWithLegalVersionAndCipherSuite02

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, eine TLS-Verbindung aufzubauen, bei der ausschließlich TLS1.2 mit der Cipher-Suite TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 angeboten wird.

Kurzbeschreibung

Es wird ein Verbindungsaufbau initiiert, bei dem ausschließlich TLS1.2 / TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 angeboten wird. Der Verbindungsaufbau muss erfolgreich sein.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.242 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.

- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.243 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand, wobei im Client-Hello nur eine der zulässigen Cipher-Suites angeboten wird.	• Der TLS-Verbindungsaufbau ist erfolgreich.

Tabelle 4.244 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.245 Ablaufbeschreibung

4.63 TC.CLS.TLS.MustDoHandshakeWithLegalVersionAndCipherSuite03

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, eine TLS-Verbindung aufzubauen, bei der ausschließlich TLS1.2 mit der Cipher-Suite TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 angeboten wird.

Kurzbeschreibung

Es wird ein Verbindungsaufbau initiiert, bei dem ausschließlich TLS1.2 / TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 angeboten wird. Der Verbindungsaufbau muss erfolgreich sein. Da die Verwendung von TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 nur eine SOLL-Anforderung ist, kann dieser Testfall zu einem falsch negativen Ergebnis führen.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10
- ICS.TA.TLS.HanHandshake.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.246 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.247 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand, wobei im Client-Hello nur eine der zulässigen Cipher-Suites angeboten wird.	• Der TLS-Verbindungsaufbau ist erfolgreich.

Tabelle 4.248 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.249 Ablaufbeschreibung

4.64 TC.CLS.TLS.MustDoHandshakeWithLegalVersionAndCipherSuite04

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, eine TLS-Verbindung aufzubauen, bei der ausschließlich TLS1.2 mit der Cipher-Suite TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 angeboten wird.

Kurzbeschreibung

Es wird ein Verbindungsaufbau initiiert, bei dem ausschließlich TLS1.2 / TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 angeboten wird. Der Verbindungsaufbau muss erfolgreich sein. Da die Verwendung von TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 nur eine SOLL-Anforderung ist, kann dieser Testfall zu einem falsch negativen Ergebnis führen.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.30

- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10
- ICS.TA.TLS.HanHandshake.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.250 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.251 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand, wobei im Client-Hello nur eine der zulässigen Cipher-Suites angeboten wird.	• Der TLS-Verbindungsaufbau ist erfolgreich.

Tabelle 4.252 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.253 Ablaufbeschreibung

4.65 TC.CLS.TLS.MustDoHandshakeWithLegalVersionAndCipherSuite05

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, eine TLS-Verbindung aufzubauen, bei der ausschließlich TLS1.2 mit der Cipher-Suite TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 angeboten wird.

Kurzbeschreibung

Es wird ein Verbindungsaufbau initiiert, bei dem ausschließlich TLS1.2 / TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 angeboten wird. Der Verbindungsaufbau muss erfolgreich sein. Da die Verwendung von TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 nur eine SOLL-Anforderung ist, kann dieser Testfall zu einem falsch negativen Ergebnis führen.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10
- ICS.TA.TLS.HanHandshake.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.254 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.255 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand, wobei im Client-Hello nur eine der zulässigen Cipher-Suites angeboten wird.	• Der TLS-Verbindungsaufbau ist erfolgreich.

Tabelle 4.256 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.257 Ablaufbeschreibung

4.66 TC.CLS.TLS.MustDoHandshakeWithLegalVersionAndCipherSuite06

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, eine TLS-Verbindung aufzubauen, bei der ausschließlich TLS1.3 mit der Cipher-Suite TLS_AES_128_GCM_SHA256 angeboten wird.

Kurzbeschreibung

Es wird ein Verbindungsaufbau initiiert, bei dem ausschließlich TLS1.3 / TLS_AES_128_GCM_SHA256 angeboten wird. Der Verbindungsaufbau muss erfolgreich sein.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.30
- REQ.TA.TLS.Handshake.30
- REQ.TA.TLS.OpenHanSessionAsServer.10

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10
- ICS.TA.TLS.HanHandshake.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.258 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.259 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand, wobei im Client-Hello nur eine der zulässigen Cipher-Suites angeboten wird.	• Der TLS-Verbindungsaufbau ist erfolgreich.

Tabelle 4.260 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.261 Ablaufbeschreibung

4.67 TC.CLS.TLS.MustDoHandshakeWithLegalVersionAndCipherSuite07

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, eine TLS-Verbindung aufzubauen, bei der ausschließlich TLS1.3 mit der Cipher-Suite TLS_AES_256_GCM_SHA384 angeboten wird.

Kurzbeschreibung

Es wird ein Verbindungsaufbau initiiert, bei dem ausschließlich TLS1.3 / TLS_AES_256_GCM_SHA384 angeboten wird. Der Verbindungsaufbau muss erfolgreich sein. Da die Verwendung von TLS 1.3 sowie TLS_AES_256_GCM_SHA384 nur SOLL-Anforderungen sind, kann dieser Testfall zu einem falsch negativen Ergebnis führen.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.30
- REQ.TA.TLS.Handshake.30
- REQ.TA.TLS.OpenHanSessionAsServer.10

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10
- ICS.TA.TLS.HanHandshake.10
- ICS.TA.TLS.HanHandshake.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.262 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.263 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand, wobei im Client-Hello nur eine der zulässigen Cipher-Suites angeboten wird.	• Der TLS-Verbindungsaufbau ist erfolgreich.

Tabelle 4.264 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.265 Ablaufbeschreibung

4.68 TC.CLS.TLS.MustDoHandshakeWithLegalVersionAndCipherSuite08

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, eine TLS-Verbindung aufzubauen, bei der ausschließlich TLS1.3 mit der Cipher-Suite TLS_AES_128_CCM_SHA256 angeboten wird.

Kurzbeschreibung

Es wird ein Verbindungsaufbau initiiert, bei dem ausschließlich TLS1.3 / TLS_AES_128_CCM_SHA256 angeboten wird. Der Verbindungsaufbau muss erfolgreich sein. Da die Verwendung von TLS 1.3 sowie TLS_AES_128_CCM_SHA256 nur SOLL-Anforderungen sind, kann dieser Testfall zu einem falsch negativen Ergebnis führen.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.30
- REQ.TA.TLS.Handshake.30
- REQ.TA.TLS.OpenHanSessionAsServer.10

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10
- ICS.TA.TLS.HanHandshake.10
- ICS.TA.TLS.HanHandshake.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.266 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.

- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.267 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand, wobei im Client-Hello nur eine der zulässigen Cipher-Suites angeboten wird.	• Der TLS-Verbindungsaufbau ist erfolgreich.

Tabelle 4.268 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.269 Ablaufbeschreibung

4.69 TC.CLS.TLS.MustDoHandshakeWithSigAlgoCertExtensionInClient-Hello

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, einen TLS-Handshake durchzuführen, wenn das SMGW ein Client-Hello sendet, in dem die signature_algorithms_cert-Extension verwendet wird.

Kurzbeschreibung

Zunächst wird ein Verbindungsaufbau initiiert. Dabei wird vom Client die signature_algorithms_cert gesendet. Der Prüfgegenstand muss den Verbindungsaufbau erfolgreich durchführen.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.30
- REQ.TA.TLS.OpenHanSessionAsClient.10

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10
- ICS.TA.TLS.HanHandshake.10
- ICS.TA.TLS.HanHandshake.40

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.270 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface.
2	Starten eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.271 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand, wobei im Client-Hello die zulässigen Algorithmen in der Signature-Algorithms- und der Signature-Algorithms-Cert-Extension angeboten werden.	• Der TLS-Verbindungsaufbau ist erfolgreich.

Tabelle 4.272 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Beenden der Verbindung zum CLS-Gerät.
2	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.273 Ablaufbeschreibung

4.70 TC.CLS.TLS.MustGiveAllSupportedParametersInClientHello

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand alle von ihm unterstützten TLS-Versionen, Cipher-Suites und elliptischen Kurven im Client-Hello angibt.

Kurzbeschreibung

Zunächst wird ein Verbindungsaufbau abgewartet. Das dabei vom Prüfgegenstand versendete Client-Hello muss dabei alle nachfolgend beschriebenen Parameter enthalten. Verpflichtend ist die Verwendung von TLS 1.2. Dabei sind die Cipher-Suites TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 und TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 verpflichtend sowie als SOLL-Anforderung die Cipher-Suites TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 und TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 gefordert. Außerdem sind die elliptischen Kurven secp256r1, brainpoolP256r1 und brainpoolP384r1 verpflichtend sowie als SOLL-Anforderung

die Kurven brainpoolP512r1 und secp384r1 gefordert. Die Verwendung von TLS 1.3 ist empfohlen. Wird TLS 1.3 verwendet, ist die Cipher-Suite TLS_AES_128_GCM_SHA256 verpflichtend sowie als SOLL-Anforderung die Cipher-Suites TLS_AES_256_GCM_SHA384 und TLS_AES_128_CCM_SHA256 gefordert. Außerdem sind die Kurven brainpoolP256r1tls13, brainpoolP384r1tls13 und secp256r1 verpflichtend sowie als SOLL-Anforderung die Kurven brainpoolP512r1tls13 und secp384r1 gefordert. Da nicht alle Parameter verpflichtend sind, kann dies zu falsch negativen Testergebnissen führen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.10
- REQ.TA.TLS.Handshake.30
- REQ.TA.TLS.Handshake.50
- REQ.TA.TLS.Handshake.70
- REQ.TA.TLS.OpenHanSessionAsClient.10
- REQ.TA.TLS.OpenHanSessionAsClient.20

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20
- ICS.TA.TLS.HanHandshake.20
- ICS.TA.TLS.HanHandshake.30

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.274 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN Interface.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.275 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand.	• Die Liste der unterstützten TLS-Versionen enthält TLS 1.2.

Nr.	Beschreibung	Erwartetes Ergebnis
		• Die Liste der unterstützten TLS-Versionen enthält TLS 1.3. Da die Verwendung von TLS 1.3 nur empfohlen ist, liefert diese Assertion ggf. ein falsch negatives Ergebnis. • Die Liste der unterstützten Cipher-Suites enthält TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256. • Die Liste der unterstützten Cipher-Suites enthält TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256. • Die Liste der unterstützten Cipher-Suites enthält TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384. Da die Cipher-Suite nur eine SOLL-Anforderung ist, liefert diese Assertion ggf. ein falsch negatives Ergebnis. • Die Liste der unterstützten Cipher-Suites enthält TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256. Da die Cipher-Suite nur eine SOLL-Anforderung ist, liefert diese Assertion ggf. ein falsch negatives Ergebnis. • Die Liste der unterstützten Cipher-Suites enthält TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384. Da die Cipher-Suite nur eine SOLL-Anforderung ist, liefert diese Assertion ggf. ein falsch negatives Ergebnis. • Die Liste der unterstützten elliptischen Kurven beinhaltet secp256r1. • Die Liste der unterstützten elliptischen Kurven beinhaltet brainpoolP256r1. • Die Liste der unterstützten elliptischen Kurven beinhaltet brainpoolP384r1. • Die Liste der unterstützten elliptischen Kurven beinhaltet brainpoolP512r1. Da die Kurve nur eine SOLL-Anforderung ist, liefert diese Assertion ggf. ein falsch negatives Ergebnis. • Die Liste der unterstützten elliptischen Kurven beinhaltet secp384r1. Da die Kurve nur eine SOLL-Anforderung ist, liefert diese Assertion ggf. ein falsch negatives Ergebnis. • Die Liste der unterstützten Cipher-Suites enthält TLS_AES_128_GCM_SHA256. Da die Verwendung von TLS 1.3 nur empfohlen ist, liefert diese Assertion ggf. ein falsch negatives Ergebnis. • Die Liste der unterstützten Cipher-Suites enthält TLS_AES_256_GCM_SHA384. Da die Verwendung von TLS 1.3 nur empfohlen ist und die Cipher-Suite nur eine SOLL-Anforderung ist, liefert diese Assertion ggf. ein falsch negatives Ergebnis. • Die Liste der unterstützten Cipher-Suites enthält TLS_AES_128_CCM_SHA256. Da die Verwendung von TLS 1.3 nur empfohlen ist und die Cipher-Suite nur eine SOLL-Anforderung ist, liefert diese Assertion ggf. ein falsch negatives Ergebnis. • Die Liste der unterstützten elliptischen Kurven beinhaltet brainpoolP256r1tls13. Da die Verwendung von TLS 1.3 nur empfohlen ist, liefert diese Assertion ggf. ein falsch negatives Ergebnis. • Die Liste der unterstützten elliptischen Kurven beinhaltet brainpoolP384r1tls13. Da die Verwendung von TLS 1.3 nur empfohlen ist, liefert diese Assertion ggf. ein falsch negatives Ergebnis. • Die Liste der unterstützten elliptischen Kurven beinhaltet secp256r1. Da die Verwendung von TLS 1.3 nur empfoh-

Nr.	Beschreibung	Erwartetes Ergebnis
		len ist, liefert diese Assertion ggf. ein falsch negatives Ergebnis. • Die Liste der unterstützten elliptischen Kurven beinhaltet brainpoolP512r1tls13. Da die Kurve nur eine SOLL-Anforderung ist, liefert diese Assertion ggf. ein falsch negatives Ergebnis. • Die Liste der unterstützten elliptischen Kurven beinhaltet secp384r1. Da die Kurve nur eine SOLL-Anforderung ist, liefert diese Assertion ggf. ein falsch negatives Ergebnis.

Tabelle 4.276 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Schließen der Verbindung zum Prüfgegenstand.
2	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
3	Stoppen des virtuelles SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.277 Ablaufbeschreibung

4.71 TC.CLS.TLS.MustGiveEncryptThenMacExtensionInClientHello

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Encrypt-Then-MAC-Extension im Client-Hello angibt und sie bei Verwendung einer CBC-basierten Cipher-Suite verwenden kann.

Kurzbeschreibung

Zunächst wird ein Verbindungsaufbau abgewartet. Das dabei vom Prüfgegenstand versendete Client-Hello muss dabei die Encrypt-Then-MAC-Extension sowie die CBC-basierte Cipher Suite TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 enthalten.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.80

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20
- ICS.TA.TLS.HanHandshake.50
- ICS.TA.TLS.HanHandshake.80

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.278 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface.
2	Starten eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.279 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die Encrypt-Then-MAC Extension und die geforderte CBC-Cipher-Suite gesetzt ist.	• Der TLS-Verbindungsaufbau ist erfolgreich. • Die Liste der unterstützten Cipher-Suites enthält TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256. • Das Client-Hello enthält die Encrypt-Then-MAC-Extension.

Tabelle 4.280 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Schließen der Verbindung zum Prüfgegenstand.
2	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.281 Ablaufbeschreibung

4.72 TC.CLS.TLS.MustGiveExtendedMasterSecretExtensionInClientHello

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Extended-Master-Secret-Extension im Client-Hello angibt.

Kurzbeschreibung

Zunächst wird ein Verbindungsaufbau abgewartet. Das vom Prüfgegenstand versendete Client-Hello muss dabei die Extended-Master-Secret-Extension enthalten.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.Handshake.90

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

- ICS.TA.TLS.HanHandshake.90

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.282 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.283 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die Extended-Master-Secret-Extension gesetzt ist.	• Der TLS-Verbindungsaufbau ist erfolgreich. • Das Client-Hello enthält die Extended-Master-Secret-Extension.

Tabelle 4.284 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Schließen der Verbindung zum Prüfgegenstand.
2	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
3	Stoppen des virtuelles SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.285 Ablaufbeschreibung

4.73 TC.CLS.TLS.MustNotCommunicateWithSmgwWithUnknownTrustAnchorClsAsClient

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand mit einem SMGW kommuniziert, das ein Zertifikat präsentiert, welches eine gültige Chain-of-Trust zu einer anderen als der ihm bekannten Root-CAs nachweist.

Kurzbeschreibung

Es wird mit einem SMGW, welches ein GW_HAN_TLS_CRT aus der SM-PKI hat, das Root-CA-Zertifikat der SM-PKI importiert. Anschließend wartet der Testfall einen Verbindungsaufbau vom CLS-Gerät ab. Das SMGW

präsentiert dabei ein Zertifikat, welches keine Chain-of-Trust zu dem vom CLS-Gerät verwendeten Vertrauensanker besitzt. Der Prüfgegenstand muss den Verbindungsaufbau abbrechen.

Abgedeckte Anforderungen

- REQ.FA.ImportSmgwTrustAnchor.30
- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.IOP.KS.HAN.10
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.20

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.286 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Neustart des virtuellen SMGW mit GW_HAN_TLS_CRT aus der SM-PKI.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.
4	Import des Root-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
5	Import des Sub-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
6	Neustarten des virtuellen SMGW mit GW_HAN_TLS_CRT aus einer anderen PKI.

Tabelle 4.287 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand.	• Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Client sendet "unknown_ca", "bad_certificate" oder "close_notify" als TLS-Alert. Es ist möglich, dass in zukünftigen Versionen dieses Testfalls die Möglichkeit, den Verbindungsaufbau mit "close_notify" abzubrechen, entfällt.

Tabelle 4.288 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Neustarten des SMGW mit einem GW_HAN_TLS_CRT aus der bekannten PKI und deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Stoppen des virtuellen SMGW.
3	Stoppen des gestarteten Tracings.

Tabelle 4.289 Ablaufbeschreibung

4.74 TC.CLS.TLS.MustNotCommunicateWithSmgwWithUnknownTrust-AnchorClsAsServer

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand mit einem SMGW kommuniziert, das ein Zertifikat präsentiert, welches eine gültige Chain-of-Trust zu einer anderen als der ihm bekannten Root-CAs nachweist.

Kurzbeschreibung

Es wird mit einem SMGW, welches ein GW_HAN_TLS_CRT aus der SM-PKI hat, das Root-CA-Zertifikat der SM-PKI importiert. Anschließend baut der Testfall eine Verbindung zu einem CLS-Gerät mit einem virtuellen SMGW auf, das dabei ein Zertifikat präsentiert, welches keine Chain-of-Trust zu dem vom CLS-Gerät verwendeten Vertrauensanker besitzt. Der Prüfgegenstand muss den Verbindungsaufbau abweisen.

Abgedeckte Anforderungen

- REQ.FA.ImportSmgwTrustAnchor.30
- REQ.HKS.TLSPROXY.SRV.30
- REQ.IOP.KS.HAN.10
- REQ.TA.TLS.Handshake.130
- REQ.TA.TLS.Handshake.20

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.290 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.

Nr.	Beschreibung
2	Neustart des virtuellen SMGW mit GW_HAN_TLS_CRT aus der SM-PKI.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.
4	Import des Root-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
5	Import des Sub-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
6	Neustarten des virtuellen SMGW mit GW_HAN_TLS_CRT aus einer anderen PKI.

Tabelle 4.291 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand.	• Der TLS-Verbindungsaufbau schlägt fehl. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Server aus. • Der TLS-Server sendet "unknown_ca", "bad_certificate" oder "close_notify" als TLS-Alert. Es ist möglich, dass in zukünftigen Versionen dieses Testfalls die Möglichkeit, den Verbindungsaufbau mit "bad_certificate" oder "close_notify" abzubrechen, entfällt.

Tabelle 4.292 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Neustarten des SMGW mit einem GW_HAN_TLS_CRT aus der bekannten PKI und deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Stoppen des virtuellen SMGW.
3	Stoppen des gestarteten Tracings.

Tabelle 4.293 Ablaufbeschreibung

4.75 TC.CLS.TLSPROXY.MustNotRenegotiateClsAsServer

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand Versuche des Clients, eine TLS-Session-Renegotiation durchzuführen, abweist.

Kurzbeschreibung

Es wird eine Verbindung aufgebaut. Daraufhin wird versucht, eine Session-Renegotiation vorzunehmen. Der Prüfgegenstand muss daraufhin einen "no_renegotiation"-Alert mit dem Level "warning" senden und darf die verwendeten kryptographischen Parameter nicht ändern. Die bestehende Verbindung darf nicht abgebrochen werden.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.294 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Starten eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.
4	Stoppen des virtuellen SMGW.

Tabelle 4.295 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Versuch mit einer TLS-Renegotiation die Cipher-Suite zu wechseln, wobei im Client-Hello ausschließlich genau eine andere verpflichtend zu implementierende Cipher-Suite angegeben wird.	• Der Server sendet einen Alert auf einen Handshake, der ein Renegotiation versucht.
2	Schließen der Verbindung zum Prüfgegenstand.	-

Tabelle 4.296 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Starten eines virtuellen SMGW.
2	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.297 Ablaufbeschreibung

4.76 TC.CLS.TLS.MustNotRespondWithTruncatedHmac

Version: 1.0.0

Zweck

Der Testfall prüft, dass der Prüfgegenstand die Truncated-HMAC-Extension im Server-Hello nicht verwendet, auch wenn der Client diese angefordert hat.

Kurzbeschreibung

Zunächst wird ein Verbindungsaufbau initiiert. Das dabei versendete Client-Hello enthält die Truncated-HMAC-Extension. Der Prüfgegenstand muss den Verbindungsaufbau erfolgreich durchführen, ohne die Truncated-HMAC-Extension zu verwenden.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.30
- REQ.TA.TLS.OpenHanSessionAsClient.40

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10
- ICS.TA.TLS.HanHandshake.50

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.298 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface.
2	Starten eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.299 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand, wobei im Client-Hello die Truncated-HMAC-Extension angeboten wird.	• Das Server-Hello enthält keine Truncated-HMAC-Extension. • Der TLS-Verbindungsaufbau ist erfolgreich.

Tabelle 4.300 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Schließen der Verbindung zum Prüfgegenstand.
2	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.301 Ablaufbeschreibung

4.77 TC.CLS.TLS.MustNotUseTrunctedHmacExtensionClsAsClient

Version: 1.0.0

Zweck

Der Testfall prüft, dass der Prüfgegenstand die Truncated-HMAC-Extension nicht im Client-Hello angibt und sie, wenn der Server sie dennoch auswählt, nicht verwendet.

Kurzbeschreibung

Zunächst wird ein Verbindungsaufbau abgewartet. Das dabei vom Prüfgegenstand versendete Client-Hello darf dabei die Truncated-HMAC-Extension nicht enthalten. Daraufhin wählt der Server im Server-Hello die Truncated-HMAC-Extension dennoch aus. Der Prüfgegenstand muss einen "unsupported_extension"-Alert senden und den Verbindungsaufbau abbrechen.

Abgedeckte Anforderungen

- REQ.HKS.NTP-TLS.30
- REQ.HKS.TLSPROXY.CLI.30
- REQ.HKS.TLSPROXY.SOCKSCLI.30
- REQ.TA.TLS.OpenHanSessionAsClient.40

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20
- ICS.TA.TLS.HanHandshake.50

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.302 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface.
2	Starten eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.303 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand, wobei im Server-Hello die Truncated-HMAC-Extension gesetzt ist und eine CBC-Cipher-Suite verwendet wird.	• Es wird vor Ablauf des Timeouts ein TLS-Verbindungsaufbau initiiert. • Der TLS-Verbindungsaufbau schlägt fehl. • Das Client-Hello enthält keine Truncated-HMAC-Extension. • Der TLS-Alert zum Abbruch des TLS-Verbindungsaufbaus geht vom Client aus. • Der TLS-Alert hat das Level "fatal". • Der TLS-Client sendet "unsupported_extension" als TLS-Alert.

Tabelle 4.304 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Schließen der Verbindung zum Prüfgegenstand.
2	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.305 Ablaufbeschreibung

4.78 TC.CLS.TLS.MustRespondWithEncryptThenMac01

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Encypt-Then-MAC-Extension im Server-Hello verwendet, sofern eine CBC-basierte Cipher-Suite verwendet wird.

Kurzbeschreibung

Zunächst wird ein Verbindungsaufbau initiiert. Das dabei versendete Client-Hello enthält die Encrypt-Then-MAC-Extension sowie die Cipher-Suite TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256. Der Prüfgegenstand muss den Verbindungsaufbau erfolgreich mit Encrypt-then-MAC durchführen.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.30
- REQ.TA.TLS.Handshake.80

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10
- ICS.TA.TLS.HanHandshake.50
- ICS.TA.TLS.HanHandshake.80

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.306 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface.
2	Starten eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.307 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand, wobei im Client-Hello nur TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 sowie die Encrypt-Then-MAC Extension angeboten wird.	• Das Server-Hello enthält die encrypt_then_mac-Extension. • Der TLS-Verbindungsaufbau ist erfolgreich.

Tabelle 4.308 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.309 Ablaufbeschreibung

4.79 TC.CLS.TLS.MustRespondWithEncryptThenMac02

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Encypt-Then-MAC-Extension im Server-Hello verwendet, sofern eine CBC-basierte Cipher-Suite verwendet wird.

Kurzbeschreibung

Zunächst wird ein Verbindungsaufbau initiiert. Das dabei versendete Client-Hello enthält die Encrypt-Then-MAC-Extension sowie die Cipher-Suite TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384. Der Prüfgegenstand muss den Verbindungsaufbau erfolgreich mit Encrypt-then-MAC durchführen. Da die Verwendung TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 nur eine SOLL-Anforderung ist, kann dieser Testfall ein falsch-negatives Ergebnis liefern.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.30
- REQ.TA.TLS.Handshake.80
- REQ.TA.TLS.OpenHanSessionAsClient.20

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10
- ICS.TA.TLS.HanHandshake.20
- ICS.TA.TLS.HanHandshake.50
- ICS.TA.TLS.HanHandshake.80

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.310 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.

- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface.
2	Starten eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.311 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand, wobei im Client-Hello nur TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 sowie die Encrypt-Then-MAC Extension angeboten wird.	• Das Server-Hello enthält die encrypt_then_mac-Extension. • Der TLS-Verbindungsaufbau ist erfolgreich.

Tabelle 4.312 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.313 Ablaufbeschreibung

4.80 TC.CLS.TLS.MustRespondWithExtendedMasterSecret

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand die Extended-Master-Secret-Extension im Server-Hello verwendet, wenn der Client diese angefordert hat.

Kurzbeschreibung

Zunächst wird ein Verbindungsaufbau initiiert. Das dabei versendete Client-Hello enthält die Extended-Master-Secret-Extension. Der Prüfgegenstand muss den Verbindungsaufbau erfolgreich mit einem Extended-Master-Secret durchführen.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.30
- REQ.TA.TLS.Handshake.90

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10
- ICS.TA.TLS.HanHandshake.90

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.314 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface.
2	Starten eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.315 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand, wobei im Client-Hello die Extended-Master-Secret-Extension angeboten wird.	• Das Server-Hello enthält die Extended-Master-Secret-Extension. • Der TLS-Verbindungsaufbau ist erfolgreich.

Tabelle 4.316 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Schließen der Verbindung zum Prüfgegenstand.
2	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.317 Ablaufbeschreibung

4.81 TC.CLS.TLSPROXY.MustAcceptConnection

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand dazu in der Lage ist, einen vom SMGW initiierten Kanal anzunehmen.

Kurzbeschreibung

Es wird ein Verbindungsaufbau initiiert. Der Verbindungsaufbau muss erfolgreich sein.

Abgedeckte Anforderungen

- REQ.FA.AcceptProxyCh.20
- REQ.FAKAT.TlsProxy.20
- REQ.HKS.TLSPROXY.SRV.20

- REQ.HKS.TLSPROXY.SRV.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.318 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-TLS-Port des aktuellen SMGW.
2	Start eines virtuellen SMGW.

Tabelle 4.319 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.	• Innerhalb des Timeouts wird eine Antwort der API empfangen. • Der HTTP-Rückgabe-Code der Hersteller-API entspricht dem Code OK (200)
2	Aufbau einer Verbindung zum Prüfgegenstand.	• Der TLS-Verbindungsaufbau ist erfolgreich.

Tabelle 4.320 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Schließen der Verbindung und stoppen des virtuellen SMGW.
3	Stoppen des gestarteten Tracings.

Tabelle 4.321 Ablaufbeschreibung

4.82 TC.CLS.TLSPROXY.MustCommunicateWithOtherSmgwInPinningModeChainOfTrustClsAsClient

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in Pairing Mode PKI auch nach erfolgter Kommunikation noch mit einem anderen SMGW, welches ein Zertifikat aus der SM-PKI präsentiert, kommuniziert.

Kurzbeschreibung

Es wird mit einem SMGW, welches ein GW_HAN_TLS_CRT aus der SM-PKI hat, das Root- und Sub-CA-Zertifikat der SM-PKI importiert und auf einen Verbindungsaufbau gewartet, welcher erfolgreich sein muss. Anschließend wird mit einem anderen SMGW (abweichender Common Name, aber ebenfalls aus der SM-PKI) erneut ein Verbindungsaufbau abgewartet, der ebenfalls erfolgreich sein muss.

Abgedeckte Anforderungen

- REQ.FAKAT.SmgwAssociation.40

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.322 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-TLS-Port des aktuellen SMGW.
2	Starten des ersten virtuellen SMGW mit GW_HAN_TLS_CRT aus der SM-PKI.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.
4	Import des Root-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
5	Import des Sub-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
6	Deaktivieren des "Direct Trust" für das initial gepinnte Zertifikat.
7	Warten auf den Verbindungsaufbau durch den Prüfgegenstand.
8	Trennen der Verbindung zum Prüfgegenstand.
9	Stoppen des ersten virtuellen SMGW.
10	Starten des zweiten virtuellen SMGW mit GW_HAN_TLS_CRT aus der SM-PKI.

Tabelle 4.323 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand.	• Der TLS-Verbindungsaufbau ist erfolgreich.

Tabelle 4.324 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Trennen der Verbindung zum Prüfgegenstand.

Nr.	Beschreibung
3	Stoppen des zweiten virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.325 Ablaufbeschreibung

4.83 TC.CLS.TLSPROXY.MustCommunicateWithOtherSmgwInPinning-ModeChainOfTrustClsAsServer

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in Pairing Mode PKI auch nach erfolgter Kommunikation noch mit einem anderen SMGW, welches ein Zertifikat aus der SM-PKI präsentiert, kommuniziert.

Kurzbeschreibung

Es wird mit einem SMGW, welches ein GW_HAN_TLS_CRT aus der SM-PKI hat, das Root- und Sub-CA-Zertifikat der SM-PKI importiert und ein Verbindungsaufbau gestartet, welcher erfolgreich sein muss. Anschließend wird mit einem anderen SMGW (abweichender Common Name, aber ebenfalls aus der SM-PKI) erneut ein Verbindungsaufbau gestartet, der ebenfalls erfolgreich sein muss.

Abgedeckte Anforderungen

- REQ.FAKAT.SmgwAssociation.40

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.326 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-TLS-Port des aktuellen SMGW.
2	Starten des ersten virtuellen SMGW mit GW_HAN_TLS_CRT aus der SM-PKI.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.
4	Import des Root-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
5	Import des Sub-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
6	Deaktivieren des "Direct Trust" für das initial gepinnte Zertifikat.
7	Aufbau einer Verbindung zum Prüfgegenstand mit dem ersten SMGW.
8	Trennen der Verbindung zum Prüfgegenstand.

Nr.	Beschreibung
9	Stoppen des ersten virtuellen SMGW.
10	Starten des zweiten virtuellen SMGW mit GW_HAN_TLS_CRT aus der SM-PKI.

Tabelle 4.327 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand mit dem zweiten SMGW.	• Der TLS-Verbindungsaufbau ist erfolgreich.

Tabelle 4.328 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Trennen der Verbindung zum Prüfgegenstand.
3	Stoppen des zweiten virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.329 Ablaufbeschreibung

4.84 TC.CLS.TLSPROXY.MustCommunicateWithPinnedSmgwInPinning-ModeDirectTrustClsAsClient

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, ein SMGW-Zertifikat zu pinnen.

Kurzbeschreibung

Über die Hersteller-API wird zunächst der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein Verbindungsaufbau abgewartet, bei dem das korrekte Zertifikat verwendet wird. Die Verbindung muss erfolgreich aufgebaut werden.

Abgedeckte Anforderungen

- REQ.FA.PinSmgwCertificate.20
- REQ.FA.PinSmgwCertificate.30
- REQ.FAKAT.SmgwAssociation.20

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.330 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.

- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN Interface.
2	Starten des virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.331 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand.	• Der TLS-Verbindungsaufbau ist erfolgreich.

Tabelle 4.332 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Verbindung zum CLS-Gerät beenden.
2	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.333 Ablaufbeschreibung

4.85 TC.CLS.TLSPROXY.MustCommunicateWithPinnedSmgwInPinningModeDirectTrustClsAsServer

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand dazu in der Lage ist, ein SMGW-Zertifikat zu pinnen.

Kurzbeschreibung

Über die Hersteller-API wird zunächst der FA.PinSmgwCertificate aufgerufen. Im Anschluss wird ein Verbindungsaufbau initiiert, bei dem das korrekte Zertifikat verwendet wird. Die Verbindung muss erfolgreich aufgebaut werden.

Abgedeckte Anforderungen

- REQ.FA.PinSmgwCertificate.20
- REQ.FA.PinSmgwCertificate.30
- REQ.FAKAT.SmgwAssociation.20

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.334 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN Interface.
2	Starten des virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.335 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand.	• Der TLS-Verbindungsaufbau ist erfolgreich.

Tabelle 4.336 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Schließen der Verbindung zum Prüfgegenstand.
2	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.337 Ablaufbeschreibung

4.86 TC.CLS.TLSPROXY.MustCommunicateWithSmgwInPinningMode-ChainOfTrustClsAsClient

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, in Pairing Mode PKI mit einem SMGW, welches ein Zertifikat aus der SM-PKI präsentiert, zu kommunizieren.

Kurzbeschreibung

Es wird mit einem SMGW, welches ein GW_HAN_TLS_CRT aus der SM-PKI hat, das Root- und Sub-CA-Zertifikat der SM-PKI importiert und auf einen Verbindungsaufbau gewartet. Dieser muss erfolgreich sein.

Abgedeckte Anforderungen

- REQ.FA.ImportSmgwTrustAnchor.30
- REQ.FAKAT.SmgwAssociation.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.338 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-TLS-Port des aktuellen SMGW.
2	Starten eines virtuellen SMGW mit GW_HAN_TLS_CRT aus der SM-PKI.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.
4	Import des Root-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
5	Import des Sub-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
6	Deaktivieren des "Direct Trust" für das initial gepinnte Zertifikat.

Tabelle 4.339 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau durch den Prüfgegenstand.	• Der Verbindungsaufbau ist erfolgreich.

Tabelle 4.340 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Trennen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.341 Ablaufbeschreibung

4.87 TC.CLS.TLSPROXY.MustCommunicateWithSmgwInPinningMode-ChainOfTrustClsAsServer

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, in Pairing Mode PKI mit einem SMGW, welches ein Zertifikat aus der SM-PKI präsentiert, zu kommunizieren.

Kurzbeschreibung

Es wird mit einem SMGW, welches ein GW_HAN_TLS_CRT aus der SM-PKI hat, das Root- und Sub-CA-Zertifikat der SM-PKI importiert und ein Verbindungsaufbau initiiert. Dieser muss erfolgreich sein.

Abgedeckte Anforderungen

- REQ.FA.ImportSmgwTrustAnchor.30
- REQ.FAKAT.SmgwAssociation.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.342 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-TLS-Port des aktuellen SMGW.
2	Starten eines virtuellen SMGW mit GW_HAN_TLS_CRT aus der SM-PKI.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.
4	Import des Root-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
5	Import des Sub-CA-Zertifikats der SM-PKI als Vertrauensanker über die Hersteller-API.
6	Deaktivieren des "Direct Trust" für das initial gepinnte Zertifikat.

Tabelle 4.343 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufbau einer Verbindung zum Prüfgegenstand.	• Der Verbindungsaufbau ist erfolgreich.

Tabelle 4.344 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Trennen der Verbindung zum Prüfgegenstand.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.345 Ablaufbeschreibung

4.88 TC.CLS.TLSPROXY.MustExchangeDataClsAsClient

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand dazu in der Lage ist, über das SMGW Daten mit einem EMT auszutauschen.

Kurzbeschreibung

Es wird ein Verbindungsaufbau abgewartet. Daraufhin werden Daten ausgetauscht, indem eine von der vom Hersteller des CLS-Geräts zu implementierende API abgerufene Nachricht an das CLS-Gerät gesendet wird.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.CLI.20
- REQ.HKS.TLSPROXY.CLI.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.346 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.

Tabelle 4.347 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.	• Innerhalb des Timeouts wird eine Antwort der API empfangen. • Der HTTP-Rückgabe-Code der Hersteller-API auf die Route zum Zertifikatspinning entspricht dem Code OK (200).
2	Warten auf den Verbindungsaufbau durch den Prüfgegenstand.	• Der TLS-Verbindungsaufbau ist erfolgreich.
3	Warten, ob Daten versendet werden.	• Es werden Daten versendet.

Tabelle 4.348 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Schließen der Verbindung zum Prüfgegenstand.
2	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.

Nr.	Beschreibung
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.349 Ablaufbeschreibung

4.89 TC.CLS.TLSPROXY.MustExchangeDataClsAsServer

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand dazu in der Lage ist, über das SMGW Daten mit einem EMT auszutauschen.

Kurzbeschreibung

Es wird ein Verbindungsaufbau initiiert. Daraufhin werden Daten ausgetauscht, indem eine von der vom Hersteller des CLS-Geräts zu implementierende API abgerufene Nachricht an das CLS-Gerät gesendet wird.

Abgedeckte Anforderungen

- REQ.HKS.TLSPROXY.SRV.20
- REQ.HKS.TLSPROXY.SRV.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.350 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Abholen der ersten Nachricht an das CLS-Gerät von der Hersteller-API.
2	Starten des Tracings auf dem HAN-Interface-Port.
3	Start eines virtuellen SMGW.

Tabelle 4.351 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.	• Innerhalb des Timeouts wird eine Antwort der API empfangen. • Der HTTP-Rückgabe-Code der Hersteller-API auf die Route zum Zertifikatspinning entspricht dem Code OK (200).

Nr.	Beschreibung	Erwartetes Ergebnis
2	Aufbau einer Verbindung zum Prüfgegenstand.	• Der TLS-Verbindungsaufbau ist erfolgreich.
3	Senden einer initialen Nachricht und warten, ob Daten versendet werden.	• Es werden Daten versendet.

Tabelle 4.352 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Schließen der Verbindung zum Prüfgegenstand.
2	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.353 Ablaufbeschreibung

4.90 TC.CLS.TLSPROXY.MustInitiateSocksConnection

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, mithilfe des SOCKS-Protokolls einen Kanal aufzubauen (HKS3).

Kurzbeschreibung

Es wird abgewartet, ob das CLS-Gerät einen Kanal mittels SOCKS aufbaut. Der Verbindungsaufbau muss erfolgreich sein.

Abgedeckte Anforderungen

- REQ.FA.ProxyRequestCh.20
- REQ.FAKAT.TlsProxy.10
- REQ.HKS.TLSPROXY.SOCKSCLI.20
- REQ.HKS.TLSPROXY.SOCKSCLI.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.354 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.

Tabelle 4.355 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau mittels SOCKS durch den Prüfgegenstand.	• Der TLS-Verbindungsaufbau ist erfolgreich.

Tabelle 4.356 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Schließen der Verbindung zum Prüfgegenstand.
2	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.357 Ablaufbeschreibung

4.91 TC.CLS.TLSPROXY.MustInitiateTlsSniConnection

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, mithilfe von TLS SNI einen Kanal aufzubauen (HKS3).

Kurzbeschreibung

Es wird abgewartet, ob das CLS-Gerät einen Kanal mittels TLS SNI aufbaut. Der Verbindungsaufbau muss erfolgreich sein.

Abgedeckte Anforderungen

- REQ.FA.ProxyRequestCh.20
- REQ.FAKAT.TlsProxy.10
- REQ.HKS.TLSPROXY.SOCKSCLI.20
- REQ.HKS.TLSPROXY.SOCKSCLI.30

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.358 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.

- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.

Tabelle 4.359 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Warten auf den Verbindungsaufbau mittels TLS SNI durch den Prüfgegenstand.	• Der TLS-Verbindungsaufbau ist erfolgreich. • Der Client sendet eine Server Name Extension. • Der in der Server Name Extension angegebene "name_type" ist "host_name". • Der in der Server Name Extension angegebene Hostname endet nicht auf einen Punkt.

Tabelle 4.360 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Schließen der Verbindung zum Prüfgegenstand.
2	Stoppen des virtuellen SMGW.
3	Stoppen des gestarteten Tracings.

Tabelle 4.361 Ablaufbeschreibung

4.92 TC.CLS.TLSPROXY.MustTerminateConnectionClsAsClient

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, einen bereits etablierten Kanal ordnungsgemäß zu schließen.

Kurzbeschreibung

Es wird ein Verbindungsaufbau abgewartet. Daraufhin wird der Kanal wieder geschlossen. Das Schließen des Kanals muss ordnungsgemäß erfolgen.

Abgedeckte Anforderungen

- REQ.FAKAT.TlsProxy.30
- REQ.TA.TLS.Close.30
- REQ.TA.TLS.Close.90

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.20

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.362 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.
4	Warten auf den Verbindungsaufbau durch den Prüfgegenstand.

Tabelle 4.363 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Beenden der Verbindung.	• Das CLS-Gerät beendet den Kanal ordnungsgemäß.

Tabelle 4.364 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Schließen der Verbindung zum Prüfgegenstand.
2	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
3	Stoppen des virtuellen SMGW.
4	Stoppen des gestarteten Tracings.

Tabelle 4.365 Ablaufbeschreibung

4.93 TC.CLS.TLSPROXY.MustTerminateConnectionClsAsServer

Version: 1.0.0

Zweck

Der Testfall prüft, ob der Prüfgegenstand in der Lage ist, einen bereits etablierten Kanal ordnungsgemäß zu schließen.

Kurzbeschreibung

Es wird ein Verbindungsaufbau initiiert. Daraufhin wird der Kanal wieder geschlossen. Das Schließen des Kanals muss ordnungsgemäß erfolgen.

Abgedeckte Anforderungen

- REQ.FAKAT.TlsProxy.40
- REQ.TA.TLS.Close.40
- REQ.TA.TLS.Close.80

Relevante Implementation-Conformance-Statements (ICS)

- ICS.IOP.HKS.TLSPROXY.10

Vorbedingungen

Status	Bedeutung
ClsDeviceIsUnpaired	Das CLS-Gerät hat noch nicht mit einem SMGW kommuniziert bzw. es wurde zurückgesetzt und hat seitdem nicht wieder mit einem SMGW kommuniziert.

Tabelle 4.366 Status

Testfallparameter

- CurrentActiveEmt: Der derzeit ausgewählte aktive Externe Marktteilnehmer.
- CurrentClsDevice: Das CLS-Gerät, das aktuell geprüft wird.
- CurrentManufacturerTool: Das aktuell gewählte Herstellertool.
- CurrentSMGW: Das aktuell genutzte SMGW-Objekt.

Vorbereitende Testschritte

Nr.	Beschreibung
1	Starten des Tracings auf dem HAN-Interface-Port.
2	Start eines virtuellen SMGW.
3	Aufruf des FA.PinSmgwCertificate über die Hersteller-API.
4	Aufbau einer Verbindung zum Prüfgegenstand.

Tabelle 4.367 Ablaufbeschreibung

Testschritte

Nr.	Beschreibung	Erwartetes Ergebnis
1	Beenden der Verbindung.	• Das CLS-Gerät beendet den Kanal ordnungsgemäß.

Tabelle 4.368 Ablaufbeschreibung

Nachbereitende Testschritte

Nr.	Beschreibung
1	Deaktivieren aller Zertifikate, die im Prüfgegenstand zur Validierung des GW_HAN_TLS_CRT verwendet werden.
2	Stoppen des virtuellen SMGW.
3	Stoppen des gestarteten Tracings.

Tabelle 4.369 Ablaufbeschreibung

Literaturverzeichnis

[CLS-Api] *Schnittstellbeschreibung für die proprietäre Auslösung von Fachanwendungsfällen.* https://cls-api.s-mtpf.io/ Bundesamt für Sicherheit in der Informationstechnik.

[DS] *Detailspezifikationen zur TR-03109-5 - Anforderungen an die Interoperabilität eines CLS-Kommunikationsadapters.* 2023. Bundesamt für Sicherheit in der Informationstechnik.

[TR-03109-1] *Technische Richtlinie TR-03109-1, v.1.1: Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems.* 2021. Bundesamt für Sicherheit in der Informationstechnik.

[TR-03109-3] *Technische Richtlinie BSI-TR-03109-3: Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen.* 2014. Bundesamt für Sicherheit in der Informationstechnik.

[TR-03109-5] *Technische Richtlinie BSI-TR-03109-5 Version 1.0, Kommunikationsadapter.* 2023. Bundesamt für Sicherheit in der Informationstechnik.

[TRZertWeb] *Allgemeine Informationen zu Zertifizierungen nach Technischen Richtlinien.* 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 Bundesamt für Sicherheit in der Informationstechnik.