関係各部署　御中 To departments concerned	Confidential level	PROTECTED 関係者外秘	原紙保管 Storage of original	M/Y　/
			コピー保管 Storage of copy	M/Y　/

無線通信セキュリティ評価仕様書 Test Specification of Wireless communication security	制御電子プラットフォーム開発部 制御ネットワーク・アーキ開発室 4G E/E Architecture Development Div System network & architecture development dept 4G			
	No. SEC-ePF-WLS-TST-SPEC-a00-02-a			
	承認 Approved 平林	調査 Checked 松井	作成 Created 玉樹	Oct. 31, 2022 Omission of signature (approved electronically)

適用先 **Target**	車載ネットワークに接続され、車外と無線通信を行う ECU。 ECUs that are connected to the in-vehicle network and communicate wirelessly with outside target of the vehicle.
特記 **Special note**	【展開ルール Distribution rule】 必要に応じて、関係会社・関係部署（海外事業体、ボデーメーカ、ECU サプライヤ）への展開をお願いします。 Please distribute this document to affiliated companies, or departments (e.g. overseas business entities, car body manufacturers, or ECU suppliers) if necessary. 【問合せ先　Contact Information】 制御電子プラットフォーム開発部　制御ネットワーク・アーキ開発室 セキュリティ仕様問合せ窓口 E/E Architecture Development Div　System network & architecture development dept Contact for security inquiries Mail:epf-sec-sp@mega.tec.toyota.co.jp

1. 変更履歴

Version	変更内容	日付	変更者
a00-00-a	新規作成	2022/02/03	46F 垣屋・清川
a00-01-a	誤記修正	2022/05/23	46F 清川
	通信における大量のメッセージについて明確化(WLSTST_00001)	2022/06/09	46F 安江
	3.1. 要求仕様書と評価仕様書のトレースの誤り修正		
	証明書検証の明確化(WLSTST_04003, WLSTST_04012, WLSTST_04018, WLSTST_04025)		
a00-02-a	ファイアウォールに関する評価の明確化(WLSTST_02001)	2022/08/04	46F 玉樹
	表紙のフォーマット変更		

目次

2. はじめに

2.1. 本書の目的

車外との無線通信時、通信内容の盗聴や改ざん、および、なりすましを防ぐため、通信路の保護、相互認証を行う。

本書では上位文書[1]で定義された通信路の保護、相互認証の要件に関する評価要件を定義する。

2.2. 適用範囲

本書の適用範囲は、車外と直接無線通信を行う全ての ECU、及び TLS 終端となる全ての ECU である。

2.3. 前提条件

特になし。

2.4. 要求事項の記載

【WLSTST_*****】と記載されている部分が本書で要求する仕様とする。ただし、（補足）と記載されているものは補足事項のため要求仕様ではない。

2.5. 上位文書

上位文書を表 2.1 に示す。

表 2.1. 上位文書一覧

No.	文書名	Ver.	主管
1	無線通信セキュリティ要求仕様書	SEC-ePF-WLS-REQ-SPEC-a00-08-*	46F

2.6. 関連文書

関連文書を表 2.2 に示す。

表 2.2. 関連文書一覧

No	文書名	Ver(最新版を適用ください)	主管
1	車両サイバーセキュリティ及びプライバシー用語定義書	SEC-ePF-TRM-GUD-PROC-***-**-*	46F
2	共通脆弱性対策要求仕様書	SEC-ePF-VUL-CMN-REQ-SPEC-***-**-*	46F
3	ECU 脆弱性対策評価仕様書	SEC-ePF-VUL-ECU-TST-SPEC-***-**-*	46F

3. 評価概要

3.1. 要求仕様書と評価仕様書のトレース

本節では、上位文書[1]の要求 ID と本書規定の評価 ID との関連を示す。

DoS 対策に関する一覧を表 3.1、Firewall に関する一覧を表 3.2、センタと接続する場合の認証・暗号化・改ざん検知に関する一覧を表 3.3、センタ以外の車外機器と接続する場合の認証・暗号化・改ざん検知に関する一覧を表 3.4 に示す。

表 3.1. 要求仕様と評価仕様のトレーサビリティ確認表（DoS 対策）

要求仕様書		評価仕様書		
分類	ID	ID	評価項目がない理由	生産時機能
共通	WLSREQ_00100	－	要求が欠番のため	－
	WLSREQ_00110	－	要求が欠番のため	－
	WLSREQ_00120	WLSTST_00001	－	－
	WLSREQ_00130	WLSTST_00001	－	－

表 3.2. 要求仕様と評価仕様のトレーサビリティ確認表（ファイアウォール）

要求仕様書		評価仕様書		
分類	ID	ID	評価項目がない理由	生産時機能
IP 通信以外	WLSREQ_00200	WLSTST_01001	－	－
IP 通信	WLSREQ_00201	WLSTST_02001	－	－
	WLSREQ_00202	WLSTST_02002	－	－
	WLSREQ_00203	WLSTST_02003	－	－
	WLSREQ_00204	－	要求が欠番のため	－
	WLSREQ_00205	WLSTST_02004	－	－
	WLSREQ_00206	WLSTST_02005	－	－
	WLSREQ_00207	WLSTST_02006	－	－
	WLSREQ_00208	WLSTST_02007	－	－
	WLSREQ_00209	WLSTST_02008	－	－
	WLSREQ_00210	WLSTST_02009	－	－

表 3.3. 要求仕様と評価仕様のトレーサビリティ確認表（センタと接続する場合の認証・暗号化・改ざん検知）

要求仕様書		評価仕様書		
分類	ID	ID	評価項目がない理由	生産時機能
TLS 以外	WLSREQ_00400	WLSTST_03001	－	－
		WLSTST_03007	－	－
	WLSREQ_00580	WLSTST_03002	－	－
		WLSTST_03008	－	－
	WLSREQ_00410	WLSTST_03003	－	－
	WLSREQ_00590	WLSTST_03004	－	－
		WLSTST_03009	－	－
	WLSREQ_00420	WLSTST_03005	－	－
		WLSTST_03010	－	－
	WLSREQ_00600	WLSTST_03006	－	－
		WLSTST_03011	－	－
	WLSREQ_00610	WLSTST_03005	－	－
		WLSTST_03010	－	－
TLS	WLSREQ_00121	WLSTST_04001	－	－
		WLSTST_04014	－	－
	WLSREQ_00122	WLSTST_04002	－	－
		WLSTST_04015	－	－
	WLSREQ_00401	WLSTST_04003	－	－
		WLSTST_04016	－	－
	WLSREQ_00402	WLSTST_04004	－	－
		WLSTST_04017	－	－
	WLSREQ_00411	WLSTST_04005	－	－
		WLSTST_04018	－	－
	WLSREQ_00430	WLSTST_04006	－	－
	WLSREQ_00431	WLSTST_04019	－	－
	WLSREQ_00440	WLSTST_04007	－	－
	WLSREQ_00441	WLSTST_04020	－	－
	WLSREQ_00450	WLSTST_04008	－	－
		WLSTST_04021	－	－
	WLSREQ_00460	WLSTST_04009	－	－
		WLSTST_04022	－	－
	WLSREQ_00470	WLSTST_04010	－	－

要求仕様書		評価仕様書		
分類	ID	ID	評価項目がない理由	生産時機能
		WLSTST_04023	ー	ー
	WLSREQ_00480	―	運用に関する要求のため	―
	WLSREQ_00490	―	車両開発後の要求のため	―
	WLSREQ_00500	WLSTST_04011	ー	ー
		WLSTST_04024	ー	ー
	WLSREQ_00510	ー	要求が欠番のため	ー
	WLSREQ_00520	WLSTST_04011	ー	ー
		WLSTST_04024	ー	ー
	WLSREQ_00530	WLSTST_04026	ー	ー
	WLSREQ_00540	WLSTST_04012	ー	ー
	WLSREQ_00550	WLSTST_04025	ー	ー
	WLSREQ_00560	WLSTST_04005	ー	ー
		WLSTST_04018	ー	ー
	WLSREQ_00611	WLSTST_04013	ー	ー
		WLSTST_04027	ー	ー

表 3.4. 要求仕様と評価仕様のトレーサビリティ確認表（センタ以外の車外機器と接続する場合の認証・暗号化・改ざん検知）

要求仕様書		評価仕様書		
分類	ID	ID	評価項目がない理由	生産時機能
Wi-Fi/ Bluetooth 以外	WLSREQ_00300	WLSTST_05001	－	－
		WLSTST_05003	－	－
	WLSREQ_00350	－	車両開発後の要求のため	－
	WLSREQ_00360	－	車両開発後の要求のため	－
	WLSREQ_00310	WLSTST_05002	－	－
		WLSTST_05004	－	－
	WLSREQ_00370	WLSTST_05002	－	－
		WLSTST_05004	－	－
Wi-Fi	WLSREQ_00311	WLSTST_06001	－	－
		WLSTST_06003	－	－
	WLSREQ_00312	WLSTST_06001	－	－
		WLSTST_06003	－	－
	WLSREQ_00313	WLSTST_06001	－	－
		WLSTST_06003	－	－
	WLSREQ_00314	－	車両開発後の要求のため	－
	WLSREQ_00317	WLSTST_06004	－	－
	WLSREQ_00318	－	車両開発後の要求のため	－
	WLSREQ_00315	－	車両開発後の要求のため	－
	WLSREQ_00371	WLSTST_06002	－	－
		WLSTST_06005	－	－
Bluetooth	WLSREQ_00316	WLSTST_07001	－	－
		WLSTST_07004	－	－
	WLSREQ_00319	WLSTST_07002	－	－
		WLSTST_07005	－	－
	WLSREQ_00320	WLSTST_07005	－	－
	WLSREQ_00372	WLSTST_07003	－	－
		WLSTST_07006	－	－

上記評価項目の合格条件を全て満たす場合のみ合格とする。

3.2. 評価項目一覧

評価項目の一覧を以下に示す。

DoS 対策に関する一覧を表 3.5、Firewall に関する一覧を表 3.6、認証・暗号化・改ざん検知のうち、センタに関する一覧を表 3.7、センタ以外に関する一覧を表 3.8 に示す。

表 3.5 評価項目一覧（DoS 対策）

分類	試験番号	試験項目	適用対象	
			サーバ	クライアント
共通	WLSTST_00001	大量メッセージ受信時の DoS 対策	○	○

表 3.6 評価項目一覧（ファイアウォール）

分類	試験番号	試験項目	適用対象	
			サーバ	クライアント
IP 通信以外	WLSTST_01001	不要な通信の遮断	○	○
IP 通信	WLSTST_02001	不要な TCP/UDP 通信の遮断	○	○
	WLSTST_02002	TCP 通信規則評価	○	○
	WLSTST_02003	車両外からの TCP 接続要求の遮断	－	○
	WLSTST_02004	不正な TCP 接続要求による DoS 対策（TCP タイムアウトの最小化）	○	－
	WLSTST_02005	不正な TCP 接続要求による DoS 対策（ハーフオープン状態の管理）	○	－
	WLSTST_02006	不要な ICMP リクエストの遮断	○	○
	WLSTST_02007	TCP/UDP ポートの受信パケット数制限	○	○
	WLSTST_02008	同一 IP アドレスの同時接続数制限	○	－
	WLSTST_02009	不要なブロードキャストアドレスの遮断	○	○

表 3.7 評価項目一覧（認証・暗号化・改ざん検知、センタ）

分類	試験番号	試験項目	適用対象	
			サーバ	クライアント
TLS 以外	WLSTST_03001	サーバ認証	－	○
	WLSTST_03002	セッションハイジャック対策	－	○
	WLSTST_03003	クライアント認証	－	○
	WLSTST_03004	クライアント認証鍵の更新・切替	－	○

	WLSTST_03005	通信の暗号化と改ざん検知	－	○
	WLSTST_03006	通信経路暗号化用の暗号鍵の更新	－	○
	WLSTST_03007	接続相手の認証	○	－
	WLSTST_03008	セッションハイジャック対策	○	－
	WLSTST_03009	クライアント認証鍵の更新・切替	○	－
	WLSTST_03010	通信の暗号化と改ざん検知	○	－
	WLSTST_03011	通信経路暗号化用の暗号鍵の更新	○	－
TLS	WLSTST_04001	TLS 圧縮機能の無効化	－	○
	WLSTST_04002	TLS 再ネゴシエーション機能の無効化	－	○
	WLSTST_04003	サーバ認証（TLS1.2 以降）	－	○
	WLSTST_04004	サーバ認証（TLS1.1 以前）の無効化	－	○
	WLSTST_04005	クライアント認証（TLS1.2 以降）	－	○
	WLSTST_04006	サーバ認証の演算処理保護	－	○
	WLSTST_04007	クライアント認証の演算処理保護	－	○
	WLSTST_04008	公開鍵の保護	－	○
	WLSTST_04009	クライアント認証用の秘密鍵の保護	－	○
	WLSTST_04010	秘密鍵の外部メモリへの暗号化保存	－	○
	WLSTST_04011	ルート証明書の切替	－	○
	WLSTST_04012	サーバ証明書の失効確認	－	○
	WLSTST_04013	通信の改ざん検知（TLS1.2 以降）	－	○
	WLSTST_04014	TLS 圧縮機能の無効化	○	－
	WLSTST_04015	TLS 再ネゴシエーション機能の無効化	○	－
	WLSTST_04016	サーバ認証（TLS1.2 以降）	○	－
	WLSTST_04017	サーバ認証（TLS1.1 以前）の無効化	○	－
	WLSTST_04018	クライアント認証（TLS1.2 以降）	○	－
	WLSTST_04019	サーバ認証の演算処理保護	○	－
	WLSTST_04020	クライアント認証の演算処理保護	○	－
	WLSTST_04021	公開鍵の保護	○	－
	WLSTST_04022	クライアント認証用の秘密鍵の保護	○	－
	WLSTST_04023	秘密鍵の外部メモリへの暗号化保存	○	－
	WLSTST_04024	ルート証明書の切替	○	－
	WLSTST_04025	クライアント証明書の失効確認	○	－
	WLSTST_04026	サーバ証明書の発行	○	－
	WLSTST_04027	通信の改ざん検知（TLS1.2 以降）	○	－

表 3.8　評価項目一覧（認証・暗号化・改ざん検知、センタ以外）

分類	試験番号	試験項目	適用対象	
			サーバ	クライアント
Wi-Fi/ BT 以外	WLSTST_05001	車外機器認証	－	○
	WLSTST_05002	通信の暗号化と改ざん検知	－	○
	WLSTST_05003	車外機器認証	○	－
	WLSTST_05004	通信の暗号化と改ざん検知	○	－
Wi-Fi	WLSTST_06001	WPA2 以降の使用	－	○
	WLSTST_06002	IEEE802.11w のサポート	－	○
	WLSTST_06003	通信の改ざん検知（Wi-Fi）	－	○
	WLSTST_06004	WPA2 以降の使用	○	－
	WLSTST_06005	IEEE802.11w のサポート	○	－
	WLSTST_06006	WPA-PSK の認証情報の変更	○	－
	WLSTST_06007	通信の改ざん検知（Wi-Fi）	○	－
BT	WLSTST_07001	Bluetooth 実装ガイド	－	○
	WLSTST_07002	Bluetooth 認証方式	－	○
	WLSTST_07003	通信の改ざん検知（Bluetooth）	－	○
	WLSTST_07005	Bluetooth 実装ガイド	○	－
	WLSTST_07006	Bluetooth 認証方式	○	－
	WLSTST_07007	通信の改ざん検知（Bluetooth）	○	－

4. 評価環境

評価環境を図 4.1 に示す。

・ECU は、本評価の評価対象

・テスタは、ECU と無線通信を行う車外機器を模擬するツールを想定

・RAM モニタは、デバッガ装置を想定

図 4.1. 評価環境

5. 評価詳細

5.1. DoS 攻撃対策に関する評価

【WLSTST_00001】 大量メッセージ受信時の DoS 対策	
試験内容	車外から大量メッセージを受信したとき、上位文書[1]の【WLSREQ_00120】に従い特定したそれぞれの機能の処理性能を維持できることを確認する
事前条件	なし
試験手順	(1) テスタから以下に示す通信を ECU に送信する A) 実効スループットを実現する通信 B) 通信機能に割り当てられた ECU のリソース上限を消費する通信 (2)上位文書[1]の【WLSREQ_00120】で特定したそれぞれの機能の処理性能が維持できていることを確認できる適切な手順を ECU 設計部署にて検討する
測定項目	(a)試験手順(2)に依る
合否判定	・測定項目(a)で、上位文書[1]の【WLSREQ_00120】で特定したそれぞれの機能の処理性能が維持できていること
備考	―

5.2. ファイアウォールに関する評価

5.2.1. IP 通信以外を使用する場合の評価

【WLSTST_01001】 不要な通信の遮断	
試験項目	車外との通信は許可する通信のみを通信可能とし、不要な通信を遮断することを確認する
事前条件	ECU 設計部署が許可する通信を定義している
試験手順	(1)許可された通信をテスタから送信する (2)RAM モニタにて試験手順(1)に対する ECU の受信結果を確認する (3)許可された通信以外をテスタから送信する (4)RAM モニタにて試験手順(3)に対する ECU の受信結果を確認する
測定項目	(a) 試験手順(2)の受信結果 (b) 試験手順(4)の受信結果
合否判定	・測定項目(a)で、通信が受信されていること ・測定項目(b)で、通信が受信されていないこと
備考	―

5.2.2. IP 通信を用いる場合の評価

【WLSTST_02001】 不要な TCP/UDP 通信の遮断	
試験項目	サービス開始時・コネクション確立時に使用する TCP/UDP ポートを開き、サービス終了時・コネクション終了時に閉じていることを確認する
事前条件	ECU 設計部署が通信を許可する TCP/UDP ポートを定義している
試験手順	<使用する TCP/UDP ポートがシステムポートもしくはユーザポートの場合> (1)テスタは ECU に対し、関連文書[3]の VULETS_01001 を実施する (2)テスタは、ECU とのコネクションを確立する (3)テスタは、ECU とのコネクションを終了する (4)テスタは ECU に対し、関連文書[3]の VULETS_01001 を実施する <使用する TCP/UDP ポートがダイナミックポートの場合> (5)テスタは ECU に対し、関連文書[3]の VULETS_01001 を実施する (6)ECU は、テスタとのコネクションを確立する

	(7) テスタは ECU に対し、関連文書[3]の VULETS_01001 を実施する (8)ECU は、テスタとのコネクションを終了する (9)テスタは ECU に対し、関連文書[3]の VULETS_01001 を実施する
測定項目	<使用する TCP/UDP ポートがシステムポートもしくはユーザポートの場合> (a)試験手順(1)の実施結果 (b)試験手順(4)の実施結果 <使用する TCP/UDP ポートがダイナミックポートの場合> (c)試験手順(5)の実施結果 (d)試験手順(6)(8)の通信ログ (e)試験手順(7)の実施結果 (f)試験手順(9)の実施結果
合否判定	<使用する TCP/UDP ポートがシステムポートもしくはユーザポートの場合> ・測定項目(a)で不要なポートは閉じていること ・測定項目(b)が測定項目(a)と一致すること <使用する TCP/UDP ポートがダイナミックポートの場合> ・測定項目(c)で不要なポートは閉じていること ・測定項目(d)で、測定項目(c)に含まれないポートが ECU の送信元ポートとなっていること ・測定項目(e)で、測定項目(c)および測定項目(d)で確認したポート以外のポートは閉じていること ・測定項目(f)が測定項目(c)と一致すること
備考	・システムポート、ユーザポートは静的に割り当てられる TCP/UDP ポート ・ダイナミックポートは動的に割り当てられる TCP/UDP ポート

【WLSTST_02002】TCP 通信規則評価	
試験項目	・確立中コネクションに関連するパケットのうち、TCP 通信規則に準拠したパケットのみが許可されていることを確認する。 ・確立中コネクションに関するパケットのうち TCP 通信規則に従わないパケットを遮断し、そのコネクションを切断することを確認する
事前条件	なし
試験手順	(1)ECU はテスタとの TCP コネクションを確立する (2)テスタから ECU に対して、TCP 通信規則に準拠したパケットを受信させる (3)テスタで ECU からの通信を取得する (4)テスタから ECU に対して、TCP 通信規則に従わないパケットを受信させる (5)RAM モニタにて(4)に対する ECU の受信結果を確認する (6)テスタを用いて試験手順(1)にて確立した TCP コネクションに TCP 通信規則準拠したパケットを送信する (7)テスタで ECU からの通信を取得する
測定項目	(a)試験手順(3)の通信ログ (b)試験手順(5)の受信結果 (c)試験手順(7)の通信ログ
合否判定	・測定項目(a)に試験手順(2)で送信したパケットの確認応答が含まれていること ・測定項目(b)でパケットが受理されていないこと ・測定項目(c)に試験手順(6)で送信したパケットの確認応答が含まれていないこと
備考	―

【WLSTST_02003】 車両外からの TCP 接続要求の遮断	
試験項目	TCP 通信のサーバ機能を持たない場合、車両外からの TCP 接続要求を棄却することを確認する
事前条件	なし
試験手順	(1)テスタを用いて TCP 接続要求を送信する (2)テスタで ECU からの通信を取得する
測定項目	(a)試験手順(2)の通信ログ
合否判定	・測定項目(a)で、TCP 接続要求に対する ECU の確認応答が含まれていないこと
備考	TCP 通信のサーバ機能を持つ場合、本評価項目は対象外

【WLSTST_02004】不正な TCP 接続要求による DoS 対策（TCP タイムアウトの最小化）	
試験項目	ECU は通信品質を満足する範囲内で TCP タイムアウト時間を最小化していることを確認する
事前条件	なし
試験手順	(1)ECU が通信品質を満足する範囲内で TCP タイムアウト時間を最小化していることを確認できる適切な手順を ECU 設計部署にて検討する。
測定項目	(a)試験手順(1)に依る
合否判定	・測定項目(a)で、TCP タイムアウト時間が通信品質を満足する範囲で最小化できていること
備考	—

【WLSTST_02005】不正な TCP 接続要求による DoS 対策（ハーフオーブン状態の管理）	
試験項目	ハーフオープン状態（TCP 接続要求に対する ACK 応答待ち）の TCP コネクションのデータでリソースが枯渇しないことを確認する
事前条件	なし
試験手順	(1)テスタを用いて SYN パケットを大量に ECU に受信させる “大量”については、上位文書[1]の【WLSREQ_00120】参照 (2)テスタは ECU から受信する SYN/ACK パケットを無視する (3)ECU のリソースが枯渇していないことを確認できる適切な手順を ECU 設計部署にて検討する。
測定項目	(a)試験手順(3)に依る
合否判定	・試験手順(a)で ECU のリソースが枯渇していないこと
備考	—

【WLSTST_02006】不要な ICMP リクエストの遮断	
試験項目	全ての ICMP パケットを遮断することを確認する もしできない場合は、タイプコード毎に許可するパケットのみ受信し、少なくとも ICMP エコーリクエストは遮断することを確認する。
事前条件	タイプコード毎に許可するパケットのみを受信する場合、ECU 設計部署が通信を許可するタイプコードを定義している
試験手順	<すべての ICMP パケットを遮断する場合> (1)テスタを用いて全てのタイプコードの ICMP パケットを ECU に受信させる (2)RAM モニタを用いて試験手順(1) に対する ECU の受信結果を確認する

	<タイプコード毎に許可するパケットのみを受信する場合> (3)テスタを用いて ICMP エコーリクエストを ECU に受信させる (4)RAM モニタを用いて試験手順(3) に対する ECU の受信結果を確認する (5)テスタを用いて許可されていない全てのタイプコードの ICMP パケットを ECU に受信させる (6)RAM モニタを用いて試験手順(5) に対する ECU の受信結果を確認する
測定項目	(a) 試験手順(2)の受信結果 (b) 試験手順(4)の受信結果 (c) 試験手順(6)の受信結果
合否判定	・測定項目(a)ですべてのパケットが受理されていないこと ・測定項目(b)でパケットが受理されていないこと ・測定項目(c)ですべてのパケットが受理されていないこと
備考	—

【WLSTST_02007】TCP/UDP ポートの受信パケット数制限	
試験項目	ECU は単位時間当たりに許可する受信パケット数を定義し、その値を超過したパケットを受信した場合に、超過分のパケットを破棄することを確認する
事前条件	ECU 設計部署が単位時間当たりに許可する受信パケット数を定義している
試験手順	試験手順(1)～(3)を開けている TCP/UDP ポートすべてに対して実施する (1)テスタを用いて単位時間内に、許可されたパケット数と、さらに追加の 1 パケットを ECU に受信させる (2)RAM モニタを用いて試験手順(1)に対する ECU の受信結果を確認する (3)テスタで ECU からの通信を取得する(TCP のみ)
測定項目	(a)試験手順(2)の受信結果 (b)試験手順(3)の通信ログ
合否判定	・測定項目(a)でパケットが破棄されていること ・測定項目(b)に試験手順(1)で送信したパケットの確認応答が含まれていないこと
備考	—

【WLSTST_02008】同一 IP アドレスの同時接続数制限	
試験項目	車両外から TCP コネクションが確立されるポートがある場合、同じ IP アドレスからの同時コネクション数を制限することを確認する
事前条件	ECU 設計部署が同じ IP アドレスからの同時 TCP コネクション数を定義している
試験手順	車両外から TCP コネクションが確立されるポートが複数ある場合すべてのポートに対して、試験手順(1)～(3)を実施する

	(1)テスタは同一の IP アドレスから最大数の TCP コネクションを ECU と確立する (2)テスタを用いて TCP 接続要求を試験手順(1)と同一の IP アドレスで送信する (3)テスタで ECU からの通信を取得する
測定項目	(a) 試験手順(3)の通信ログ
合否判定	・測定項目(a)で、試験手順(2)の TCP 接続要求に対する ECU の確認応答が含まれていないこと
備考	—

【WLSTST_02009】不要なブロードキャストアドレスの遮断	
試験項目	宛先が不要なブロードキャストアドレスのパケットを破棄することを確認する
事前条件	ECU 設計部署がブロードキャストアドレス宛の通信を許可する TCP/UDP ポートを定義している
試験手順	<ブロードキャストアドレス宛の通信を受信可能な TCP/UDP ポートがない場合> (1)テスタを用いて開けている TCP/UDP ポートにブロードキャストアドレス宛のパケットを送信する (2)RAM モニタを用いて試験手順(1)に対する ECU の受信結果を確認する (3)テスタで ECU からの通信を取得する(TCP のみ) <ブロードキャストアドレス宛の通信を受信可能な TCP/UDP ポートがある場合> (4)テスタを用いて開けている TCP/UDP ポートのうち、ブロードキャストアドレス宛の通信を許可する TCP/UDP ポート以外に、ブロードキャストアドレス宛のパケットを送信する (5)RAM モニタを用いて試験手順(4)に対する ECU の受信結果を確認する (6)テスタで ECU からの通信を取得する(TCP のみ)
測定項目	(a)試験手順(2)の受信結果 (b)試験手順(3)の通信ログ (c)試験手順(5)の受信結果 (d)試験手順(6)の通信ログ
合否判定	・測定項目(a)でパケットが破棄されていること ・測定項目(b)に試験手順(1)で送信したパケットの確認応答が含まれていないこと ・測定項目(c)でパケットが破棄されていること ・測定項目(d)に試験手順(4)で送信したパケットの確認応答が含まれていないこと
備考	—

5.3. 認証、暗号化、改ざん検知に関する評価

5.3.1. センタと接続する場合の評価

5.3.1.1. TLS 以外を用いる場合の評価

5.3.1.1.1. クライアントの評価

【WLSTST_03001】サーバ認証	
試験項目	・接続相手を認証していることを確認する ・認証が失敗した場合、認証相手に応答しないことを確認する
事前条件	なし
試験手順	＜接続相手が正規＞ ⑴ECU は、テスタに対して無線接続を要求する ⑵テスタは、正しい認証情報を用いて、ECU との認証を実施する ⑶試験手順⑵ で ECU がテスタを認証した結果を確認できる適切な手順を ECU 設計部署にて検討する ＜接続相手が不正＞ ⑷ECU は、テスタに対して無線接続を要求する ⑸テスタは、誤った認証情報を用いて、ECU との認証を実施する ⑹テスタで ECU からの通信を取得する ⑺試験手順⑸で ECU がテスタを認証した結果を確認できる適切な手順を ECU 設計部署にて検討する
測定項目	⑷試験手順⑶の ECU の認証結果 ⑹試験手順⑹の通信ログ ⑹試験手順⑺の ECU の認証結果
合否判定	・測定項目⑷が成功 ・測定項目⑹にテスタへの応答が含まれていないこと ・測定項目⑹が失敗
備考	―

【WLSTST_03002】セッションハイジャック対策	
試験項目	攻撃者によるセッション乗っ取り対策を実施していることを確認する
事前条件	なし
試験手順	(1)セッション乗っ取り対策を確認できる適切な手順を ECU 設計部署で検討する。 ただし、実動作での確認が難しい場合は設計仕様の確認でも可とする
測定項目	(a)試験手順(1)に依る
合否判定	・測定項目(a)でセッション乗っ取り対策が実施されている
備考	—

【WLSTST_03003】クライアント認証	
試験項目	センターサービスの不正利用防止を目的としたクライアント認証のための処理をサーバ接続時に行うことを確認する
事前条件	なし
試験手順	(1)ECU は、テスタに対して無線接続を要求する (2)テスタは、ECU とのクライアント認証を実施する (3)テスタは、ECU との通信を取得する
測定項目	(a)試験手順(3)の通信ログ
合否判定	・測定項目(a)のクライアント認証が ECU 設計部署で採用した認証仕様に準拠している
備考	—

【WLSTST_03004】クライアント認証鍵（対称鍵）の更新・切替	
試験項目	クライアント認証に対称鍵を使用する場合、機密性と完全性を担保して対称鍵を更新、または切替できることを確認する
事前条件	なし
試験手順	(1)クライアント認証鍵の更新、または切替処理を確認できる適切な手順を ECU 設計部署で検討する
測定項目	(a)試験手順(1)に依る
合否判定	・測定項目(a)でクライアント認証鍵の機密性と完全性が担保されている
備考	—

【WLSTST_03005】通信の暗号化と改ざん検知	
試験項目	・車外のセンタやサービスへの接続時は通信路の暗号化と改ざん検知を行うことを確認する ・センタから受信したメッセージの改ざんを検知した場合、当該メッセージを破棄していることを確認する
事前条件	なし
試験手順	＜通信路の暗号化と改ざん検知＞ ⑴ECU は、テスタとの認証を完了させる ⑵ECU からテスタに対しメッセージを送信させ、テスタは ECU との通信を取得する ⑶テスタは、ECU 設計部署で採用した暗号・改ざん検知アルゴリズムを適用したメッセージを ECU に送信する ⑷RAM モニタで ECU のメッセージ受信結果を確認する ＜メッセージの改ざん検知の確認＞ ⑸テスタは、改ざんしたメッセージ（例：メッセージ認証子を誤った値に変更）を ECU に送信する ⑹RAM モニタで ECU のメッセージ受信結果を確認する
測定項目	⒜試験手順⑵でテスタが受信したメッセージ ⒝試験手順⑷の ECU のメッセージ受信結果 ⒞試験手順⑹の ECU のメッセージ受信結果
合否判定	・測定項目⒜で ECU からテスタへのメッセージが ECU 設計部署で採用した暗号・改ざん検知アルゴリズムに準拠している ・測定項目⒝が受信成功 ・測定項目⒞で改ざんされたメッセージを破棄している
備考	―

【WLSTST_03006】通信経路暗号化用の暗号鍵の更新	
試験項目	通信経路の暗号化に使用する暗号鍵は、機密性と完全性を確保して更新できることを確認する
事前条件	なし
試験手順	(1)通信経路の暗号化に使用する暗号鍵が機密性と完全性を確保して更新できることを確認できる適切な手順を ECU 設計部署で検討する
測定項目	(a)試験手順(1)に依る
合否判定	・測定項目(a)で暗号鍵の機密性と完全性が確保されている
備考	―

5.3.1.1.2. サーバの評価

【WLSTST_03007】接続相手の認証	
試験項目	・接続相手を認証していることを確認する ・認証が失敗した場合、認証相手に応答しないことを確認する
事前条件	なし
試験手順	＜接続相手が正規＞ ⑴テスタは、正しい認証情報を用いて、ECU に対し認証を要求する ⑵RAM モニタで、ECU がテスタを認証した結果を確認する ＜接続相手が不正＞ ⑶テスタは、誤った認証情報を用いて、ECU に対し認証を要求する ⑷テスタは、ECU との通信を取得する ⑸RAM モニタで、ECU がテスタを認証した結果を確認する
測定項目	⑷試験手順⑵の ECU の認証結果 ⑹試験手順⑷の通信ログ ⑽試験手順⑸の ECU の認証結果
合否判定	・測定項目⑷が成功 ・測定項目⑹でテスタへの応答が含まれていない ・測定項目⑽が失敗
備考	―

【WLSTST_03008】セッションハイジャック対策	
試験項目	攻撃者によるセッション乗っ取り対策を実施していることを確認する
事前条件	なし
試験手順	(1)セッション乗っ取り対策を確認できる適切な手順を ECU 設計部署で検討する。
測定項目	(a)試験手順(1)に依る
合否判定	・測定項目(a)でセッション乗っ取り対策が実施されている
備考	―

【WLSTST_03009】クライアント認証鍵（対称鍵）の更新・切替	
試験項目	クライアント認証に対称鍵を使用する場合、機密性と完全性を担保して対称鍵を更新、または切替できることを確認する
事前条件	なし
試験手順	(1)クライアント認証鍵の更新、または切替処理を確認できる適切な手順を ECU 設計部署で検討する
測定項目	(a)試験手順(1)に依る
合否判定	・測定項目(a)がクライアント認証鍵の機密性と完全性が担保されている
備考	―

【WLSTST_03010】通信の暗号化と改ざん検知	
試験項目	・車外のセンタやサービスへの接続時は通信路の暗号化と改ざん検知を行うことを確認する ・センタから受信したメッセージの改ざんを検知した場合、当該メッセージを破棄していることを確認する
事前条件	なし
試験手順	＜通信路の暗号化と改ざん検知＞ (1)テスタは、ECU との無線通信を確立させる (2)ECU からテスタに対しメッセージを送信させ、テスタは ECU との通信を取得する (3)テスタは、ECU 設計部署で採用した暗号・改ざん検知アルゴリズムを適用したメッセージを ECU に送信する (4)RAM モニタで ECU のメッセージ受信結果を確認する

	＜メッセージの改ざん検知＞ ⑸テスタは、改ざんしたメッセージ（例：メッセージ認証子を誤った値に変更）を ECU に送信する ⑹RAM モニタで ECU のメッセージ受信結果を確認する
測定項目	⒜試験手順⑵ でテスタが受信したメッセージ ⒝試験手順⑷の ECU のメッセージ受信結果 ⒞試験手順⑹の ECU のメッセージ受信結果
合否判定	・測定項目⒜が ECU 設計部署で採用した暗号・改ざん検知アルゴリズムに準拠している ・測定項目⒝が受信成功 ・測定項目⒞で、改ざんしたメッセージを破棄している
備考	―

【WLSTST_03011】通信経路暗号化用の暗号鍵の更新	
試験項目	通信経路の暗号化に使用する暗号鍵は、機密性と完全性を確保して更新できることを確認する
事前条件	なし
試験手順	⑴通信経路の暗号化に使用する暗号鍵が機密性と完全性を確保して更新できることを確認できる適切な手順を ECU 設計部署で検討する
測定項目	⒜試験手順⑴に依る
合否判定	・測定項目⒜で暗号鍵の機密性と完全性が確保されている
備考	―

5.3.1.2.TLS を用いる場合の評価

5.3.1.2.1. クライアントの評価

【WLSTST_04001】 TLS 圧縮機能の無効化	
試験項目	TLS 圧縮機能を無効化していることを確認する
事前条件	なし
試験手順	(1)ECU は、テスタに対し TLS ハンドシェイクを要求する (2)テスタは、TLS ハンドシェイクの中で ECU に対し TLS 圧縮機能を要求する (3)RAM モニタで、ECU の TLS ハンドシェイク結果を確認する
測定項目	(a)試験手順(3)の ECU の TLS ハンドシェイク結果
合否判定	・測定項目(a)の TLS ハンドシェイク失敗
備考	―

【WLSTST_04002】 TLS 再ネゴシエーション機能の無効化	
試験項目	TLS 再ネゴシエーション機能を無効化していることを確認する
事前条件	・【WLSTST_04003】の評価が終了していること
試験手順	(1)ECU は、テスタとの TLS セッションを確立する (2)テスタは、ECU に対して、TLS 再ネゴシエーション要求を送信する (3)テスタは ECU との通信を取得する
測定項目	(a)試験手順(3)の ECU からの TLS 再ネゴシエーション要求に対する応答
合否判定	・測定項目(a)で TLS 再ネゴシエーション要求を棄却している
備考	―

【WLSTST_04003】サーバ認証（TLS1.2 以降）	
試験項目	・サーバ認証は TLS 標準（バージョン 1.2 以降）のシーケンスに従っていることを確認し、センタと接続することを確認する ・中間 CA を想定した多階層のサーバ認証に対応していることを確認する
事前条件	なし
試験手順	＜接続相手が不正＞ ⑴ECU は、テスタに対し、TLS ハンドシェイクを要求する ⑵テスタは、ECU に誤ったルート証明書をルートとするサーバ証明書と中間証明書を送信する ⑶RAM モニタで ECU のサーバ認証結果を確認する ＜有効期限が切れたサーバ証明書＞ ⑷ECU は、テスタに対し、TLS ハンドシェイクを要求する ⑸テスタは、ECU に対して有効期限が切れたサーバ証明書を送信する ⑹RAM モニタで、ECU のサーバ認証結果を確認する ＜接続相手が正規＞ ⑺ECU は、テスタに対し、TLS ハンドシェイクを要求する ⑻テスタは、ECU に正しいルート証明書をルートとするサーバ証明書と中間証明書を応答する ⑼RAM モニタで ECU のサーバ認証結果を確認する
測定項目	⑷試験手順⑶のサーバ認証結果 ⑹試験手順⑹のサーバ認証結果 ⑹試験手順⑼のサーバ認証結果
合否判定	・測定項目⑷が失敗 ・測定項目⑹が失敗 ・測定項目⑹が成功
備考	―

【WLSTST_04004】サーバ認証（TLS1.1 以前）の無効化	
試験項目	TLS1.1 バージョン以前を無効化していることを確認する
事前条件	・【WLSTST_04003】の評価が終了していること
試験手順	＜TLS バージョン 1.0＞ ⑴ECU は、テスタに対し、TLS ハンドシェイクを要求する ⑵テスタは、ECU に対し、TLS バージョン 1.0 を要求する

	⑶RAM モニタで ECU の TLS ハンドシェイク結果を確認する ＜TLS バージョン 1.1＞ ⑷ECU は、テスタに対し、TLS ハンドシェイクを要求する ⑸テスタは、ECU に対し、TLSージョン 1.1 を要求する ⑹RAM モニタで ECU の TLS ハンドシェイク結果を確認する
測定項目	⑷試験手順⑶の ECU の TLS ハンドシェイク結果 ⑹試験手順⑹の ECU の TLS ハンドシェイク結果
合否判定	・測定項目⑷が失敗 ・測定項目⑹が失敗
備考	―

【WLSTST_04005】クライアント認証（TLS1.2 以降）	
試験項目	トヨタセンターとの接続は、以下の何れかの方式でクライアント認証することを確認する -TLS（バージョン 1.2 以降）標準のシーケンス -上位文書[1]の Appendix A のシーケンス
事前条件	なし
試験手順	＜クライアント認証に TLS 標準シーケンスを採用した場合＞ 施する ⑴ECU は、テスタに対し TLS ハンドシェイクを要求する ⑵テスタは、ECU に対し TLS 標準シーケンスに従いクライアント認証を要求する ⑶テスタは、ECU との通信を取得する ＜クライアント認証に上位文書[1]の Appendix A を採用した場合＞⑷ECU は、テスタに対し TLS ハンドシェイクを要求する ⑸テスタは、ECU に対し上位文書[1]の Appendix A に従いクライアント認証を要求する ⑹テスタは、ECU との通信を取得する
測定項目	⑷試験手順⑶の通信ログ ⑹試験手順⑹の通信ログ
合否判定	・測定項目⑷でクライアント認証が TLS 標準(バージョン 1.2 以降)に準拠している ・測定項目⑹でクライアント認証が上位文書[1]の Appendix A に準拠している
備考	―

【WLSTST_04006】サーバ認証の演算処理保護	
試験項目	サーバ認証の演算が耐タンパ領域、またはセキュア領域で処理されていることを確認する
事前条件	なし
試験手順	⑴ECU は、テスタに対し TLS ハンドシェイクを要求する ⑵テスタは、ECU とのサーバ認証を実施する ⑶ECU のサーバ認証の署名検証処理が実施されているメモリ領域を確認できる適切な手順を ECU 設計部署にて検討する。ただし、耐タンパ領域、またはセキュア領域での処理を実動作で確認が難しい場合に限り設計仕様の確認でも可とする
測定項目	⑷試験手順⑵に依る
合否判定	・測定項目⑷で、耐タンパ領域、もしくはセキュア領域で行われていること
備考	―

【WLSTST_04007】クライアント認証の演算処理保護	
試験項目	クライアント認証の演算が耐タンパ領域で処理されていることを確認する
事前条件	なし
試験手順	＜クライアント認証に TLS 標準シーケンスを採用した場合＞ ⑴ECU は、テスタに対し TLS ハンドシェイクを要求する ⑵テスタは、ECU に対し TLS 標準シーケンスに従いクライアント認証を要求する ⑶ECU のクライアント認証の署名生成処理が実施されているメモリ領域を確認できる適切な手順を ECU 設計部署にて検討する。ただし、耐タンパ領域での処理を実動作で確認が難しい場合に限り設計仕様の確認でも可とする確認する ＜クライアント認証に上位文書[1]の Appendix A を採用した場合＞ ⑷ECU は、テスタと TLS ハンドシェイクを開始する ⑸テスタは、ECU に対し上位文書[1]の Appendix A に従いクライアント認証を要求する ⑹ECU のクライアント認証符号 (HMAC) の生成処理が実施されているメモリ領域を確認できる適切な手順を ECU 設計部署にて検討する。ただし、耐タンパ領域での処理を実動作で確認が難しい場合に限り設計仕様の確認でも可とする確認する
測定項目	⑷測定手順⑶に依る

	(b)測定手順(6)に依る
合否判定	・測定項目(a)が耐タンパ領域 ・測定項目(b)が耐タンパ領域
備考	—

【WLSTST_04008】公開鍵の保護	
試験項目	公開鍵（ルート証明書等）が完全性を担保する領域に格納されていることを確認する
事前条件	なし
試験手順	関連文書[2]【VULCMN_51200】参照 （補足）公開鍵（ルート証明書等）は、PSP のため
測定項目	
合否判定	
備考	—

【WLSTST_04009】クライアント認証用の秘密鍵の保護	
試験項目	クライアント認証に用いる秘密鍵が耐タンパ領域に格納されていることを確認する
事前条件	なし
試験手順	関連文書[2]【VULCMN_51200】,【VULCMN_52000】,【VULCMN_52200】参照 （補足）クライアント認証用の秘密鍵・共通鍵は、CSP かつ耐タンパ性が求められているため
測定項目	
合否判定	
備考	—

【WLSTST_04010】秘密鍵の外部メモリへの暗号化保存	
試験項目	キーストレージの制約により、耐タンパ性を有したハードウェア内への保管が困難である場合、セキュリティチップ内に保存した鍵を用いて暗号化した上で保管していることを確認する
事前条件	なし
試験手順	関連文書[2]【VULCMN_51200】参照
測定項目	
合否判定	
備考	—

【WLSTST_04011】ルート証明書の切替	
試験項目	・ルート証明書は下記の両方のアルゴリズムに対応していることを確認する -RSA 3072 bit 以上 -ECDSA 256bit 以上 ・ルート証明書の無効化が出来ることを確認する ・ルート証明書の切り替え（無効化）の完全性が確保できていることを確認する
事前条件	ECU は、【WLSTST_04003】の評価を終了している
試験手順	＜ルート証明書が両方のアルゴリズムに対応＞ (1)ECU は、テスタに対して TLS ハンドシェイクを要求する (2)テスタは、RSA3072bit に対応したサーバ証明書を ECU に送信する (3)RAM モニタで、ECU のサーバ認証結果を確認する (4)ECU は、テスタに対して TLS ハンドシェイクを要求する (5)テスタは、ECDSA256bit に対応したサーバ証明書を ECU に送信する (6)RAM モニタで、ECU のサーバ認証結果を確認する ＜ルート証明書の無効化＞ (7)テスタは、ECU 設計部署にて採用したルート証明書の無効化手順に従い、ECU のルート証明書を無効化する (8)ECU は、テスタに対して TLS ハンドシェイクを要求する (9)テスタは、試験手順(7)で無効化した証明書をルートにもつサーバ証明書を ECU に送信する (10)RAM モニタで、ECU のサーバ認証結果を確認する ＜ルート証明書の無効化の完全性＞ (11)ルート証明書の不正な無効化処理を受け付けないことを確認できる適切な手順を ECU 設計部署にて検討する
測定項目	(a)試験手順(3)のサーバ認証結果 (b)試験手順(6)のサーバ認証結果 (c)試験手順(10)のサーバ認証結果 (d)試験手順(11)に依る
合否判定	・測定項目(a)が成功 ・測定項目(b)が成功 ・測定項目(c)が失敗 ・測定項目(d)で不正な無効化処理を受け付けていない

備考	—

【WLSTST_04012】サーバ証明書の失効確認	
試験項目	サーバ認証時、以下の失効判断基準に従いサーバ証明書を検証し、失効している場合は、認証しないことを確認する 失効判断基準： -証明書失効リスト（CRL）、もしくは OCSP による失効状態確認
事前条件	・CRL もしくは、OCSP で失効状態となっているサーバ証明書を入手している
試験手順	＜失効したサーバ証明書＞ ⑴ECU は、テスタに対し TLS ハンドシェイクを要求する ⑵テスタは、ECU に対して失効したサーバ証明書を送信する ⑶RAM モニタで、ECU のサーバ認証結果を確認する
測定項目	ⓐ試験手順⑶のサーバ認証結果
合否判定	・測定項目ⓐが失敗
備考	—

【WLSTST_04013】通信の改ざん検知（TLS1.2 以降）	
試験項目	センタより受信したメッセージの改ざんを検知した場合、当該メッセージを破棄することを確認する
事前条件	なし
試験手順	⑴ECU は、テスタと TLS セッションを確立する ⑵テスタは、改ざんしたメッセージを ECU に送信する ⑶RAM モニタで、ECU のメッセージ受信結果を確認する
測定項	ⓐ試験手順⑶のメッセージ受信結果
合否判定	・測定項目ⓐで改ざんしたメッセージを破棄している
備考	—

5.3.1.2.2. サーバの評価

【WLSTST_04014】 TLS 圧縮機能の無効化	
試験項目	TLS 圧縮機能を無効化していることを確認する
事前条件	なし
試験手順	(1)テスタは、ECU に対して、TLS ハンドシェイクの中で TLS 圧縮機能を要求する (2)テスタは、試験手順(1)に対する ECU の応答を確認する
測定項目	(a)試験手順(2)の ECU の応答
合否判定	・測定項目(a)で ECU が TLS 圧縮機能を非サポートである
備考	—

【WLSTST_04015】 TLS 再ネゴシエーション機能の無効化	
試験項目	TLS 再ネゴシエーション機能を無効化していることを確認する
事前条件	・ECU は、【WLSTST_04016】の評価が終了していること
試験手順	(1)テスタは、ECU との TLS セッションを確立後に、TLS 再ネゴシエーションを要求する (2)テスタは、試験手順(1)に対する ECU の応答を確認する
測定項目	(a)試験手順(2)の応答
合否判定	・測定項目(a)で TLS 再ネゴシエーション要求を棄却している
備考	—

【WLSTST_04016】サーバ認証（TLS1.2 以降）	
試験項目	・サーバ認証は TLS 標準（バージョン 1.2 以降）のシーケンスに従っていることを確認し、センタと接続することを確認する ・中間 CA を想定した多階層のサーバ認証に対応していることを確認する
事前条件	なし
試験手順	(1)テスタは、ECU に対して TLS ハンドシェイクを要求する (2)テスタは、ECU との通信を取得する
測定項目	(a)試験手順(2)の通信ログ
合否判定	・測定項目(a)のサーバ認証が TLS 標準(バージョン 1.2 以降)に準拠している ・測定項目(a)で ECU がテスタに、正規のルート証明書をルートするサーバ証明書と中間証明書を応答している
備考	―

【WLSTST_04017】サーバ認証（TLS1.1 以前）の無効化	
試験項目	TLS1.1 バージョン以前を無効化していることを確認する
事前条件	【WLSTST_04016】の評価が終了していること
試験手順	＜TLS バージョン 1.0＞ (1)テスタは、ECU に対し TLS ハンドシェイクで TLS バージョン 1.0 を要求する (2)RAM モニタで ECU の TLS ハンドシェイク結果を確認する ＜TLS バージョン 1.1＞ (3)テスタは、ECU に対し TLS ハンドシェイクで TLS バージョン 1.1 を要求する (4)RAM モニタで ECU の TLS ハンドシェイク結果を確認する
測定項目	(a)試験手順(2)の ECU の TLS ハンドシェイク結果 (b)試験手順(4)の ECU の TLS ハンドシェイク結果
合否判定	・測定項目(a)が TLS ハンドシェイク失敗 ・測定項目(b)が TLS ハンドシェイク失敗
備考	―

【WLSTST_04018】クライアント認証（TLS1.2 以降）	
試験項目	TLS1.2 以降を使用するトヨタセンターとクライアント認証することを確認する
事前条件	なし
試験手順	＜接続相手が正規＞ ⑴テスタは、正しいクライアント証明書を用いて、ECU とのクライアント認証を実施する ⑵RAM モニタで、ECU のクライアント認証結果を確認する ＜接続相手が不正＞ ⑶テスタは、誤ったクライアント証明書を用いて、ECU とのクライアント認証を実施する ⑷RAM モニタで、ECU のクライアント認証結果を確認する ＜有効期限が切れたクライアント証明書＞ ⑸テスタは、ECU に対し、有効期限が切れたクライアント証明書を用いて、ECU とのクライアント認証を実施する ⑹RAM モニタで、ECU のクライアント認証結果を確認する
測定項目	⑷試験手順⑵のクライアント認証結果 ⑹試験手順⑷のクライアント認証結果 ⑻試験手順⑹のクライアント認証結果
合否判定	・測定項目⑷が成功 ・測定項目⑹が失敗 ・測定項目⑻が失敗
備考	―

【WLSTST_04019】サーバ認証の演算処理保護	
試験項目	サーバ認証の演算が耐タンパ領域、またはセキュア領域で処理されていることを確認する
事前条件	なし
試験手順	(1)テスタは、ECU に対し TLS ハンドシェイクを要求する (2)ECU のサーバ認証の署名生成処理が実施されているメモリ領域を確認できる適切な手順を ECU 設計部署で検討する。ただし、耐タンパ領域、またはセキュア領域での処理を実動作で確認が難しい場合に限り設計仕様の確認でも可とする
測定項目	(a)試験手順(2)に依る
合否判定	・測定項目(a)にて、耐タンパ領域、もしくはセキュア領域で行われていること
備考	—

【WLSTST_04020】クライアント認証の演算処理保護	
試験項目	クライアント認証の演算が耐タンパ領域で処理されていることを確認する
事前条件	なし
試験手順	(1)テスタは、ECU に対し TLS ハンドシェイクを要求する (2)ECU のクライアント認証の署名検証処理が実施されているメモリ領域を確認できる適切な手順を ECU 設計部署で検討する。ただし、耐タンパ領域での処理を実動作で確認が難しい場合に限り設計仕様の確認でも可とする
測定項目	(a)測定手順(2)に依る
合否判定	・測定項目(a)にて、耐タンパ領域で行われていること
備考	—

【WLSTST_04021】公開鍵の保護	
試験項目	公開鍵（ルート証明書等）が完全性を担保する領域に格納されていることを確認する
事前条件	なし
試験手順	関連文書[2]【VULCMN_51200】参照 （補足）公開鍵（ルート証明書等）は、PSP のため
測定項目	
合否判定	
備考	—

【WLSTST_04022】クライアント認証用の秘密鍵の保護	
試験項目	クライアント認証に用いる秘密鍵が耐タンパ領域に格納されていることを確認する
事前条件	なし
試験手順	関連文書[2]【VULCMN_51200】,【VULCMN_52000】,【VULCMN_52200】参照 （補足）クライアント認証用の秘密鍵・共通鍵は、CPS かつ耐タンパ性が求められているため
測定項目	
合否判定	
備考	—

【WLSTST_04023】秘密鍵の外部メモリへの暗号化保存	
試験項目	キーストレージの制約により、耐タンパ性を有したハードウェア内への保管が困難である場合、セキュリティチップ内に保存した鍵を用いて暗号化した上で保管していることを確認する
事前条件	なし
試験手順	関連文書[2]【VULCMN_51200】参照
測定項目	
合否判定	
備考	—

【WLSTST_04024】ルート証明書の切替	
試験項目	・ルート証明書は下記の両方のアルゴリズムに対応していることを確認する ・RSA 3072 bit 以上 ・ECDSA 256bit 以上 ・ルート証明書の無効化ができることを確認する ・ルート証明書切り替えの完全性が担保されていることを確認する
事前条件	ECU は、【WLSTST_04018】の評価が終了していること
試験手順	＜ルート証明書が両方のアルゴリズムに対応＞ (1)テスタは、ECU に対して TLS ハンドシェイクを要求する (2)テスタは、RSA3072bit に対応したクライアント証明書を ECU に送信する (3)RAM モニタで、ECU のクライアント認証結果を確認する (4)テスタは、ECU に対して TLS ハンドシェイクを要求する (5)テスタは、ECDSA256bit に対応したクライアント証明書を ECU に送信する (6)RAM モニタで、ECU のクライアント認証結果を確認する

	＜ルート証明書の無効化＞ (7)テスタは、ECU 設計部署にて採用したルート証明書の無効化手順に従い、ECU のルート証明書を無効化する (8)テスタは、ECU に対して TLS ハンドシェイクを要求する (9)テスタは、試験手順(7)で無効化した証明書をルートにもつクライアント証明書を ECU に送信する (10)RAM モニタで、ECU のクライアント認証結果を確認する ＜ルート証明書の無効化の完全性＞ (11)ルート証明書の不正な無効化処理を受け付けないことを確認できる適切な手順を ECU 設計部署にて検討する
測定項目	(a)試験手順(3)のクライアント認証の成否 (b)試験手順(6)のクライアント認証の成否 (c)試験手順(10)のクライアント認証の成否 (d)試験手順(11)に依る
合否判定	・測定項目(a)が成功 ・測定項目(b)が成功 ・測定項目(c)が失敗 ・測定項目(d)で不正な無効化処理を受け付けていない
備考	―

【WLSTST_04025】クライアント証明書の失効確認	
試験項目	クライアント認証を実施する際に、クライアント証明書を検証し、失効している場合は認証しないことを確認する 失効判断基準： -証明書失効リスト（CRL)、もしくは OCSP による失効状態確認
事前条件	・CRL もしくは、OCSP で失効状態となっているクライアント証明書を入手している
試験手順	＜失効したクライアント証明書＞ (1)テスタは、ECU に対し、失効したクライアント証明書を用いて、TLS ハンドシェイクを要求する (2)RAM モニタで、ECU のクライアント認証結果を確認する
測定項目	(a)試験手順(2)のクライアント認証結果
合否判定	・測定項目(a)が失敗
備考	―

【WLSTST_04026】サーバ証明書の発行	
試験項目	サーバ証明書の発行・更新を要求する際は、既存の鍵情報を再利用せず、 新たに公開鍵と秘密鍵の鍵ペアを生成することを確認する
事前条件	ECU に保存されているサーバ証明書（公開鍵）を入手している
試験手順	(1)テスタは、ECU にサーバ証明書用の公開鍵と秘密鍵の生成を要求する (2)ECU 設計部署にて採用したサーバ証明書の発行・更新手順に従い、試験手順(1)で生成された公開鍵を用いてサーバ証明書を発行・更新する (3)ECU に、試験手順(2)のサーバ証明書を登録する (4)テスタは、ECU に対し、TLS ハンドシェイクを要求する (5)テスタでサーバ認証結果を確認する
測定項目	(a)試験手順(1)で生成した公開鍵 (b)試験手順(5)のサーバ認証結果
合否判定	・測定項目(a)が評価前の公開鍵と異なっている ・測定項目(b)が成功
備考	・評価対象は、サーバ証明書の発行・更新に伴い、新たに公開鍵と秘密鍵の鍵ペアを生成する機能を実装する ECU とする

【WLSTST_04027】通信の改ざん検知（TLS1.2 以降）	
試験項目	センタより受信したメッセージの改ざんを検知した場合、当該メッセージを破棄することを確認する
事前条件	なし
試験手順	(1)ECU は、テスタと TLS セッションを確立する (2)テスタは、改ざんしたメッセージを ECU に送信する (3)RAM モニタで、ECU のメッセージ受信結果を確認する
測定項	(a)試験手順(3)のメッセージ受信結果
合否判定	・測定項目(a)で改ざんメッセージを破棄している
備考	—

5.3.2. センタ以外と接続する場合の評価

5.3.2.1. Wi-Fi と Bluetooth 以外を用いる場合の評価

5.3.2.1.1. クライアントの評価

【WLSTST_05001】車外機器認証	
試験項目	・接続相手を認証していることを確認する ・認証が失敗した場合は、認証相手に応答しないことを確認する
事前条件	なし
試験手順	＜接続相手が正規＞ ⑴ECU は、テスタに対し認証を要求する ⑵テスタは、正しい認証情報を用いて、ECU との認証を実施する ⑶RAM モニタで、試験手順⑵に対する ECU の認証結果を確認する ＜接続相手が不正＞ ⑷ECU は、テスタに対し認証を要求する ⑸テスタは、誤った認証情報を用いて、ECU との認証を実施する ⑹テスタは、ECU との通信を取得する ⑺RAM モニタで、試験手順⑸に対する ECU の認証結果を確認する
測定項目	⑷試験手順⑶の ECU の認証結果 ⑹試験手順⑹の通信ログ ⑹試験手順⑺の ECU の認証結果
合否判定	・測定項目⑷が成功 ・測定項目⑹にテスタへの応答が含まれていない ・測定項目⑹が失敗
備考	―

【WLSTST_05002】通信の暗号化と改ざん検知	
試験項目	・車外との接続時は通信路の暗号化と改ざん検知を行うことを確認する ・車外から受信したメッセージの改ざんを検知した場合、当該メッセージを破棄していることを確認する
事前条件	なし
試験手順	＜通信路の暗号化と改ざん検知＞ ⑴ECU は、テスタとの認証を完了した状態とする ⑵ECU からテスタに対しメッセージを送信させ、テスタは ECU との通信を取得する ⑶テスタは、ECU 設計部署で採用した暗号・改ざん検知アルゴリズムを適用したメッセージを ECU に送信する ⑷RAM モニタで ECU のメッセージ受信結果を確認する ＜メッセージの改ざん検知の確認＞ ⑸テスタは、改ざんしたメッセージ（例：メッセージ認証子を誤った値に変更）を ECU に送信する ⑹RAM モニタで ECU のメッセージ受信結果を確認する
測定項目	⑷試験手順⑵の ECU からテスタへのメッセージ ⑹試験手順⑷の ECU のメッセージ受信結果 ⑹試験手順⑹の ECU のメッセージ受信結果
合否判定	・測定項目⑷が ECU 設計部署で採用した暗号・改ざん検知アルゴリズムに準拠している ・測定項目⑹が成功 ・測定項目⑹が失敗
備考	―

5.3.2.1.2. サーバの評価

【WLSTST_05003】車外機器認証	
試験項目	・接続相手を認証していることを確認する ・認証が失敗した場合は、認証相手に応答しないことを確認する
事前条件	なし
試験手順	<接続相手が正規> ⑴テスタは、ECU に対して、正しい認証情報を用いて認証を要求する ⑵RAM モニタで、試験手順⑴に対する ECU の認証結果を確認する <接続相手が不正> ⑶テスタは、ECU に対して、誤った認証情報を用いて認証を要求する ⑷テスタは、ECU からの通信を取得する ⑸RAM モニタで、試験手順⑶に対する ECU の認証結果を確認する
測定項目	⒜試験手順⑵の ECU の認証結果 ⒝試験手順⑷の通信ログ ⒞試験手順⑸の ECU の認証結果
合否判定	・測定項目⒜が成功 ・測定項目⒝でテスタへの応答が含まれていない ・測定項目⒞が失敗
備考	―

【WLSTST_05004】通信の暗号化と改ざん検知	
試験項目	・車外との接続時は通信路の暗号化と改ざん検知を行うことを確認する ・車外から受信したメッセージの改ざんを検知した場合、当該メッセージを破棄していることを確認する
事前条件	なし
試験手順	＜通信路の暗号化と改ざん検知＞ ⑴テスタは、ECU との認証を完了させる ⑵ECU からテスタに対しメッセージを送信させ、テスタは送信されたメッセージを確認する ⑶テスタは、ECU 設計部署で採用した暗号・改ざん検知アルゴリズムを適用したメッセージを ECU に送信する ⑷RAM モニタで ECU のメッセージ受信結果を確認する ＜メッセージの改ざん検知の確認＞ ⑸テスタは、改ざんしたメッセージ（例：メッセージ認証子を誤った値に変更）を ECU に送信する ⑹RAM モニタで ECU のメッセージ受信結果を確認する
測定項目	⑷試験手順⑵の ECU からテスタへのメッセージ ⑹試験手順⑷の ECU のメッセージ受信結果 ⑹試験手順⑹の ECU のメッセージ受信結果
合否判定	・測定項目⑷が ECU 設計部署で採用した暗号・改ざん検知アルゴリズムに準拠している ・測定項目⑹が受信成功 ・測定項目⑹が改ざんされたメッセージを破棄している
備考	―

5.3.2.2.Wi-Fi を用いる場合の評価

5.3.2.2.1. クライアントの評価

【WLSTST_06001】WPA2 以降の使用	
試験項目	・WPA2 以降（WPA2、WPA3）の規格を使用していることを確認する ・WPA、WEP とは接続しないことを確認する ・WPA3 をサポートしていることを確認する ・IEEE802.11w をサポートしていることを確認する
事前条件	なし
試験手順	＜WEP＞ (1)テスタ（アクセスポイント）は、WEP 対応のビーコン情報を送信する (2)ECU が試験手順(1)のテスタとの Wi-Fi 接続を許可しているか確認する ＜WPA＞ (3)テスタ（アクセスポイント）は、WAP 対応のビーコン情報を送信する (4)ECU が試験手順(3)のテスタとの Wi-Fi 接続を許可しているか確認する ＜WPA3＞ (5)テスタ（アクセスポイント）は、WAP3 対応のビーコン情報を送信する (6)ECU が試験手順(5)のテスタとの Wi-Fi 接続を許可しているか確認する (7)ECU にテスタとの WPA3 の認証を要求させる (8)テスタで ECU との通信を取得する ・ECU が WPA2 の規格を使用している場合のみ、以下の試験手順を実施する ＜WPA2＞ (9)テスタ（アクセスポイント）は、WAP2 対応のビーコン情報を送信する (10)ECU が試験手順(9)のテスタとの Wi-Fi 接続を許可しているか確認する (11)ECU にテスタとの WPA2 の認証を要求させる (12)テスタで ECU との通信を取得する
測定項目	(a)試験手順(2)のテスタとの Wi-Fi 接続状態 (b)試験手順(4)のテスタとの Wi-Fi 接続状態 (c)試験手順(6)のテスタとの Wi-Fi 接続状態 (d)試験手順(8)の通信ログ (e)試験手順(10)のテスタとの Wi-Fi 接続状態 (f)試験手順(12)の通信ログ

合否判定	・測定項目(a)は、テスタとの Wi-Fi 接続を許可していない ・測定項目(b)は、テスタとの Wi-Fi 接続を許可していない ・測定項目(c)は、テスタとの Wi-Fi 接続を許可している ・測定項目(d)は、ECU が IEEE802.11w の使用を要求している ・測定項目(e)は、テスタとの Wi-Fi 接続を許可している ・測定項目(f)は、ECU が IEEE802.11w の使用を要求している
備考	―

【WLSTST_06002】通信の改ざん検知（Wi-Fi）	
試験項目	車外から受信したメッセージの改ざんを検知した場合、当該メッセージに対し破棄されていることを確認する
事前条件	ECU は【WLSTST_06001】の評価を終了している
試験手順	(1)ECU は、テスタとの WPA2 以降の認証を完了させる (2)テスタは、改ざんしたメッセージ（例：メッセージ認証子を誤った値に変更）を ECU に送信する (3)RAM モニタで、ECU のメッセージ受信結果を確認する
測定項目	(a)試験手順(3)のメッセージ受信結果
合否判定	・測定項目(a)で改ざんしたメッセージを破棄している
備考	―

5.3.2.2.2. サーバの評価

【WLSTST_06003】WPA2 以降の使用	
試験項目	・WPA2 以降（WPA2、WAP3）の規格を使用していることを確認する ・WPA、WEP とは接続しないことを確認する ・WPA3 をサポートしていることを確認する ・IEEE802.11w をサポートしていることを確認する
事前条件	なし
試験手順	＜ECU が Wi-Fi のビーコン情報を送信できる場合＞ ⑴ECU にビーコン情報で送信させる ⑵テスタは、ECU のビーコン情報を確認する ＜ECU が Wi-Fi のビーコン情報を送信できない場合＞ ⑶テスタは、ECU に対し、probe 要求を送信する ⑷テスタは、ECU からの probe 応答を受信する
測定項目	⑷試験手順⑵の ECU のビーコン情報 ⑹試験手順⑷の ECU の probe 応答
合否判定	・測定項目⑷は、WEP と WPA を非サポート、WPA3 をサポートしていること WPA2 のサポート状態は、ECU 設計部署が決定した設定と一致していること ECU が IEEE802.11w の使用を要求していること ・測定項目⑹は、WEP と WPA を非サポート、WPA3 をサポートしていること WPA2 のサポート有無は、ECU 設計部署が決定した設定と一致していること ECU が IEEE802.11w の使用を要求していること
備考	―

【WLSTST_06004】WPA-PSK の認証情報の変更	
試験項目	PSK をユーザが変更をする場合は以下を満たしていることを確認する ・文字数が 8 文字以上であること ・上位文書[1]の【WLSREQ_00360】を満たせないパスワードが設定される場合、ユーザにリスクを提示すること
事前条件	なし
試験手順	＜ECU 設計部署が上位文書[1]の【WLSREQ_00360】を満たさないパスワードへの変更を許容する設計としている場合＞ ⑴ECU に対し、上位文書[1]の【WLSREQ_00360】を満たすパスワードへの変更

	を要求する ⑵試験手順⑴のパスワード変更結果を確認する ⑶ECU に対し、文字数が 8 文字以上かつ、上位文書[1]の【WLSREQ_00360】を満たさないパスワードへの変更を要求する ⑷試験手順⑶のパスワード変更結果と、ユーザへのリスク提示有無を確認する ⑸ECU に対し、文字数が 8 文字未満のパスワードへの変更を要求する ⑹試験手順⑸のパスワード変更結果を確認する ＜ECU 設計部署が上位文書[1]の【WLSREQ_00360】を満たさないパスワードへの変更を許容しない設計としている場合＞ ⑺ECU に対し、上位文書[1]の【WLSREQ_00360】を満たすパスワードへの変更を要求する ⑻試験手順⑺のパスワード変更結果を確認する ⑼ECU に対し、文字数が 8 文字以上かつ、上位文書[1]の【WLSREQ_00360】を満たさないパスワードへの変更を要求する ⑽試験手順⑼のパスワード変更結果を確認する ⑾ECU に対し、文字数が 8 文字未満のパスワードへの変更を要求する ⑿試験手順⑾のパスワード変更結果を確認する
測定項目	⑷試験手順⑵のパスワード変更結果 ⑹試験手順⑷のパスワード変更結果とリスク提示有無 ⑻試験手順⑹のパスワード変更結果 ⑽試験手順⑻のパスワード変更結果 ⑿試験手順⑽のパスワード変更結果 ⒀試験手順⑿のパスワード変更結果
合否判定	・測定項目⑷が成功 ・測定項目⑹のパスワード変更が成功、かつリスク提示あり ・測定項目⑻が失敗 ・測定項目⑽が成功 ・測定項目⑿が失敗 ・測定項目⒀が失敗
備考	―

【WLSTST_06005】通信の改ざん検知（Wi-Fi）	
試験項目	車外から受信したメッセージの改ざんを検知した場合、当該メッセージを破棄することを確認する
事前条件	なし
試験手順	(1)テスタは、ECU との Wi-Fi 認証を完了した状態とする (2)テスタは、改ざんしたメッセージ（例：メッセージ認証子を誤った値に変更）を ECU に送信する (3)RAM モニタで、ECU のメッセージ受信結果を確認する
測定項目	(a)試験手順(3)のメッセージ受信結果
合否判定	・測定項目(a)で改ざんメッセージを破棄している
備考	—

5.3.2.3.Bluetooth を用いる場合の評価

5.3.2.3.1. クライアントの評価

【WLSTST_07001】Bluetooth 実装ガイド	
試験項目	Bluetooth を介した不正通信による車載機への侵入を防ぐために、Bluetooth 機能は NIST SP800-121（Guide to Bluetooth Security）に基づいて開発されていることを確認する
事前条件	なし
試験手順	⑴ECU は、テスタにペアリングを要求する ⑵テスタは、ECU との通信を取得する
測定項目	(a)試験手順⑵の通信ログに対し、NIST SP800-121 の Bluetooth Security Check List の Recommended Practice の全項目
合否判定	・測定項目(a)の全項目が合格
備考	―

【WLSTST_07002】Bluetooth 認証方式	
試験項目	車載 Bluetooth 機能は、SSP モード（Classic の場合）、もしくは LE Secure Connection モード(LE の 場合)で外部デバイスとペアリングすることを確認する
事前条件	なし
試験手順	＜ECU が Bluetooth Classic をサポートしている場合＞ ⑴ECU は、テスタに対しペアリングを要求する ⑵テスタで、ECU との通信を取得する ＜ECU が Bluetooth LE をサポートしている場合＞ ⑶ECU は、テスタに対しペアリングを要求する ⑷テスタは、ECU との通信を取得する
測定項目	(a)試験手順⑵の通信ログ (b)試験手順⑷の通信ログ
合否判定	・測定項目(a)で、ECU はペアリング要求で SSP モードのみを要求している ・測定項目(b)で、ECU はペアリング要求で LE Secure Connection モードのみを要求している
備考	―

【WLSTST_07003】通信の改ざん検知（Bluetooth）	
試験項目	車外から受信したメッセージの改ざんを検知した場合、当該メッセージを破棄していることを確認する
事前条件	なし
試験手順	(1)ECU は、テスタとのペアリングを完了した状態とする (2)テスタは、改ざんしたメッセージ（例：メッセージ認証子を誤った値に変更）を ECU に送信する (3)RAM モニタで、ECU のメッセージ受信結果を確認する
測定項目	(a)試験手順(3)のメッセージ受信結果
合否判定	・測定項目(a)で改ざんしたメッセージを破棄している
備考	―

5.3.2.3.2. サーバの評価

【WLSTST_07004】Bluetooth 実装ガイド	
試験項目	Bluetooth を介した不正通信による車載機への侵入を防ぐために、Bluetooth 機能は NIST SP800-121（Guide to Bluetooth Security）に基づいて開発されていることを確認する
事前条件	なし
試験手順	⑴テスタは、ECU に対してペアリングを要求する ⑵テスタは、ECU との通信を取得する
測定項目	(a)試験手順⑵の通信ログに対し、NIST SP800-121 の Bluetooth Security Check List の Recommended Practice の全項目
合否判定	・測定項目(a)の全項目が合格
備考	―

【WLSTST_07005】Bluetooth 認証方式	
試験項目	・車載 Bluetooth 機能は、SSP モード（Classic の場合）、もしくは LE Secure Connection モード(LE の 場合)で外部デバイスとペアリングすることを確認する ・ペアリング要求に対して認証を行うことを確認する
事前条件	なし
試験手順	＜ECU が Bluetooth Classic をサポートしている場合＞ ⑴テスタは、ECU に対し Bluetooth 認証方式を PIN モードでペアリングを要求する ⑵RAM モニタで、ECU のペアリング結果を確認する ⑶テスタは、ECU に対し Bluetooth 認証方式を SSP モードかつ”Just Works 以外”となるようにペアリングを要求する ⑷テスタは、ECU との通信を取得する ⑸テスタは、ECU に対し Bluetooth 認証方式を SSP モードかつ”Just Works”となるようにペアリングを要求する ⑹RAM モニタで、ECU のペアリング結果を確認する ＜ECU が Bluetooth LE をサポートしている場合＞

	(7)テスタは、ECU に対し Bluetooth 認証方式を LE Secure Connection モードでペアリングを要求する (8)テスタは、ECU との通信を取得する (9)テスタは、ECU に対し Bluetooth 認証方式を LE Legacy Pairing モードでペアリングを要求する (10)RAM モニタで、ECU のペアリング結果を確認する
測定項目	(a)試験手順(2)の ECU のペアリング結果 (b)試験手順(4)の通信ログ (c)試験手順(6)の ECU のペアリング結果 (d)試験手順(8)の通信ログ (e)試験手順(10)の ECU のペアリング結果
合否判定	・測定項目(a)でテスタからのペアリング要求を棄却している ・測定項目(b)で Bluetooth 認証方式が SSP モードである ・測定項目(c)でテスタからのペアリング要求を棄却している ・測定項目(d)で Bluetooth 認証方式が LE Secure Connection モードである ・測定項目(e)でテスタからのペアリング要求を棄却している
備考	—

【WLSTST_07006】通信の改ざん検知（Bluetooth）	
試験項目	車外から受信したメッセージの改ざんを検知した場合、当該メッセージを破棄していることを確認する
事前条件	なし
試験手順	⑴ECU は、テスタとのペアリングを完了した状態とする ⑵テスタは、改ざんしたメッセージ（例：メッセージ認証子を誤った値に変更）を ECU に送信する ⑶RAM モニタで、ECU のメッセージ受信結果を確認する
測定項目	⑷試験手順⑶のメッセージ受信結果
合否判定	・測定項目⑷の改ざんメッセージを破棄している
備考	―

1. Revision Record

Version	Contents of revision	Date	Revised
a00-00-a	Initial Release	Feb. 03, 2022	46F Kakiya/Kiyokawa
a00-01-a	Correct editorial error	May. 23, 2022	46F Kiyokawa
	Clarify a large number of messages in terms of communication(WLSTST_00001)	Jun. 09, 2022	46F Yasue
	Correct traceability errors in section 3.1 Traceability of requirements specification and test specification		
	Clarify the Certificate verification (WLSTST_04003, WLSTST_04012, WLSTST_04018, WLSTST_04025)		
a00-02-a	Clarify the evaluation related to firewall(WLSTST_02001)	Aug. 04, 2022	46F Tamaki
	Change format of cover page		

Table of Contents

2. Introduction

2.1. Purpose of this Document

When the ECU communicate wirelessly with outside target of the vehicle, the ECU protects communication channel and authenticates mutually in order to prevent eavesdropping, tampering and spoofing of communication data.

This document defines the test requirements related to the requirements of communication channel protection and mutual authentication defined in the upper document [1].

2.2. Scope

The scope of this document is every ECU that communicates directly with outside target of the vehicle using wireless communication protocol and every TLS terminal ECU.

2.3. Preconditions

Nothing.

2.4. Description of Requirements

A requirement in this document shall be labeled as 【WLSTST_*****】. Provided, however, that what is labeled as (Supplement) is a supplementary item and therefore is not a requirement specification.

2.5. Upper-level Documents

The upper-level document is shown in Table 2-1.

Table 2-1 Upper-level document

No.	Document name	Version	Issued
1	Requirements Specification of Wireless Communication Security	SEC-ePF-WLS-REQ-SPEC-a00-06-*	46F

2.6. Related Documents

The related documents are shown in Table 2-2.

Table 2-2 Related documents

No	Document name	Version (see the latest version)	Issued
1	Terms and Definitions related to Vehicle Cybersecurity and Privacy	SEC-ePF-TRM-GUD-PROC-***-**-*	46F
2	Requirements Specification of Common Vulnerability Countermeasure	SEC-ePF-VUL-CMN-REQ-SPEC-***-**-*	46F
3	Test specification of vulnerability countermeasure for ECU	SEC-ePF-VUL-ECU-TST-SPEC-***-**-*	46F

3. Outline of Evaluation

3.1. Traceability of requirements specification and test specification

This section describes the traceability of requirement IDs in upper-level documents [1] and test IDs specified in this document.

The list related to countermeasure against DoS attacks is shown in Table 3-1. The list related to Firewall is shown in Table 3-2. The list related to authentication, encryption and tamper detection in the case of connecting with center is shown in Table 3-3. The list related to authentication, encryption and tamper detection in the case of connecting with devices outside of vehicle except for center is shown in Table 3-4.

Table 3-1 Confirmation list of Traceability for requirements specification and test specification (countermeasure against DoS attacks)

Requirements Specification		Test Specification		
Classification	ID	ID	Reason for no evaluation items	Production-time functions
Common	WLSREQ_00100	-	The requirement is deleted	-
	WLSREQ_00110	-	The requirement is deleted	-
	WLSREQ_00120	WLSTST_00001	-	-
	WLSREQ_00130	WLSTST_00001	-	-

Table 3-2 Confirmation list of Traceability for requirements specification and test specification (Firewall)

Requirements Specification		Test Specification		
Classification	ID	ID	Reason for no evaluation items	Production-time functions
Except for IP communication	WLSREQ_00200	WLSTST_01001	-	-
IP communication	WLSREQ_00201	WLSTST_02001	-	-
	WLSREQ_00202	WLSTST_02002	-	-
	WLSREQ_00203	WLSTST_02003	-	-
	WLSREQ_00204	-	The requirement is deleted	-
	WLSREQ_00205	WLSTST_02004	-	-
	WLSREQ_00206	WLSTST_02005	-	-
	WLSREQ_00207	WLSTST_02006	-	-
	WLSREQ_00208	WLSTST_02007	-	-
	WLSREQ_00209	WLSTST_02008	-	-
	WLSREQ_00210	WLSTST_02009	-	-

Table 3-3 Confirmation list of Traceability for requirements specification and test specification (authentication, encryption and tamper detection in the case of connecting with center)

Requirements Specification		Test Specification		
Classification	ID	ID	Reason for no evaluation items	Production-time functions
Except for TLS	WLSREQ_00400	WLSTST_03001	-	-
		WLSTST_03007	-	-
	WLSREQ_00580	WLSTST_03002	-	-
		WLSTST_03008	-	-
	WLSREQ_00410	WLSTST_03003	-	-
	WLSREQ_00590	WLSTST_03004	-	-
		WLSTST_03009	-	-
	WLSREQ_00420	WLSTST_03005	-	-
		WLSTST_03010	-	-
	WLSREQ_00600	WLSTST_03006	-	-
		WLSTST_03011	-	-
	WLSREQ_00610	WLSTST_03005	-	-

Requirements Specification		Test Specification		
Classification	ID	ID	Reason for no evaluation items	Production-time functions
		WLSTST_03010	-	-
TLS	WLSREQ_00121	WLSTST_04001	-	-
		WLSTST_04014	-	-
	WLSREQ_00122	WLSTST_04002	-	-
		WLSTST_04015	-	-
	WLSREQ_00401	WLSTST_04003	-	-
		WLSTST_04016	-	-
	WLSREQ_00402	WLSTST_04004	-	-
		WLSTST_04017	-	-
	WLSREQ_00411	WLSTST_04005	-	-
		WLSTST_04018	-	-
	WLSREQ_00430	WLSTST_04006	-	-
	WLSREQ_00431	WLSTST_04019	-	-
	WLSREQ_00440	WLSTST_04007	-	-
	WLSREQ_00441	WLSTST_04020	-	-
	WLSREQ_00450	WLSTST_04008	-	-
		WLSTST_04021	-	-
	WLSREQ_00460	WLSTST_04009	-	-
		WLSTST_04022	-	-
	WLSREQ_00470	WLSTST_04010	-	-
		WLSTST_04023	-	-
	WLSREQ_00480	-	The requirement is related to operations	-
	WLSREQ_00490	-	The requirement is for after vehicle development	-
	WLSREQ_00500	WLSTST_04011	-	-
		WLSTST_04024	-	-
	WLSREQ_00510	-	The requirement is deleted	-
	WLSREQ_00520	WLSTST_04011	-	-
		WLSTST_04024	-	-
	WLSREQ_00530	WLSTST_04026	-	-
	WLSREQ_00540	WLSTST_04012	-	-
	WLSREQ_00550	WLSTST_04025	-	-

Requirements Specification		Test Specification		
Classification	ID	ID	Reason for no evaluation items	Production-time functions
	WLSREQ_00560	WLSTST_04005	-	-
		WLSTST_04018	-	-
	WLSREQ_00611	WLSTST_04013	-	-
		WLSTST_04027	-	-

Table 3-4 Confirmation list of Traceability for requirements specification and test specification (authentication, encryption and tamper detection in the case of connecting with devices outside of vehicle except for center)

Requirements Specification		Test Specification		
Classification	ID	ID	Reason for no evaluation items	Production-time functions
Except for Wi-Fi / Bluetooth	WLSREQ_00300	WLSTST_05001	-	-
		WLSTST_05003	-	-
	WLSREQ_00350	-	The requirement is for after vehicle development	-
	WLSREQ_00360	-	The requirement is for after vehicle development	-
	WLSREQ_00310	WLSTST_05002	-	-
		WLSTST_05004	-	-
	WLSREQ_00370	WLSTST_05002	-	-
		WLSTST_05004	-	-
Wi-Fi	WLSREQ_00311	WLSTST_06001	-	-
		WLSTST_06003	-	-
	WLSREQ_00312	WLSTST_06001	-	-
		WLSTST_06003	-	-
	WLSREQ_00313	WLSTST_06001	-	-
		WLSTST_06003	-	-
	WLSREQ_00314	-	The requirement is for after vehicle development	-
	WLSREQ_00317	WLSTST_06004	-	-
	WLSREQ_00318	-	The requirement is for after vehicle development	-

	WLSREQ_00315	-	The requirement is for after vehicle development	-
	WLSREQ_00371	WLSTST_06002	-	-
		WLSTST_06005	-	-
Bluetooth	WLSREQ_00316	WLSTST_07001	-	-
		WLSTST_07004	-	-
	WLSREQ_00319	WLSTST_07002	-	-
		WLSTST_07005	-	-
	WLSREQ_00320	WLSTST_07005	-	-
	WLSREQ_00372	WLSTST_07003	-	-
		WLSTST_07006	-	-

The test is passed only if all pass/fail judgement for Test items above are passed.

3.2. List of test items

The list of items is shown below.

The list related to countermeasure against DoS attacks is shown in Table 3-5. The list related to Firewall is shown in Table 3-6. The list related to authentication, encryption and tamper detection in the case of connecting with center is shown in Table 3-7. The list related to authentication, encryption and tamper detection in the case of connecting with devices outside of vehicle except for center is shown in Table 3-8.

Table 3-5 List of test items (countermeasure against DoS attacks)

Classification	Test specification ID	Test items	Applicable target	
			Server	Client
Common	WLSTST_00001	Countermeasure against DoS attacks as receiving a large number of messages	○	○

Table 3-6 List of test items(Firewall)

Classification	Test specification ID	Test items	Applicable target	
			Server	Client
Except for IP communication	WLSTST_01001	Discarding unnecessary communication	○	○
IP communication	WLSTST_02001	Discarding unnecessary TCP/UDP communication	○	○

	WLSTST_02002	TCP communication rule evaluation	○	○
	WLSTST_02003	Discarding the TCP connection establishment request from outside of vehicle	－	○
	WLSTST_02004	Countermeasure against DoS attacks using malicious TCP connection establishment request (minimizing TCP connection timeout period)	○	－
	WLSTST_02005	Countermeasure against DoS attacks using malicious TCP connection establishment request (half-open status management)	○	－
	WLSTST_02006	Discarding unnecessary ICMP Requests	○	○
	WLSTST_02007	Limiting the number of packets received on TCP/UDP ports	○	○
	WLSTST_02008	Limiting the number of simultaneous connections from same IP address	○	－
	WLSTST_02009	Dropping packets addressed to an unnecessary broadcast address	○	○

Table 3-7 List of test items(authentication, encryption and tamper detection in the case of connecting with center)

Classification	Test specification ID	Test items	Applicable target	
			Server	Client
Except for TLS	WLSTST_03001	Server authentication	－	○
	WLSTST_03002	Countermeasure against session hijacking	－	○
	WLSTST_03003	Client authentication	－	○
	WLSTST_03004	Updating/Switching of Client authentication key	－	○
	WLSTST_03005	Encryption and tamper detection of communication channel	－	○
	WLSTST_03006	Updating the encryption key for communication channel encryption	－	○
	WLSTST_03007	Authentication for the connection counterpart	○	－
	WLSTST_03008	Countermeasure against session hijacking	○	－
	WLSTST_03009	Updating/Switching of Client authentication key	○	－
	WLSTST_03010	Encryption and tamper detection of communication	○	－

		channel		
	WLSTST_03011	Updating the encryption key for communication channel encryption	○	–
TLS	WLSTST_04001	Disabling the TLS compression function	–	○
	WLSTST_04002	Disabling the TLS renegotiation function	–	○
	WLSTST_04003	Server authentication (TLS1.2 or later)	–	○
	WLSTST_04004	Disabling Server authentication (TLS1.1 and earlier)	–	○
	WLSTST_04005	Client authentication (TLS1.2 or later)	–	○
	WLSTST_04006	Protection for server authentication processing	–	○
	WLSTST_04007	Protection for client authentication processing	–	○
	WLSTST_04008	Protection for the public key	–	○
	WLSTST_04009	Protection for the private key used for client authentication	–	○
	WLSTST_04010	Encrypt and store private key in external memory	–	○
	WLSTST_04011	Switching the Root Certificate	–	○
	WLSTST_04012	Server Certificate Revocation check	–	○
	WLSTST_04013	Tamper detection of communication (TLS1.2 or later)	–	○
	WLSTST_04014	Disabling the TLS compression function	○	–
	WLSTST_04015	Disabling the TLS renegotiation function	○	–
	WLSTST_04016	Server authentication (TLS1.2 or later)	○	–
	WLSTST_04017	Disabling Server authentication (TLS1.1 and earlier)	○	–
	WLSTST_04018	Client authentication (TLS1.2 or later)	○	–
	WLSTST_04019	Protection for server authentication processing	○	–
	WLSTST_04020	Protection for client authentication processing	○	–
	WLSTST_04021	Protection for the public key	○	–
	WLSTST_04022	Protection for the private key used for client authentication	○	–
	WLSTST_04023	Encrypt and store private key in external memory	○	–
	WLSTST_04024	Switching the Root Certificate	○	–
	WLSTST_04025	Client Certificate Revocation check	○	–
	WLSTST_04026	Issuing a Server Certificate	○	–
	WLSTST_04027	Tamper detection of communication (TLS1.2 or later)	○	–

Table 3-8 List of test items

(authentication, encryption and tamper detection in the case of connecting with devices outside of vehicle except for center)

Classification	Test specification ID	Test items	Applicable target	
			Server	Client
Except for Wi-Fi / BT	WLSTST_05001	External Device Authentication	―	○
	WLSTST_05002	Encryption and tamper detection of communication channel	―	○
	WLSTST_05003	External Device Authentication	○	―
	WLSTST_05004	Encryption and tamper detection of communication channel	○	―
Wi-Fi	WLSTST_06001	Using WPA2 or later	―	○
	WLSTST_06002	Tamper detection of communication (Wi-Fi)	―	○
	WLSTST_06003	Using WPA2 or later	○	―
	WLSTST_06004	Changing a confirmation information of WPA-PSK	○	―
	WLSTST_06005	Tamper detection of communication (Wi-Fi)	○	―
BT	WLSTST_07001	Bluetooth implementation guide	―	○
	WLSTST_07002	Bluetooth authentication method	―	○
	WLSTST_07003	Tamper detection of communication (Bluetooth)	―	○
	WLSTST_07004	Bluetooth implementation guide	○	―
	WLSTST_07005	Bluetooth authentication method	○	―
	WLSTST_07006	Tamper detection of communication (Bluetooth)	○	―

4. Evaluation environment

The evaluation environment is shown in Figure 4.1.

- ECU is subject to evaluation.
- Tools to simulate a device outside of vehicle that communicate wirelessly with the ECU are assumed as Tester.
- Debugger devices are assumed as the RAM monitor.

Figure 4.1 Evaluation environment

5. Evaluation details

5.1. Evaluation related to Countermeasure against DoS attacks

【WLSTST_00001】Countermeasure against DoS attacks as receiving a large number of messages	
Test content	This test confirms that an ECU remains the pre-determined performance of each function defined in accordance with 【WLSREQ_00120】 in upper-level document [1] during receiving a large number of messages from outside of the vehicle.
Prerequisites	None
Test Procedure	(1) The tester transmits the following communication to the ECU. A) communication that achieves effective throughput B) communication that exhausts the upper limit of the resource in ECU allocated for the communication function (2) ECU design dept. consider the proper test procedure that confirms the performance of each function defined in accordance with 【WLSREQ_00120】 in upper-level document [1] is remained.
Measurement items	(a) Depend on the test procedure (2).
Pass/Fail Judgment	・ In the measurement item (a), the performance of each function defined in accordance with 【WLSREQ_00120】 in upper-level document [1] shall be remained.
Remarks	—

5.2. Evaluations related to Firewall

5.2.1. Evaluations for using except for IP communication

【WLSTST_01001】 Discarding unnecessary communication	
Test content	This test confirms that the ECU permits only permitted communications and discard unnecessary communication in communication from outside of vehicle.
Prerequisites	The ECU design dept. defines the permitted communication.
Test Procedure	(1) The tester transmits permitted communication. (2) Confirm the reception result for test procedure (1) by using the RAM monitor. (3) The tester transmits except for permitted communication. (4) Confirm the reception result for test procedure (3) by using the RAM monitor.
Measurement items	(a) Reception result in the test procedure (2). (b) Reception result in the test procedure (4).
Pass/Fail Judgment	・ In the measurement item (a), communication shall be received. ・ In the measurement item (b), communication shall not be received.
Remarks	—

5.2.2. Evaluations for using IP communication

【WLSTST_02001】 Discarding unnecessary TCP/UDP communication	
Test content	This test confirms that the ECU opens only the required TCP/UDP ports when an associated service starts or the ECU requests connection establishment, and the ECU closes those TCP/UDP ports when the service finishes or the ECU terminates connection .
Prerequisites	The ECU design dept. defines TCP/UDP ports permitted to communicate
Test Procedure	<For the TCP/UDP ports using System Ports or User Ports> (1) The tester performs 【VULSTS_01001】in the related document [3] for the ECU. (2) The ECU establishes a connection with the tester. (3) The ECU terminates a connection with the tester. (4) The tester performs 【VULSTS_01001】in the related document [3] for the ECU. <For the TCP/UDP ports using Dynamic Ports> (5) The tester performs 【VULSTS_01001】in the related document [3] for the ECU. (6) The ECU establishes a connection with the tester. (7) The tester performs 【VULSTS_01001】in the related document [3] for the ECU.

	(8) The ECU terminates a connection with the tester. (9) The tester performs 【VULSTS_01001】 in the related document [3] for the ECU.
Measurement items	<For the TCP/UDP ports using System Ports or User Ports> (a) Performing result in the test procedure (1). (b) Performing result in the test procedure (4). <For the TCP/UDP ports using Dynamic Ports> (c) Performing result in the test procedure (5). (d) Communication log in the test procedure (6)(8). (e) Performing result in the test procedure (7). (f) Performing result in the test procedure (9).
Pass/Fail Judgment	<For the TCP/UDP ports using System Ports or User Ports> ・ In the measurement item (a), unnecessary ports shall be closed. ・ The measurement item (b) shall be the same as the measurement item (a). <For the TCP/UDP ports using Dynamic Ports> ・ In the measurement item (c), unnecessary ports shall be closed. ・ In the measurement item (d), the port not included in the measurement item (c) shall be the source port of the ECU. ・ In the measurement item (e), the ports other than the ports included in the measurement item (c) and (d) shall be closed. ・ The measurement item (f) shall be the same as the measurement item (c).
Remarks	・ System Ports and User Ports are TCP/UDP Ports assigned statically. ・ Dynamic Ports are TCP/UDP Ports assigned dynamically.

【WLSTST_02002】	TCP communication rule evaluation
Test content	・ This test confirms that the ECU permits only packets that comply with TCP protocol out of the packets that are communicated in established connection. ・ This test confirms that the ECU discards packets that do not comply with TCP protocol out of the packets that are communicated in established connection and disconnect the TCP connection.
Prerequisites	None
Test Procedure	(1) The ECU establishes a TCP connection with the tester. (2) The ECU receives a packet that complies with TCP protocol form the tester. (3) The tester obtains communication from the ECU. (4) The ECU receives a packet that does not comply with TCP protocol form the tester. (5) Confirm the reception result for test procedure (4) by using the RAM monitor. (6) The tester transmits a packet that complies with TCP protocol to TCP connection established in test procedure (1). (7) The tester obtains communication from the ECU.
Measurement items	(a) Communication log in the test procedure (3). (b) Reception result in the test procedure (5). (c) Communication log in the test procedure (7).
Pass/Fail Judgment	・ In the measurement item (a), the acknowledgment for the packet transmitted in the test procedure (2) shall be included. ・ In the measurement item (b), packets shall not be accepted. ・ In the measurement item (c) the acknowledgment for the packet transmitted in the test procedure (6) shall not be included.
Remarks	—

【WLSTST_02003】	Discarding the TCP connection establishment request from outside of vehicle
Test content	This test confirms that the ECU discards the TCP connection establishment request from outside of vehicle if the ECU does not have server function of TCP communication.
Prerequisites	None
Test Procedure	(1) The tester transmits a TCP connection establishment request. (2) The tester obtains communication from the ECU.
Measurement items	(a) Communication log in the test procedure (2).
Pass/Fail Judgment	・ In the measurement item (a), the acknowledgement for TCP connection establishment request shall not be included.

Remarks	If the ECU have server function of TCP communication, this evaluation item is excluded.

【WLSTST_02004】 Countermeasure against DoS attacks using malicious TCP connection establishment request (minimizing TCP connection timeout period)	
Test content	This test confirms that the ECU minimizes TCP connection timeout period within the range that satisfies communication quality.
Prerequisites	None
Test Procedure	(1) The ECU design dept. considers the proper test procedure that confirms the ECU minimizes TCP connection timeout period within the range that satisfies communication quality.
Measurement items	(a) Depend on the test procedure (1).
Pass/Fail Judgment	・ In the measurement item (a), TCP connection timeout period shall be minimized within the range that satisfies communication quality.
Remarks	—

【WLSTST_02005】Countermeasure against DoS attack using malicious TCP connection establishment request (half-open status management)	
Test content	This test confirms that the ECU does not exhaust resources due to the data related to TCP connection in half-open status (Waiting for ACK response for TCP connection establishment request).
Prerequisites	None
Test Procedure	(1) The ECU receives a large number of SYN packets by using the tester. Refer to upper-level document [1] about “a large number”. (2) The tester ignores SYN/ACK packets form ECU. (3) The ECU design dept. considers the proper test procedure that confirms the ECU does not exhaust resources.
Measurement items	(a) Depend on the test procedure (3).
Pass/Fail Judgment	・ In the measurement item (a), the ECU shall not exhaust resources.
Remarks	—

【WLSTST_02006】 Discarding unnecessary ICMP Requests	
Test content	This test confirms that the ECU discards all ICMP packets. If the ECU can't discard all ICMP packets, this test confirms that the ECU receives only the permitted packets by each type/code and discard ICMP echo requests at least.
Prerequisites	If the ECU receives only the permitted packets by each type/code, the ECU design dept. defines the type/code permitted to communicate.
Test Procedure	<For the ECU discarding all ICMP packets> (1) The ECU receives all types/codes of ICMP packets by using the tester. (2) Confirm the reception result for test procedure (1) by using the RAM monitor. <For the ECU receiving only permitted packets by each type/code> (3) The ECU receives a ICMP echo request by using the tester. (4) Confirm the reception result for test procedure (3) by using the RAM monitor. (5) The ECU receives all types/codes of ICMP packets that are not permitted by using the tester. (6) Confirm the reception result for test procedure (5) by using the RAM monitor.
Measurement items	(a) Reception result in the test procedure (2). (b) Reception result in the test procedure (4). (c) Reception result in the test procedure (6).
Pass/Fail Judgment	・ In the measurement item (a), all packets shall not be accepted. ・ In the measurement item (b), the packet shall not be accepted. ・ In the measurement item (c), all packets shall not be accepted.
Remarks	—

【WLSTST_02007】 Limiting the number of packets received on TCP/UDP ports	
Test content	This test confirms that the ECU defines the permitted number of packets received per unit time for open TCP/UDP ports and the ECU drops the packets that exceed the limit and does not response to the sender.
Prerequisites	The ECU design dept. defines the permitted number of packets received per unit time.
Test Procedure	Perform the test procedure (1) to (3) for all TCP/UDP open ports. (1) The ECU receives the permitted number of packets and one more packet within a unit time period by using the tester. (2) Confirm the reception result for test procedure (1) by using the RAM monitor. (3) The tester obtains communication from the ECU. (only TCP)
Measurement items	(a) Reception result in the test procedure (2). (b) Communication log in the test procedure (3).

Pass/Fail Judgment	・ In the measurement item (a), the last packet received by the ECU shall be dropped. ・ In the measurement item (b), the acknowledgment for the packet transmitted in the test procedure (1) shall not be included.
Remarks	—

【WLSTST_02008】 Limiting the number of simultaneous connections from same IP address	
Test content	This test confirms that the ECU limits the number of simultaneous connections from same IP address if there are ports that the TCP connection are established from outside of vehicle.
Prerequisites	The ECU design dept. defines the number of simultaneous TCP connections from the same IP address.
Test Procedure	If there are multiple ports that TCP connections are established from outside of vehicle, perform the test procedure (1) to (3) for all ports. (1) The tester establishes the maximum number of TCP connections from same IP address with the ECU. (2) Transmit a TCP connection establishment request with the same IP address as in the test procedure (1) by using the tester. (3) The tester obtains communication from the ECU.
Measurement items	(a) Communication log in the test procedure (3).
Pass/Fail Judgment	・ In the measurement item (a), the acknowledgement for TCP connection establishment request in the test procedure (2) shall not be included.
Remarks	—

【WLSTST_02009】 Dropping packets addressed to an unnecessary broadcast address	
Test content	This test confirms that the ECU drops the packets addressed to an unnecessary broadcast address.
Prerequisites	The ECU design dept. defines TCP/UDP ports that are permitted communication addressed to broadcast address.
Test Procedure	<In the case that the ECU does not have TCP/UDP ports that are permitted to receive communication addressed to broadcast address> (1) Transmit a packet addressed to broadcast addresses to TCP/UDP open ports by using the tester. (2) Confirm the reception result for test procedure (1) by using the RAM monitor. (3) The tester obtains communication from the ECU. (only TCP) <In the case that the ECU has TCP/UDP ports that are permitted to receive communication

	addressed to broadcast address> (4) Transmit a packet addressed to broadcast addresses to except for TCP/UDP ports that permit communication addressed to broadcast address out of TCP/UDP open ports by using the tester. (5) Confirm the reception result for test procedure (4) by using the RAM monitor. (6) The tester obtains communication from the ECU. (only TCP)
Measurement items	(a) Reception result in test procedure (2). (b) Communication log in the test procedure (3). (c) Reception result in test procedure (5). (d) Communication log in the test procedure (6).
Pass/Fail Judgment	・ In the measurement item (a), the packet shall be dropped. ・ In the measurement item (b), the acknowledgment for the packet transmitted in the test procedure (1) shall not be included. ・ In the measurement item (c), the packet shall be dropped. ・ In the measurement item (d), the acknowledgment for the packet transmitted in the test procedure (4) shall not be included.
Remarks	—

5.3. Evaluations for Authentication, Encryption, and Tamper Detection

5.3.1. Evaluations related to connection with center

5.3.1.1. Evaluations for using except for TLS Communication

5.3.1.1.1. Evaluations for Client

【WLSTST_03001】 Server authentication	
Test content	・ This test confirms that the ECU authenticates a connection counterpart. ・ This test confirms that the ECU does not respond to the authentication counterpart if the authentication fails.
Prerequisites	None
Test Procedure	<Connection counterpart is authorized> (1) The ECU requests a wireless connection to the tester. (2) The tester performs authentication with the ECU using correct confidential information. (3) The ECU design dept. considers the proper test procedure to confirm the result of the ECU's authenticating the tester in the test procedure (2). <Connection counterpart is unauthorized> (4) The ECU requests a wireless connection to the tester. (5) The tester performs authentication with the ECU using incorrect confidential information. (6) The tester obtains communication from the ECU. (7) The ECU design dept. considers the proper test procedure to confirm the result of the ECU's authenticating the tester in the test procedure (5).
Measurement items	(a) Authentication result of the ECU in the test procedure (3) (b) Communication log in the test procedure (6) (c) Authentication result of the ECU in the test procedure (7)
Pass/Fail Judgments	・ Measurement item (a) shall be success. ・ In the measurement item (b), the response to the tester shall be not included. ・ Measurement item (c) shall be failure.
Remarks	—

【WLSTST_03002】 Countermeasure against session hijacking	
Test content	This test confirms that the ECU prevents session hijacking by attackers.
Prerequisites	None
Test Procedure	(1) The ECU design dept. considers the proper test procedure to confirm the session hijacking countermeasure.
Measurement items	(a) Depend on the test procedure (1).
Pass/Fail Judgments	・ In the measurement item (a), the countermeasure against session hijacking shall be implemented.
Remarks	—

【WLSTST_03003】 Client authentication	
Test content	This test confirms that the ECU performs operations for client authentication to prevent unauthorized use of center service when connecting with server.
Prerequisites	None
Test Procedure	(1) The ECU requests a wireless connection to the tester. (2) The tester performs client authentication with the ECU. (3) The tester obtains communication from the ECU.
Measurement items	(a) Communication log in the test procedure (3).
Pass/Fail Judgment	・ In measurement item (a), the client authentication shall comply with the authentication specifications defined by the ECU Design Dept.
Remarks	—

【WLSTST_03004】 Updating/Switching of Client authentication key	
Test content	This test confirms that the symmetric key is updated or switched in the way to ensure its integrity and confidentiality if the ECU uses a symmetric key for client authentication.
Prerequisites	None
Test Procedure	(1) The ECU design dept. considers the proper test procedure to confirm the updating or switching process of client authentication key.
Measurement items	(a) Depend on the test procedure (1)
Pass/Fail Judgment	・ In the measurement item (a), the confidentiality and integrity of the client authentication key shall be ensured.
Remarks	—

【WLSTST_03005】	Encryption and tamper detection of communication channel
Test content	・ This test confirms the ECU encrypts the channel and detects tampering when connecting with outside of vehicle center or service. ・ This test confirms that the ECU drops the received message if the ECU detects a tampering of the received message from center.
Prerequisites	None
Test Procedure	<Encryption and tamper detection of communication channel> (1) The ECU completes the authentication with the tester. (2) The ECU transmits a message to the tester, and the tester obtains communication from the ECU. (3) The tester transmits a message applying the encryption and tamper detection algorithms which the ECU design dept. defines to the ECU. (4) Confirm the message reception result of ECU by using the RAM monitor. <Confirmation of tamper detection of message> (5) The tester transmits a tampered message (e.g. changing the message authentication code to the incorrect value) to the ECU. (6) Confirm the message reception result of ECU by using the RAM monitor.
Measurement items	(a) Received message of the tester in the test procedure (2) (b) Message reception result of ECU in the test procedure (4) (c) Message reception result of ECU in the test procedure (6)
Pass/Fail Judgment	・ In the measurement item (a), the message from the ECU to the tester shall comply with the encryption and tamper detection algorithms defined by the ECU design dept. ・ Measurement item (b) shall be success. ・ In the Measurement item (c), the ECU shall drop the tampered message.
Remarks	—

【WLSTST_03006】 Updating the encryption key for communication channel encryption	
Test content	This test confirms that encryption key used to encrypt a channel is updated in the way to ensure its integrity and confidentiality.
Prerequisites	None
Test Procedure	(1) The ECU design dept. considers the proper test procedure to confirm that the encryption key used to encrypt a channel is updated in the way to ensure its integrity and confidentiality.
Measurement items	(a) Depend on the test procedure (1)
Pass/Fail Judgment	・ In the measurement item (a), the confidentiality and integrity of the encryption key shall be ensured.
Remarks	—

5.3.1.1.2. Evaluations for server

【WLSTST_03007】 Authentication for the connection counterpart	
Test content	・ This test confirms that the ECU authenticates a connection counterpart. ・ This test confirms that the ECU does not respond to the authentication counterpart if the authentication fails.
Prerequisites	None
Test Procedure	<Connection counterpart is authorized> (1) The tester requests authentication to the ECU using the correct confidential information. (2) Confirm the result which the ECU authenticates the tester by using the RAM monitor. <Connection counterpart is unauthorized> (3) The tester requests authentication to the ECU using the incorrect confidential information. (4) The tester obtains the communication from the ECU. (5) Confirm the result which the ECU authenticates the tester by using the RAM monitor.
Measurement items	(a) The authentication result of ECU in the test procedure (2) (b) Communication log in the test procedure (4) (c) The authentication result of ECU in the test procedure (5)
Pass/Fail Judgment	・ Measurement item (a) shall be success. ・ In the measurement item (b), the ECU shall not respond to the tester when authentication fails. ・ Measurement item (c) shall be failure.
Remarks	—

【WLSTST_03008】 Countermeasure against session hijacking	
Test content	This test confirms that the ECU prevents session hijacking by attackers.
Prerequisites	None
Test Procedure	(1) The ECU design dept. considers the proper test procedure to confirm the session hijacking countermeasure.
Measurement items	(a) Depend on the test procedure (1).
Pass/Fail Judgment	・ In the measurement item (a), the countermeasure against session hijacking shall be implemented.
Remarks	—

【WLSTST_03009】 Updating/Switching of Client Authentication Key	
Test content	This test confirms that the symmetric key is updated or switched in the way to ensure its integrity and confidentiality, if the ECU uses a symmetric key for client authentication.
Prerequisites	None
Test Procedure	(1) The ECU design dept. considers the proper test procedure to confirm the updating or switching process of client authentication key.
Measurement items	(a) Depend on the test procedure (1)
Pass/Fail Judgment	・ In the measurement item (a), the confidentiality and integrity of the client authentication key shall be ensured.
Remarks	—

【WLSTST_03010】 Encryption and tamper detection of communication channel	
Test content	・ This test confirms that the ECU encrypts the channel and detect tampering when connecting with outside of vehicle center or service. ・ This test confirms that the ECU drops the received message if the ECU detects a tampering of the received message from center.
Prerequisites	None
Test Procedure	<Encryption and tamper detection of communication channel> (1) The tester establishes wireless communication with the ECU. (2) The ECU transmits a message to the tester, and the tester obtains communication from the ECU.

	(3) The tester transmits a message applying the encryption and tamper detection algorithms which the ECU design dept. defines to the ECU. (4) Confirm the message reception result of ECU by using the RAM monitor. <Confirmation of tamper detection of message> (5) The tester transmits a tampered message (e.g., changing the message authentication code to the incorrect value) to the ECU. (6) Confirm the message reception result of ECU by using the RAM monitor.
Measurement items	(a) Received message of the tester in the test procedure (2) (b) Message reception result of ECU in the test procedure (4) (c) Message reception result of ECU in the test procedure (6)
Pass/Fail Judgment	・ In the measurement item (a), the message from the ECU to the tester shall comply with the encryption and tamper detection algorithms defined by the ECU design dept. ・ Measurement item (b) shall be success. ・ In the measurement item (c), the ECU shall drop the tampered message.
Remarks	—

【WLSTST_03011】 Updating the encryption key for communication channel encryption	
Test content	This test confirms that encryption key used to encrypt a channel is updated in the way to ensure its integrity and confidentiality.
Prerequisites	None
Test Procedure	(1) The ECU design dept. considers the proper test procedure to confirm that the encryption key used to encrypt a channel is updated in the way to ensure its integrity and confidentiality.
Measurement items	(a) Depend on the test procedure (1)
Pass/Fail Judgment	・ In the measurement item (a), the confidentiality and integrity of the encryption key shall be ensured.
Remarks	—

5.3.1.2.Evaluation for using TLS Communication

5.3.1.2.1. Evaluations for client

【WLSTST_04001】 Disabling the TLS compression function	
Test content	This test confirms that the ECU disables the TLS compression function.
Prerequisites	None
Test Procedure	(1) The ECU requests a TLS handshake to the tester. (2) The tester requests the ECU to use TLS compression function in the TLS handshake. (3) Confirm the TLS handshake result of ECU by using the RAM monitor.
Measurement items	(a) The TLS handshake result of ECU in the test procedure (3).
Pass/Fail Judgment	・ Measurement item (a) shall be failure.
Remarks	—

【WLSTST_04002】 Disabling the TLS renegotiation function	
Test content	This test confirms that the ECU disables the TLS renegotiation function.
Prerequisites	The ECU completes the evaluation of【WLSTST_04003】.
Test Procedure	(1) The ECU establishes a TLS session with the tester. (2) The tester transmits a TLS re-negotiation request to the ECU. (3) The tester obtains communication from the ECU.
Measurement items	(a) Response for the TLS re-negotiation request from the ECU in the test procedure (3).
Pass/Fail Judgment	・ In the measurement item (a), the TLS re-negotiation request shall be rejected.
Remarks	—

【WLSTST_04003】 Server authentication (TLS1.2 or later)	
Test content	・ This test confirms that the ECU performs server authentication in accordance with TLS standard (version 1.2 or later) sequence. ・ This test confirms that server authentication supports multi-layered authentication such as using intermediate CA.
Prerequisites	None
Test Procedure	<Connecting counterpart is unauthorized> (1) The ECU requests a TLS handshake to the tester. (2) The tester transmits the server certificate and the intermediate certificate which are rooted at incorrect root certificate to the ECU. (3) Confirm the server authentication result of the ECU by using the RAM monitor. <Expired server certificate> (4) The ECU requests a TLS handshake to the tester. (5) The tester transmits an expired server certificate to the ECU. (6) Confirm the server authentication of the ECU by using the RAM monitor. <Connecting counterpart is authorized> (7) The ECU requests a TLS handshake to the tester. (8) The tester transmits the server certificate and the intermediate certificate which are rooted at correct root certificate to the ECU. (9) Confirm the server authentication result of the ECU by using the RAM monitor.
Measurement items	(a) Server authentication result in the test procedure (3). (b) Server authentication result in the test procedure (6). (c) Server authentication result in the test procedure (9).
Pass/Fail Judgment	・ Measurement item (a) shall be failure. ・ Measurement item (b) shall be failure. ・ Measurement item (c) shall be success.
Remarks	—

【WLSTST_04004】 Disabling Server authentication (TLS1.1 and earlier)	
Test content	This test confirms that TLS 1.1 and earlier versions is disabled.
Prerequisites	・The ECU completes the evaluation of【WLSTST_04003】.
Test Procedure	<TLS version 1.0> (1) The ECU requests a TLS handshake to the tester. (2) The tester requests TLS version 1.0 to the ECU. (3) Confirm TLS handshake result of the ECU by using the RAM monitor. <TLS version 1.1> (4) The ECU requests a TLS handshake to the tester. (5) The tester requests TLS version 1.1 to the ECU. (6) Confirm TLS handshake result of the ECU by using the RAM monitor.
Measurement items	(a) TLS handshake result of the ECU in the test procedure (3). (b) TLS handshake result of the ECU in the test procedure (6).
Pass/Fail Judgment	・ Measurement item (a) shall be failure. ・ Measurement item (b) shall be failure.
Remarks	-

【WLSTST_04005】 Client authentication (TLS1.2or later)	
Test content	This test confirms that the ECU performs client authentication in one of the following ways when the ECU connects with Toyota center. -TLS (version 1.2 or later) standard sequence. -The sequence of Appendix A in the upper-level document [1].
Prerequisites	None
Test Procedure	＜In the case that TLS standard sequence is used for client authentication＞ (1) The ECU requests a TLS handshake to the tester. (2) The tester requests a client authentication to the ECU in accordance with the TLS standard sequence. (3) The tester obtains communication from the ECU. ＜In the case that Appendix A in the upper-level document [1] is used for client authentication＞ (4) The ECU requests a TLS handshake to the tester. (5) The tester requests a client authentication to the ECU in accordance with Appendix A in the upper-level document [1]. (6) The tester obtains communication from the ECU.
Measurement items	(a) Communication log in the test procedure (3). (b) Communication log in the test procedure (6).
Pass/Fail Judgment	・ In the measurement item (a), client authentication shall comply with the TLS standard (version 1.2 or later). ・ In the measurement item (b), client authentication shall comply with Appendix A in the upper-level document [1].
Remarks	―

【WLSTST_04006】 Protection for server authentication processing	
Test content	This test confirms that the ECU processes server authentication in anti-tampering area or secure area.
Prerequisites	None
Test Procedure	(1) The ECU requests a TLS handshake to the tester. (2) The tester performs the server authentication with the ECU. (3) The ECU design dept. considers the proper test procedure to confirm the memory area which the signature verification processing for server authentication in the ECU is being performed. However, it is possible to confirm the design specification only when it is difficult to confirm the processing in anti-tampering area or secure area in actual operation.
Measurement items	(a) Depend on the test procedure (2).
Pass/Fail Judgment	・ In the measurement item (a), the processing area shall be anti-tampering area or secure area.
Remarks	—

【WLSTST_04007】 Protection for client authentication processing	
Test content	This test confirms that the ECU shall processes operations for client authentication in anti-tampering area.
Prerequisites	None
Test Procedure	＜In the case that TLS standard sequence is used for client authentication＞ (1) The ECU requests a TLS handshake to the tester. (2) The tester requests a client authentication to the ECU in accordance with the TLS standard sequence. (3) The ECU design dept. considers the proper test procedure to confirm the memory area which the signature generation processing for client authentication in the ECU is being performed. However, it is possible to confirm the design specification only when it is difficult to confirm the processing in anti-tampering area in actual operation. ＜In the case that Appendix A in the upper-level document [1] is used for client authentication＞ (4) The ECU requests a TLS handshake to the tester. (5) The tester requests a client authentication to the ECU in accordance with Appendix A in the upper-level document [1]. (6) The ECU design dept. considers the proper test procedure to confirm the memory area which the generation processing for client authentication code (HMAC) in the ECU is being performed. However, it is possible to confirm the design specification only when it is difficult to confirm the processing in anti-tampering area in actual operation.
Measurement items	(a) Depend on the test procedure (3). (b) Depend on the test procedure (6).
Pass/Fail Judgment	・ Measurement item (a) shall be anti-tampering area ・ Measurement item (b) shall be anti-tampering area
Remarks	—

【WLSTST_04008】 Protection for the public key	
Test content	This test confirms that the public key (e.g. Root Certificate) is stored in the area ensured integrity.
Prerequisites	None
Test Procedure Measurement items Pass/Fail Judgment	Refer to 【VULCMN_51200】in the related document [2]. (Supplement) Public key (e.g. Root certificate) is PSP.
Remarks	—

【WLSTST_04009】 Protection for the private key used for client authentication	
Test content	This test confirms that private key used for client authentication is stored in anti-tampering area.
Prerequisites	None
Test Procedure Measurement items Pass/Fail Judgment	Refer to 【VULCMN_51200】, 【VULCMN_52000】 and 【VULCMN_52200】 in the related document [2]. (Supplement) The private key for client authentication is required to be CSP and tamper resistance.
Remarks	—

【WLSTST_04010】Encrypt and store private key in external memory	
Test content	This test confirms that the ECU encrypts the keys using a key stored in security-chip and stores the keys if it is difficult for the ECU to store private key in anti-tampering hardware due to the limitation of key storage size.
Prerequisites	None
Test Procedure Measurement items Pass/Fail Judgment	Refer to 【VULCMN_51200】 in the related document [2].
Remarks	—

【WLSTST_04011】 Switching the Root Certificate	
Test content	・This test confirms that the ECU supports both algorithms below for Root Certificates. -ECDSA/256 bits or more -RSA/3072 bits or more ・This test confirms that the ECU disables a Root certificate. ・This test confirms that the integrity of Root certificate switching is ensured.
Prerequisites	The ECU completes the evaluation of 【WLSTST_04003】.
Test Procedure	<Root certificates support both algorithms> (1) The ECU requests a TLS handshake to the tester. (2) The tester transmits the server certificate corresponding to RSA3072bit to the ECU. (3) Confirm the server authentication result of the ECU by using the RAM monitor. (4) The ECU requests a TLS handshake to the tester. (5) The tester transmits the server certificate corresponding to ECDSA256bit to the ECU. (6) Confirm the server authentication result of the ECU by using the RAM monitor. <Disabling a Root Certificate> (7) The tester disables a root certificate of the ECU in accordance with the procedure for disabling a root certificate defined by the ECU design dept. (8) The ECU request a TLS handshake to the tester. (9) The tester transmits the server certificate which roots the certificate disabled in the test procedure (7). (10) Confirm the server authentication result of the ECU by using the RAM monitor. < Integrity of disabling a root certificate> (11) The ECU design dept. considers the proper test procedure to confirm that the ECU does not accept a malicious disabling processing for a root certificate.
Measurement items	(a) Server authentication result of the ECU in test procedure (3). (b) Server authentication result of the ECU in test procedure (6). (c) Server authentication result of the ECU in test procedure (10). (d) Depend on the test procedure (11).
Pass/Fail Judgment	・ Measurement item (a) shall be success. ・ Measurement item (b) shall be success. ・ Measurement item (c) shall be failure. ・ In the Measurement item (d), the ECU does not accept the malicious disabling processing

	for a root certificate.
Remarks	—

【WLSTST_04012】 Server Certificate Revocation check	
Test content	This test confirms that the ECU verifies Client Certificate in accordance with the following certificate revocation criteria. In addition, the ECU does not authenticate the client if it has been invalid. Certificate revocation criteria: -Revocation status confirmation by Certificate Revocation List(CRL) or OCSP.
Prerequisites	・Server certificate revoked by CRL or OCSP is obtained.
Test Procedure	<Revoked server certificate> (1) The ECU requests a TLS handshake to the tester. (2) The tester transmits a revoked server certificate to the ECU. (3) Confirm the server authentication of the ECU by using the RAM monitor.
Measurement items	(a) Server authentication result in the test procedure (3).
Pass/Fail Judgment	・ Measurement item (a) shall be failure.
Remarks	—

【WLSTST_04013】 Tamper detection of communication (TLS1.2 or later)	
Test content	This test confirms that the ECU drops the received message if the ECU detects a tampering of the received message from center.
Prerequisites	None
Test Procedure	(1) The ECU establishes a TLS session with the tester. (2) The tester transmits a tampered message to the ECU. (3) Confirm the message reception result of the ECU by using the RAM monitor.
Measurement term	(a) Message reception result in the test procedure (3).
Pass/Fail Judgment	・ In the measurement item (a), the ECU shall drop the tampered message.
Remarks	—

5.3.1.2.2. Evaluations for server

【WLSTST_04014】 Disabling the TLS Compression function	
Test content	This test confirms that the ECU disables the TLS compression function.
Prerequisite	None
Test Procedure	(1) The tester requests the TLS compression function to the ECU in the TLS handshake. (2) The tester confirms the response of the ECU for the test procedure (1).
Measurement items	(a) The ECU response in the test procedure (2).
Pass/Fail Judgment	・ In the measurement item (a), the ECU shall not support TLS compression function.
Remarks	—

【WLSTST_04015】 Disabling the TLS Renegotiation function	
Test content	This test confirms that the ECU disables the TLS renegotiation function.
Prerequisites	The ECU completes the evaluation of 【WLSTST_04016】.
Test Procedure	(1) The tester requests a TLS renegotiation after the tester establishes a TLS session with the ECU. (2) The tester confirms the response from the ECU for the test procedure (1).
Measurement items	(a) The response in the test procedure (2).
Pass/Fail Judgment	・ In the measurement item (a), the ECU shall reject the TLS re-negotiation request.
Remarks	—

【WLSTST_04016】 Server authentication (TLS1.2 or later)	
Test content	・This test confirms that the ECU performs server authentication in accordance with TLS standard (version 1.2 or later) sequence. ・This test confirms that server authentication supports multi-layered authentication such as using intermediate CA.
Prerequisites	None
Test Procedure	(1) The tester requests a TLS handshake to the ECU. (2) The tester obtains communication from the ECU.
Measurement items	(a) Communication log in the test procedure (2).
Pass/Fail Judgment	・ In the measurement item (a), the server authentication shall comply with TLS standard (version 1.2 or later). ・ In the measurement item (a), the ECU shall respond to the tester with a server certificate and an intermediate certificate that root the correct root certificate.
Remarks	—

【WLSTST_04017】 Disabling Server authentication (TLS1.1 and earlier)	
Test content	This test confirms that TLS 1.1 and earlier versions are disabled.
Prerequisites	The ECU completes the evaluation of【WLSTST_04016】.
Test Procedure	<TLS version 1.0> (1) The tester requests TLS version 1.0 to the ECU in the TLS handshake. (2) Confirm TLS handshake result of the ECU by using the RAM monitor. <TLS version 1.1> (3) The tester requests TLS version 1.1 to the ECU in the TLS handshake. (4) Confirm TLS handshake result of the ECU by using the RAM monitor.
Measurement items	(a) The TLS handshake result of the ECU in the test procedure (2). (b) The TLS handshake result of the ECU in the test procedure (4).
Pass/Fail Judgment	・ Measurement item (a) shall be failure. ・ Measurement item (b) shall be failure.
Remarks	—

【WLSTST_04018】 Client authentication (TLS1.2 or later)	
Test content	This test confirms that the ECU performs client authentication with Toyota center using TLS version 1.2 or later.
Prerequisites	None
Test Procedure	<Connecting counterpart is authorized> (1) The tester performs client authentication using the correct client certificate with the ECU. (2) Confirm the client authentication result of the ECU by using the RAM monitor. <Connecting counterpart is unauthorized> (3) The tester performs client authentication using the incorrect client certificate with the ECU. (4) Confirm the client authentication result of the ECU by using the RAM monitor. <Expired client certificate> (5) The tester performs client authentication using the expired client certificate with the ECU. (6) Confirm the client authentication result of the ECU by using the RAM monitor.
Measurement items	(a) Client authentication result of the ECU in the test procedure (2). (b) Client authentication result of the ECU in the test procedure (4). (c) Client authentication result of the ECU in the test procedure (6).
Pass/Fail Judgment	・ Measurement item (a) shall be success. ・ Measurement item (b) shall be failure. ・ Measurement item (c) shall be failure.
Remarks	—

【WLSTST_04019】Protection for server authentication processing	
Test content	This test confirms that the ECU processes server authentication in anti-tampering area or secure area.
Prerequisites	None
Test Procedure	(1) The tester requests a TLS handshake to the ECU. (2) The ECU design dept. considers the proper test procedure to confirm the memory area which the signature verification processing for server authentication in the ECU is being performed. However, it is possible to confirm the design specification only when it is difficult to confirm the processing in anti-tampering area or secure area in actual operation.
Measurement items	(a) Depend on the test procedure (2).
Pass/Fail Judgment	・ In the measurement item (a), the processing area shall be anti-tampering area or secure area.
Remarks	—

【WLSTST_04020】Protection for client authentication processing	
Test content	This test confirms that the ECU processes operations for client authentication in anti-tampering area.
Prerequisites	None
Test Procedure	(1) The tester requests a TLS handshake to the ECU. (2) The ECU design dept. considers the proper test procedure to confirm the memory area which the signature generation processing for client authentication in the ECU is being performed. However, it is possible to confirm the design specification only when it is difficult to confirm the processing in anti-tampering area in actual operation.
Measurement items	(a) Depend on the test procedure (2).
Pass/Fail Judgment	・ In the measurement item (a), the processing area shall be anti-tampering area.
Remarks	—

【WLSTST_04021】 Protection for the public key	
Test content	This test confirms that the public key (e.g. Root Certificate) is stored in the area ensured integrity.
Prerequisites	None
Test Procedure Measurement items Pass/Fail Judgment	Refer to 【VULCMN_51200】in the related document [2]. (Supplement) Public key (e.g. Root certificate) is PSP.
Remarks	—

【WLSTST_04022】Protection for the private key used for client authentication	
Test content	This test confirms that private key used for client authentication is stored in anti-tampering area.
Prerequisites	None
Test Procedure Measurement items Pass/Fail Judgment	Refer to 【VULCMN_51200】, 【VULCMN_52000】 and 【VULCMN_52200】 in the related document [2]. (Supplement) The private key for client authentication is required to be CSP and tamper resistance.
Remarks	—

【WLSTST_04023】Encrypt and store private key in external memory	
Test content	This test confirms that the ECU encrypts the keys using a key stored in security-chip and stores the keys if it is difficult for the ECU to store private key and symmetric key in anti-tampering hardware due to the limitation of key storage size.
Prerequisites	None
Test Procedure Measurement items Pass/Fail Judgment	Refer to 【VULCMN_51200】 in the related document [2].
Remarks	—

【WLSTST_04024】Switching the Root Certificate	
Test content	・This test confirms that the ECU supports both algorithms below for Root Certificates. -ECDSA/256 bits or more -RSA/3072 bits or more ・This test confirms that the ECU disables a Root certificate. ・This test confirms that the integrity of Root certificate switching is ensured.
Prerequisites	The ECU completes the evaluation of 【WLSTST_04018】.
Test Procedure	<Root certificates support both algorithms> (1) The tester requests a TLS handshake to the ECU. (2) The tester transmits the client certificate corresponding to RSA3072bit to the ECU. (3) Confirm the client authentication result of the ECU by using the RAM monitor. (4) The tester requests a TLS handshake to the ECU. (5) The tester transmits the client certificate corresponding to ECDSA256bit to the ECU. (6) Confirm the client authentication result of the ECU by using the RAM monitor. <Disabling a Root Certificate> (7) The tester disables a root certificate of the ECU in accordance with the procedure for disabling a root certificate defined by the ECU design dept. (8) The tester requests a TLS handshake to the ECU. (9) The tester transmits the client certificate which roots the certificate disabled in the test procedure (7). (10) Confirm the client authentication result of the ECU by using the RAM monitor. < Integrity of disabling a root certificate> (11) The ECU design dept. considers the proper test procedure to confirm that the ECU does not accept a malicious disabling processing for a root certificate.
Measurement items	(a) The server authentication result of the ECU in test procedure (3). (b) The server authentication result of the ECU in test procedure (6). (c) The server authentication result of the ECU in test procedure (10). (d) Depend on the test procedure (11).
Pass/Fail Judgment	・ Measurement item (a) shall be success. ・ Measurement item (b) shall be success. ・ Measurement item (c) shall be failure. ・ In the measurement item (d), the ECU does not accept the malicious disabling processing for a root certificate.

Remarks	—

【WLSTST_04025】Client Certificate Revocation Invalid check	
Test content	This test confirms that the ECU verifies Client Certificate in accordance with the following certificate revocation criteria. In addition, the ECU does not authenticate the client if it has been invalid. Certificate revocation criteria: -Revocation status confirmation by Certificate Revocation List(CRL) or OCSP.
Prerequisites	・ Client certificate revoked by CRL or OCSP is obtained.
Test Procedure	<Revoked client certificate> (1) The tester requests a TLS handshake using the revoked client certificate to the tester. (2) Confirm the client authentication result of the ECU by using the RAM monitor.
Measurement items	(a) Client authentication result in the test procedure (2)
Pass/Fail Judgment	・ Measurement item (a) shall be failure.
Remarks	—

【WLSTST_04026】 Issuing a Server Certificate	
Test content	This test confirms that the ECU does not reuse current key information in ECU and generate a new private and public key pair when the ECU requests issuing and updating a Server Certificate.
Prerequisites	The server certificate (public key) stored in the ECU is obtained.
Test Procedure	(1) The tester requests to generate a public key and private key for server certificate to the ECU. (2) The evaluator issues and updates a server certificate using the public key generated in the test procedure (1) in accordance with the issuing and updating procedure defined by the ECU design dept. (3) The evaluator registers the server certificate issued in the test procedure (2) to the ECU. (4) The tester requests a TLS handshake to the ECU. (5) Confirm the server authentication result by using the tester.
Measurement items	(a) The public key generated in the test procedure (1). (b) The server authentication result in the test procedure (5).
Pass/Fail Judgment	・ Measurement item (a) shall be different from the public key before this test. ・ Measurement item (b) shall be success.
Remarks	The scope of this test is the ECU implemented the function to generate a public key and a private key for issuing and updating a server certificate.

【WLSTST_04027】Tamper detection of communication (TLS1.2 or later)	
Test content	This test confirms that the ECU drops the received message if the ECU detects a tampering of the received message from center.
Prerequisites	None
Test Procedure	(1) The ECU establishes a TLS session with the tester. (2) The tester transmits a tampered message to the ECU. (3) Confirm the message reception result of the ECU by using the RAM monitor.
Measurement term	(a) The message reception result in the test procedure (3).
Pass/Fail Judgment	・ In the measurement item (a), the ECU shall drop the tampered message.
Remarks	—

5.3.2. Evaluations related to Connection with Devices outside of vehicle except for Center

5.3.2.1. Evaluations for using except for Wi-Fi/Bluetooth

5.3.2.1.1. Evaluations for Client

【WLSTST_05001】 External Device Authentication	
Test content	・ This test confirms that the ECU authenticates each connection counterpart. ・ This test confirms that the ECU does not respond to the authentication counterpart if the authentication fails.
Prerequisites	None
Test Procedure	<Connection counterpart is authorized> (1) The ECU requests an authenticate to the tester. (2) The tester performs authentication with the ECU by using the correct confidential information. (3) Confirm the authentication result of the ECU for the test procedure (2) by using the RAM monitor. <Connection counterpart is unauthorized> (4) The ECU requests an authenticate to the tester. (5) The tester performs authentication with the ECU using the incorrect confidential information. (6) The tester obtains communication from the ECU. (7) Confirm the authentication result of the ECU for the test procedure (5) by using the RAM monitor.
Measurement items	(a) Authentication result of the ECU in the test procedure (3). (b) Communication log in the test procedure (6). (c) Authentication result of the ECU in the test procedure (7).
Pass/Fail Judgment	・ Measurement item (a) shall be success ・ In the measurement item (b), the response to the tester shall not be included. ・ Measurement item (c) shall be failure.
Remarks	—

【WLSTST_05002】 Encryption and tamper detection of communication channel	
Test content	・ This test confirms that the ECU encrypts the channel and detects tampering when

	connecting with outside of vehicle. ・ This test confirms that the ECU drops the received message if the ECU detects tampering of the received message from outside of vehicle.
Prerequisites	None
Test Procedure	<Encryption and tamper detection of communication channel> (1) The ECU completes the authentication with the tester. (2) The ECU transmits a message to the tester, and the tester obtains communication from the ECU. (3) The tester transmits a message applying the encryption and tamper detection algorithms which the ECU design dept. defines to the ECU. (4) Confirm the message reception result of ECU by using the RAM monitor. <Confirmation of tamper detection of message> (5) The tester transmits a tampered message (e.g., changing the message authentication code to the invalid value) to the ECU. (6) Confirm the message reception result of ECU by using the RAM monitor.
Measurement items	(a) Message from the ECU to the tester in the test procedure (2). (b) Message reception result of the ECU in the test procedure (4). (c) Message reception result of the ECU in the test procedure (6).
Pass/Fail Judgment	・ Measurement item (a) shall comply with the encryption and tamper detection algorithms defined by the ECU design dept. ・ Measurement item (b) shall be success. ・ Measurement item (c) shall be failure.
Remarks	—

5.3.2.1.2. Evaluations for server

【WLSTST_05003】 External Device Authentication	
Test content	・ This test confirms that the ECU authenticates each connection counterpart. ・ This test confirms that the ECU does not respond to the authentication counterpart if the authentication fails.
Prerequisites	None
Test Procedure	<Connection counterpart is authorized> (1) The tester requests an authentication to the ECU by using the correct confidential information. (2) Confirm the authentication result of the ECU for the test procedure (1) by using the RAM monitor. <Connection counterpart is unauthorized> (3) The tester requests an authentication to the ECU by using the incorrect confidential information. (4) The tester obtains communication from the ECU. (5) Confirm the authentication result of the ECU for the test procedure (1) by using the RAM monitor.
Measurement items	(a) Authentication result of the ECU in the test procedure (2). (b) Communication log in the test procedure (4) (c) Authentication result of the ECU in the test procedure (5).
Pass/Fail Judgment	・ Measurement item (a) shall be success. ・ In the measurement item (b), the response to the tester shall not be included. ・ Measurement item (c) shall be failure.
Remarks	—

【WLSTST_05004】 Encryption and tamper detection of communication channel	
Test content	・This test confirms that the ECU encrypts the channel and detects tampering when connecting with outside of vehicle. ・This test confirms that the ECU drops the received message if the ECU detects tampering of the received message from outside of vehicle.
Prerequisites	None
Test Procedure	<Encryption and tamper detection of communication channel> (1) The tester completes the authentication with the ECU. (2) The ECU transmits a message to the tester, and the tester obtains communication from the ECU. (3) The tester transmits a message applying the encryption and tamper detection algorithms which the ECU design dept. defines to the ECU. (4) Confirm the message reception result of ECU by using the RAM monitor. <Confirmation of tamper detection of message> (5) The tester transmits a tampered message (e.g., changing the message authentication code to the invalid value) to the ECU. (6) Confirm the message reception result of ECU by using the RAM monitor.
Measurement items	(a) Message from the ECU to the tester in the test procedure (2). (b) Message reception result of the ECU in the test procedure (4). (c) Message reception result of the ECU in the test procedure (6).
Pass/Fail Judgment	・ Measurement item (a) shall comply with the encryption and tamper detection algorithms defined by the ECU design dept. ・ Measurement item (b) shall be success. ・ In the measurement item (c), the ECU shall drop the tampered message.
Remarks	—

5.3.2.2.Evaluations for using Wi-Fi

5.3.2.2.1. Evaluations for client

【WLSTST_06001】 Using WPA2 or later	
Test content	・ This test confirms that the ECU uses WPA2 or later (WPA2, WPA3) standards. ・ This test confirms that the ECU does not connect with WEP and WPA ・ This test confirms that the ECU supports WPA3. ・ This test confirms that the ECU supports IEEE 802.11w.
Prerequisites	None
Test Procedure	＜WEP＞ (1) The tester (Access Point) transmits a WEP-enabled beacon information. (2) Confirm whether the ECU permits to connect with the tester in the test procedure (1). ＜WPA＞ (3) The tester (Access Point) transmits a WPA-enabled beacon information. (4) Confirm whether the ECU permits to connect with the tester in the test procedure (3). ＜WPA3＞ (5) The tester (Access Point) transmits a WPA3-enabled beacon information. (6) Confirm whether the ECU permits to connect with the tester in the test procedure (5). (7) The ECU request an authentication of WPA3 with the tester. (8) The tester obtains communication from ECU. ・ Perform the following test procedures only if the ECU supports WPA2. ＜WPA2＞ (9) The tester (Access Point) transmits a WPA2-enabled beacon information. (10)Confirm whether the ECU permits to connect with the tester in the test procedure (9). (11)The ECU request an authentication of WPA2 with the tester. (12)The tester obtains communication from ECU.
Measurement items	(a) Status of Wi-Fi connection with the tester in the test procedure (2). (b) Status of Wi-Fi connection with the tester in the test procedure (4). (c) Status of Wi-Fi connection with the tester in the test procedure (6). (d) Communication log in the test procedure (8). (e) Status of Wi-Fi connection with the tester in the test procedure (10). (f) Communication log in the test procedure (12).
Pass/Fail	・ In the measurement item (a), the ECU shall not permit connection with the tester.

Judgment	・ In the measurement item (b), the ECU shall not permit connection with the tester. ・ In the measurement item (c), the ECU shall permit connection with the tester. ・ In the measurement item (d), the ECU shall request using IEEE802.11w. ・ In the measurement item (e), the ECU shall permit connection with the tester. ・ In the measurement item (f), the ECU shall request using IEEE802.11w.
Remarks	—

【WLSTST_06002】 Tamper detection of communication (Wi-Fi)	
Test content	This test confirms that the ECU drops the received message if the ECU detects a tampering of the received message from outside of the vehicle.
Prerequisites	The ECU completes evaluation of 【WLSTST_06001】
Test Procedure	(1) The ECU completes the authentication of WPA2 or later with the tester. (2) The tester transmits a tampered message (e.g., changing the message authentication code to the invalid value) to the ECU. (3) Confirm the message reception result of ECU by using the RAM monitor.
Measurement items	(a) Message reception result of the ECU in the test procedure (3).
Pass/Fail Judgment	・ In the measurement item (a), the ECU shall drop the tampered message.
Remarks	—

5.3.2.2.2. Evaluations for server

【WLSTST_06003】	Using WPA2 or later
Test content	・ This test confirms that the ECU uses WPA2 or later (WPA2, WPA3) standards. ・ This test confirms that the ECU does not connect with WEP and WPA. ・ This test confirms that the ECU supports WPA3. ・ This test confirms that the ECU supports IEEE 802.11w.
Prerequisites	None
Test Procedure	＜In the case that the ECU transmits a beacon information＞ (1) The ECU transmits a beacon information. (2) The tester confirms the beacon information from the ECU. ＜In the case that the ECU does not transmit a beacon information＞ (3) The tester transmits a probe request to the ECU. (4) The tester receives a probe response from the ECU.
Measurement items	(a) Beacon information of the ECU in the test procedure (2). (b) Probe response from ECU in the test procedure (4).
Pass/Fail Judgment	・ In the measurement item (a), WEP and WPA shall not be supported, and WPA3 shall be supported, and the status of WPA2 support shall match the setting defined by the ECU design dept., and the ECU shall request using IEEE802.11w. ・ In the measurement item (b), WEP and WPA shall not be supported, and WPA3 is supported, and the status of WPA2 support matches the setting defined by the ECU design dept., and the ECU requests using IEEE802.11w.
Remarks	—

【WLSTST_06004】	Changing a confirmation information of WPA-PSK
Test content	・ This test confirms that when a user changes the default PSK, it satisfies the followings: -The number of character strings is 8 and more. -If the user changes to a password which does not satisfy 【WLSREQ_00360】, the ECU notifies the risk of it.
Prerequisites	None

Test Procedure	<In the case that the ECU design dept. permits changing to a password which does not satisfy 【WLSREQ_00360】 in the upper-level document [1]> (1) Request changing to a password which satisfies 【WLSREQ_00360】 in the upper-level document [1] to the ECU. (2) Confirm the result of changing password in the test procedure (1). (3) Request changing to a password which does not satisfy 【WLSREQ_00360】 in the upper-level document [1] and satisfies the number of character strings is 8 and more to the ECU. (4) Confirm the result of changing password and the presence or absent of risk notification for the user in the test procedure (3). (5) Request changing to a password which the number of character strings is 7 and less to the ECU. (6) Confirm the result of changing password in the test procedure (5). < In the case that the ECU design dept. does not permit changing to a password which does not satisfy 【WLSREQ_00360】 in the upper-level document [1] > (7) Request changing to a password which satisfies 【WLSREQ_00360】 in the upper-level document [1] to the ECU. (8) Confirm the result of changing password in the test procedure (1). (9) Request changing to a password which does not satisfy 【WLSREQ_00360】 in the upper-level document [1] and satisfies the number of character strings is 8 and more to the ECU. (10) Confirm the result of changing password and the presence or absent of risk notification for the user in the test procedure (3). (11) Request changing to a password which the number of character strings is 7 and less to the ECU. (12) Confirm the result of changing password in the test procedure (5).
Measurement items	(a) Result of changing password in the test procedure (2) (b) Result of changing password and presence or absent of risk notify in the test procedure (4) (c) Result of changing password in the test procedure (6) (d) Result of changing password in the test procedure (8) (e) Result of changing password in the test procedure (10) (f) Result of changing password in the test procedure (12)
Pass/Fail Judgment	・ Measurement item (a) shall be success. ・ In the measurement item (b), result of changing password shall be success and risk notification shall be presence.

	・ Measurement item (c) shall be failure. ・ Measurement item (d) shall be success. ・ Measurement item (e) shall be failure. ・ Measurement item (f) shall be failure.
Remarks	—

【WLSTST_06005】 Tamper detection of communication (Wi-Fi)	
Test content	This test confirms that the ECU drops the received message if the ECU detects a tampering of the received message from outside of the vehicle.
Prerequisites	None
Test Procedure	(1) The tester completes the authentication of WPA2 or later with the ECU. (2) The tester transmits a tampered message (e.g., changing the message authentication code to the invalid value) to the ECU. (3) Confirm the message reception result of ECU by using the RAM monitor.
Measurement items	(a) Message reception result of the ECU in the test procedure (3).
Pass/Fail Judgment	・ In the measurement item (a), the ECU shall drop the tampered message.
Remarks	—

5.3.2.3.Evaluations for using Bluetooth

5.3.2.3.1. Evaluations for client

【WLSTST_07001】 Bluetooth implementation guide	
Test content	This test confirms that Bluetooth function is developed based on NIST SP800-121（Guide to Bluetooth Security） to prevent intrusion to in-vehicle devices by using malicious communication via Bluetooth.
Prerequisites	None
Test Procedure	(1) The ECU requests pairing to the tester. (2) The tester obtains communication from the ECU.
Measurement items	(a) All Recommended Practice items in Bluetooth Security Check List of NIST SP800-121 for the communication log in the test procedure (2).
Pass/Fail Judgment	・ All items of measurement items (a) shall be passed.
Remarks	—

【WLSTST_07002】 Bluetooth authentication method	
Test content	This test confirms that In-vehicle Bluetooth function of the ECU pairs external devices by using SSP mode (in the case of Classic) or LE Secure Connection mode (in the case of LE).
Prerequisites	None
Test Procedure	<In the case that the ECU supports Bluetooth Classic> (1) The ECU requests a pairing to the tester. (2) The tester obtains communication from the ECU. <In the case that the ECU supports Bluetooth LE> (3) The ECU requests a pairing to the tester. (4) The tester obtains communication from the ECU.
Measurement items	(a) Communication log in the test procedure (2). (b) Communication log in the test procedure (4).
Pass/Fail Judgment	・ In the measurement item (a), the ECU shall request only SSP mode in the pairing request. ・ In the measurement item (b), the ECU shall request only LE Secure connection mode in the pairing request.
Remarks	—

【WLSTST_07003】 Tamper detection of communication (Bluetooth)	
Test content	This test confirms that the ECU drops the received message if the ECU detects a tampering of the received message from outside of the vehicle.
Prerequisites	None
Test Procedure	(1) The ECU completes the pairing with the tester. (2) The tester transmits a tampered message (e.g., changing the message authentication code to the invalid value) to the ECU. (3) Confirm the message reception result of ECU by using the RAM monitor.
Measurement items	(a) Message reception result in the test procedure (3).
Pass/Fail Judgment	・ In the measurement item (a), the ECU shall drop the tampered message.
Remarks	—

5.3.2.3.2. Evaluations for server

【WLSTST_07004】 Bluetooth implementation guide	
Test content	This test confirms that Bluetooth function is developed based on NIST SP800-121（Guide to Bluetooth Security） to prevent intrusion to in-vehicle devices by using unauthorized communication via Bluetooth.
Prerequisites	None
Test Procedure	(1) The tester requests pairing to the ECU. (2) The tester obtains communication from the ECU.
Measurement items	(a) All Recommended Practice items in Bluetooth Security Check List of NIST SP800-121 for the communication log in the test procedure (2).
Pass/Fail Judgment	・ All items of measurement items (a) shall be passed.
Remarks	-

【WLSTST_07005】 Bluetooth authentication method	
Test content	・This test confirms that In-vehicle Bluetooth function of the ECU pairs external devices by using SSP mode (in the case of Classic) or LE Secure Connection mode (in the case of LE). ・This test confirms that in-vehicle Bluetooth function of the ECU authenticates the Bluetooth pairing request.
Prerequisites	None
Test Procedure	<In the case that the ECU supports Bluetooth Classic> (1) The tester requests a pairing with PIN mode of Bluetooth authentication method to the ECU. (2) Confirm the pairing result of the ECU by using the RAM monitor. (3) The tester requests a pairing with SSP mode and “except for Just Works” of Bluetooth authentication method to the ECU. (4) The tester obtains communication from the ECU. (5) The tester requests a pairing with SSP mode and “Just Works” of Bluetooth authentication method to the ECU. (6) Confirm the pairing result of the ECU by using the RAM monitor.

	<In the case that the ECU supports Bluetooth LE > (7) The tester requests a pairing with LE Secure Connection mode of Bluetooth authentication method to the ECU. (8) The tester obtains communication from the ECU. (9) The tester requests a pairing with LE Legacy Pairing mode of Bluetooth authentication method to the ECU. (10) Confirm the pairing result of the ECU by using the RAM monitor.
Measurement items	(a) Pairing result of the ECU in the test procedure (2). (b) Communication log in the test procedure (4). (c) Pairing result of the ECU in the test procedure (6). (d) Communication log in the test procedure (8). (e) Pairing result of the ECU in the test procedure (10).
Pass/Fail Judgment	・ In the measurement item (a), the ECU shall reject the pairing request from the tester. ・ In the measurement item (b), Bluetooth authentication method shall be SSP mode. ・ In the measurement item (c), the ECU shall reject the pairing request from the tester. ・ In the measurement item (d), Bluetooth authentication method shall be LE Secure connection mode. ・ In the measurement item (e), the ECU shall reject the pairing request from the tester.
Remarks	—

【WLSTST_07006】 Tamper detection of communication (Bluetooth)	
Test content	This test confirms that the ECU drops the received message if the ECU detects a tampering of the received message from outside of the vehicle.
Prerequisites	None
Test Procedure	(1) The ECU completes the pairing with the tester. (2) The tester transmits a tampered message (e.g., changing the message authentication code to the invalid value) to the ECU. (3) Confirm the message reception result of ECU by using RAM monitor.
Measurement items	(a) Message reception result in the test procedure (3).
Pass/Fail Judgment	・ In the measurement item (a), the ECU shall drop the tampered message.
Remarks	—