関係各部署　御中

To departments concerned

Confidentiality classification	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 /

セキュアブート評価仕様書
Requirements Specification of Secure Boot

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
System Network & Architecture Development Dept. 4G
E/E Architecture Development Div.

No. SEC-ePF-IDS-SBT-TST-SPEC-a01-02-a

承認 Approved by	調査 Checked by	作成 Created by	
平林	平井 宮内	古川	2023/03/31

適用先 Target	本書の適用条件は別文書にて定義される The condition to apply this document are defined by another document.
特記 Special note	【展開規則　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 System Network & Architecture Development Dept. E/E Architecture Development Div. Contact for Security Inquiries email: epf-sec-sp@mega.tec.toyota.co.jp

変更履歴

Version	変更内容	日付	変更者
a01-00-a	SEC-19PF-SBT-TST-SPEC-a00-00-a をベースに Post19 向けに新規作成	2021/04/05	46F 4G 松本
a01-00-b	英訳を追加	2021/05/14	46F 4G 松本
a01-01-a	・要求削除に追従し評価項目削除（SBTTST_00008 削除） ・表 2.1 のトレーサビリティを更新 ・SBTTST_00204 追加	2021/12/24	46F 4G 松本
a01-01-b	・誤記修正	2022/06/09	46F 4G 竹山
a01-02-a	・表 2.1 のトレーサビリティを更新 ・SBTTST_00204 修正 ・SBTTST_00205 追加	2023/03/31	46F 4G 古川

目次

1. はじめに

1.1. 本書の目的

本書では、セキュアブート要求仕様書（上位文書[1]）によって定義された要件を評価する為の評価要件を定義する。

1.2. 適用範囲

本書の適用範囲は、セキュアブート要求仕様書にもとづいてセキュアブートを実施する ECU とする。

1.3. 前提条件

なし

1.4. 要求事項の記載

【SBTTST_*****】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。

1.5. 関連文書

上位文書、参照文書、参考文書を示す。なお、関連文書のバージョンは ECU の要求仕様書に従うこと。

1.5.1. 上位文書

表 1-1 上位文書

No	文書名	Ver
1	セキュアブート要求仕様書	最新版
2	共通脆弱性対策要件書	最新版

1.5.2. 参照文書

表 1-2 参照文書

No	文書名	Ver
-	-	-

1.5.3. 参考文書

表 1-3 参考文書

No	文書名	Ver
–	–	–

2. 評価概要

2.1. 評価環境

セキュアブート機能は、ハードウェアやソフト構成により実現手段が異なり、実機評価が困難な要求があることから実機評価が困難な場合に限り、設計確認による評価を許容する。

図 2-1 に実機評価における評価環境を示す。

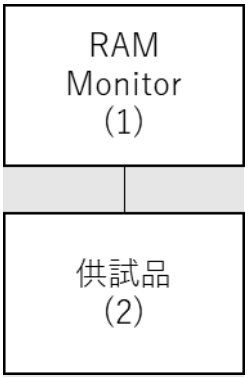

図 2-1 評価環境

注(1) RAM モニタはデバッガ装置を想定。

注(2)供試品は原則納入用のハードウェア、ソフトウェアにて構成されること。

2.2. 評価項目一覧

評価項目の一覧を表 2.1 に示す。

表 2.1 セキュアブートの試験項目一覧

分類	試験番号	試験項目	対応する要求
ソフトウェアの完全性検証	SBTTST_00001	RoT 確認 1	SBTREQ_00001
	SBTTST_00002	RoT 確認 2	SBTREQ_00001
	SBTTST_00003	RoT 確認 3	SBTREQ_00001
	SBTTST_00004	起動時の動作確認	SBTREQ_00003
	SBTTST_00005	完全性検証プログラム 1	SBTREQ_00002 SBTREQ_00004 SBTREQ_00008
	SBTTST_00006	完全性検証プログラム 2	SBTREQ_00002 SBTREQ_00005～00008
	SBTTST_00007	バックグラウンド検証 1	SBTREQ_00007
	SBTTST_00009	起動時間制約への影響確認	SBTREQ_01002
	SBTTST_00010	一時的故障対応	SBTREQ_00009

	SBTTST_00011	リプログラミング時の動作確認 1	SBTREQ_00011
	SBTTST_00012	リプログラミング時の動作確認 2	SBTREQ_00011
	SBTTST_00013	セキュアブート NG 時動作 1	SBTREQ_00010
	SBTTST_00014	セキュアブート NG 時動作 2	SBTREQ_00010
	SBTTST_00015	暗号アルゴリズムの確認	SBTREQ_00012
	SBTTST_00016	WakeUp 時の動作確認 1	SBTREQ_00013 SBTREQ_00014
	SBTTST_00017	WakeUp 時の動作確認 2	SBTREQ_00013 SBTREQ_00014
ソフトウェアの完全性検証失敗時の外部通知	SBTTST_00101	ECU 解析	SBTREQ_00101
鍵運用	SBTTST_00201	共通鍵の確認 1	SBTREQ_01102
	SBTTST_00202	共通鍵の確認 2	SBTREQ_01103
	SBTTST_00203	公開鍵の確認	SBTREQ_01103
	SBTTST_00204	鍵運用の確認 1	SBTREQ_01104
	SBTTST_00205	鍵運用の確認 2	SBTREQ_01003

上記試験項目のうち、対象となる項目の合否判定を全て満たす場合、合格と判定すること。

（※）SBTREQ_01101 は号口で使用する共通鍵/秘密鍵が漏洩した場合の要件であり、「開発後の要求」に該当するため本書の試験対象外とする。

3. 評価要求

以下に評価要求を定義する

3.1. ソフトウェアの完全性検証

【SBTTST_00001】 RoT 確認 1	
試験内容	RoT 内のソフトウェアの完全性検証プログラムが書き換え不可であることを確認する
試験方法	設計確認 or 実機評価
事前条件	なし
試験手順	【実機評価の場合】 1. RoT 内のソフトウェアの完全性検証プログラムが書き込まれている領域を読み込み 2. RoT 内のソフトウェアの完全性検証プログラムが書き込まれている領域を書き込み（1 とは異なるプログラム） 3. RoT 内のソフトウェアの完全性検証プログラムが書き込まれている領域を読み込み
測定項目	なし
合否判定	【設計確認の場合】 以下の設計情報に基づき試験内容が確認できること ・RoT 内のソフトウェアの完全性検証プログラムの保存場所と保存場所のメモリ特性 【実機評価の場合】 1 で取得したソフトウェアの完全性検証プログラムと、3 で取得したソフトウェアの完全性検証プログラムが等しいこと
備考	なし。

【SBTTST_00002】 RoT 確認 2	
試験内容	【共通鍵暗号方式の場合のみ】 ① 共通鍵が書き換え不可であることを確認する。 ただしセキュリティ的に保護された書き換え処理は除く。 （例：SHE プロトコルに従った鍵値の書き換え） ② RoT 以外から読み取りできないことを確認する
試験方法	① 設計確認 or 実機評価 ② 設計確認
事前条件	なし
試験手順	【実機評価の場合】 1. 共通鍵が書き込まれている領域を読み込み 2. 共通鍵が書き込まれている領域を書き込み 3. 共通鍵が書き込まれている領域を読み込み
測定項目	なし
合否判定	① 【設計確認の場合】 以下の設計情報に基づき試験内容①が確認できること ・共通鍵の保存場所と保存場所のメモリ特性 【実機評価の場合】 1 で取得された値と、3 で取得された値が等しいこと ② 以下の設計情報に基づき試験内容②が確認できること ・共通鍵の保存場所と保存場所のメモリ特性
備考	なし。

【SBTTST_00003】 RoT 確認 3	
試験内容	【公開鍵暗号方式の場合のみ】 公開鍵または公開鍵のハッシュ値が書き換え不可であることを確認する。 ただしセキュリティ的に保護された書き換え処理は除く。
試験方法	設計確認 or 実機評価
事前条件	なし
試験手順	【実機評価の場合】 1. 公開鍵 or 公開鍵のハッシュ値が書き込まれている領域を読み込み 2. 公開鍵 or 公開鍵のハッシュ値が書き込まれている領域を書き込み 3. 公開鍵 or 公開鍵のハッシュ値が書き込まれている領域を読み込み
測定項目	なし
合否判定	【設計確認の場合】 以下の設計情報に基づき試験内容が確認できること ・公開鍵 or 公開鍵のハッシュ値の保存場所と保存場所のメモリ特性 【実機評価の場合】 1 で取得された値と、3 で取得された値が等しいこと
備考	なし。

【SBTTST_00004】 起動時の動作確認	
試験内容	ECU 起動またはリセット時、ソフトウェア起動前に RoT 内の完全性検証プログラムを起動することを確認する
試験方法	設計確認 or 実機評価
事前条件	なし
試験手順	【実機評価の場合】 1. デバッガで RoT 内の完全性検証プログラムの先頭番地にブレークポイントを設定する 2. デバッガの設定をプログラムの実行履歴を残す状態にしたうえで、今までの履歴を消去する 3. プログラムを実行し、ブレークポイントでの実行停止を促す
測定項目	なし
合否判定	【設計確認の場合】 以下の設計情報に基づき試験内容が確認できること ・リセット解除後、最初に起動されるプログラムを決定する仕組み ・リセット解除後、最初に起動されるプログラムが配置されている領域 【実機評価の場合】 3 の結果として、プログラムの実行履歴には何も実行履歴がない、またはリセットベクタを参照したこと以外には何も残っていないこと
備考	なし。

【SBTTST_00005】 完全性検証プログラム 1	
試験内容	最初に起動するソフトウェア(RoT 内の完全性検証プログラムの次に起動するソフトウェア)が RoT 内の完全性検証プログラムで検証されることを確認する
試験方法	設計確認
事前条件	なし
試験手順	なし
測定項目	なし
合否判定	以下の設計情報に基づき試験内容が確認できること ・RoT 内の完全性検証プログラムを利用した検証と起動後における検証対象となるソフトウェアの呼び出し順序
備考	なし。

【SBTTST_00006】 完全性検証プログラム 2	
試験内容	RoT に保管された完全性検証プログラムを利用した検証から順々に検証のチェーンが組まれていることを確認する
試験方法	設計確認
事前条件	なし
試験手順	なし
測定項目	なし
合否判定	以下の設計情報に基づき試験内容が確認できること ・RoT 内の完全性検証プログラムを利用した検証と起動後における検証ソフトウェアの呼び出し順序
備考	なし。

【SBTTST_00007】 バックグラウンド検証 1	
試験内容	【バックグランド検証を実施する場合のみ】 バックグラウンド検証が実施されていることの確認
試験方法	実機評価
事前条件	なし
試験手順	1. バックグラウンド検証の対象ソフトウェアを改ざん 2. ECU を起動
測定項目	なし
合否判定	2 の結果としてバックグラウンド検証で検証エラーとなり、検証エラー時の動作（機能縮退等）となること
備考	なし。

【SBTTST_00009】 起動時間制約への影響確認	
試験内容	ECU 起動時間等の性能制約に影響を与えていないことを確認する
試験方法	設計確認
事前条件	なし
試験手順	なし
測定項目	なし
合否判定	以下の設計情報に基づき試験内容が確認できること ・ECU 起動時間制約 ・ECU 起動時間(最悪ケース)
備考	なし。

【SBTTST_00010】一時的故障対応	
試験内容	一時的な故障を考慮した検証リトライもしくは ECU リセットが行われることを確認する
試験方法	設計確認
事前条件	なし
試験手順	なし
測定項目	なし
合否判定	以下の設計情報に基づき試験内容が確認できること ・検証リトライもしくは ECU リセットを行う必要のある検証処理 ・検証リトライもしくは ECU リセットを行う設計箇所
備考	なし。

【SBTTST_00011】リプログラミング時の動作確認 1	
試験内容	【共通鍵暗号方式の場合のみ】 該当ソフトウェアに対する MAC が書き込めているか確認する。 書き込んだ MAC を使用してソフトウェアの完全性を検証しているか確認する。
試験方法	実機評価
事前条件	なし
試験手順	1.ECU を起動 2.リプロ実施(ソフトウェアと MAC を更新) 3.ECU を再起動
測定項目	なし
合否判定	1 でリプロ対象ソフトが起動すること 3 でリプロ対象ソフトが起動すること
備考	なし。

【SBTTST_00012】リプログラミング時の動作確認 2	
試験内容	【公開鍵暗号方式の場合のみ】 該当ソフトウェアに対するデジタル署名が書き込めているか確認する。 書き込んだデジタル署名を使用してソフトウェアの完全性を検証しているか確認する。
試験方法	実機評価
事前条件	なし
試験手順	1.ECU を起動 2.リプロ実施(ソフトウェアとデジタル署名を更新) 3.ECU を再起動
測定項目	なし
合否判定	1 でリプロ対象ソフトが起動すること 3 でリプロ対象ソフトが起動すること
備考	なし。

【SBTTST_00013】セキュアブート NG 時動作 1	
試験内容	完全性検証に失敗した制御ソフトウェアが起動しないことを確認する。 制御ソフトウェア以外は、お客様の安全に影響がない動作になっていることを確認する。
試験方法	設計確認
事前条件	なし
試験手順	なし
測定項目	なし
合否判定	以下の設計情報に基づき試験内容が確認できること ・完全性検証失敗時の動作
備考	なし。

【SBTTST_00014】セキュアブート NG 時動作 2	
試験内容	【バックグランド検証を実施する場合のみ】 バックグラウンド検証失敗時、お客様の安全に影響がない動作になっていることを確認する。
試験方法	設計確認
事前条件	なし
試験手順	なし
測定項目	なし
合否判定	以下の設計情報に基づき試験内容が確認できること ・バックグラウンド検証失敗時の動作
備考	なし。

【SBTTST_00015】暗号アルゴリズムの確認	
試験内容	要件(SBTREQ_00012)で指定された暗号アルゴリズムが使用されていることを確認する。
試験方法	設計確認
事前条件	なし
試験手順	なし
測定項目	なし
合否判定	以下の設計情報に基づき試験内容が確認できること ・使用する暗号アルゴリズム(鍵長含む)
備考	なし。

【SBTTST_00016】WakeUp 時の動作確認 1	
試験内容	【WakeUp 時にソフトウェアの完全性検証を実施する場合のみ】 WakeUp 時にソフトウェアの完全性検証を実施しているか確認する。
試験方法	実機評価
事前条件	なし
試験手順	1.ECU を起動 2.ECU 起動中に MAC or デジタル署名を更新せずリプロ 3.Sleep 要因発生 4.WakeUp 要因発生
測定項目	なし
合否判定	4 でソフトウェアの完全性検証が失敗すること
備考	なし。

【SBTTST_00017】WakeUp 時の動作確認 2	
試験内容	【WakeUp 時にバックグラウンド検証を実施する場合のみ】 WakeUp 時にバックグラウンドを実施しているか確認する。
試験方法	実機評価
事前条件	なし
試験手順	1.ECU を起動 2.ECU 起動中にリプロ バックグラウンド検証対象部分：MAC or デジタル署名を更新しない バックグラウンド検証対象部分以外：MAC or デジタル署名を更新する 3.Sleep 要因発生 4.WakeUp 要因発生
測定項目	なし
合否判定	4 でバックグラウンド検証が失敗すること
備考	なし。

3.2. ソフトウェアの完全性検証失敗時の外部通知

【SBTTST_00101】ECU 解析	
試験内容	ECU 解析によりソフトウェア完全性検証に失敗していることが判定できること
試験方法	設計確認
事前条件	なし
試験手順	なし
測定項目	なし
合否判定	以下の設計情報に基づき試験内容が確認できること ・ECU 解析手段
備考	なし。

3.3. 鍵運用

【SBTTST_00201】共通鍵の確認 1	
試験内容	【共通鍵暗号方式の場合のみ】 リプログラミングの共通鍵とソフトウェアの完全性検証の共通鍵は、異なる鍵を使うことを確認する
試験方法	設計確認
事前条件	なし
試験手順	なし
測定項目	なし
合否判定	以下の設計情報に基づき試験内容が確認できること ・リプログラミングの共通鍵の生成手順 ・ソフトウェアの完全性検証の共通鍵の生成手順
備考	なし。

【SBTTST_00202】共通鍵の確認 2	
試験内容	【共通鍵暗号方式の場合のみ】 ソフトウェア完全性検証で使用する共通鍵はソフト品番ごとに異なっていることを確認する
試験方法	設計確認
事前条件	なし
試験手順	なし
測定項目	なし
合否判定	以下の設計情報に基づき試験内容が確認できること ・ソフトウェア完全性検証で使用する共通鍵の生成手順
備考	なし。

【SBTTST_00203】公開鍵の確認	
試験内容	【公開鍵暗号方式の場合のみ】 ソフトウェア完全性検証で使用する公開鍵、秘密鍵は ECU×サプライヤ×マイコン型式で１つになっているか確認する
試験方法	設計確認
事前条件	なし
試験手順	なし

測定項目	なし
合否判定	以下の設計情報に基づき試験内容が確認できること ・ソフトウェア完全性検証で使用する公開鍵、秘密鍵の生成手順
備考	なし。

【SBTTST_00204】鍵運用の確認 1	
試験内容	セキュアブートで使用する鍵の生成者を確認する
試験方法	設計確認
事前条件	なし
試験手順	セキュアブートで使用する鍵の生成者が記載された資料を確認する
測定項目	セキュアブートで使用する鍵の生成者を確認する
合否判定	鍵の生成者が、ECU 設計部署が決めた生成者になっていること。
備考	なし。

【SBTTST_00205】鍵運用の確認 2	
試験内容	セキュアブートで使用する鍵の乱数性を確認する
試験方法	関連文書[2]の VULCMN_50200、VULCMN_50300 に従う
事前条件	↑
試験手順	↑
測定項目	↑
合否判定	↑
備考	なし。

Revision Record

Version	Contents of revision	Date	Revised
a01-00-a	New for Post19 based on SEC-19PF-SBT-TST-SPEC-a00-00-a	2021/04/05	46F 4G Matsumoto
a01-00-b	Add English translation.	2021/05/14	46F 4G Matsumoto
a01-01-a	- Delete a test item (SBTTST_00008) - Update traceability (Table 2-1) - Add a test item (SBTTST_00204)	2021/12/24	46F 4G Matsumoto
a01-01-b	- Editorial errors corrected	2022/06/09	46F 4G Takeyama
a01-02-a	- Traceability (Table 2-1) updated - SBTTST_00204 modified - SBTTST_00205 added	2023/03/31	46F 4G Furukawa

Table of Contents

1. Introduction

1.1. Purpose of this Document

This document defines the evaluation requirements for evaluating the requirements defined by the Secure Boot Requirements Specification (Upper Document [1]).

1.2. Scope of this Document

This document shall apply to an ECU to which secure boot is to be introduced.

1.3. Prerequisites

None

1.4. Description of requirements

Requirements of this document are described as 【SISBT_*****】

Such a description as “(note)” are not a requirement but a just note.

1.5. Related Documents

The parent document, the reference document, and the reference document are shown. The version of the relevant document must conform to the requirements specifications of the ECU.

1.5.1. Higher-level document

Table 1-1 Top Documents1

No	Document name	Ver
1	Requirements Specification of Secure Boot	Latest version
2	Requirements Specification of Common Vulnerability Countermeasure	Latest version

1.5.2. Referenced document

Table 1-2 References2

No	Document name	Ver
-	-	-

1.5.3. Reference document

Table 1-3. Reference Documentation3

No	Document name	Ver
-	-	-

2. 2. Summary of Evaluation

2.1. Evaluation environment

Some of requirements may be difficult to test on the hardware because the implementation way of secure boot depends on hardware or on software architecture. In this case, design check is acceptable for test method.

The test environment on the hardware is shown in Figure 2-1

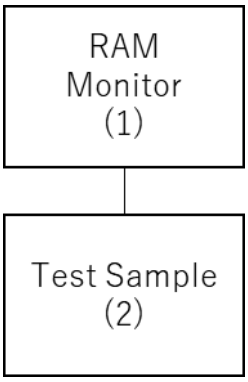

Figure 2-1 Test Environment

Note (1): A debugger device is assumed as the RAM monitor.

Note (2): The test sample shall be in principle composed of hardware and software to be delivered.

2.2. Test Item List

The test item list is shown in Table 2-1.

Table 2-1 List of Test Items

Classification	Test number	Test Item	Corresponding request
Software integrity validation	SBTTST_00001	Verification of RoT-1	SBTREQ_00001
	SBTTST_00002	Verification of RoT-2	SBTREQ_00001
	SBTTST_00003	Verification of RoT-3	SBTREQ_00001
	SBTTST_00004	Verification of Startup Behavior	SBTREQ_00003
	SBTTST_00005	Integrity verification program-1	SBTREQ_00002 SBTREQ_00004 SBTREQ_00008
	SBTTST_00006	Integrity verification program-2	SBTREQ_00002 SBTREQ_00005 - 00008
	SBTTST_00007	Integrity verification in the background-1	SBTREQ_00007
	SBTTST_00009	Effect on the performance requirements on the ECU startup time	SBTREQ_01002

	SBTTST_00010	Retry for temporary breakdown	SBTREQ_00009
	SBTTST_00011	Operation in Reprograming-1	SBTREQ_00011
	SBTTST_00012	Operation in Reprograming-2	SBTREQ_00011
	SBTTST_00013	Fail operation in secure boot-1	SBTREQ_00010
	SBTTST_00014	Fail operation in secure boot-2	SBTREQ_00010
	SBTTST_00015	Crypto algorithm	SBTREQ_00012
	SBTTST_00016	Operation during WakeUp 1	SBTREQ_00013 SBTREQ_00014
	SBTTST_00017	Operation during WakeUp 2	SBTREQ_00013 SBTREQ_00014
Requirements on Notification to the Outside when Verification of Software Integrity Fails	SBTTST_00101	ECU analysis	SBTREQ_00101
Key operations	SBTTST_00201	Symmetric key test-1	SBTREQ_01102
	SBTTST_00202	Symmetric key test-2	SBTREQ_01103
	SBTTST_00203	Asymmetric key test	SBTREQ_01103
	SBTTST_00204	Key operations test-1	SBTREQ_01104
	SBTTST_00205	Key operations test-2	SBTREQ_01003

If all applicable test items are judged “pass”, the test sample shall be judged as “passed”.

(※) SBTREQ_01101 is out of scope because it is the requirement in case of leakage of symmetric/asymmetric keys on the market and it is regarded as “the requirement after development”.

3. Evaluation request

Test requirements are defined below.

3.1. Verification of Software Integrity

【SBTTST_00001】Verification of RoT-1	
Contents of test	The integrity verification program for software in RoT shall not be rewritable.
Test method	design check or test on the hardware
Precondition	None
Test Procedure	[in case of test on the hardware] 1. Readout the memory area of the integrity verification program for the software in RoT 2. Write a different program on the memory area of the integrity verification program for the software in RoT (The written program is different from the program of 1) 3. Read out the memory area of the integrity verification program for the software in RoT
Measuring item	None
Pass-fail judgment	[in case of design check] “Contents of test” shall be confirmed by the following design information: - The memory area and its characteristic where the integrity verification program for the software in RoT is stored. [in case of test on the hardware] The red out program of 1 shall be equal to the red out program of 3
Remark	None

【SBTTST_00002】Verification of RoT-2	
Contents of test	[applicable only when symmetric key cryptography is adopted] (1) The symmetric key shall not be rewritable. But as an exception, the rewriting operations protected by security function shall be permitted. (e.g., the rewriting operation based on SHE specification.) (2) The symmetric key shall not be readable except from RoT.
Test method	(1) Design check or test on the hardware (2) Design check
Precondition	None
Test Procedure	[in case of test on the hardware] 1. Readout the symmetric key 2. Write a different key value to the symmetric key 3. Readout symmetric key
Measuring item	None
Pass-fail judgment	(1) [in case of design check] “(1) in Contents of test” shall be confirmed by the following design information: - The memory area and its characteristic where the symmetric key is stored. [in case of test on the hardware] The red out value of 1 shall be equal to the red out value of 3 (2) “(2) in Contents of test” shall be confirmed by the following design information: The memory area and its characteristic where the symmetric key is stored.
Remark	None

【SBTTST_00003】Verification of RoT-3	
Contents of test	[applicable only when asymmetric key cryptography is adopted] The asymmetric key or the hash value of asymmetric key shall not be rewritable. But as an exception, the rewriting operations protected by security function shall be permitted.
Test method	design check or test on the hardware
Precondition	None
Test Procedure	[in case of test on the hardware] 1. Readout the asymmetric key or the hash value of asymmetric key 2. Write a different value to the asymmetric key or the hash value of asymmetric key 3. Readout the asymmetric key or the hash value of asymmetric key
Measuring item	None
Pass-fail judgment	[in case of design check] “Contents of test” shall be confirmed by the following design information: -The memory area and its characteristic where the asymmetric key or the hash value of asymmetric key is stored. [in case of test on the hardware] The red out value of 1 shall be equal to the red out value of 3.
Remark	None

【SBTTST_00004】Verification of Startup Behavior	
Contents of test	When startup or reset of ECU, the integrity verification program in RoT shall start up before startup of the software.
Test method	Design check or test on the hardware
Precondition	None
Test Procedure	[in case of test on the hardware] 1. Set the breakpoint in debugger at the start of the integrity verification program in RoT 2. Configure the debugger settings that any program execution history can be recorded. 3. Run the program and then the program will stop at the breakpoint of 2
Measuring item	None
Pass-fail judgment	[in case of design check] “Contents of test” shall be confirmed by the following design information: - The way how the first startup program after reset is decided - The area where the first startup program after reset is stored [in case of test on the hardware] After 3, the history of program recorded in debugger shall contain nothing or shall contain only the run of reset vector.
Remark	None

【SBTTST_00005】Integrity verification program-1	
Contents of test	The first startup software (the software which start up next to the integrity verification program) shall be verified by the integrity verification program in RoT.
Test method	design check
Precondition	None
Test Procedure	None
Measuring item	None
Pass-fail judgment	“Contents of test” shall be confirmed by the following design information: The sequence of both the verification by the integrity verification program and the startup of the software verified first after ECU startup.
Remark	None

【SBTTST_00006】Integrity verification program-2	
Contents of test	A “chain” of verification processes shall be connected in sequence starting from a verification using the integrity verification program stored in the RoT
Test method	Design check
Precondition	None
Test Procedure	None
Measuring item	None
Pass-fail judgment	“Contents of test” shall be confirmed by the following design information: The sequence both the verification by the integrity verification program in RoT and the other verifications after ECU startup.
Remark	None

【SBTTST_00007】Integrity verification in the background-1	
Contents of test	[applicable only when the integrity verification in the background is adopted] The integrity verification in the background shall be done.
Test method	Test on the hardware
Precondition	None
Test Procedure	1. Tamper the programs which are the target for the integrity verification in the background 2. start up ECU
Measuring item	None
Pass-fail judgment	As the result of 2, the verification error shall occur in the integrity verification in the background and the operations when secure boot error occurs shall run (e.g., fallback).
Remark	None

【SBTTST_00009】Effect on the performance requirements on the ECU startup time	
Contents of test	Secure boot shall not affect the performance requirements on the ECU startup time
Test method	Design check
Precondition	None
Test Procedure	None
Measuring item	None
Pass-fail judgment	“Contents of test” shall be confirmed by the following design information: - The performance requirements on the ECU startup time - The ECU startup time(worst time)
Remark	None

【SBTTST_00010】 Temporary failure handling	
Contents of test	If verification of software integrity fails, the verification shall be retried, or the ECU shall be reset with a possible temporary breakdown considered.
Test method	Design check
Precondition	None
Test Procedure	None
Measuring item	None
Pass-fail judgment	“Contents of test” shall be confirmed by the following design information: - The verifications of software integrity which need verification retries or ECU reset. - The design information which triggers verification retries or ECU reset.
Remark	None

【SBTTST_00011】Operation in Reprograming-1	
Contents of test	[applicable only when symmetric key cryptography is adopted] In reprograming, the MAC of target software for reprograming shall be written. The written MAC shall be used in the integrity verification for the software.
Test method	Test on the hardware
Precondition	None
Test Procedure	1. Start up ECU 2. Reprogram both software and its MAC

	3. restart up ECU
Measuring item	None
Pass-fail judgment	The target software shall run after 1. The target software shall run after 3.
Remark	None

【SBTTST_00012】Operation in Reprograming-2	
Contents of test	[applicable only when asymmetric key cryptography is adopted] In reprograming, the digital signature of target software for reprograming shall be written. The written digital signature shall be used in the integrity verification for the software.
Test method	Test on the hardware
Precondition	None
Test Procedure	1. Start up ECU 2. Reprogram both software and its digital signature 3. Restart up ECU
Measuring item	None
Pass-fail judgment	The target software shall run after 1. The target software shall run after 3.
Remark	None

【SBTTST_00013】Fail operation in secure boot-1	
Contents of test	Control software which failed with secure boot shall not be started. The other software than control software shall run so as not to affect safety of the customer.
Test method	Design check
Precondition	None
Test Procedure	None
Measuring item	None
Pass-fail judgment	“Contents of test” shall be confirmed by the following design information: The operation in secure boot error
Remark	None

【SBTTST_00014】Fail operation in secure boot-2	
Contents of test	[applicable only when the integrity verification in the background is adopted] When error occurs in background verification, software shall run so as not to affect safety of the customer.
Test method	Design check
Precondition	None
Test Procedure	None
Measuring item	None
Pass-fail judgment	“Contents of test” shall be confirmed by the following design information: The operation in background verification error
Remark	None

【SBTTST_00015】 Verifying Cryptographic Algorithms	
Contents of test	The crypto algorithms which are defined in the requirement (SBTREQ_00012) shall be used.
Test method	Design check
Precondition	None
Test Procedure	None
Measuring item	None
Pass-fail judgment	“Contents of test” shall be confirmed by the following design information: The used crypto algorithms (including crypto key length)
Remark	None

【SBTTST_00016】 Verifying Operation at WakeUp-1	
Contents of test	[Only when performing software integrity validation at WakeUp time] Verify that software-integrity validation is in place at the time of WakeUp.
Test method	Evaluation of actual equipment
Precondition	None
Test Procedure	1. Launch ECU 2. Repro without updating MAC or digital signature during ECU startup 3. Sleep factor generation 4. WakeUp factor generation
Measuring item	None
Pass-fail judgment	Software Integrity Verification Fails in 4
Remark	None

【SBTTST_00017】 Checking Operation at WakeUp-2	
Contents of test	[Only when background validation is performed at WakeUp] Verify that the background is in place at the time of WakeUp.
Test method	Evaluation of actual equipment
Precondition	None
Test Procedure	1. Launch ECU 2. Repro during ECU startup Background Verified Part: Do Not Update MAC or Digital Signature Non-part subject to background validation: Updating MAC or digital signature 3. Sleep factor generation 4. WakeUp factor generation
Measuring item	None
Pass-fail judgment	Background validation fails in 4
Remark	None

3.2. Requirements on Notification to the Outside when Verification of Software Integrity Fails

【SBTTST_00101】 ECU analysis	
Contents of test	It shall be able to be judged by ECU analysis whether the software integrity verification fails or not.
Test method	Design check
Precondition	None
Test Procedure	None
Measuring item	None
Pass-fail judgment	“Contents of test” shall be confirmed by the following design information: - The way to analyze ECU
Remark	None

3.3. Key Operations

【SBTTST_00201】Symmetric key test-1	
Contents of test	[applicable only when symmetric key cryptography is adopted] The symmetric key used for reprograming shall be different from the key used for integrity verification of the software
Test method	Design check
Precondition	None
Test Procedure	None
Measuring item	None
Pass-fail judgment	“Contents of test” shall be confirmed by the following design information: - How to generate symmetric key used for reprograming - How to generate symmetric key used for integrity verification of the software
Remark	None

【SBTTST_00202】Symmetric key test-2	
Contents of test	[applicable only when symmetric key cryptography is adopted] A unique symmetric key shall be generated for each software part number
Test method	Design check
Precondition	None
Test Procedure	None
Measuring item	None
Pass-fail judgment	“Contents of test” shall be confirmed by the following design information: - How to generate symmetric key used for integrity verification of the software
Remark	None

【SBTTST_00203】Asymmetric key test	
Contents of test	[applicable only when asymmetric key cryptography is adopted] The pair of a public key and a private key shall be unique for each combination of ECU × supplier × microcontroller model.
Test method	design check

Precondition	None
Test Procedure	None
Measuring item	None
Pass-fail judgment	“Contents of test” shall be confirmed by the following design information: - How to generate the pair of a public key and a private key used for integrity verification of the software
Remark	None

【SBTTST_00204】Key operations test-1	
Contents of test	Verify that who generate the secure boot keys.
Test method	design check
Precondition	None
Test Procedure	Check the design document in which who will generate the secure boot keys.
Measuring item	The description about who will generate the secure boot keys.
Pass-fail judgment	The key generator shall have been chosen by the ECU designer.
Remark	None

【SBTTST_00205】Key operations test-2	
Contents of test	Verify the randomness of the keys used in the Secure Boot.
Test method	In accordance with VULCMN_50200 and VULCMN_50300 of [2].
Precondition	↑
Test Procedure	↑
Measuring item	↑
Pass-fail judgment	↑
Remark	None