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 /

標準リプログラミングセキュリティ評価仕様書

Test Specification of Standard Reprogramming 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-RPR-TST-SPEC-a01-03-a

承認 Approved	調査 Checked	作成 Created	2022/12/22
平林	松井	玉樹	Omission of signature (approved electronically)

適用先 Target	標準リプログラミング/OTA リプログラミングを実施する ECU ECUs that implementing standard reprogramming or OTA reprogramming
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。 If necessary, please expand to affiliated companies and departments (overseas business entities, body manufacturers, ECU suppliers). 【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
a01-00-a	新規作成	2020/6/26	46F 早川
a01-01-a	要件全体の修正	2021/12/23	46F 早川
	英訳追加		
a01-02-a	表紙の変更	2022/10/20	46F 安江
	上位文書の更新(Version の更新(No1)) 関連文書の更新(主管の更新(No2, No8)。No9 追加)		
	合否判定の誤り修正 (RPRTST_00017, RPRTST_00018)		
	評価の実施方法を関連文書を参照する記載に変更 (RPRTST_00010, RPRTST_00014)		
	表 3.1 の更新		
a01-03-a	参照先の要件を追加（RPRTST_00019）	2022/11/01	46F 玉樹

目次

2. はじめに

2.1. 本書の目的

リプログラミング機能を悪用する攻撃に対し、リプログラミングセキュリティ対策を導入する。

本書では、標準リプログラミングセキュリティ機能が要求通りに動作していることを確認するための評価方法を定義する。

2.2. 適用範囲

本書の適用範囲は、標準リプログラミングセキュリティ要求仕様書にもとづいて標準リプログラミングセキュリティ対策を実施する ECU とする。

2.3. 要求事項の記載

【RPRTST_*****】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。

2.4. 前提条件

特になし。

2.5. 上位文書

表 2-1 上位文書

No	仕様書	Ver(最新版を適用ください)	主管
1	標準リプログラミングセキュリティ要求仕様書	SEC-ePF-RPR-REQ-SPEC-a01-07-*	46F

2.6. 関連文書

表 2-2 関連文書

No	仕様書	Ver(最新版を適用ください)	主管
1	(欠番)	―	―
2	Wired Reprogramming Specification Flash Bootloader Software	wrfbs-*****-***-*	46F
3	(欠番)	―	―
4	(欠番)	―	―
5	共通脆弱性対策要求仕様書	SEC-ePF-VUL-CMN-REQ-SPEC-***-**-*	46F
6	(欠番)	―	―
7	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
8	Wired Reprogramming Evaluation Specification Flash Bootloader Software	wr-evl***-***-*	46F
9	Diagnostic design specification UDS Protocol -Evaluation-	diaguds-evl***-***-*	46F

3. 評価概要

評価項目の一覧を表 3.1 に示す。

表 3.1 標準リプログラミングセキュリティの試験項目一覧

要求仕様書	評価仕様書		
ID	ID	評価項目がない理由	生産時機能
RPRREQ_00001	RPRTST_00001	－	－
RPRREQ_00002	－	車両外システムへの要求のため	－
RPRREQ_00003	RPRTST_00001	－	－
RPRREQ_00004	RPRTST_00006	－	－
RPRREQ_00005	－	車両外システムへの要求のため	－
RPRREQ_00006	RPRTST_00006	－	－
RPRREQ_00007	RPRTST_00006	－	－
RPRREQ_00008	－	運用に関する要求のため	－
RPRREQ_00009	RPRTST_00017	－	－
RPRREQ_00010	－	要求事項が欠番のため	－
RPRREQ_00011	RPRTST_00006	－	－
RPRREQ_00012	－	車両外システムへの要求のため	－
RPRREQ_00013	RPRTST_00006	－	－
RPRREQ_00014	RPRTST_00006	－	－
RPRREQ_00015	－	要求事項が欠番のため	－
RPRREQ_00016	－	要求事項が欠番のため	－
RPRREQ_00017	RPRTST_00006	－	－
RPRREQ_00018	RPRTST_00018	－	－
RPRREQ_00019	RPRTST_00018	－	－
RPRREQ_00020	RPRTST_00018	－	－
RPRREQ_00021	RPRTST_00007	－	－
RPRREQ_00022	RPRTST_00010	－	－
RPRREQ_00023	RPRTST_00010	－	－
RPRREQ_00024	RPRTST_00010	－	－
RPRREQ_00025	－	要求事項が欠番のため	－
RPRREQ_00026	－	要求事項が欠番のため	－
RPRREQ_00027	RPRTST_00010	－	－
RPRREQ_00028	RPRTST_00014	－	－
RPRREQ_00029	－	運用に関する要求のため	－

要求仕様書	評価仕様書		
ID	ID	評価項目がない理由	生産時機能
RPRREQ_00030	－	車両外システムへの要求のため	－
RPRREQ_00031	RPRTST_00001, RPRTST_00006	－	－
RPRREQ_00032	－	車両外システムへの要求のため	－
RPRREQ_00033	－	車両外システムへの要求のため	－
RPRREQ_00034	－	車両外システムへの要求のため	－
RPRREQ_00037	－	運用に関する要求のため	－
RPRREQ_00038	－	運用に関する要求のため	－
RPRREQ_00039	－	運用に関する要求のため	－
RPRREQ_00040	－	車両外システムへの要求のため	－
RPRREQ_00041	RPRTST_00006		－
RPRREQ_00042	－	車両開発後の要求のため	－
RPRREQ_00043	RPRTST_00018	－	－
RPRREQ_00044	RPRTST_00019	－	－
RPRREQ_00045	RPRTST_00001	－	－
RPRREQ_00046	RPRTST_00001	－	－
RPRREQ_00047	－	車両外システムへの要求のため	－
RPRREQ_00048	RPRTST_00001	－	－
RPRREQ_00049	RPRTST_00006	－	－
RPRREQ_00050	－	運用に関する要求のため	－

【RPRTST_00001】～【RPRTST_00019】の合否判定を全て満たす場合、合格と判定すること。なお、以下の ID は欠番である。

RPRTST_00002, 00003, 00004, 00005, 00008, 00009, 00011, 00012, 00013, 00015, 00016

4. 評価環境

評価環境は図 4-1 を用いる。

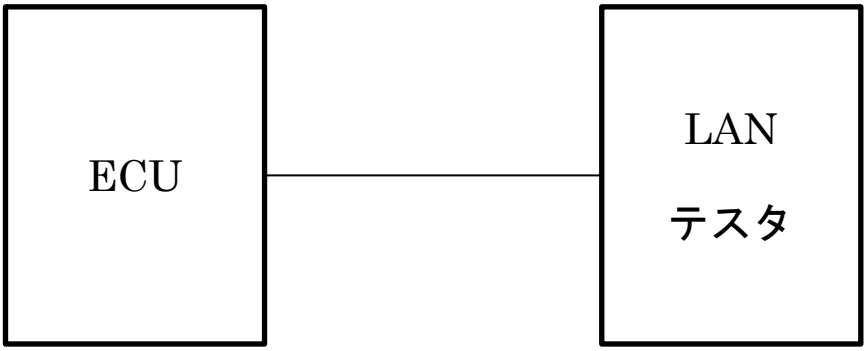

図 4-1　評価環境

注(1) LAN テスタは CANoe(Vector)を想定している。

注(2) 他仕様を参照している評価項目に関しては、参照先の評価環境に準ずること。

5. 評価詳細

5.1. リプログラミングツール認証

【RPRTST_00001】 ツール認証評価	
試験内容	リプログラミングツール認証が正常に動作することを確認する。
事前条件	・LAN テスタは、入力される Seed 値に対して正しい Key 値を生成できる。 (Key 値生成方法は上位文書[1]参照) ・LAN テスタで使用するツール認証キーと同じ鍵が ECU に書き込まれている
試験手順	関連文書[8] SecurityAccess(SID27)に関する評価項目参照
測定項目	
合否判定	
備考	LAN テスタの正しい入出力の組み合わせ例 ・入力 ツール認証キー：0xF0E1D2C3B4A5968778695A4B3C2D1E0F Seed：0x0123456789ABCDEF0123456789ABCDEF ・出力 Key：0x3C98617360B249907EC507605881DDE9

5.2. 書き込みプログラムの復号・改ざん検知

(補足)復号機能単独での評価が困難であるため、復号後の改ざん検知が想定通りの動作をすることで、間接的に復号が正しく完了していることを確認する。

【RPRTST_00006】復号・改ざん検知評価	
試験内容	復号・改ざん検知が正常に動作することを確認する。
事前条件	・復号、改ざん検知機能が動作する設定となっている。(動作条件は上位文書[1]参照) ・リプロ対象のプログラムの暗号化、署名生成が完了している。 ・プログラム暗号化に使用したシステムキーと同じ鍵と、プログラム署名生成に使用した署名生成キーに対応する署名検証キーが、ECU に書き込まれている。
試験手順	関連文書[8] RoutineControl(SID31)に関する評価項目参照
測定項目	
合否判定	
備考	なし。

【RPRTST_00007】改ざん検知評価(改ざん検知時の動作)	
試験内容	改ざんを検知した時に、アプリケーションソフトウェアが動作しないことを確認する。
事前条件	・【RPRTST-00006】の評価が完了している。
試験手順	(1) 不正な署名のファイルを使用して、改ざんを検知した状態にする。

	(関連文書[8] RoutineControl(SID31)の routineControlOptionRecord が Invalid となっているファイルを用いた評価項目を完了させる) (2) ECU を再起動する。
測定項目	(a) (2)のリプロ対象アプリケーションソフトウェアの起動有無
合否判定	■判断基準 ● 測定項目(a)で、アプリケーションソフトウェアが起動しないこと
備考	「アプリケーションソフトウェアが起動しないこと」に関する具体的な確認方法までは言及しない。「本来動作するはずの制御機能が動作しないこと」などで確認すること。

【RPRTST_00017】 復号動作条件

試験内容	復号動作条件が正しいことを確認する。
事前条件	・改ざん検知機能が動作する設定となっている。(動作条件は上位文書[1]参照) ・リプロ対象のプログラムの暗号化、署名生成が完了している。
試験手順	(1) LAN テスタから送信する平文/暗号文通知を平文として、平文のプログラムを用いて、関連文書[2]の RoutineControl(checkMemoryFlashdriver)までの処理を実施する。 (2) 関連文書[2]の RoutineControl(checkMemoryFlashdriver)以降の処理を実施する。(妥当性検証の動作有無は任意) (3) LAN テスタから送信する平文/暗号文通知を平文として、暗号文のプログラムを用いて、関連文書[2]の RoutineControl(checkMemoryFlashdriver)までの処理を実施する。
測定項目	(a) (1)の RoutineControl(checkMemoryFlashdriver)のレスポンス (b) (3)の RoutineControl(checkMemoryFlashdriver)のレスポンス
合否判定	■判断基準 ● 測定項目(a)が以下となること。

A_Data_byte	Parameter	Byte Value
#1	routineControl Response SID	0x71
#2	routineControlType = startRoutine	0x01
#3	routineIdentifier[byte#1](MSB)	0xDD
#4	routineIdentifier[byte#2](LSB)	0x00
#5	routineInfo	0x02
#6	routineStatusRecord[routineStatus #1](checkStatus)	0x02
#7	routineStatusRecord[routineStatus #2](failedCause)	0x00

● 測定項目(b)が以下となること。

A_Data_byte	Parameter	Byte Value

	#1	routineControl Response SID	0x71
	#2	routineControlType = startRoutine	0x01
	#3	routineIdentifier[byte#1](MSB)	0xDD
	#4	routineIdentifier[byte#2](LSB)	0x00
	#5	routineInfo	0x02
	#6	routineStatusRecord[routineStatus #1](checkStatus)	0x01
	#7	routineStatusRecord[routineStatus #2](failedCause)	0x02
備考	平文でのプログラム書き込みを実施しない場合は、本評価の省略を許容する。 RoutineControl(checkMemoryFlashdriver)での評価が困難な場合は、 RoutineControl(checkMemorySoftware/Data)で代替しても良い。		

【RPRTST_00018】 改ざん検知動作条件

試験内容	改ざん検知動作条件が正しいことを確認する。
事前条件	・リプロ対象のプログラムの署名生成が完了している。
試験手順	(1) 暗号化フラグ(セキュリティプロパティ#1)を評価パターンに従って設定する。 (2) 関連文書[2]の RoutineControl(checkMemoryFlashdriver)までの処理を実施する。 その際、checkTypeIdentifier、checkData は評価パターンに従って設定する。 (3) 関連文書[2]の RoutineControl(checkMemoryFlashdriver)以降の処理を実施する。 (妥当性検証の動作有無は任意) (4) 以下の全ての評価パターンに対して、試験手順(1)~(3)を繰り返し実施する。

評価パターン

No.	暗号化フラグ	checkTypeIdentifier	checkData
1	ON	0x01	正しい署名
2	ON	0x01	不正な署名
3	ON	0x01 以外	checkTypeIdentifier に従った正しい値
4	OFF	0x01	正しい署名
5	OFF	0x01	不正な署名
6	OFF	0x01 以外	checkTypeIdentifier に従った正しい値

測定項目	(a) (2)の RoutineControl (checkMemoryFlashdriver)のレスポンス
合否判定	■判断基準 ● 各評価パターンで、測定項目(a)が以下となること。

No.	RoutineControl (checkMemoryFlashdriver) のレスポンス

1	ポジティブレスポンス(verificationSuccess)
2	ポジティブレスポンス(verificationFailed)
3	ポジティブレスポンス(verificationFailed)
4	ポジティブレスポンス(verificationSuccess)
5	ポジティブレスポンス(verificationFailed)
6	ポジティブレスポンス(verificationSuccess)

ポジティブレスポンス(verificationSuccess)

A_Data_byte	Parameter	Byte Value
#1	routineControl Response SID	0x71
#2	routineControlType = startRoutine	0x01
#3	routineIdentifier[byte#1](MSB)	0xDD
#4	routineIdentifier[byte#2](LSB)	0x00
#5	routineInfo	0x02
#6	routineStatusRecord[routineStatus #1](checkStatus)	0x02
#7	routineStatusRecord[routineStatus #2](failedCause)	0x00

ポジティブレスポンス(verificationFailed)

A_Data_byte	Parameter	Byte Value
#1	routineControl Response SID	0x71
#2	routineControlType = startRoutine	0x01
#3	routineIdentifier[byte#1](MSB)	0xDD
#4	routineIdentifier[byte#2](LSB)	0x00
#5	routineInfo	0x02
#6	routineStatusRecord[routineStatus #1](checkStatus)	0x01
#7	routineStatusRecord[routineStatus #2](failedCause)	0x01 or 0x02

備考	市場利用しない評価パターンに関しては、省略することを許容する。 RoutineControl(checkMemoryFlashdriver)での評価が困難な場合は、 RoutineControl(checkMemorySoftware/Data)で代替しても良い。

5.3. 書き込みプログラムバージョン情報妥当性検証

【RPRTST_00010】妥当性検証	
試験内容	妥当性検証機能が正常に動作することを確認する。
事前条件	・妥当性検証機能が動作する設定となっている。(動作条件は上位文書[1]参照) ・ECU に書き込まれているプログラムより新しいバージョンのプログラムが用意でき

	ている。 ・ECU に書き込まれているプログラムより古いバージョンのプログラムが用意できている。
試験手順 測定項目	関連文書[8] TC_WR 4.7.1.4_1, TC_WR 4.7.1.4_2, TC_WR 4.7.1.7_1, TC_WR 4.7.1.7_2 参照。
合否判定	■判断基準 ● 関連文書[8] TC_WR 4.7.1.4_1, TC_WR 4.7.1.4_2 および TC_WR 4.7.1.7_1, TC_WR 4.7.1.7_2 参照。 ● TC_WR 4.7.1.7_1 および TC_WR 4.7.1.7_2 実施後、アプリケーションソフトウェアが起動しないこと。
備考	「アプリケーションソフトウェアが起動しないこと」に関する具体的な確認方法までは言及しない。「本来動作するはずの制御機能が動作しないこと」などで確認すること。

5.4. その他の要求

【RPRTST_00014】フェールセーフの確認	
試験内容	車両が動いている相当の状態で、通信停止要求を行い、要求を受け付けないことを確認する。
事前条件 試験手順 測定項目 合否判定	関連文書[9] TC_UDS.7.5.2.4 参照
備考	なし。

5.5. 非機能要求

【RPRTST_00019】 乱数評価	
試験内容	SEED に使用する乱数のエントロピー値が要求値を満た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[5]【VULCMN_50200】,【VULCMN_50300】参照
測定項目	(a) エントロピー値
合否判定	■判断基準 ● 測定項目(a)が 40bit 以上であること。
備考	なし。

1. Revision Record

Version	Changes	Date	Revised
a01-00-a	Initial release	Jun. 26, 2020	46F Hayakawa
a01-01-a	Modify the overall requirement	Dec. 23, 2021	46F Hayakawa
	Add English translation		
a01-02-a	Update cover page	Oct. 20, 2022	46F Yasue
	Update Upper-Level Document (change Version column No1) Update Releated Document (change Issued column(No2, No8), Add No9)		
	Modify the Pass/fail determination (RPRTST_00017, RPRTST_00018)		
	Change test execution method to reference Related Document (RPRTST_00010, RPRTST_00014)		
	Update Table 3.1		
a01-03-a	Add reference requirement (RPRTST_00019)	Nov. 01, 2022	46F Tamaki

Contents

2. Introduction

2.1. Purpose of this Specification

Reprogramming security measures are introduced against attacks misusing the reprogramming function.

This specification defines evaluation methods to confirm that the standard reprogramming security function is operating in accordance with the requirements.

2.2. Scope

This specification covers ECUs performing standard reprogramming security measures in accordance with the Requirements Specification of Standard Reprogramming Security.

2.3. Description of Requirement Items

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

2.4. Precondition

None.

2.5. Upper-Level Documents

Table 2-1: **Upper-Level Documents**

No.	Specification	Version (use the latest version)	Issued
1	Requirements Specification of Standard Reprogramming Security	SEC-ePF-RPR-REQ-SPEC-a01-07-*	46F

2.6. Related Documents

Table 2-2: **Related Documents**

No.	Specification	Version (use the latest version)	Issued
1	(Deleted)	-	-
2	Wired Reprogramming Specification Flash Bootloader Software	wrfbs-*****-***-*	46F
3	(Deleted)	-	-
4	(Deleted)	-	-
5	Requirements Specification of Common Vulnerability Countermeasure	SEC-ePF-VUL-CMN-REQ-SPEC-***-**-*	46F
6	(Deleted)	-	-
7	Teams and Definitions related to Vehicle Cybersecurity and Privacy	SEC-ePF-TRM-GUD-PROC-***-**-*	46F
8	Wired Reprogramming Evaluation Specification Flash Bootloader Software	wr-evl***-***-*	46F
9	Diagnostic design specification UDS Protocol -Evaluation-	diaguds-evl***-***-*	46F

3. Evaluation Outline

Table 3.1 lists the evaluation items.

Table 3.1 : List of Standard Reprogramming Security Evaluation Items

Requirement Specification	Test Specification		
ID	ID	Reason for no evaluation items	Production-time function
RPRREQ_00001	RPRTST_00001	—	—
RPRREQ_00002	—	For requirement to outside vehicle systems	—
RPRREQ_00003	RPRTST_00001	—	—
RPRREQ_00004	RPRTST_00006	—	—
RPRREQ_00005	—	For requirement to outside vehicle systems	—
RPRREQ_00006	RPRTST_00006	—	—
RPRREQ_00007	RPRTST_00006	—	—
RPRREQ_00008	—	For requirement related to operations	—
RPRREQ_00009	RPRTST_00017	—	—
RPRREQ_00010	—	For deleted requirements	—
RPRREQ_00011	RPRTST_00006	—	—
RPRREQ_00012	—	For requirement to outside vehicle systems	—
RPRREQ_00013	RPRTST_00006	—	—
RPRREQ_00014	RPRTST_00006	—	—
RPRREQ_00015	—	For deleted requirements	—
RPRREQ_00016	—	For deleted requirements	—
RPRREQ_00017	RPRTST_00006	—	—
RPRREQ_00018	RPRTST_00018	—	—
RPRREQ_00019	RPRTST_00018	—	—
RPRREQ_00020	RPRTST_00018	—	—
RPRREQ_00021	RPRTST_00007	—	—
RPRREQ_00022	RPRTST_00010	—	—
RPRREQ_00023	RPRTST_00010	—	—
RPRREQ_00024	RPRTST_00010	—	—
RPRREQ_00025	—	For deleted requirements	—
RPRREQ_00026	—	For deleted requirements	—
RPRREQ_00027	RPRTST_00010	—	—
RPRREQ_00028	RPRTST_00014	—	—
RPRREQ_00029	—	For requirement related to operations	—
RPRREQ_00030	—	For requirement to outside vehicle systems	—

Requirement Specification	Test Specification		
ID	ID	Reason for no evaluation items	Production-time function
RPRREQ_00031	RPRTST_00001, RPRTST_00006	—	—
RPRREQ_00032	—	For requirement to outside vehicle systems	—
RPRREQ_00033	—	For requirement to outside vehicle systems	—
RPRREQ_00034	—	For requirement to outside vehicle systems	—
RPRREQ_00037	—	For requirement related to operations	—
RPRREQ_00038	—	For requirement related to operations	—
RPRREQ_00039	—	For requirement related to operations	—
RPRREQ_00040	—	For requirement to outside vehicle systems	—
RPRREQ_00041	RPRTST_00006		—
RPRREQ_00042	—	For requirement after vehicle development	—
RPRREQ_00043	RPRTST_00018	—	—
RPRREQ_00044	RPRTST_00019	—	—
RPRREQ_00045	RPRTST_00001	—	—
RPRREQ_00046	RPRTST_00001	—	—
RPRREQ_00047	—	For requirement to outside vehicle systems	—
RPRREQ_00048	RPRTST_00001	—	—
RPRREQ_00049	RPRTST_00006	—	—
RPRREQ_00050	—	For requirement related to operations	—

The test is passed if the pass/fail conditions are met for each of **RPRTST_00001** to **RPRTST_00019**. The following IDs are deleted.

RPRTST_00002, 00003, 00004, 00005, 00008, 00009, 00011, 00012, 00013, 00015, 00016

4. Evaluation Environment

Use the evaluation environment shown in Fig. 4-1.

Fig. 4-1: **Evaluation Environment**

Note 1: CANoe (Vector) is assumed for the LAN tester.

Note 2: Regarding test items making reference to other specifications, follow the evaluation environment defined in the reference specifications.

5. Evaluation Details

5.1. Reprogramming Tool Authentication

RPRTST_00001: Tool authentication evaluation	
Test content	This test confirms that reprogramming tool authentication operates correctly.
Prerequisites	・LAN tester can generate the correct Key value for the input Seed value. (Refer to upper-level document [1] for how to generate the Key value) ・The same key as the tool authentication key used by the LAN tester is written to the ECU.
Test procedure Measurement item Pass/fail determination	Refer to evaluation item of SecurityAccess(SID27) in related document [8]
Remarks	Example of correct input/output combination of LAN tester - Input Tool authentication key: 0xF0E1D2C3B4A5968778695A4B3C2D1E0F Seed: 0x0123456789ABCDEF0123456789ABCDEF - Output Key: 0x3C98617360B249907EC507605881DDE9

5.2. Program Decryption and Tampering Detection

(Supplement) It is difficult to separately evaluate the decryption function. Therefore, if tampering detection operates as expected after decryption, this means it is indirectly confirmed that the decryption has been correctly completed.

RPRTST_00006: Decryption and tampering detection evaluation	
Test content	This test confirms that decryption and tampering detection operate correctly.
Prerequisites	・Decryption and tamper detection function are set to operate. (Refer to upper-level document [1] for operation conditions) ・Encryption and signature generation of reprogramming program are completed. ・The same system key used for program encryption, and the signature verification key that corresponds to the signature generation key used for program signnature generation are written to the ECU.
Test procedure Measurement item Pass/fail determination	Refer to evaluation item of SecurityAccess(SID31) in related document [8]
Remarks	None.

RPRTST_00007: Tampering detection evaluation (Operation if tampering is detected)	
Test content	This test confirms that the application software does not operate if tampering is detected .
Prerequisites	・Evaluation of **RPRTST_00006** has been completed.
Test procedure	(1) Use an unauthorized signature to make the state of tampering detected. (Complete the evaluation item using the file in which routineControlOptionRecord of RoutineControl (SID31) described in related document [8] is Invalid.) (2) Restart the ECU.
Measurement item	(a) Whether or not the application software target for reprogramming in (2) starts.
Pass/fail determination	■ Decision criteria ● The application software shall not start in measurement item (a).
Remarks	This specification will not specifically describe how to confirm that “the application software does not start”. Pass/fail determination may be made, for example, by confirming that control functions that should operate do not operate.

RPRTST_00017: Decryption operating conditions	
Test content	This test confirms that decryption operating conditions is correct.
Prerequisites	・Tamper detection function are set to operate. (Refer to upper-level document [1] for operation conditions) ・Encryption and signature generation of reprogramming program is completed.
Test procedure	(1) Set plaintext/ciphertext notification sent from the LAN tester to plaintext, and use plaintext program to carry out the process up to RoutineControl(checkMemoryFlashdriver) described in related document [2]. (2) Carry out the process after RoutineControl(checkMemoryFlashdriver) described in related document [2]. (Whether the validation function operates or not is optional) (3) Set plaintext/ciphertext notification sent from the LAN tester to plaintext and use ciphertext program to carry out the process up to RoutineControl(checkMemoryFlashdriver) described in related document [2].
Measurement item	(a) Response of RoutineControl(checkMemoryFlashdriver) in (1) (b) Response of RoutineControl(checkMemoryFlashdriver) in (3)
Pass/fail determination	■ Decision criteria ● Measurement item (a) shall be as follows

A_Data_byte	Parameter	Byte Value
#1	routineControl Response SID	0x71
#2	routineControlType = startRoutine	0x01
#3	routineIdentifier[byte#1](MSB)	0xDD

	#4 routineIdentifier[byte#2](LSB) 0x00 #5 routineInfo 0x02 #6 routineStatusRecord[routineStatus #1](checkStatus) 0x02 #7 routineStatusRecord[routineStatus #2](failedCause) 0x00 ● Measurement item (b) shall be as follows A_Data_byte / Parameter / Byte Value #1 routineControl Response SID 0x71 #2 routineControlType = startRoutine 0x01 #3 routineIdentifier[byte#1](MSB) 0xDD #4 routineIdentifier[byte#2](LSB) 0x00 #5 routineInfo 0x02 #6 routineStatusRecord[routineStatus #1](checkStatus) 0x01 #7 routineStatusRecord[routineStatus #2](failedCause) 0x02
Remarks	If the program is not written in plaintext, it is permissible to omit this evaluation. If it is difficult to evaluate with RoutineControl(checkMemoryFlashdriver), it can be substituted with RoutineControl(checkMemorySoftware/Data).

RPRTST_00018: Tampering detection operating conditions	
Test content	This test confirms that tampering detection operating conditions is correct.
Prerequisites	・Signature generation of reprogramming program is completed.
Test procedure	(1) Set an encryption flag (security property #1) according to evaluation patterns. (2) Carry out the process up to RoutineControl(checkMemoryFlashdriver) described in related document [2]. In this case, set the checkTypeIdentifier and checkData according to evaluation patterns. (3) Carry out the process after RoutineControl(checkMemoryFlashdriver) described in related document [2]. (Whether the validation function operates or not is optional) (4) Repeat test procedure (1) to (3) for all of the following evaluation patterns. Evaluation Patterns No. / Encryption flag / checkTypeIdentifier / checkData 1 ON 0x01 Correct signature 2 ON 0x01 Unauthorized signature 3 ON Except 0x01 Correct value according

				to checkTypeIdentifier
	4	OFF	0x01	Correct signature
	5	OFF	0x01	Unauthorized signature
	6	OFF	Except 0x01	Correct value according to checkTypeIdentifier

Measurement item: (a) Response of RoutineControl(checkMemoryFlashdriver) in (2)

Pass/fail determination

■ Decision criteria

- Measurement item (a) shall be as follows in each evaluation patterns.

No.	Response to RoutineControl (checkMemoryFlashdriver) service
1	Positive response(verificationSuccess)
2	Positive response(verificationFailed)
3	Positive response(verificationFailed)
4	Positive response(verificationSuccess)
5	Positive response(verificationFailed)
6	Positive response(verificationSuccess)

Positive response(verificationSuccess)

A_Data_byte	Parameter	Byte Value
#1	CommunicationControl Response SID	0x71
#2	routineControlType = startRoutine	0x01
#3	routineIdentifier[byte#1] (MSB)	0xDD
#4	routineIdentifier[byte#2] (LSB)	0x00
#5	routineInfo	0x02
#6	routineStatusRecord[routineStatus #1](checkStatus)	0x02
#7	routineStatusRecord[routineStatus #2](failedCause)	0x00

Positive response(verificationFailed)

A_Data_byte	Parameter	Byte Value
#1	routineControl Response SID	0x71
#2	routineControlType = startRoutine	0x01
#3	routineIdentifier[byte#1](MSB)	0xDD
#4	routineIdentifier[byte#2](LSB)	0x00
#5	routineInfo	0x02
#6	routineStatusRecord[routineStatus #1](checkStatus)	0x01
#7	routineStatusRecord[routineStatus #2](failedCause)	0x01 or

			0x02
Remarks	Evaluation patters not used in the field is permissible to omit. If it is difficult to evaluate with RoutineControl(checkMemoryFlashdriver), it can be substituted with RoutineControl(checkMemorySoftware/Data).		

5.3. Version Information Validation of Writing Program

RPRTST_00010: Validation evaluation	
Test content	This test confirms that the validation function operates correctly.
Prerequisites	・Validation function are set to operate. (Refer to upper-level document [1] for operation conditions) ・The newer version program than the program being written to ECU is available. ・The older version program than the program being written to ECU is available.
Test procedure Measurement item	Refer to TC_WR 4.7.1.4_1, TC_WR 4.7.1.4_2, TC_WR 4.7.1.7_1 and TC_WR 4.7.1.7_2 in Related Documet[8].
Pass/fail determination	■ Decision criteria ● Refer to TC_WR 4.7.1.4_1, TC_WR 4.7.1.4_2, TC_WR 4.7.1.7_1 and TC_WR 4.7.1.7_2 in Related Documet[8]. ● The application software shall not start after TC_WR 4.7.1.7_1 and TC_WR 4.7.1.7_2 execution.
Remarks	This specification will not specifically describe how to confirm that “the application software does not start”. Pass/fail determination may be made, for example, by confirming that control functions that should operate do not operate.

5.4. Other Requirement

RPRTST_00014: Fail-safe confirmation	
Test content	This test confirms that the communication stop request does not accept if the vehicle is in motion.
Prerequisites Test procedure Measurement item Pass/fail determination	Refer to TC_UDS.7.5.2.4 in Related Document[9].
Remarks	None.

5.5. Non-Functional Requirement

RPRTST_00019: Random number evaluation	
Test content	This test confirms that random numbers used for the SEED satisfy the requirements.
Prerequisites	None.
Test procedure	Refer to [VULCMN_50200] and [VULCMN_50300] in Related Document [5].
Measurement item	(a) Entropy value
Pass/fail determination	■ Decision criteria ● Measurement item (a) shall be 40 bits or higher.
Remarks	None.