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要求仕様書
Requirements 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-REQ-SPEC-a01-09-a

承認 Approved	調査 Checked	作成 Created	2023/3/30
平林	平井	玉樹 安江	Omission of signature (approved electronically)

適用先 **Target**	・標準リプログラミングを実施する ECU ・OTA リプログラミングを実施する ECU ・リプロ鍵管理・暗号化システム ・リプログラミングツール ECUs that implementing standard reprogramming or OTA reprogramming Reprogramming Key Management and Encryption System Reprogramming Tool
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 【問い合わせ先 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	2020/04/28	46F 早川
a01-01-a	4.2.1　復号処理の明確化 4.2.2　復号対象の明確化 4.2.3/4.3.3/4.4.3　各機能動作有無判定条件の変更 4.4.1　妥当性検証要件の明確化 5.1　112bit のセキュリティ強度の鍵削除 セキュリティプロパティ#2 変更 鍵保存要件の変更 セキュリティプロパティ#1 変更 その他　記載レベルアップ	2020/12/22	46F 早川
a01-02-a	4.4.1　バージョン情報妥当性検証の実装例の具体化 5.1　セキュリティプロパティ#2 設定値の追記 5.1.1　セキュリティプロパティ#1 設定値の追記	2021/04/01	46F 早川
a01-03-a	4.3.3　改ざん検知動作条件の修正 4.5　その他の要求の明確化 その他　英訳追加	2021/05/20	46F 早川
a01-03-b	6.3　ｻﾌﾞﾏｲｺﾝ/ｽﾚｰﾌﾞ ECU 構成の場合の考え方追加	2021/07/30	46F 早川
a01-04-a	5.1　リプロスペックパラメータの表に CSP/PSP の列を追加	2021/08/16	46F 早川
	4.4.3　妥当性検証の動作条件を変更	2021/08/24	46F 早川
	6.4　暗号鍵変更条件を追加	2021/08/25	46F 早川
a01-04-b	2.5 関連仕様書を更新	2021/10/05	46F 安江
a01-05-a	5.1.1.4 乱数要件の変更	2021/11/25	46F 垣屋
a01-06-a	4.3.2 改ざん検知対象の明確化	2022/05/30	46F 安江
	表 5-1 の誤記修正		
a01-07-a	5.1.1.4 乱数についての要求の明確化(RPRREQ_00044)	2022/07/22	46F 安江
	関連文書[2]の記載に合わせ、RSASSA-PKCS1_v1_5 を削除（RPRREQ_00011、図 5-1）	2022/09/14	46F 玉樹
	4.3.4.改ざん検知後の処理の明確化	2022/09/14	46F 清川
	表紙のフォーマット変更	2022/09/15	46F 安江
	2.6 関連文書を更新 3.2 各機能の処理順番に関する補足を追加	2022/10/07	46F 玉樹
	2.5、2.6 章構成変更 2.6 関連文書[10]を追加 3.3 表 3-2 を更新 4.4.1 妥当性検証方式明確化のための要求追加(RPRREQ_00050)	2022/10/19	46F 安江

a01-08-a	参照先の要件を追加（RPRREQ_00044） 用語統一のため修正（RPRREQ_00017） 6.1.1 対象データがデータレコード部であることを明確化	2022/11/01	46F 玉樹
	OTA リプログラミング仕様との整合修正(2.1, 2.2, 2.3, 3.1, 3.2, 3.3, 4.1, 4.1.2, 4.2.3, 4.3.3, 5.1, 5.1.1.2, 5.1.1.4 章)	2022/11/09	46F 安江
a01-09-a	5.1.1 CSP/PSP 保護についての要求の明確化（RPEREQ_00031） 2.6 公的関連文書の外部リンクを追加	2023/01/27	46F 玉樹
	関連文書[2]の記載に合わせ、RSASSA-PKCS1_v1_5 を追加（RPRREQ_00011、図 5-1）	2023/02/08	46F 安江
	表 3-2 に車両開発後要求列を追加	2023/02/09	46F 玉樹
	表紙を修正（適用先欄）	2023/02/24	46F 玉樹
	4.3.1 RSASSA-PSS に関する saltLength 要件を追加（RPRREQ__00011）	2023/03/13	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要求仕様書(関連文書[2][3])および OTA リプログラミング要求仕様書(関連文書[5])を適用する ECU に対して、リプログラミングセキュリティ対策を実現するための手法を定義する。

2.2. 適用範囲

本書の適用範囲は、標準リプログラミング要求仕様書(関連文書[2][3]) および OTA リプログラミング要求仕様書(関連文書[5])にもとづいてリプログラミングを実施する ECU とする。

2.3. 前提条件

標準リプログラミング要求仕様書(関連文書[2][3])および OTA リプログラミング要求仕様書(関連文書[5])以外の書き換え機能に対するセキュリティ機能は共通脆弱性対策要求仕様書(関連文書[6])を参照すること。

2.4. 要求事項の記載

【RPRREQ_*****】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

表 2-1 上位文書一覧

No	仕様書	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コンセプト定義書	SEC-24PF-VCL-CPT-INST-DOC-***-**-*	46F

2.6. 関連文書

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	(欠番)	-	-
2	Wired Reprogramming Specification Flash Bootloader Software	wrfbs-rd***-***-*	46F
3	Wired Reprogramming Specification Reprogramming Sequence	wrrs-rd***-***-*	46F
4	(欠番)	-	-
5	OTA4.0 ソフト更新システム要求仕様書	otasu40-systemreq-rd***-***-*	OTA 推進室

6	共通脆弱性対策要求仕様書	SEC-ePF-VUL-CMN-REQ-SPEC-***-**-*	46F
7	リプログラミングセキュリティ運用規定	SEC-ePF-RPR-OPE-STD-***-**-*	情セキ
8	車両サイバーセキュリティ及びプライバシ用語定義書	SEC-ePF-TRM-GUD-PROC-***-**-*	46F
9	Wired reprogramming Toyota Standard Specification	twr-rd***-***-*	46F
10	車両サイバーセキュリティ ECU 開発プロセス運用手順書（社内限）	SEC-ISO-VCL-PRD-PCD-PROC-***-**-*	46F

表 2-3 公的関連文書一覧

No	名称/外部リンク	対象機能
1	NIST FIPS197 https://csrc.nist.gov/publications/detail/fips/197/final	AES128
2	NIST SP800-38A https://csrc.nist.gov/publications/detail/sp/800-38a/final	CBC モード
3	NIST FIPS PUB 180-4 https://csrc.nist.gov/publications/detail/fips/180/4/final	SHA-256
4	Public-Key Cryptography Standard (PKCS)#1 v2.2 https://www.rfc-editor.org/rfc/rfc8017	RSA
5	SEC 1:Elliptic Curve Cryptography または ANSI X9.62 https://www.secg.org/sec1-v2.pdf	ECDSA

3. 要求概要

3.1. システム構成

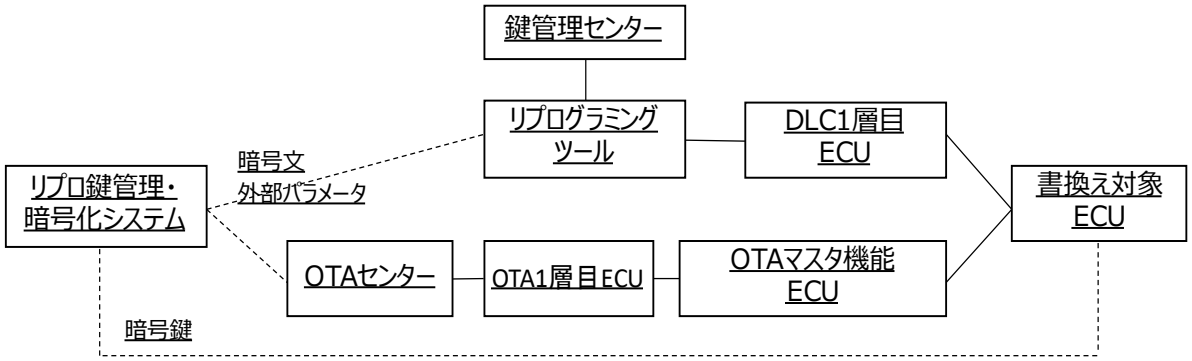


図 3-1 に本仕様を構成するエンティティを図示する。また、表 3-1 に各エンティティの役割を概説する。

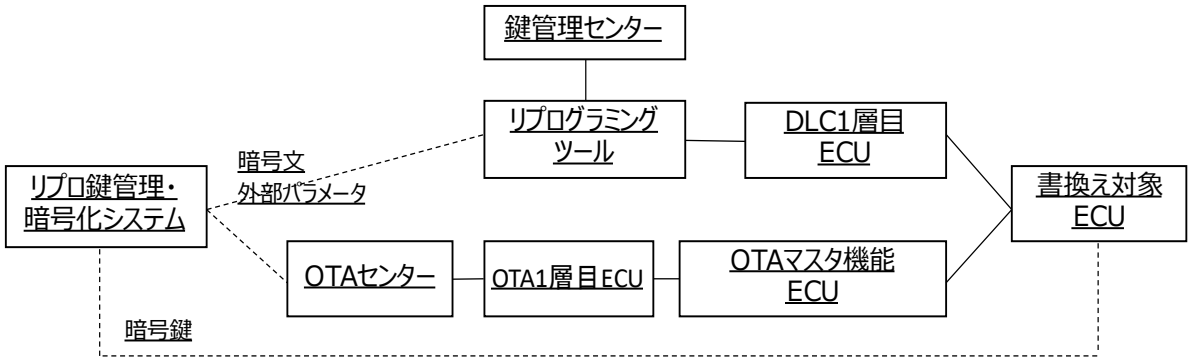


図 3-1 システム構成

表 3-1 エンティティー覧

エンティティ名	説明
リプロ鍵管理・暗号化システム	鍵生成、外部パラメータ生成、暗号文・署名生成機能を有するシステム
鍵管理センター	有線リプロで、車の接続先が正しいことを保証するためのセンター
リプログラミングツール	有線リプロで、プログラムを書き込むツール
DLC1 層目 ECU	有線リプロで、DLC 経由でリプログラミングツールと接続する ECU
OTA センター	OTA リプロで、プログラムを配信するセンター
OTA1 層目 ECU	OTA リプロで、通信機経由で OTA センターと接続する ECU

OTA マスタ機能 ECU	OTA リプロで、OTA センターから受信した書き込みプログラムを、書換え対象 ECU へ配信する ECU
書き換え対象 ECU	リプログラミングによりプログラムを書き換える ECU

3.2. 動作シーケンス

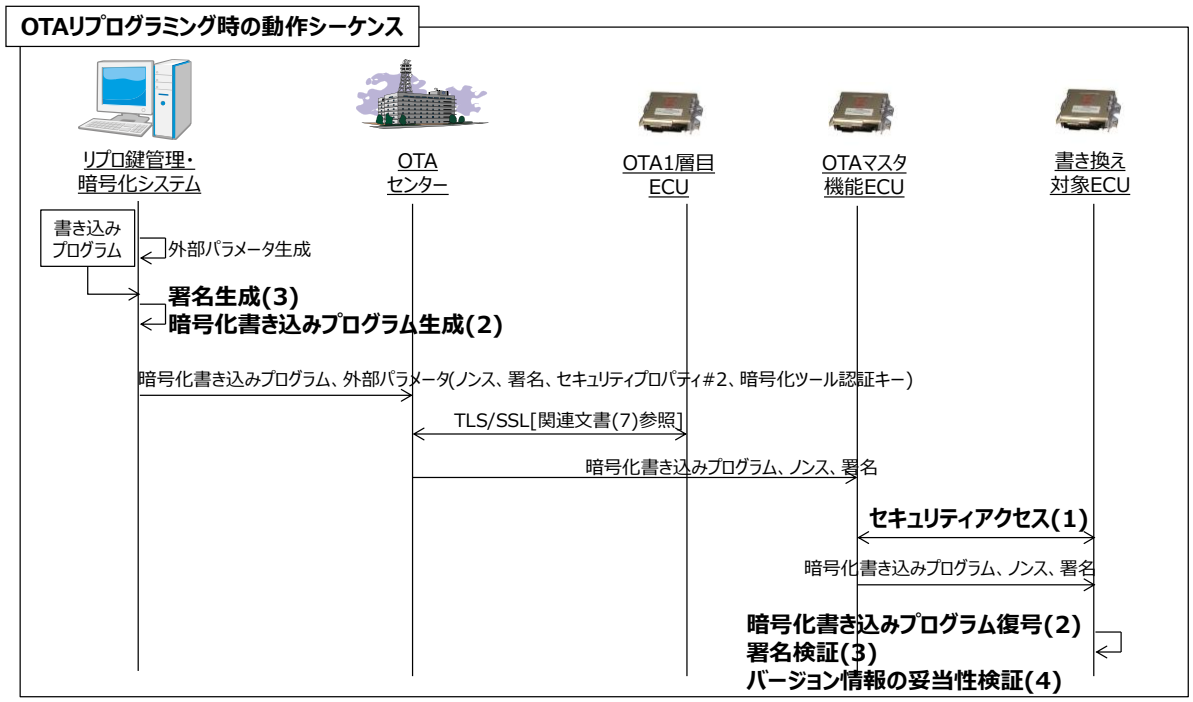
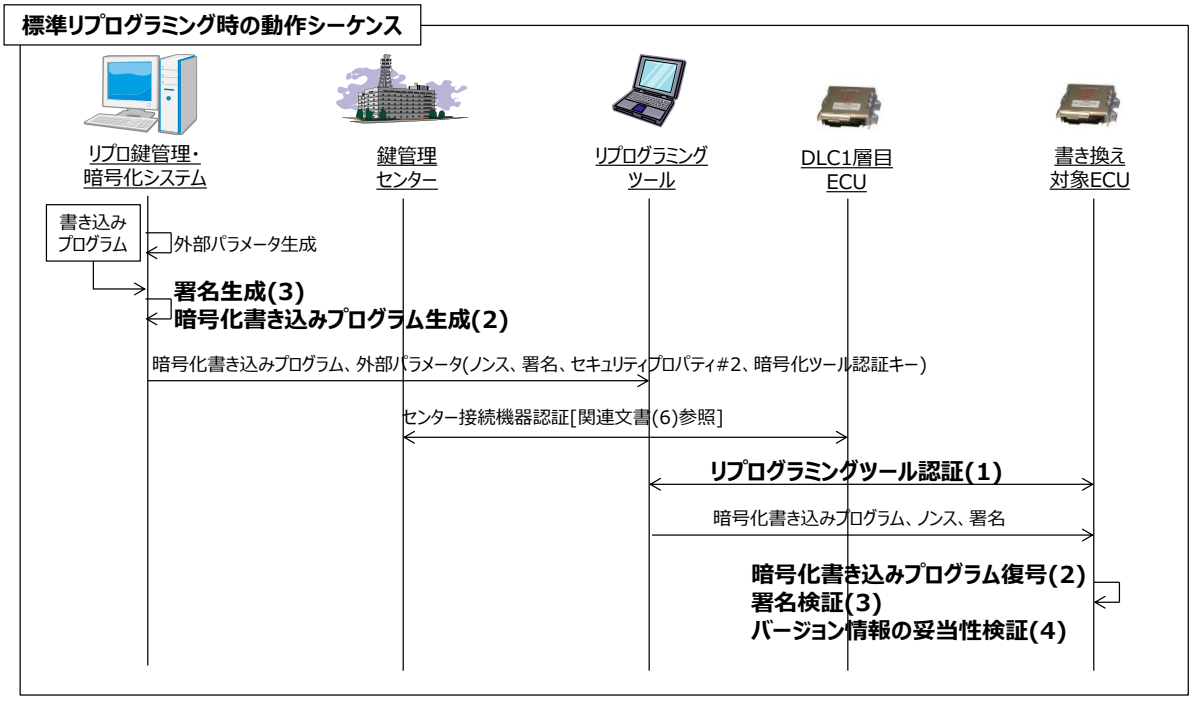


図 3-2 にリプロセキュリティの概要図を示す。



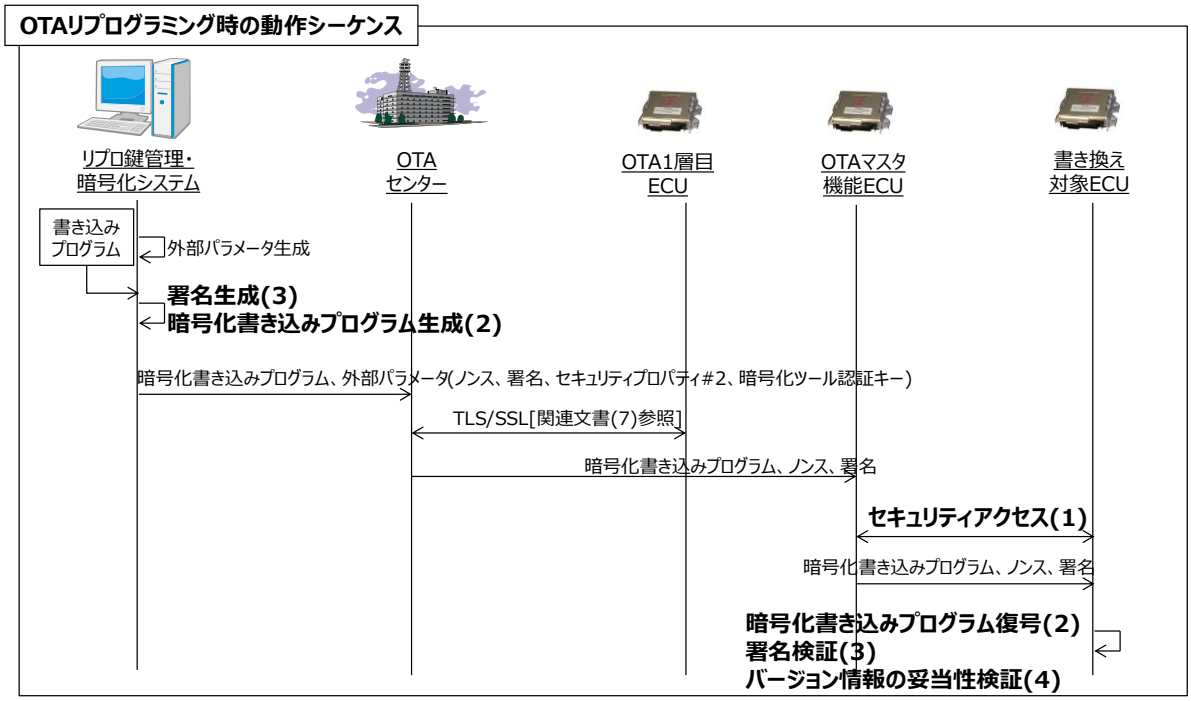


図 3-2 リプロセキュリティ概要

本書では以下の機能について規定する。

(1) リプログラミングツール認証/セキュリティアクセス

正規の書き込み元であることを認証することで、非正規の書き込み元から不正なプログラムが書き込まれることを防止

(2) 書き込みプログラム暗号化・復号

書き込みプログラムを暗号化することで、漏洩しても解析、改ざんに利用されることを防止

(3) 書き込みプログラム改ざん検知

書き込みプログラムに署名を付与することで、改ざんされたことを検知できるようし、不正なプログラムが動作することを防止

(4) 書き込みプログラムのバージョン情報妥当性検証

書き込みプログラムのバージョン情報の妥当性を検証することで、ロールバック攻撃などによって不正なバージョンのプログラムが動作することを防止

（補足）これらの機能の処理順番は関連文書[9]を参照すること。

3.3. 要求一覧

各エンティティが対応すべき要求事項の一覧を表 3-2 に示す。要求事項の詳細については、4 章以降を参照。

表 3-2 要求事項対応表

要求事項番号	車両開発後要求	リプロ鍵管理・暗号化システム	リプログラミングツール	OTA マスタ機能 ECU	書き換え対象 ECU	
					有線リプロ	OTA リプロ
RPRREQ_00001	–		○	○	○	○
RPRREQ_00002	–		○	○		
RPRREQ_00003	–				○	○
RPRREQ_00004	–	○			○	○
RPRREQ_00005	–	○				
RPRREQ_00006	–				○	○
RPRREQ_00007	–	○			○	○
RPRREQ_00008	–	○			○	○
RPRREQ_00009	–				○	○
RPRREQ_00011	–	○			○	○
RPRREQ_00012	–	○				
RPRREQ_00013	–				○	○
RPRREQ_00014	–	○			○	○
RPRREQ_00017	–	○			○	○
RPRREQ_00018	–				○	○
RPRREQ_00019	–				○	○
RPRREQ_00020	–				○	○
RPRREQ_00021	–				○	○
RPRREQ_00022	–				○	○
RPRREQ_00023	–				○	○
RPRREQ_00024	–				○	○
RPRREQ_00025	–					
RPRREQ_00026	–					
RPRREQ_00027	–				○	○

要求事項番号	車両開発後要求	リプロ鍵管理・暗号化システム	リプログラミングツール	OTA マスタ機能 ECU	書き換え対象 ECU	
					有線リプロ	OTA リプロ
RPRREQ_00028	–				○	○
RPRREQ_00029	–	○			○	○
RPRREQ_00030	–		○			
RPRREQ_00031	–				○	○
RPRREQ_00032	–	○				
RPRREQ_00033	–		○			
RPRREQ_00034	–	○				
RPRREQ_00037	–	○			○	○
RPRREQ_00038	–	○			○	○
RPRREQ_00039	–	○			○	○
RPRREQ_00040	–		○	○		
RPRREQ_00041	–				○	○
RPRREQ_00042	○				○	○
RPRREQ_00043	–				○	○
RPRREQ_00044	–				○	○
RPRREQ_00045	–		○	○	○	○
RPRREQ_00046	–		○	○	○	○
RPRREQ_00047	–		○	○		
RPRREQ_00048	–				○	○
RPRREQ_00049	–				○	○
RPRREQ_00050	–				○	○

4. 機能要求詳細

4.1. リプログラミングツール認証

リプログラミングツール認証は、OTA リプログラミングで規定しているセキュリティアクセスを含む。

4.1.1. 方式の概要

【RPRREQ_00001】

リプログラミングツール認証は以下の方式を用いること。

方式 ： CHAP（Challenge Handshake Authentication Protocol）認証方式

KEY 値演算アルゴリズム ： AES128　ECB モード　　[公的関連文書[]参照]

KEY 値演算時に使用する鍵 ： ツール認証キー

4.1.2. リプログラミングツール認証処理

書き換え対象 ECU はツール認証キーを用いて、リプログラミングツールおよび OTA マスタ機能 ECU の認証を行う。詳細は関連文書[2]および[5]を参照すること。

【RPRREQ_00002】

リプログラミングツールおよび OTA マスタ機能 ECU では、リプログラミングツール認証時に以下の処理を実施すること。

(1) 書き換え対象 ECU に対して SEED 要求を行う。

(2) 暗号化ツール認証キーをサービスキーで復号する。

(3) 書き換え対象 ECU から受け取った SEED 値とツール認証キーを用いて、KEY 値を生成する。

(4) 算出した KEY 値を書き換え対象 ECU へ送信する。

【RPRREQ_00003】

書き換え対象 ECU ではリプログラミングツール認証時に以下の処理を実施すること。

(5) SEED 値を生成し、SEED 値をリプログラミングツールまたは OTA マスタ機能 ECU へと送信する。

(6) 生成した SEED 値とツール認証キーを用いて KEY 値を生成する。

(7) リプログラミングツールまたは OTA マスタ機能 ECU から受け取った KEY 値と(6)で生成した KEY 値を比較し、一致しているか確認をする。一致の場合は認証成功、不一致の場合は認証失敗と判断する。

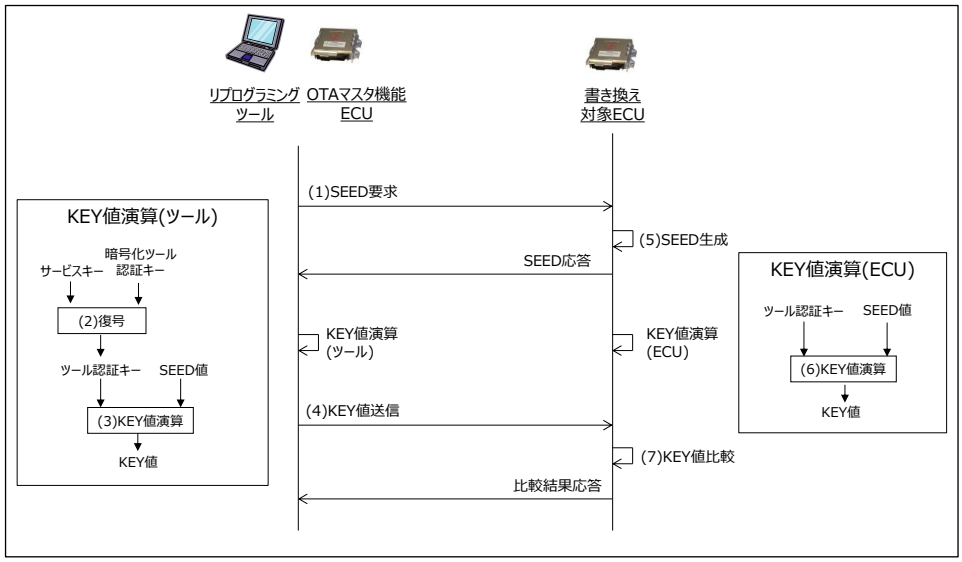


図 4-1 ツール認証シーケンス

4.2. 書き込みプログラム暗号化・復号

本章では、書き込みプログラムを暗号化・復号する際の仕様について記載する。

4.2.1. 暗号化・復号方式

【RPRREQ_00004】

書き込みプログラムの暗号化・復号には以下の方式、パラメータを用いること。

暗号化アルゴリズム ： AES128 CBC モード [公的関連文書[1]、[2]参照]

暗号化/復号に使用する鍵 ： システムキー

CBC モードの IV 値：ノンス

【RPRREQ_00005】

リプロ鍵管理・暗号化システムは、ノンス、システムキーを用いて平文の書き込みプログラムを暗号化すること。

【RPRREQ_00006】

書き換え対象 ECU は、暗号化書き込みプログラムをノンス、システムキーを用いて復号すること。

【RPRREQ_00049】

書き換え対象 ECU は、復号後の平文書き込みプログラムのうち、PKCS#7 で Padding された領域を判別、除去できること。

4.2.2. 暗号化対象

【RPRREQ_00007】

リプロでダウンロードする ROM/RAM に格納する全データ(フラッシュ制御プログラム含む)を暗号化の対象とすること。

(補足)

・差分リプロの場合は、差分抽出後の差分ファイルが対象

・圧縮リプロの場合は、圧縮後の圧縮ファイルが対象

【RPRREQ_00008】

Padding によりサイズ調整した書き込みプログラムを暗号化の対象とすること。

(補足)

・Padding はリプロ鍵管理・暗号化システムで実施する

・Padding には PKCS#7 方式を用いる

・平文でプログラムを書き込む場合は、Padding 不要である

4.2.3. 復号の動作条件

【RPRREQ_00009】

復号動作有無は、リプログラミングツールおよび OTA マスタ機能 ECU より受け取った平文/暗号文通知に従って決定すること。

4.3. 書き込みプログラム改ざん検知

本章では、書換え対象 ECU においてプログラムの改ざん検知をする際の仕様について記載する。ECU に実装する署名検証アルゴリズムは 1 種類で構わない。

4.3.1. 改ざん検知方式

【RPRREQ_00011】

改ざん検知にデジタル署名(RSA)方式を用いる場合に本要件を適用すること。

以下の方式、パラメータを用いること。

署名生成・検証アルゴリズム ： RSASSA-PSS、もしくは RSASSA-PKCS1_v1_5 [公的関連文書[4]参照]

署名生成に使用する鍵 ： 署名生成キー

署名検証に使用する鍵 ： 署名検証キー

ハッシュ関数 ： SHA-256 [公的関連文書[3]参照]

RSA Public exponent ： 65537(10 進数)

saltLength ： 32byte （saltLength は RSASSA-PSS 固有のパラメータ）

【RPRREQ_00014】

改ざん検知にデジタル署名方式(ECDSA)を用いる場合に本要件を適用すること。

以下の方式、パラメータを用いること。

署名生成アルゴリズム ： ECDSA [公的関連文書[5]参照]

署名生成に使用する鍵 ： 署名生成キー

署名検証に使用する鍵 ： 署名検証キー

ハッシュ関数 ： SHA-256 [公的関連文書[3]参照]

楕円曲線 ： P-256

【RPRREQ_00012】

リプロ鍵管理・暗号化システムは、署名生成キーを用いて書き込みプログラムの署名を生成すること。

【RPRREQ_00013】

書き換え対象 ECU は、改ざん検知対象のプログラムを受信したときは、署名検証キーを用いて受信した署名の検証をすること。

4.3.2. 改ざん検知対象

【RPRREQ_00017】

改ざん検知の対象は、以下の書き込みプログラムとすること。

・全書換えリプロの場合、リプロでダウンロードする全データ

・差分/圧縮リプロの場合、差分抽出/圧縮前の全データ

(補足)対象データの処理手順は、Appendix6.1 参照。

4.3.3. 改ざん検知の動作条件

【RPRREQ_00018】

暗号化フラグ(セキュリティプロパティ#1)が ON の場合は、必ず改ざん検知をすること。

【RPRREQ_00019】

暗号化フラグが OFF の場合、改ざん検知動作有無は、リプログラミングツールおよび OTA マスタ機能 ECU より受け取った checkTypeIdentifier(関連文書[2]参照)に従って決定すること。

【RPRREQ_00020】

書き換え対象 ECU は、暗号化フラグと、リプログラミングツールおよび OTA マスタ機能 ECU より受け取ったデジタル署名長の組み合わせが不正であった場合、不正であることが分かる情報をリプロツールに出力すること。

(補足)不正であることが分かる情報

・否定応答

・肯定応答の中の詳細コード

詳細は関連文書[2]参照。

表 4-1 改ざん検知動作判定

暗号化フラグ	checkTypeIdentifier	改ざん検知有無	判定
ON	0x01(signature)	改ざん検知あり	○
ON	0x01 以外	改ざん検知あり	×(不正)
OFF	0x01(signature)	改ざん検知あり	○
OFF	0x01 以外	改ざん検知なし	○

4.3.4. 改ざん検知後の処理

【RPRREQ_00021】

改ざん検知におけるダイジェストの比較結果が不一致となった場合、ECU は書き込みプログラムを動作させないこと。

(補足)上記以外の処理は関連文書[2]を参照すること。

(注)FLASH に書き込んでからの改ざんチェック

復号した書き込みプログラムを全て FLASH に書き込んでから改ざんチェックを実施することになる場合、ダイジェスト比較結果が不一致の時は、信頼できないプログラムが書き込まれた状態になる。

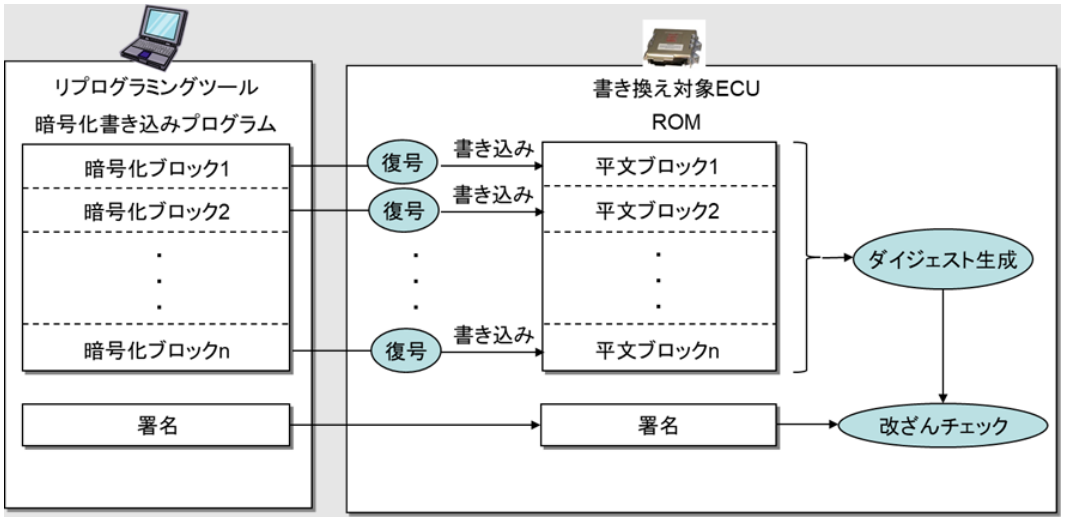


図 4-2 改ざん検知チェック実施タイミングイメージ

4.4. 書き込みプログラムのバージョン情報妥当性検証

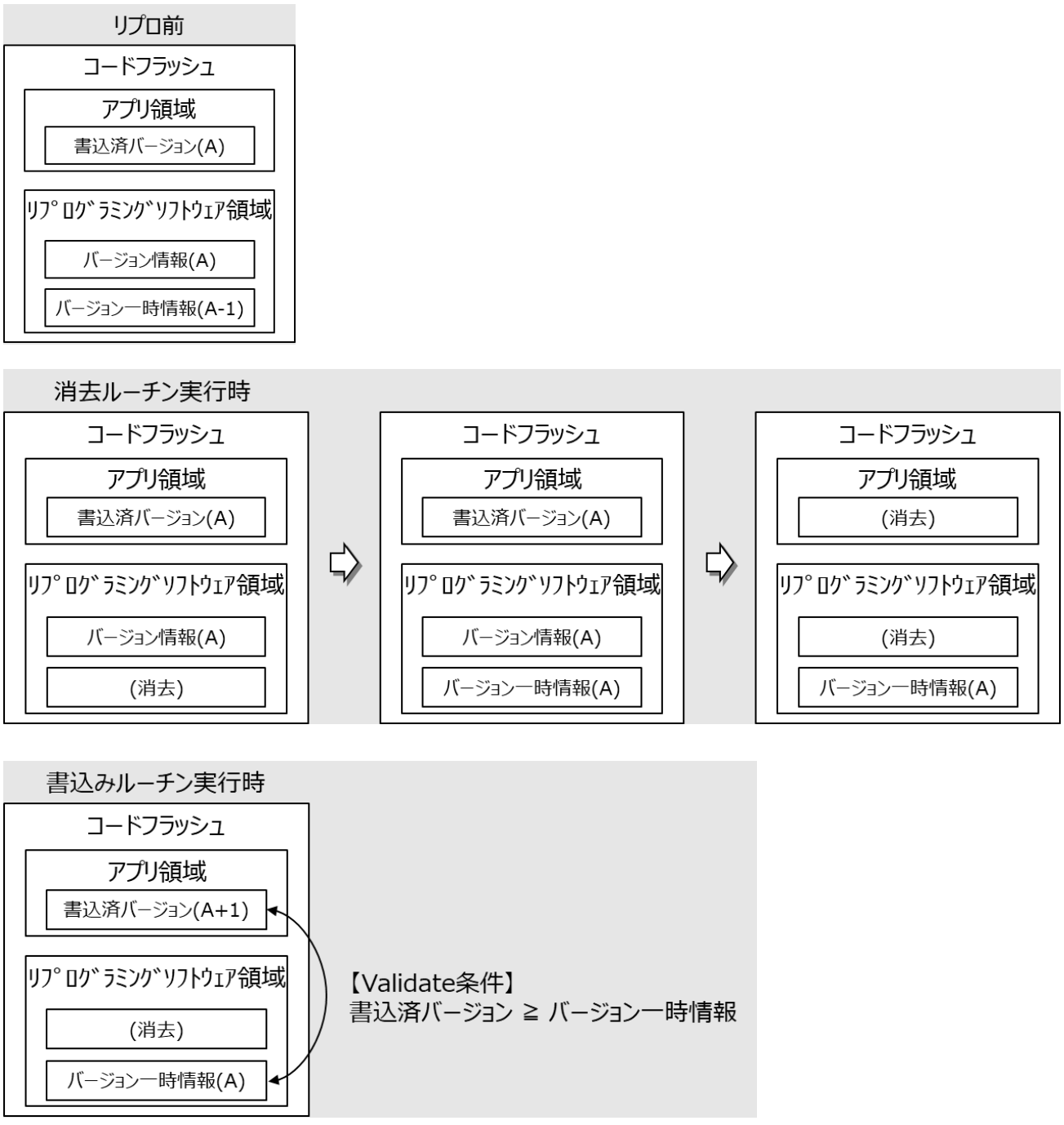
4.4.1. 妥当性検証方式

【RPRREQ_00022】

書き込み対象 ECU は、受信した書き込みプログラムのバージョンが、現在のプログラムのバージョン以上であることを検証すること。

(補足)FBL(リプログラミングソフトウェア領域)で本機能を実現できることが望ましい。

実装例：



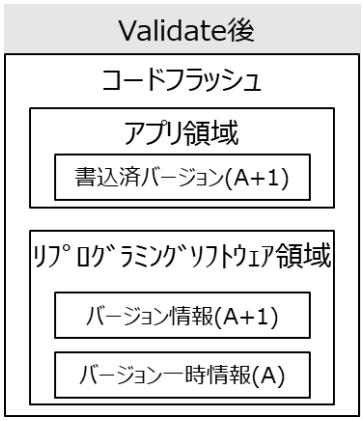


図 4-3 妥当性検証の実装例

【RPRREQ_00050】
ECU の再利用分析の結果、プログラムの変更内容がサイバーセキュリティ機能に影響すると判断された場合、書込みプログラムのバージョンを、ECU の現在のプログラムのバージョンより大きいバージョンにすること。再利用分析については関連文書[10]参照。

4.4.2. 妥当性検証対象

【RPRREQ_00023】
リプロでダウンロードしたプログラムに書き込まれているバージョン情報を妥当性検証の対象とすること。

4.4.3. 妥当性検証の動作条件

【RPRREQ_00024】
暗号化フラグ(セキュリティプロパティ#1)が ON の場合は､必ずバージョン情報妥当性検証をすること。
(補足)暗号化フラグが OFF の場合は、バージョン情報妥当性検証の実施は任意。

【RPRREQ_00025】
(欠番)

【RPRREQ_00026】
(欠番)

4.4.4. 妥当性検証後の処理

【RPRREQ_00027】
バージョン情報妥当性検証の結果、不正なバージョンと判定されたプログラムで書換え対象 ECU を動作させないこと。

4.5. その他の要求

【RPRREQ_00028】

車両が動いている間は、リプログラミングシーケンスにおける通信停止のダイアグコマンドを受け付けないこと。

5. 非機能要求詳細

5.1. パラメータ要求

リプロセキュリティでは、表 5-1 記載のパラメータを使用する。

表 5-1 リプロスペックパラメータ

分類	名称	サイズ (byte)	用途	有線リプロ	OTAリプロ	CSP/PSP
暗号鍵	システムキー	16	書き込みプログラム暗号化・復号用鍵	○	○	CSP
	ツール認証キー	16	リプログラミングツール認証時の KEY 値生成用の鍵	○	○	CSP
	署名生成キー(RSA)	384	ECU で改ざん検知をする為の署名(RSA 方式)を生成する鍵	○	○	CSP
	署名生成キー(ECDSA)	32	ECU で改ざん検知をする為の署名(ECDSA 方式)を生成する鍵	○	○	CSP
	署名検証キー(RSA)	384	ECU で改ざん検知をする為の署名(RSA 方式)を検証する鍵	○	○	PSP
	署名検証キー(ECDSA)	64	ECU で改ざん検知をする為の署名を検証(ECDSA 方式)する鍵	○	○	PSP
	サービスキー	16	リプログラミングツールでのツール認証キー暗号化・復号用の鍵	○		CSP
セキュリティプロパティ	セキュリティプロパティ#1	1	暗号化フラグ(0xFF：OFF, 0xFF 以外：ON)	○	○	PSP
外部パラメータ	暗号化ツール認証キー	16	サービスキーで暗号化されたツール認証キー	○		—
	ノンス(注 1)	16	暗号化時に暗号化対象の書き込みプログラムと組み合わせるデータ	○	○	—
	署名(RSA)	384	改ざん検知を判定するためのデータ(RSA 方式)	○	○	—
	署名(ECDSA)	64	改ざん検知を判定するためのデータ(ECDSA 方式)	○	○	—
	セキュリティプロパティ#2	1	以下セキュリティ情報をまとめたデータ(注 2) ・セキュリティ機能の ON/OFF フラグ ・暗号アルゴリズム/セキュリティ強度	○	○	—
ツール認証パラメータ	SEED 値	16	リプログラミングツール認証時の KEY 値生成用のデータ	○	○	—
	KEY 値	16	リプログラミングツール認証時に、正規のツールか判定するためのデータ	○	○	—

（注１）暗号モードが CBC モードの場合は IV が一般的な名称だが、本文書ではノンスと表記する。

（注２）セキュリティプロパティ#2 の設定値は、図 5-1 のように設定する。

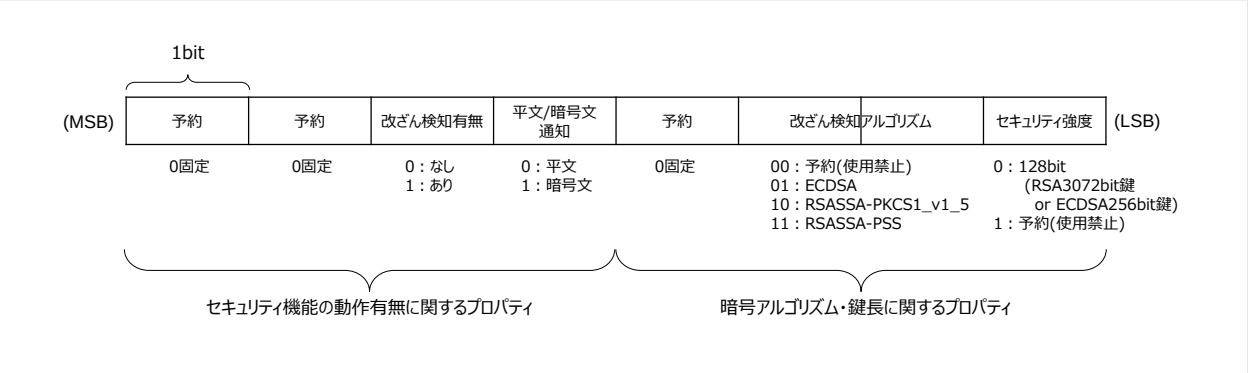


図 5-1 セキュリティプロパティ#2 構成

5.1.1. パラメータの生成・保存

本章では、パラメータの生成・保存に関する要求事項を記載する。※1 の記載があるパラメータは有線リプロの場合のみ適用する。

5.1.1.1. 暗号鍵

本書で規定する暗号鍵は、システムキー、ツール認証キー　署名生成キー、署名検証キー、サービスキーである。

【RPRREQ_00029】
システムキー、ツール認証キー※1、署名生成キー、署名検証キーは、リプログラミングセキュリティ運用規定(関連文書[7])に記載の鍵生成機能を利用して生成すること。
(補足)各暗号鍵は、共通脆弱性対策要求仕様書(関連文書[6])の要件を満たす乱数より生成される。

【RPRREQ_00030】
サービスキー※1 は、リプログラミングセキュリティ運用規定(関連文書[7])に記載の発行手順に従って入手すること。
(補足)サービスキーは、リプロツール開発者のみ必要となるパラメータである。

【RPRREQ_00031】
システムキー、ツール認証キー※1、署名検証キーは、書き換え対象 ECU のリプロ非対象領域に保存すること。 CSP/PSP の保護について共通脆弱性対策要求仕様書(関連文書[6])の要件を満たすこと。

【RPRREQ_00032】
システムキー、ツール認証キー※1、署名生成キー、署名検証キーは、リプロ鍵管理・暗号化システムに保存すること。

【RPRREQ_00033】
サービスキー※1 は、リプログラミングツールに保存すること。

【RPRREQ_00034】
サービスキー※1 は、リプロ鍵管理・暗号化システムに保存すること。

5.1.1.2. 外部パラメータ

本書で規定する外部パラメータは、暗号化ツール認証キー、ノンス、署名、セキュリティプロパティ#2 である。

【RPRREQ_00037】
暗号化ツール認証キー※1、ノンスはリプログラミングセキュリティ運用規定(関連文書[7])に記載の外部パラメータ生成機能を利用して生成すること。
(補足)暗号化ツール認証キーはツール認証キーをサービスキーで暗号化して生成する。暗号化には「AES128　ECB モード」を使用する。ノンスは、共通脆弱性対策要求仕様書(関連文書[6])の要件を満たす乱数より生成される。

【RPRREQ_00038】
署名はリプログラミングセキュリティ運用規定(関連文書[7])に記載のプログラム暗号化機能を利用して生成すること。
(補足)署名の生成方法は、4.3 を参照。

【RPRREQ_00039】
セキュリティプロパティ#2 は図 5-1 の構成にもとづき、その都度セキュリティ機能の動作有無、利用している暗号アルゴリズムに合わせて設定すること。

【RPRREQ_00040】
リプログラミングツールおよび OTA マスタ機能 ECU は、暗号化ツール認証キー※1、ノンス、署名、セキュリティプロパティ#2 を外部パラメータとして受け取り、リプロ処理が完了するまで保存すること。

【RPRREQ_00041】
書き換え対象 ECU は、ノンス、署名を外部パラメータとして受け取り、各パラメータを用いた処理が完了するまで保存すること。
(補足)各パラメータを用いた処理
　ノンス：復号

署名：改ざん検知

5.1.1.3. セキュリティプロパティ

本書で規定するセキュリティプロパティは、セキュリティプロパティ#1 である。

【RPRREQ_00042】
書き換え対象 ECU 出荷時にセキュリティプロパティ#1 を設定すること。セキュリティプロパティ#1 の暗号化フラグは、試作品の場合は OFF、号口品の場合は ON にすること。

【RPRREQ_00043】
セキュリティプロパティ#1 は、書き換え対象 ECU のリプロ非対象の領域に記憶すること。

5.1.1.4. ツール認証パラメータ

【RPRREQ_00044】
書き換え対象 ECU は、関連文書[6]の【VULCMN_00200】,【VULCMN_00300】の要件を満たす乱数により SEED 値を生成すること。ただし、乱数エントロピーとペナルティについては、以下に従うこと。

乱数エントロピー：40bit 以上
ペナルティ：任意

（補足）本機能は Post19PF の脅威分析＆リスクアセスメント結果より導出されるサイバーセキュリティ要求に紐付かないため、乱数エントロピーは 19PF 相当とする。19PF の乱数エントロピーは、C&R 認証への攻撃パターンを総当たり攻撃、耐久年数を 17 年、チャレンジ要求からレスポンス応答までの処理時間を 1 ミリ秒と仮定して算出。

【RPRREQ_00045】
書き換え対象 ECU、リプログラミングツールおよび OTA マスタ機能 ECU は、SEED 値をツール認証キーで暗号化して KEY 値を生成すること。詳細は 4.1 参照。

【RPRREQ_00046】
書き換え対象 ECU、リプログラミングツールおよび OTA マスタ機能 ECU は、KEY 値を生成するまで SEED 値を保存すること。

【RPRREQ_00047】
リプログラミングツールおよび OTA マスタ機能 ECU は、書き換え対象 ECU に送信するまで KEY 値を保存すること。

【RPRREQ_00048】
書き換え対象 ECU は、リプログラミングツールおよび OTA マスタ機能 ECU より受け取った KEY 値と比較するまで生成した KEY 値を保存すること。

6. Appendix

6.1. リプロ鍵管理・暗号化システム処理

6.1.1. モトローラ S フォーマット処理手順

リプロ鍵管理・暗号化システムにおけるプログラム(モトローラ S フォーマット)の処理手順を示す。

(1) アドレス順並び替え

署名生成対象データ(データレコード部)に対し、データレコード(レコードタイプ S3)がアドレス昇順になっていない場合は、アドレス昇順に並び替える。

(2) 領域抽出

画面入力で指定された開始アドレス、データ長から対象領域を抽出する。なお、領域の指定がない場合は、入力データ全領域を対象データとして扱う。

(3) 空き領域を 0xFF で埋める

対象データレコードのアドレスとデータ長から、空きアドレスに 0xFF を埋め込む。

(4) 署名生成

領域毎に署名を生成する。署名生成の対象範囲は 4.3.2 参照。

(5) 暗号化対象データのプレ処理

暗号化対象データ(データレコード部)に対し、(1)～(3)の処理を実施後、データ部が 16byte になるようにデータレコードの追加、結合を行い、PKCS#7 方式で Padding を行う。

(6) 暗号化

領域毎に暗号化を実施する。

(7) チェックサム再計算

暗号化後のデータレコードでチェックサムを計算し埋め込む。

(8) S0、S7 レコード付与

S0 レコード、S7 レコードを付与する。

(9) 署名ファイルと暗号化プログラムを出力

(4)で生成した署名と、(8)の暗号化プログラムを出力する。

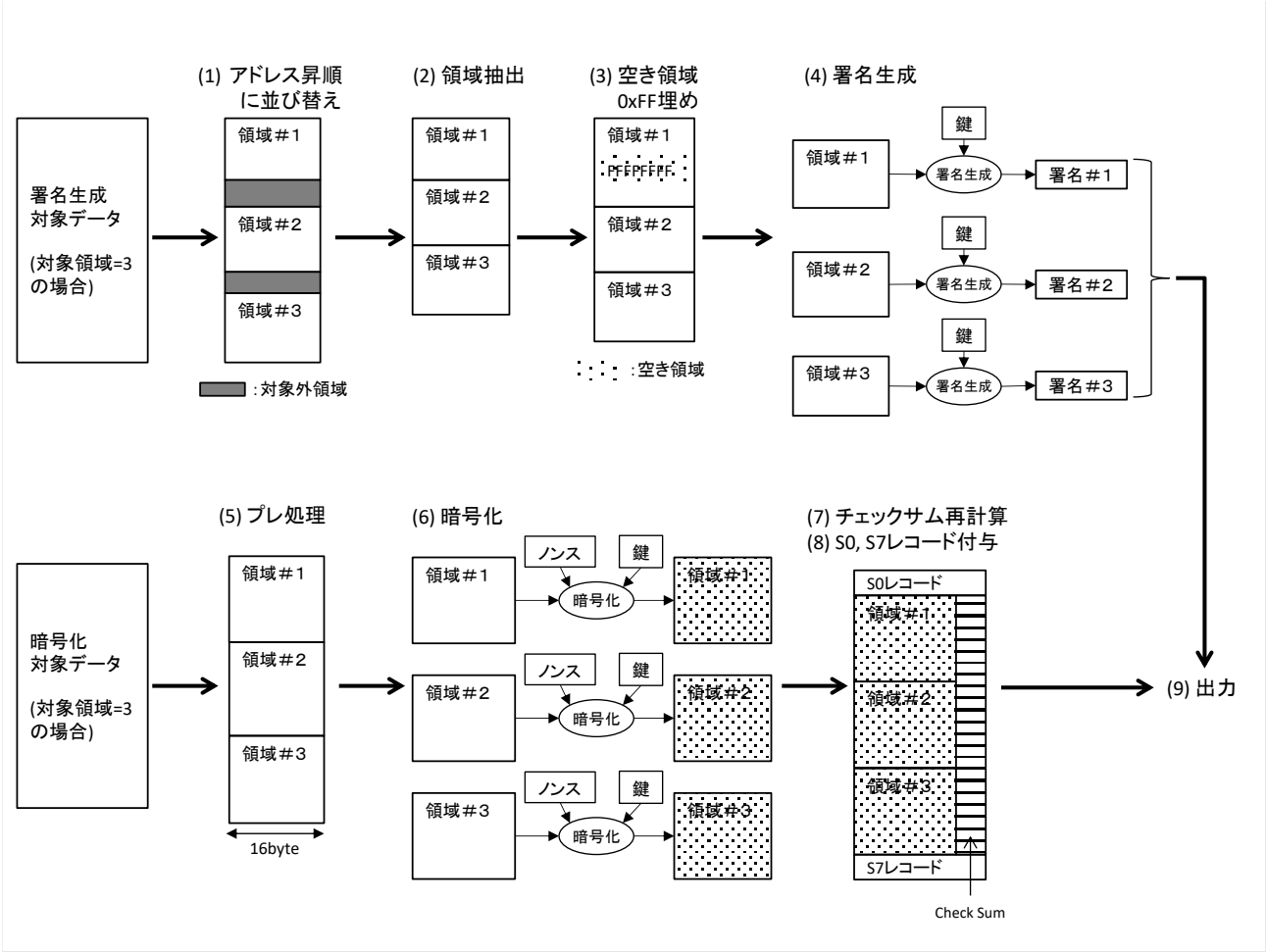


図 6-1　モトローラ S フォーマット暗号処理(対象領域=3 の場合)

6.1.2. バイナリファイル処理手順

リプロ鍵管理・暗号化システムにおけるプログラム(バイナリファイル)の処理手順を示す。

(1) 領域抽出

署名生成対象データに対し、画面入力で指定された入力データ先頭からのオフセット、データ長から対象領域を抽出する。オフセット、データ長の指定はバイト単位とする。なお、領域の指定がない場合は、入力データ全領域を対象データとして扱う。

(2) 署名生成

対象データから署名を生成する。署名生成の対象範囲は 4.3.2 参照。

(3) パディング処理

暗号化対象データに対し、(1)の処理を実施後、PKCS#7 方式でパディングを行う。

(4) 暗号化

Padding 調整済みの暗号化対象データに対し、暗号化を実施する。

(5) 署名ファイルと暗号化プログラムを出力

(2)で生成した署名と、(4)の暗号化プログラムを出力する。

6.2. リプロセキュリティ全体フロー

図 6-2 にリプロセキュリティの全体フローを示す。

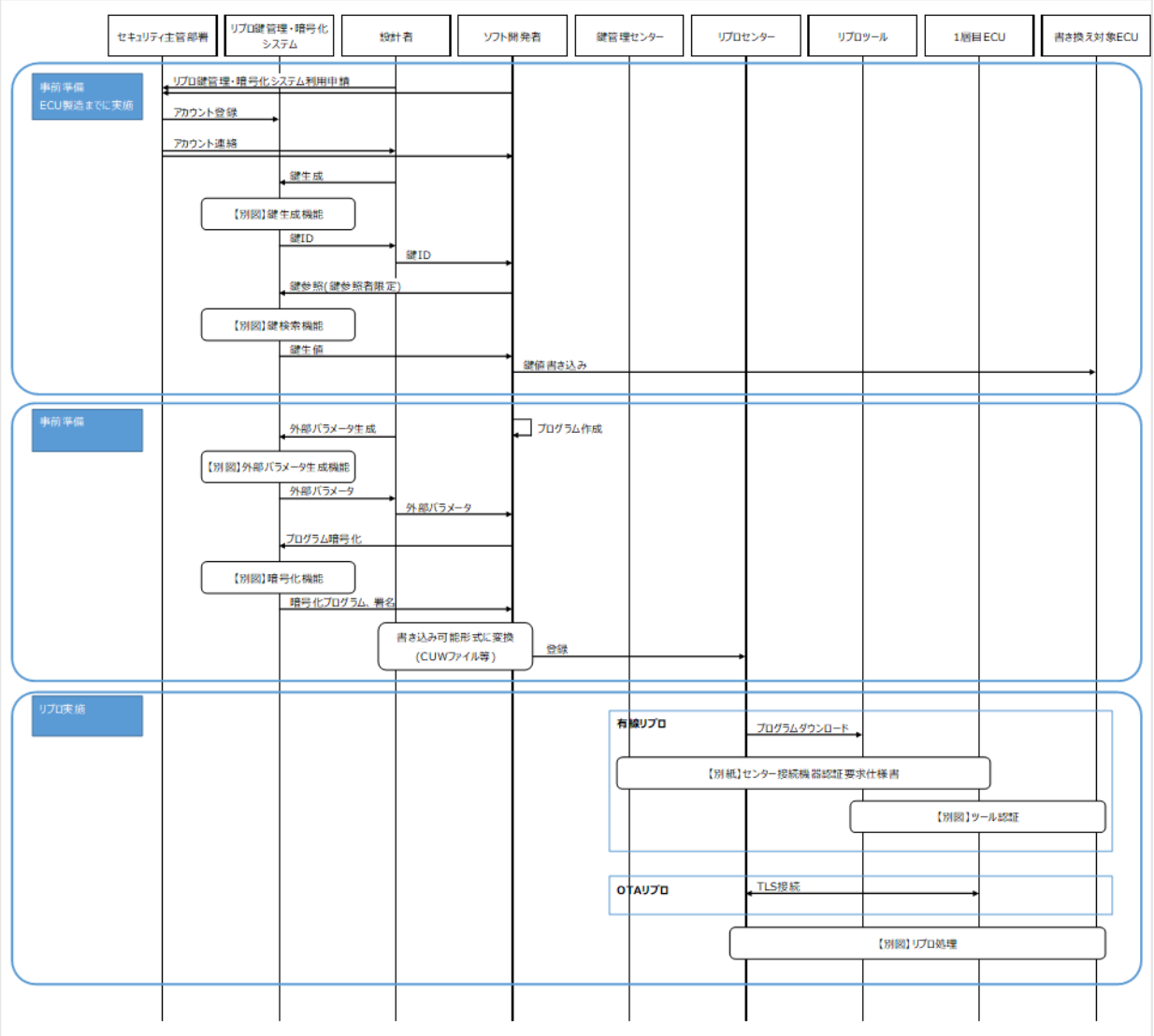


図 6-2　リプロセキュリティの全体フロー

6.2.1. ECU 出荷までの実施事項

ECU 出荷までの実施事項は以下である。

・リプロ鍵管理・暗号化システムのアカウント作成

・暗号鍵の生成(図 6-3)

・暗号鍵の参照(図 6-4)、ECU への暗号鍵の書き込み

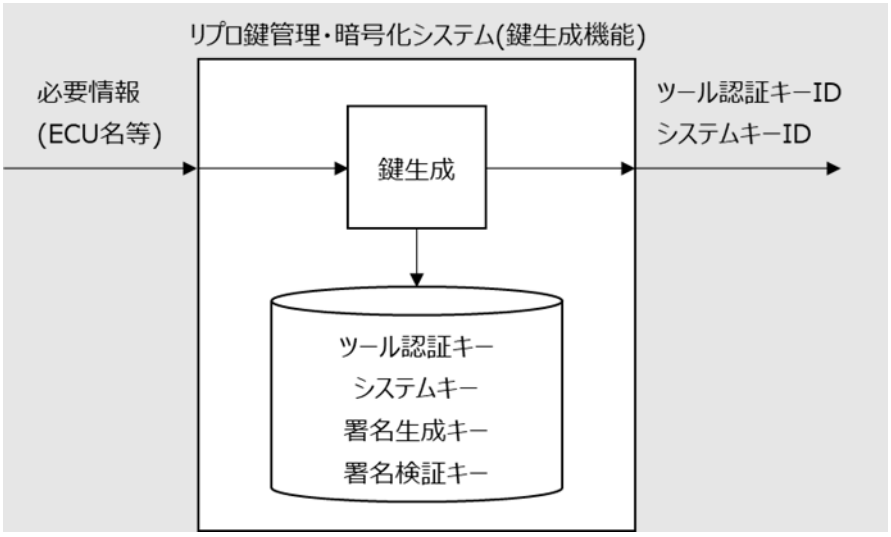


図 6-3 鍵生成機能

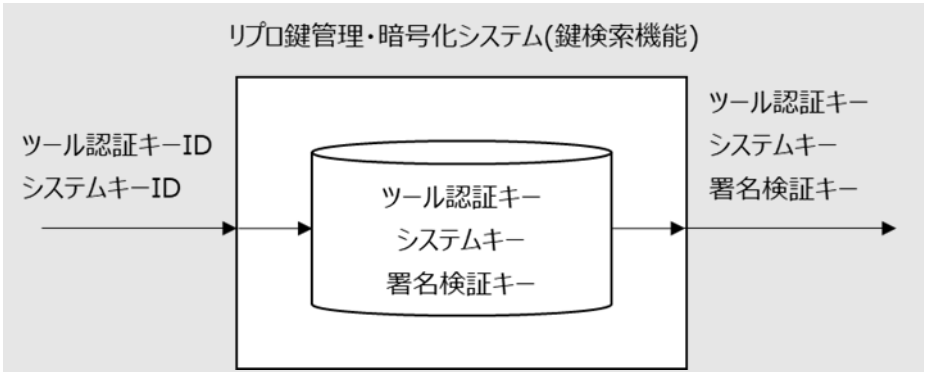


図 6-4 鍵検索機能

6.2.2. リプロ実施までの実施事項

リプロ実施までの実施事項は以下である。

・外部パラメータの生成(図 6-5)

・書き込みプログラムの暗号化、署名生成(図 6-6)

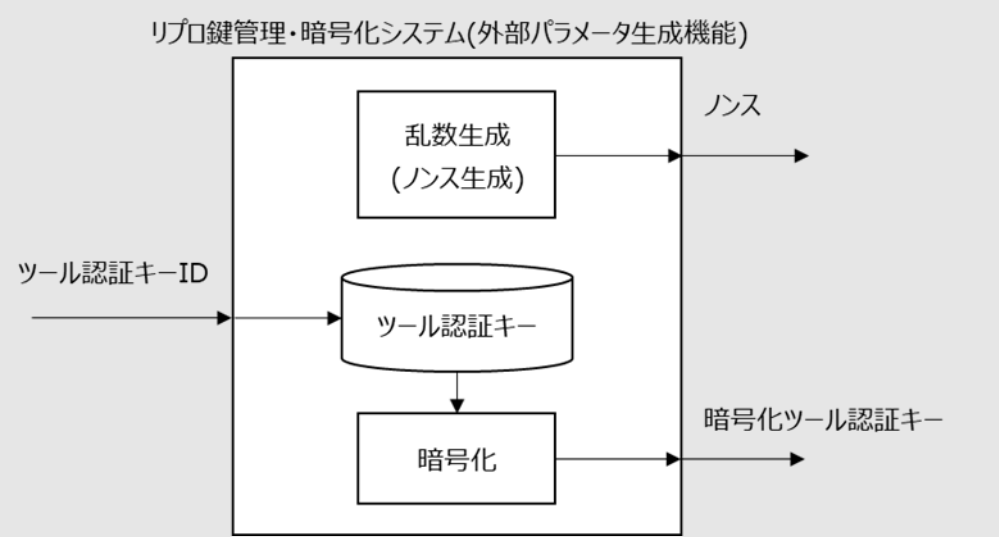


図 6-5 外部パラメータ生成機能

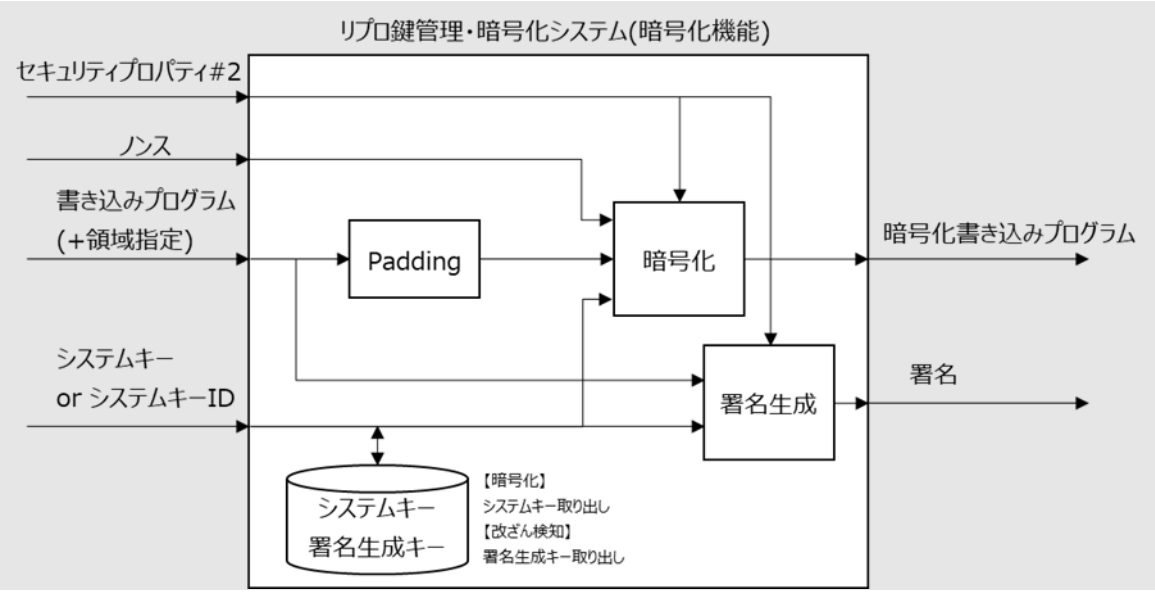


図 6-6 暗号化機能

6.2.3. リプロ時の動作

リプロ時の動作は以下である。ただし、本書ではリプロセキュリティに関する動作のみを記載する。リプロ全体の動作は関連文書[2]を参照。

・暗号化ツール認証キーを用いてツール認証を実施 （図 6-7）
・暗号化書き込みプログラムを復号 （図 6-8）
・署名を用いて改ざん検知を実施 （図 6-8）
・書き込みプログラムバージョンの妥当性を検証 （図 6-8）

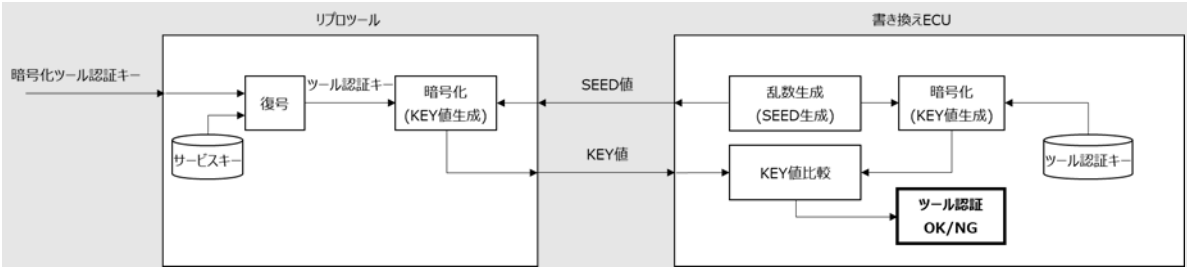


図 6-7 ツール認証処理

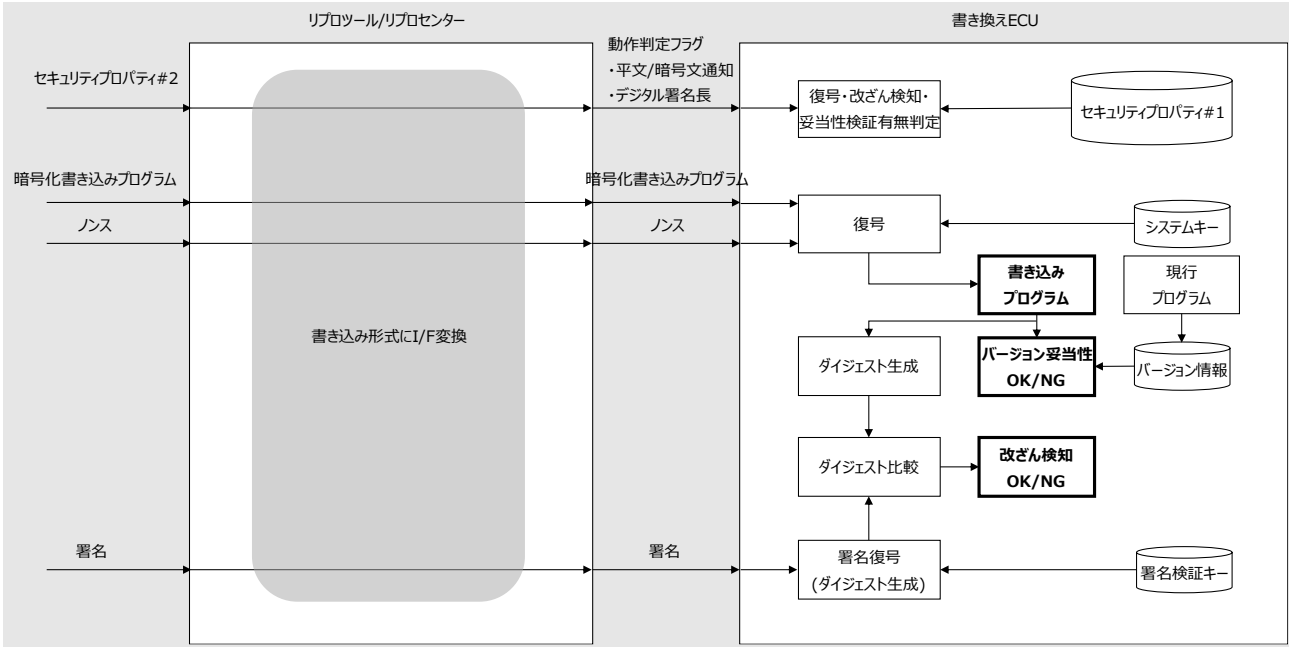


図 6-8 復号、改ざん検知、妥当性検証処理

6.3. サブマイコン/スレーブ ECU 構成の場合の対策

サブマイコン/スレーブ ECU 構成の場合の対策の考え方を記載する。

- Untrusted zone からサブマイコン/スレーブ ECU をリプロできる場合は、本書に記載の標準リプログラミングセキュリティ対策はサブマイコン/スレーブ ECU で実施する。
- Untrusted zone からサブマイコン/スレーブ ECU をリプロできない場合は、本書に記載の標準リプログラミングセキュリティ対策はサブマイコン/スレーブ ECU で実施するか、もしくはメインマイコン/マスタ ECU で実施する。

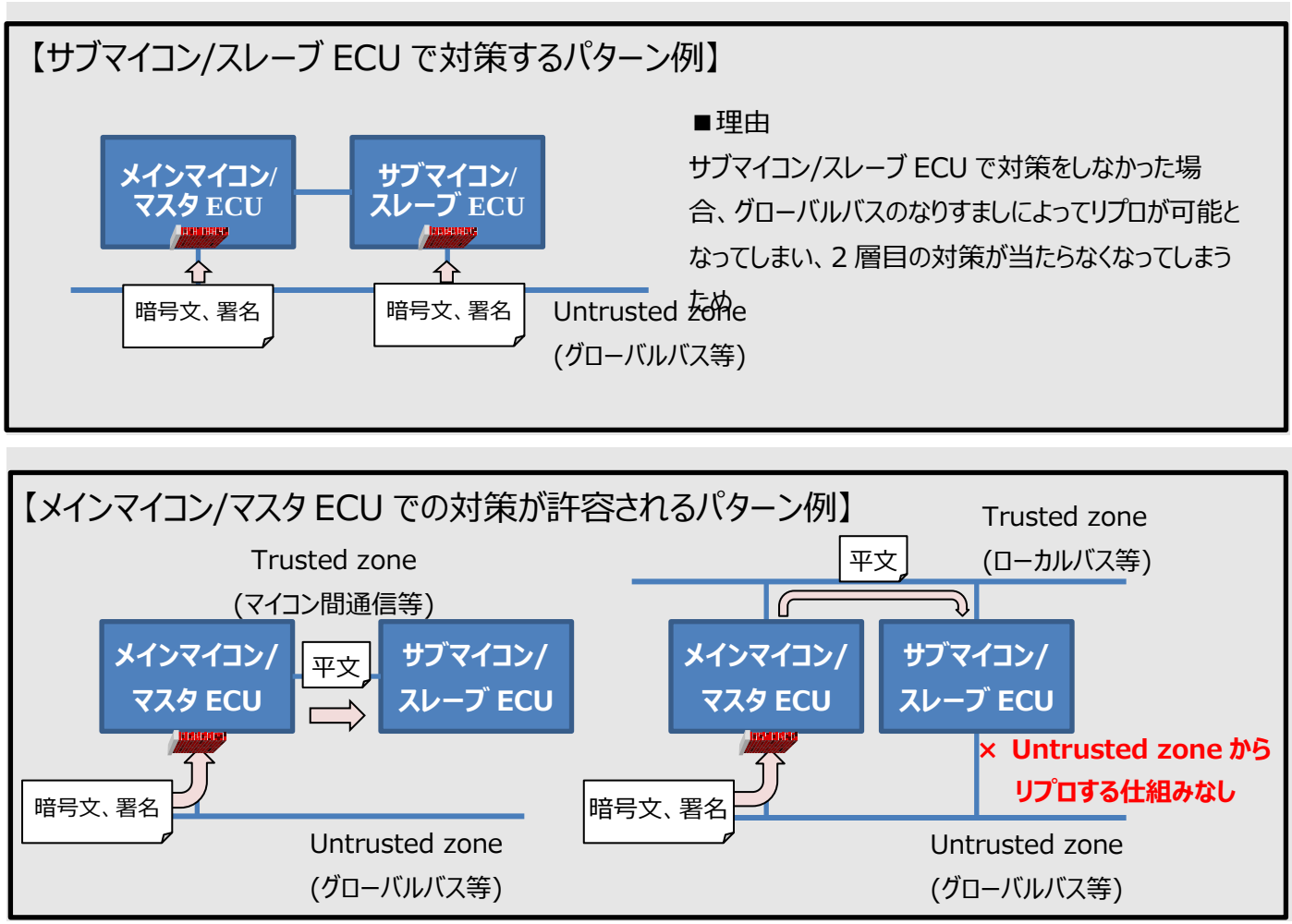


図 6-9 サブマイコン/スレーブ ECU 構成の場合の対策の考え方

6.4. 暗号鍵(ツール認証キー、システムキー、署名検証キー)の変更条件

本節では、リプログラミングセキュリティ用途で ECU に書き込み暗号鍵(ツール認証キー、システムキー、署名検証キー)の変更条件を記載する。

ソフトの変更があり、それにより影響範囲が増える場合、**表 6-1** に基づき、暗号鍵の変更を行う。

表 6-1 鍵の変更条件

#	想定ケース	ソフト	マイコン	サプライヤ	ECUノード	車両	鍵変更	備考
0	【ベース条件】	○	○	○	○	○	－	【ベース条件】
1	マイコン変更 (バックアップ対応等)	●	●	－	－	－	推奨	・ソフト変更あり ・マイコン違いの複数ECUに影響範囲拡大
2	サプライヤ変更 (車種展開のすみわけ等)	●	－	●	－	－	推奨	・ソフト変更あり ・サプライヤ違いの複数ECUに影響範囲拡大
3	ECU変更 (別ECUにソフト転用等)	●	－	－	●	－	推奨	・ソフト変更あり ・複数ECUに影響範囲拡大
4	車両変更 新規開発 (別車両で新規ECU開発)	●	－	－	－	●	推奨	・ソフト変更あり ・複数車両に影響範囲拡大
5	車両変更 ECU流用 (別車両にECU流用)	○	○	○	○	●	任意	・ソフト変更なし ・複数車両に影響範囲拡大
6	ソフト品番変更 (巻き替え/リプロソフト等)	●	○	○	○	○	任意	・ソフト変更あり ・ソフトの巻き替えであり、影響範囲は変化なし

●：変更あり　○：変更なし

※注意事項

・ソフト変更とは、ロジック変更がある場合を指す。定数変更のみの場合はソフト変更なしと解釈可能。

・車両変更とは、車種(車両コード)に変更がある場合を指す。

・鍵変更推奨のケースで鍵変更が困難な場合は、鍵漏洩時のリスクを考慮の上、設計部署で変更可否を判断すること。

1. Revision Record

Version	Contents of revision	Date	Revised
a01-00-a	Creation of new specification	Apr. 28, 2020	46F Hayakawa
a01-01-a	4.2.1 Clarification of decryption process 4.2.2 Clarification of decryption target 4.2.3/4.3.3/4.4.3 Modification of operation conditions of each function 4.4.1 Clarification of validation requirement 5.1 Deletion of 112bit security strength Modification of Security Property #2 Modification of key storage requirement Modification of Security Property #1	Dec. 22, 2020	46F Hayakawa
a01-02-a	4.4.1 Modification of version information validation method 5.1 Modification of Security Property #2 5.1.1 Modification of Security Property #1	Apr. 01, 2021	46F Hayakawa
a01-03-a	4.3.3 Modification of “operation condition of tamper detection” 4.5 Clarification of other requirements Add English translation	May 20, 2021	46F Hayakawa
a01-03-b	6.3 Addition of concept in case of configuration of sub-microcontroller/slave ECU	Jul. 30, 2021	46F Hayakawa
a01-04-a	5.1 Addition of CSP/PSP column in the Reprogramming Spec Parameter table	Aug. 16, 2021	46F Hayakawa
	4.4.3 Modification of operation condition of validation	Aug. 24, 2021	46F Hayakawa
	6.4 Addition of change conditions of cryptographic keys	Aug. 26, 2021	46F Hayakawa
a01-04-b	2.5 Update related specifications	Oct. 05, 2021	46F Yasue
a01-05-a	5.1.1.4 Modification of the random number requirement	Nov. 25, 2021	46F Kakiya
a01-06-a	4.3.2 Clarification of tamper detection target	May. 30, 2022	46F Yasue
	Correct errors in Table 5-1		
a01-07-a	5.1.1.4 Clarification of requirement for random number(RPRREQ_00044)	Jul. 22, 2022	46F Yasue
	Remove RSASSA-PKCS1_v1_5 to comply with the description in Related Document[2] (RPRREQ_00011,Figure5-1)	Sep. 14,2022	46F Tamaki
	4.3.4 Clarify the processing after tamper detection	Sep. 14,2022	46F Kiyokawa
	Change format of cover page	Sep. 15,2022	46F Yasue
	2.5 Update Related Documents 3.2. Add supplement of the processing order of each function.	Oct. 07.2022	46F Tamaki
	2.5, 2.6 Change chapter structures 2.6 Add the related document[10] 3.3 Update Table 3-2 4.4.1 Add the requirement in order to clarify the validation method(RPRREQ_00050)	Oct. 19,2022	46F Yasue

a01-08-a	Add reference requirement (RPRREQ_00044) Modify to unify terms (RPRREQ_00017) 6.1.1 Clarify that the target data is data record	Nov. 01,2022	46F Tamaki
	Modify to match the OTA reprogramming specification(Section2.1, 2.2, 2.3, 3.1, 3.2, 3.3, 4.1, 4.1.2, 4.2.3, 4.3.3, 5.1, 5.1.1.2 and 5.1.1.4	Nov. 09,2022	46F Yasue
a01-09-a	5.1.1 Clarification of requirement for protection of CSP/PSP (RPRREQ_00031) 2.6 Add external links	Jan. 27,2023	46F Tamaki
	Add RSASSA-PKCS1_v1_5 to comply with the description in Related Document[2] (RPRREQ_00011,Figure5-1)	Feb. 08, 2023	46F Yasue
	Add the After Vehicle Development column to Table 3-2.	Feb. 09, 2023	46F Tamaki
	Modify the cover page(target column)	Feb. 24, 2023	46F Tamaki
	Add the requirement of saltLength for RSASSA-PSS (RPRREQ_00011)	Mar. 13, 2023	46F Tamaki

Table of Contents

2. Introduction

2.1. Purpose of this Document

Implement Reprogramming Security countermeasure against attacks that exploit the reprogramming function. This document defines the methodology to achieve Reprogramming Security countermeasure for ECUs that apply Requirements Specification of Standard Reprogramming (Related Document [2], [3]) and Requirements Specification of OTA Reprogramming (Related Document[5]).

2.2. Scope

The scope of this document is ECU for the reprogramming based on the Requirements Specification of Standard Reprogramming (Related Document [2], [3]) and Requirements Specification of OTA Reprogramming (Related Document[5]).

2.3. Preconditions

For security functions relating to a reprogramming function other than Requirements Specification of Standard Reprograming (Related Document [2], [3]) and Requirements Specification of OTA Reprogramming (Related Document[5]), see the Requirements Specification of Common Vulnerability Countermeasure (Related Document [6]).

2.4. Description in this Document

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

2.5. Upper-level Documents

Table 2-1 Upper-level Document List

No	Specification	Ver. (See the latest version)	Issued
1	Vehicle Cybersecurity Concept Definition	SEC-24PF-VCL-CPT-INST-DOC-***-**-*	46F

2.6. Related Documents

Table 2-2 Related Document List

No	Specifications	Ver. (See the latest version)	Issued
1	(Deleted)	-	-
2	Wired Reprogramming Specification Flash Bootloader Software	wrfbs-rd***-***-*	46F

3	Wired Reprogramming Specification Reprogramming Sequence	wrrs-rd***-***-*	46F
4	(Deleted)	-	-
5	OTA4.0 SoftWare Update System Requirements Specifications	otasu40-systemreq-rd***-***-*	OTA Dept.
6	Requirements Specification of Common Vulnerability Countermeasure	SEC-ePF-VUL-CMN-REQ-SPEC-***-**-*	46F
7	Reprogramming Security Operation Regulation	SEC-ePF-RPR-OPE-STD-***-**-*	Information Security Management Dept.
8	Terms and Definitions related to Vehicle Cybersecurity and Privacy	SEC-ePF-TRM-GUD-PROC-***-**-*	46F
9	Wired reprogramming Toyota Standard Specification	twr-rd***-***-*	46F
10	Procedures of ECU Development Process for Vehicle Cybersecurity (In-house only)	SEC-ISO-VCL-PRD-PCD-PROC-***-**-*	46F

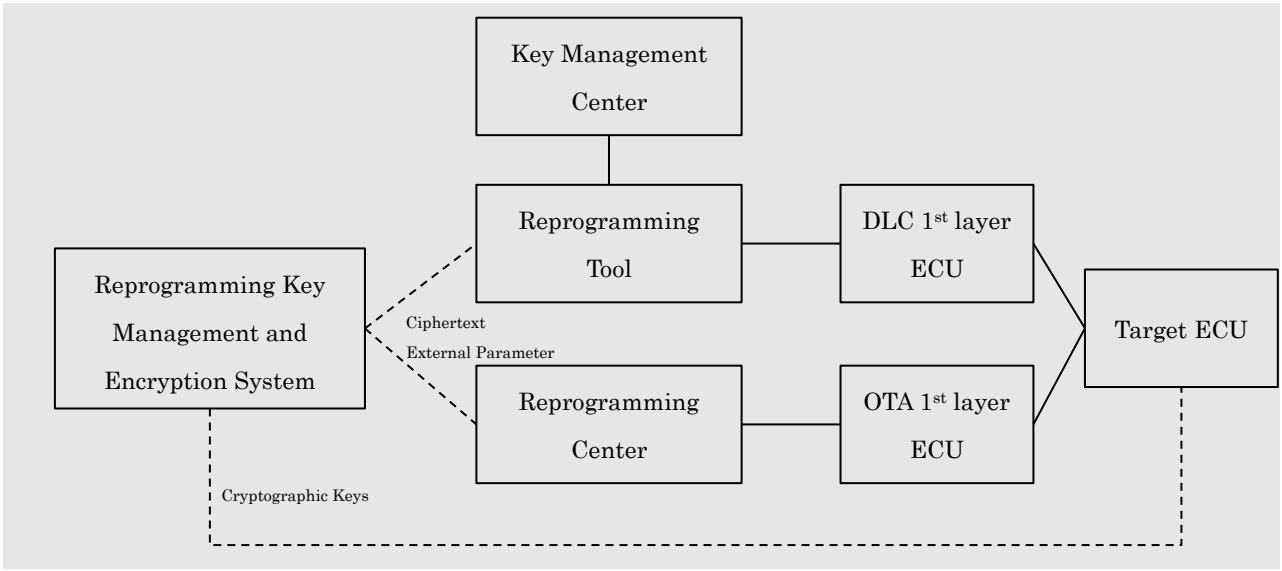
Table 2-3 Public Related Document

No	Title/ External link	Function
1	NIST FIPS197 https://csrc.nist.gov/publications/detail/fips/197/final	AES128
2	NIST SP800-38A https://csrc.nist.gov/publications/detail/sp/800-38a/final	CBC mode
3	NIST FIPS PUB 180-4 https://csrc.nist.gov/publications/detail/fips/180/4/final	SHA-256
4	Public-Key Cryptography Standard (PKCS)#1 v2.2 https://www.rfc-editor.org/rfc/rfc8017	RSA
5	SEC 1:Elliptic Curve Cryptography or ANSI X9.62 https://www.secg.org/sec1-v2.pdf	ECDSA

3. Outline of Requirement

3.1. System Configuration

Figure 3-1 shows the entities that comprise this specification. Table 3-1 shows the role of the entities.



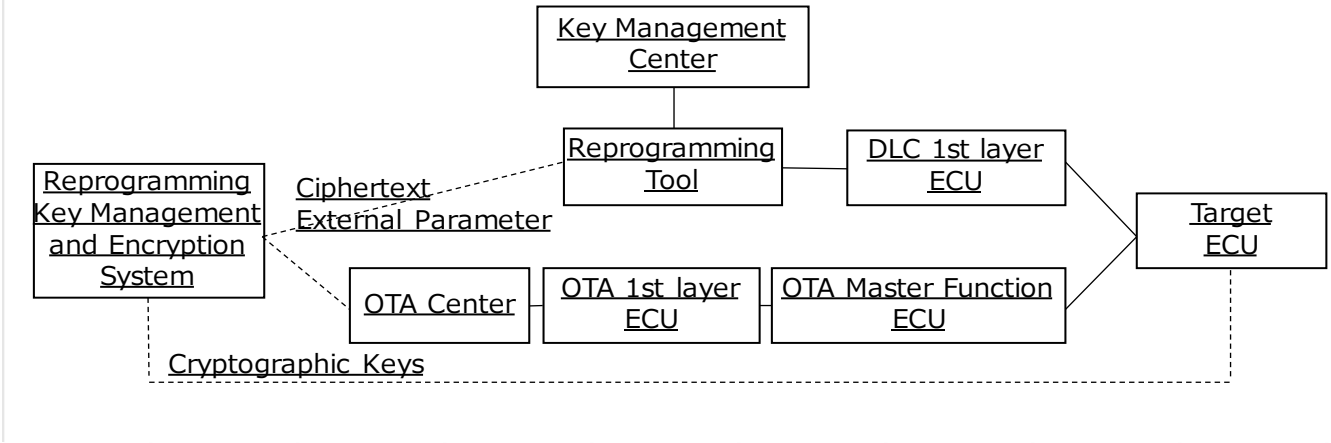


Figure 3-1 System Configuration

Table 3-1 Entity list

Entity	Description
Reprogramming Key Management and Encryption System	System with Generate Key function, Generate External Parameter function and Encrypt Program function
Key Management Center	Center to ensure that the vehicle is connected to the right place in wired reprogramming
Reprogramming Tool	Tool for reprogramming in wired reprogramming
DLC 1st layer ECU	ECU connected to the Reprogramming Tool via DLC in wired reprogramming

OTA Center	Center to deliver the program in OTA reprogramming
OTA 1st layer ECU	ECU connected to the OTA Center via Communication device in OTA reprogramming
OTA Master Function ECU	ECU which is received writing program from OTA Center and delivers to Target ECU in OTA reprogramming
Target ECU	ECU which rewrite the program by reprogramming

3.2. Sequence

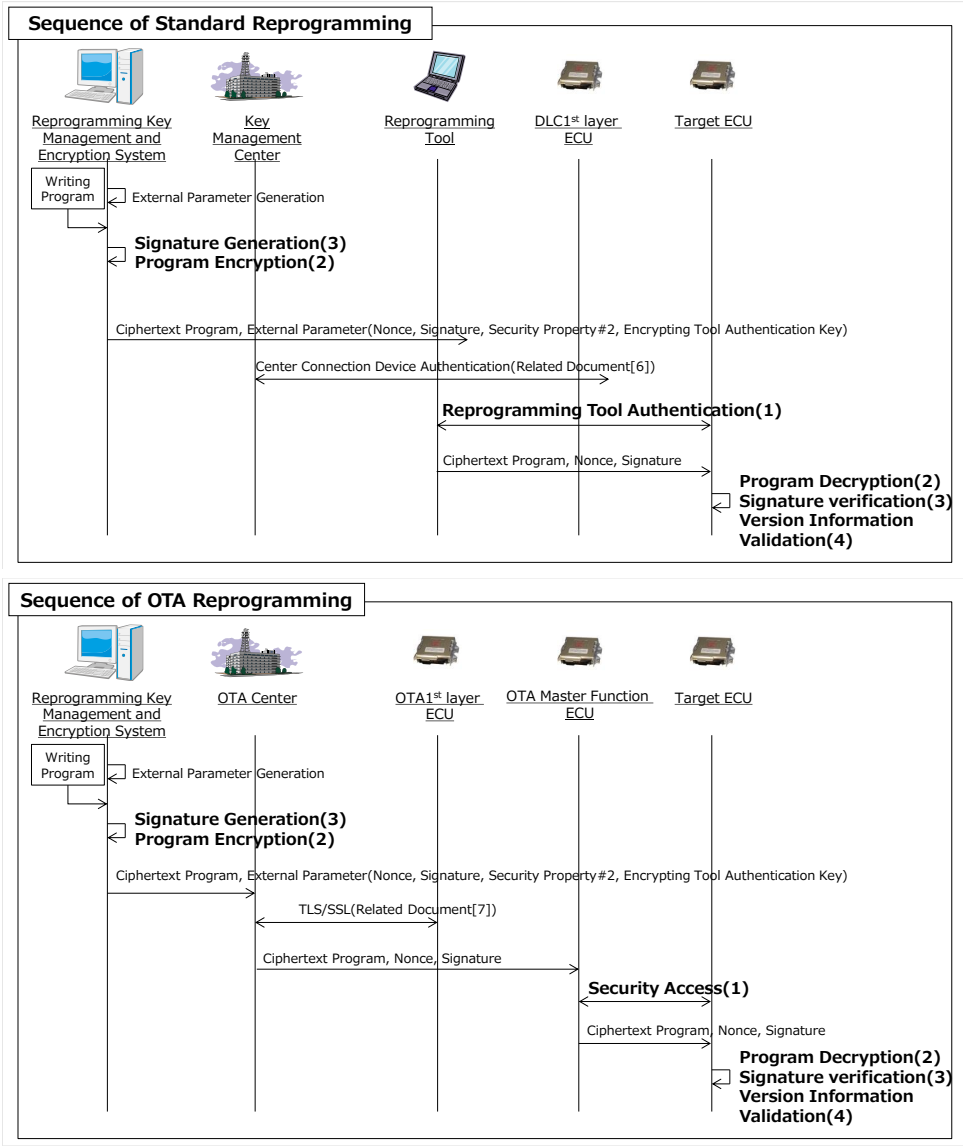


Figure 3-2 shows an overview diagram of reprogramming security.

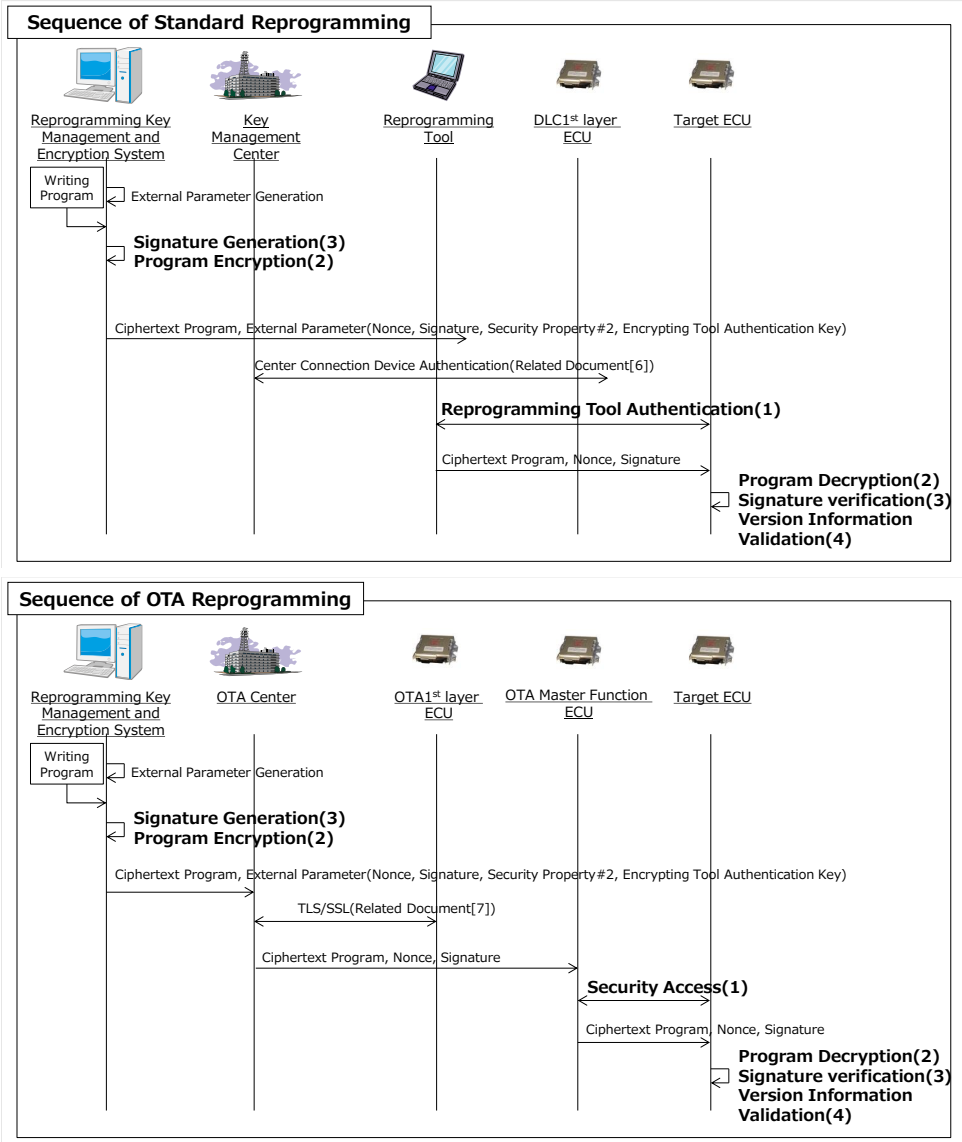


Figure 3-2 Overview diagram of Reprogramming Security

This document defines below functions.

(1) Reprogramming Tool Authentication/Security Access

Prevent that program has been written from malicious source of writting by authenticating source of writting.

(2) Program Encryption and Decryption

Prevent that leaked program has been used for analysis/tampering by encryption

(3) Tamper Detection of Program

Prevent that malicious program has been operated by tampering detection

(4) Version Information Validation of Writing Program

Prevent that malicious version program has been operated (ex. rollback attack) by version information validation.

(Supplement) See [Related Document (9)] for the processing order of the above functions.

3.3. Requirement List

Table 3-2 shows a list of requirements shall be met by each entities. For more details of the requirements, see Chapter 4.

Table 3-2 Requirement table

Requirement	After Vehicle Development	Reprogramming Key Management and Encryption System	Reprogramming Tool	OTA Master Function ECU	Target ECU	
					Wired Reprogramming	OTA Reprogramming
RPRREQ_00001	–		○	○	○	○
RPRREQ_00002	–		○	○		
RPRREQ_00003	–				○	○
RPRREQ_00004	–	○			○	○
RPRREQ_00005	–	○				
RPRREQ_00006	–				○	○
RPRREQ_00007	–	○			○	○
RPRREQ_00008	–	○			○	○
RPRREQ_00009	–				○	○
RPRREQ_00011	–	○			○	○
RPRREQ_00012	–	○				
RPRREQ_00013	–				○	○
RPRREQ_00014	–	○			○	○
RPRREQ_00017	–	○			○	○
RPRREQ_00018	–				○	○
RPRREQ_00019	–				○	○
RPRREQ_00020	–				○	○
RPRREQ_00021	–				○	○
RPRREQ_00022	–				○	○
RPRREQ_00023	–				○	○
RPRREQ_00024	–				○	○
RPRREQ_00025	–					
RPRREQ_00026	–					

Requirement	After Vehicle Development	Reprogramming Key Management and Encryption System	Reprogramming Tool	OTA Master Function ECU	Target ECU	
					Wired Reprogramming	OTA Reprogramming
RPRREQ_00027	–				○	○
RPRREQ_00028	–				○	○
RPRREQ_00029	–	○			○	○
RPRREQ_00030	–		○			
RPRREQ_00031	–				○	○
RPRREQ_00032	–	○				
RPRREQ_00033	–		○			
RPRREQ_00034	–	○				
RPRREQ_00037	–	○			○	○
RPRREQ_00038	–	○			○	○
RPRREQ_00039	–	○			○	○
RPRREQ_00040	–		○	○		
RPRREQ_00041	–				○	○
RPRREQ_00042	○				○	○
RPRREQ_00043	–				○	○
RPRREQ_00044	–				○	○
RPRREQ_00045	–		○	○	○	○
RPRREQ_00046	–		○	○	○	○
RPRREQ_00047	–		○	○		
RPRREQ_00048	–				○	○
RPRREQ_00049	–				○	○
RPRREQ_00050	–				○	○

4. Functional Requirement

4.1. Reprogramming Tool Authentication

Reprogramming Tool Authentication includes Security Access defined in OTA reprogramming.

4.1.1. Outline of Protocol

[RPRREQ_00001]

The following method shall be used for reprogramming tool authentication.

Protocol: CHAP (Challenge Handshake Authentication Protocol)

Algorithm: AES128 ECB mode [See Public Related Document [1]]

Cryptographic Key: Tool Authentication Key

4.1.2. Reprogramming Tool Authentication Process

Target ECU authenticates reprogramming tool and OTA Master Function ECU with using the Tool Authentication Key. See Related Document [2] and [5] for details.

[RPRREQ_00002]

Reprogramming tool and OTA Master Function ECU shall carry out the following processing at reprogramming tool authentication.

(1) Make the SEED request to the target ECU.

(2) The Encrypting Tool Authentication Key shall be decrypted using the Service Key.

(3) The KEY value shall be generated using the SEED value received from the target ECU and the Tool Authentication Key

(4) The calculated KEY value shall be transmitted to the target ECU.

[RPRREQ_00003]

The target ECU shall carry out the following processing at reprogramming tool authentication.

(5) The SEED value shall be generated, and be transmitted to the reprogramming tool or OTA Master Function ECU.

(6) The KEY value shall be generated using the SEED value and the Tool Authentication Key.

(7) The KEY value received from the reprogramming tool or OTA Master Function ECU shall be compared with the KEY value generated in (6) to check if they are matched. If they are matched, authentication is success. If they are not matched, authentication is failure.

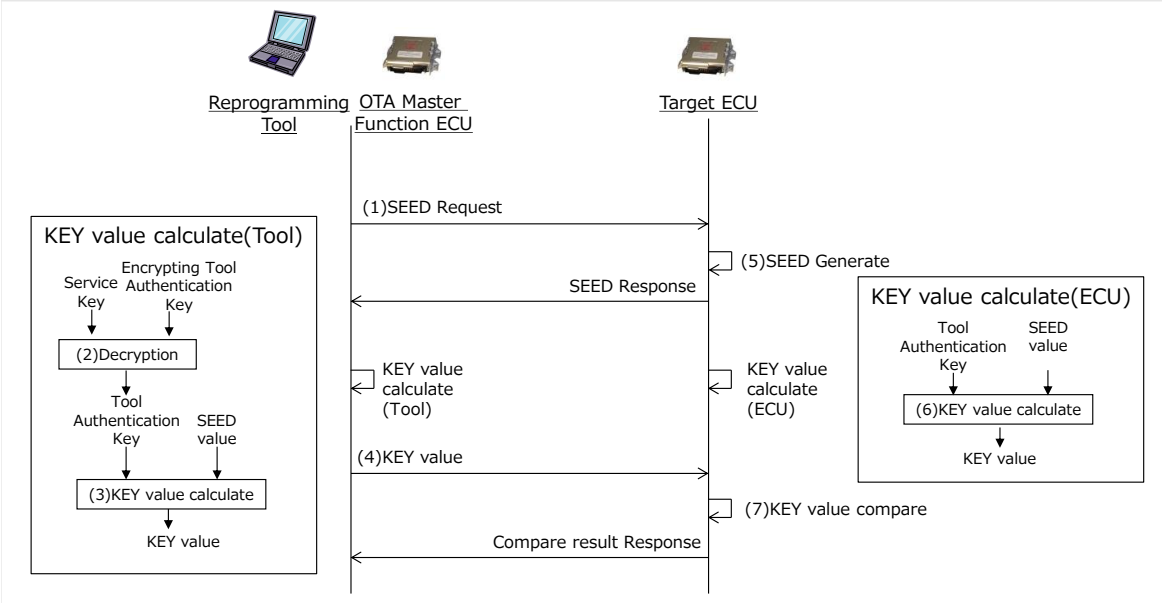


Figure 4-1 Reprogramming Tool Authentication Sequence

4.2. Program Encryption/Decryption

This chapter describes the specifications for encrypting and decrypting the writing program.

4.2.1. Encryption/Decryption Method

[RPRREQ_00004]

It shall be used the following algorithm for program encryption or decryption.

Cryptographic Algorithm: AES128 CBC mode [See Public Related Document [1], [2]]

Cryptographic Key: System Key

IV value: Nonce

[RPRREQ_00005]

The Reprogramming Key Management and Encryption System shall encrypt plaintext writing program using the Nonce and the System Key.

[RPRREQ_00006]

The target ECU shall decrypt encrypted writing program using Nonce and System Key.

[RPRREQ_00049]

The target ECU shall be able to distinguish and remove the PKCS#7 Padding area of the plaintext writing program after decryption.

4.2.2. Encryption Target

[RPRREQ_00007]

All data (include flash control program) that is downloaded by reprogramming shall be subject to encryption.

(Supplement)

・In case of Delta reprogramming, encryption target is delta file.

・In case of Compression reprogramming, encryption target is compression file.

[RPRREQ_00008]

Writing program whose size have been adjusted by padding shall be subject to encryption.

(Supplement)

・Padding is implemented in the Reprogramming Key Management and Encryption System

・Use PKCS#7 for Padding

・In case of plaintext program, Padding is not required

4.2.3. Operation Conditions of Decryption

[RPRREQ_00009]

The target ECU shall determine whether or not to implement a decryption operation in accordance with the plaintext/ciphertext notification from Reprogramming Tool and OTA Master Function ECU.

4.3. Program Tamper Detection

This chapter describes the specifications for tamper detection the writing program. Only one type of algorithm to be implemented in ECU is acceptable

4.3.1. Tamper Detection Method

[RPRREQ_00011]

In case of using RSA digital signature for tamper detection, this requirement shall be applied.

The following method and parameters shall be used.

Signature generation/verification algorithm: RSASSA-PSS or RSASSA-PKCS1_v1_5 [See Public Related Document [4]]

Key to be used for signature generation: Signature Generation Key

Key to be used for signature verification: Signature Verification Key

Hash Function: SHA-256 [See Public Related Document [3]]

RSA Public exponent: 65537 (decimal number)

SaltLength: 32byte (SaltLength is specific to RSASSA-PSS.)

[RPRREQ_00014]
In case of using ECDSA digital signature for tamper detection, this requirement shall be applied. The following method and parameters shall be used.

Signature generation/verification algorithm: ECDSA [See Public Related Document [5]]
Key to be used for signature generation: Signature Generation Key
Key to be used for signature verification: Signature Verification Key
Hash Function: SHA-256 [See Public Related Document [3]]
Elliptic Curve: P-256

[RPRREQ_00012]
The Reprogramming Key Management and Encryption System shall generate writing program signature using the Signature Generation Key.

[RPRREQ_00013]
When the program that is subject to tamper detection is received, the target ECU shall verify the signature using the Signature Verification Key.

4.3.2. Tamper Detection Target

[RPRREQ_00017]
The target area of tamper detection shall be the following writing program.
・In case of Whole Reprogramming, tamper detection target is all downloaded data.
・In case of Delta/Compression Reprogramming, tamper detection target is all data before differential extraction or compression
(Supplement) See 6.1 for processes the target data.

4.3.3. Operation Conditions of Tamper Detection

[RPRREQ_00018]
When the Encryption Flag (Security Property#1) is ON, it shall be sure tamper detection.

[RPRREQ_00019]
When the Encryption Flag is OFF, the with or without tamper detection operation shall be determined in accordance with checkTypeIdentifier from the Reprogramming Tool and OTA Master Function ECU. (See Related Document [2])

[RPRREQ_00020]
If the combination of the Encryption Flag and checkTypeIdentifier is unauthorized, the target ECU shall output the information that can be judged as unauthorized to the Reprogramming Tool and OTA Master Function ECU.

(Supplement) Example of information that can be judged as unauthorized
・Negative response
・Detail code in positive response
(See Related Document [2])

Table 4-1 Tamper Detection Operation Check

Encryption Flag	checkTypeIdentifier	With or without Tamper Detection	Judgement
ON	0x01(signature)	With Tamper Detection	○
ON	Other than 0x01	With Tamper Detection	×(unauthorized)
OFF	0x01(signature)	With Tamper Detection	○
OFF	Other than 0x01	Without Tamper Detection	○

4.3.4. Processing after Tamper Detection
[RPRREQ_00021]
If the comparison result of digest in tamper detection was “Unmatched”, the ECU shall not activate the writing program.
(Supplement) See [Related Document (2)] for processes other than the above.

(Note) Tamper detection after writing in FLASH
When a tamper is detected after the program was written in FLASH, the FLASH will be in the state where an unreliable program is written.

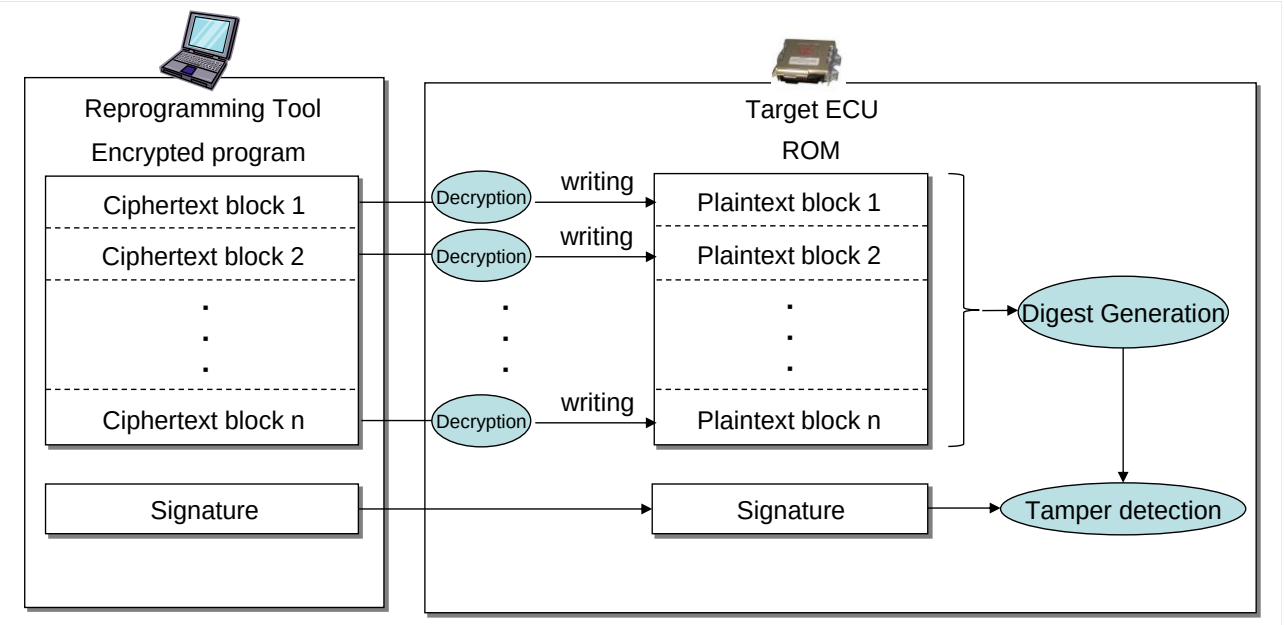


Figure 4-2 Example image of tamper detection timing

4.4. Version Information Validation of Writing Program

4.4.1. Validation Method

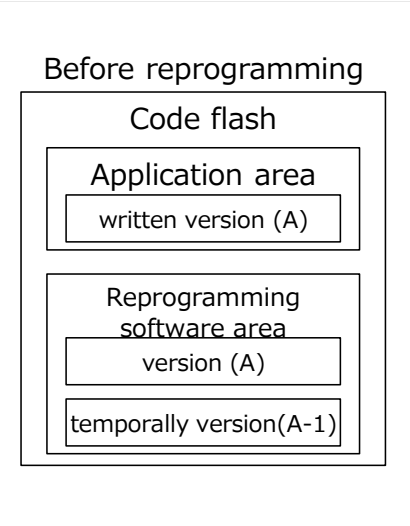
[RPRREQ_00022]

The target ECU shall validate that the version of received program is equal to or greater than the version of current program.

(Supplement)

It is desirable to be able to realize this function with FBL (Reprogramming software area)

Example :



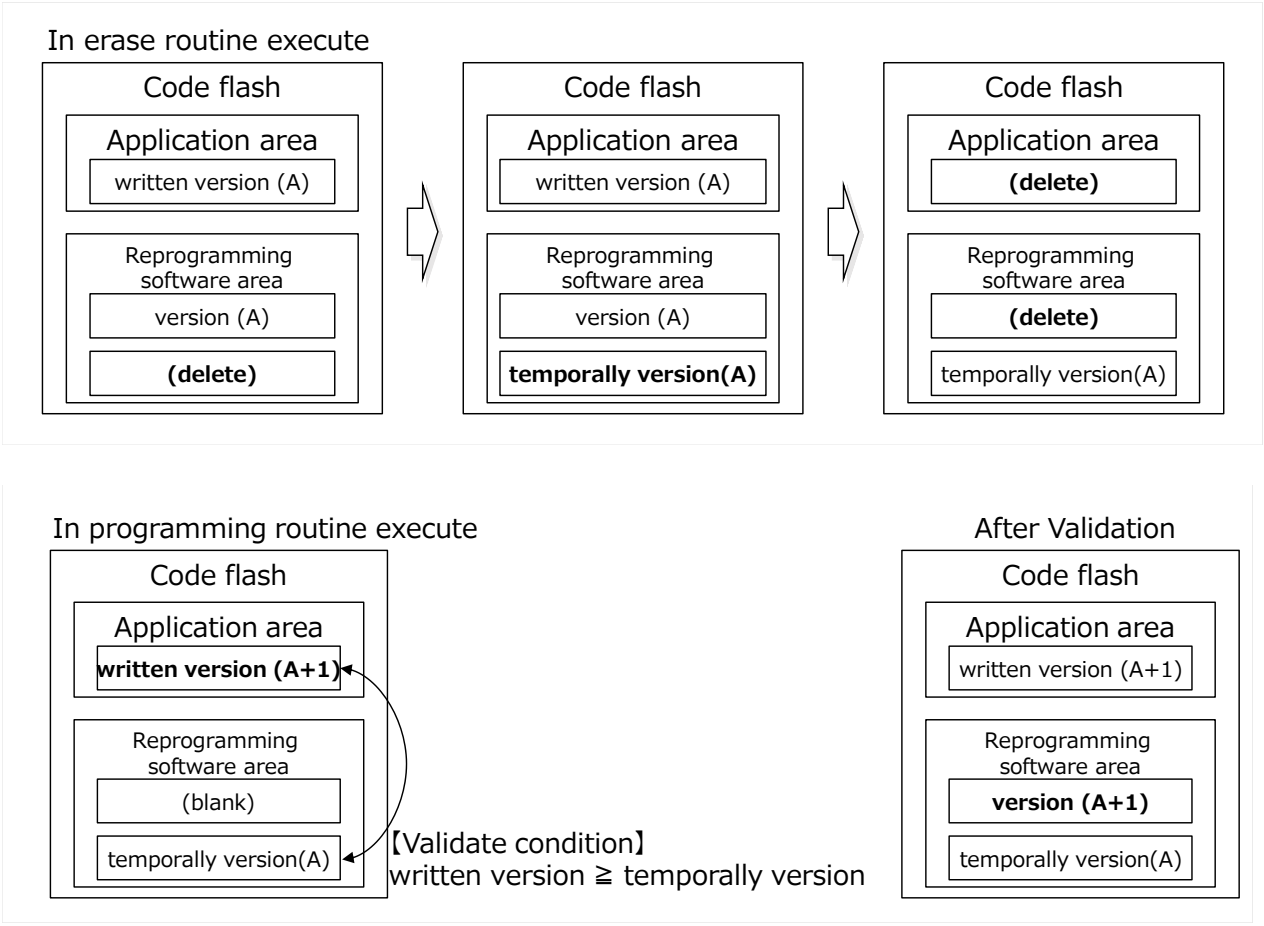


Figure 4-3 Implementation Example of Validation

[RPRREQ_00050]

As a result of reuse analysis for ECU, if it is determined that the program changes affect the cybersecurity function, the ECU designer shall set the version of writing program greater than the version of the current ECU program. Refer to Related Document[10] for ECU's reuse analysis.

4.4.2. Validation Target

[RPRREQ_00023]

The target of validation shall be the version information written into the program downloaded in reprogramming.

4.4.3. Operation Conditions of Validation

[RPRREQ_00024]

If the Encryption Flag (Security Property#1) is ON, the target ECU shall validate the Version Information.

(Supplement) If the Encryption Flag is OFF, it is optional for the ECU to validate version information..

[RPRREQ_00025]
Deleted.

[RPRREQ_00026]
Deleted.

4.4.4. Processing after Validation

[RPRREQ_00027]
The target ECU shall not be activated by a program that has been judged an invalid version as a result of version information validation.

4.5. Other Requirements

[RPRREQ_00028]
While the vehicle is moving, target ECU shall not accept the communication stop diagnostic command in the reprogramming sequence.

5. Non-Functional Requirement

5.1. Parameter Requirement

In reprogramming security, use the parameters lists in Table 5-1.

Table 5-1 Reprogramming Spec Parameter

Classification	Name	Size (byte)	Usage	Wired Reprogramming	OTA Reprogramming	CSP/ PSP
Cryptographic Key	System Key	16	A key for encrypting and decrypting the writing program	○	○	CSP
	Tool Authentication Key	16	A key for generating a KEY value for reprogramming tool authentication	○	○	CSP
	Signature Generation Key (RSA)	384	A key for generating a signature for tamper detection in the ECU (RSA)	○	○	CSP
	Signature Generation Key (ECDSA)	32	A key for generating a signature for tamper detection in the ECU (ECDSA)	○	○	CSP
	Signature Verification Key (RSA)	384	A key for verifying a signature for tamper detection in the ECU (RSA)	○	○	PSP
	Signature Verification Key (ECDSA)	64	A key for verifying a signature for tamper detection in the ECU (ECDSA)	○	○	PSP
	Service Key	16	A key for encrypting/decrypting a tool authentication key in the reprogramming tool	○		CSP
Security Property	Security Property #1	1	The Encryption Flag (0xFF : OFF, other : ON)	○	○	PSP
External Parameter	Encrypting Tool Authentication Key	16	A tool authentication key encrypted by the service key	○		-
	Nonce(Note 1)	16	Data to be combined with the writing program to be encrypted during encryption	○	○	-
	Signature(RSA)	384	Data for judging the tamper detection (RSA)	○	○	-
	Signature(ECDSA)	64	Data for judging the tamper detection (ECDSA)	○	○	-

Classification	Name	Size (byte)	Usage	Wired Reprogramming	OTA Reprogramming	CSP/ PSP
	Security Property #2	1	Data including the following security information (Note 2) ・ON/OFF flag of security function ・Encryption algorithm/security strength	○	○	-
Tool Authentication Parameter	SEED value	16	Date for generating a KEY value during authentication of a reprogramming tool	○	○	-
	KEY value	16	Data for judging whether or not a reprogramming tool is an authorized tool during authentication of the reprogramming tool	○	○	-

(Note 1) "IV" is general name in case of CBC mode, but describes as "nonce" in this document
(Note 2) The set values for Security Property #2 shall be set as shown in Figure 5-1

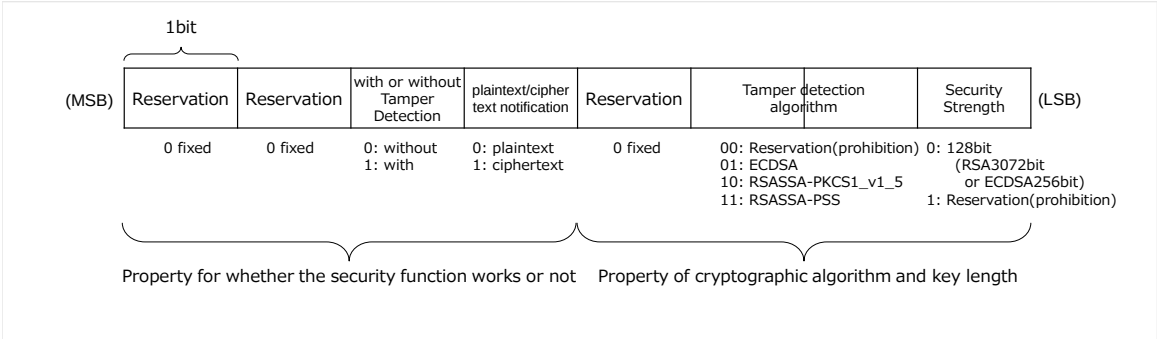


Figure 5-1 Security Property #2

5.1.1. Parameter Generation and Storage

This chapter describes the requirements for parameter generation and storage. Parameters marked *1 are applicable only for wired reprogramming.

5.1.1.1. Cryptographic Key

The cryptographic keys specified in this document are the System Key, the Tool Authentication Key, the Signature Generation Key, the Signature Verification Key and the Service Key.

[RPRREQ_00029]
The System Key, the Tool Authentication Key*1, the Signature Generation Key and the Signature Verification Key shall be generated using generate key function described in Reprogramming Security Operation Regulation (Related Document [7]).
(Supplement) Each cryptographic key is generated by random numbers that meet the requirement

of Requirements Specification of Common Vulnerability Countermeasure (Related Document [6]).

[RPRREQ_00030]
The Service Key*1 shall be obtained according to Reprogramming Security Operation Regulation (Related Document [7]).
(Supplement) Only Reprogramming Tool developer need the Service Key.

[RPRREQ_00031]
The System Key, the Tool Authentication Key*1 and the Signature Verification Key shall be stored in the non-reprogrammable area of the target ECU. The target ECU shall meet the requirement of Requirements Specification of Common Vulnerability Countermeasure (Related Document [6]) for protection of CSP/PSP.

[RPRREQ_00032]
The System Key, the Tool Authentication Key*1, the Signature Generation Key and the Signature Verification Key shall be stored in the Reprogramming Key Management and Encryption System.

[RPRREQ_00033]
The Service Key*1 shall be stored in the Reprogramming Tool.

[RPRREQ_00034]
The Service Key*1 shall be stored in the Reprogramming Key Management and Encryption System.

5.1.1.2. External Parameter

The external parameters specified in this document are the Encrypting Tool Authentication Key, the Nonce, the Signature and the Security Property #2.

[RPRREQ_00037]
The Encrypting Tool Authentication Key*1 and the Nonce shall be generated using generate external parameter function described in Reprogramming Security Operation Regulation (Related Document[7]).
(Supplement) The Encrypting Tool Authentication Key is generated by the Encrypting Tool Authentication Key with the Service Key. Use AES128 ECB mode for encryption. The Nonce is generated by random numbers that meet the requirement of Requirements Specification of Common Vulnerability Countermeasure (Related Document [6)].

[RPRREQ_00038]

The Signature shall be generated using encrypt program function described in Reprogramming Security Operation Regulation (Related Document [7]).
(Supplement) See 4.3 for how to generate Signature.

[RPRREQ_00039]
The Security Property #2 shall be set according to whether the security function work or not and the cryptographic algorithm based on Figure 5-1 at all such times.

[RPRREQ_00040]
The Reprogramming Tool and OTA Master Function ECU shall receive the Encrypting Tool Authentication Key*1, the Nonce, the Signature and the Security Property #2 as external parameter and store until reprogramming process is completed.

[RPRREQ_00041]
The target ECU shall receive the Nonce and the Signature as external parameter and store until the process with each parameter is completed.
(Supplement) Process with each parameter
Nonce: Decryption
Signature: Tamper detection

5.1.1.3. Security Property
The security property specified in this document is the Security Property #1.

[RPRREQ_00042]
The Security Property #1 shall be set at the time of the target ECU shipment. The Encryption Flag of Security Property #1 shall be set to OFF if prototype product and ON if production product.

[RPRREQ_00043]
The target ECU shall store the Security Property #1 in non-reprogrammable area.

5.1.1.4. Tool Authentication Parameter
[RPRREQ_00044]
The target ECU shall generate the SEED value by random number that meet the requirement for 【VULCMN_00200】, 【VULCMN_00300】 in Related Document [6]6. However, the entropy of the random number and the penalty shall be complied with the following.
Entropy of the random number: 40bit or more
Penalty: Option

(Supplement) The entropy of the random number is equivalent to 19PF because this function is not related to the cybersecurity requirements which are derived from threat analysis and risk assessment result for Post19PF. The entropy of the random number in 19PF is calculated assuming that the attack pattern for C&R authentication is brute force attack, the durable time is 17 years and the processing time from C&R authentication challenge request to the response is 1 ms.

[RPRREQ_00045]
The target ECU and the Reprogramming Tool and OTA Master Function ECU shall generate the KEY value by encrypting the SEED value with the Tool Authentication Key. See 4.1 for details.

[RPRREQ_00046]
The target ECU and the Reprogramming Tool and OTA Master Function ECU shall store the SEED value until generate the KEY value.

[RPRREQ_00047]
The Reprogramming Tool and OTA Master Function ECU shall store the KEY value until send it to the target ECU

[RPRREQ_00048]
The target ECU shall store the KEY value generated in the target ECU until compared with the KEY value from the Reprogramming Tool and OTA Master Function ECU.

6. Appendix

6.1. Processing of the Reprogramming Key Management and Encryption System

6.1.1. Encryption Processing of Motorola S format

This section clarifies the encryption processing of Motorola S format in the Reprogramming Key Management and Encryption System

(1) Rearrange in order of address

If the data record, the target data for which signatures are to be generated, is not in the ascending order of the address, the Reprogramming Key Management and Encryption System rearranges the addresses in ascending order.

(2) Take out the area

Extract the target area from the start address and data length specified by the screen input. If no area is specified, the entire input data area is treated as the target data.

(3) Fill the blank area with 0xFF

If there is blank area, the Reprogramming Key Management and Encryption System fills the blank area with 0xFF.

(4) Generate signature

The Reprogramming Key Management and Encryption System generates signature. Range of subject to signature generation, see 4.3.2.

(5) Pre-process the data record that is subject to encrypt

After (3), data record is added and merged so that the data part becomes 16 bytes for the data to be encrypted, and padding with PKCS#7.

(6) Encrypt

The Reprogramming Key Management and Encryption System encrypts each area.

(7) Update Check Sum

The Reprogramming Key Management and Encryption System updates the value of the check sum according to the encrypted data.

(8) Add S0 record and S7 record

The Reprogramming Key Management and Encryption System adds S0 record and S7 record.

(9) Output Signature and Encrypted Writing Program

The Reprogramming Key Management and Encryption System outputs signature in (4) and encrypted writing program in (8).

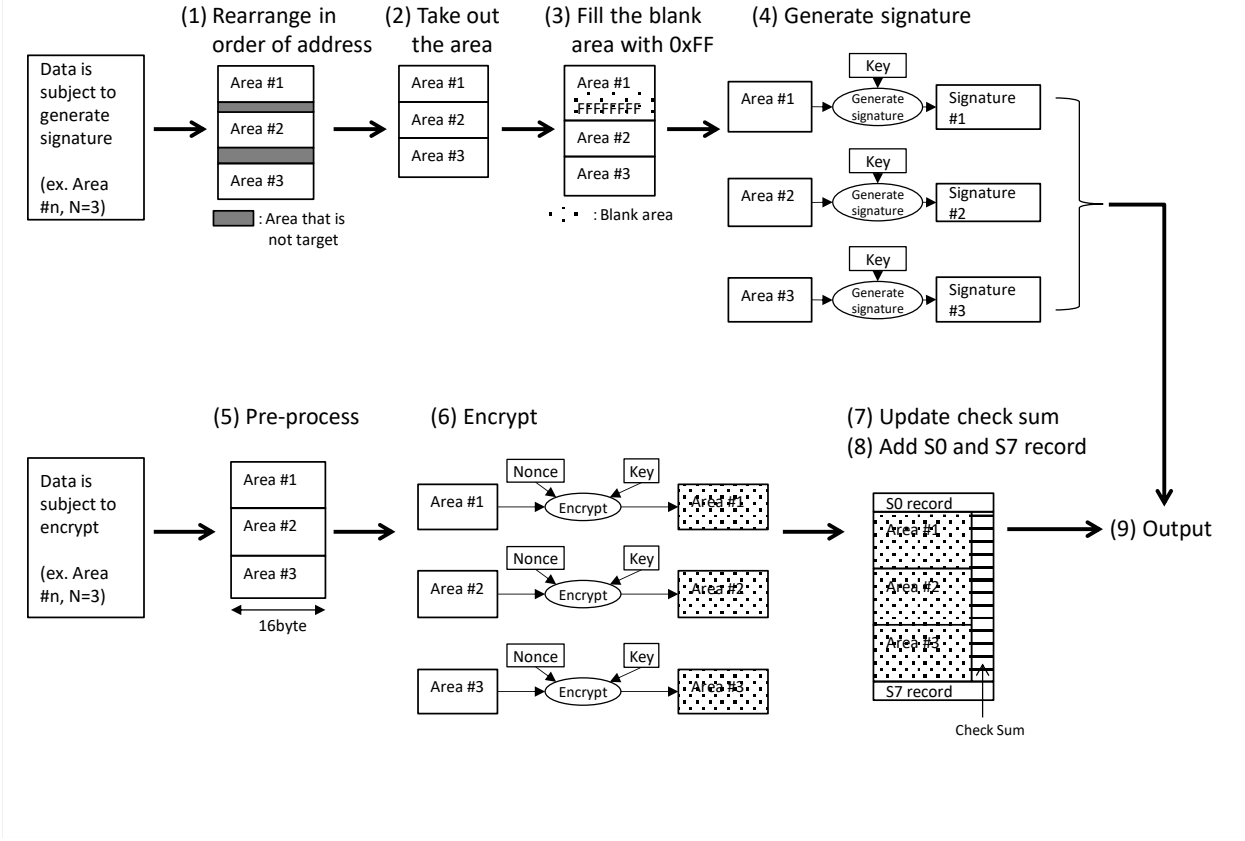


Figure 6-1 Encryption Processing of Motorola S format (ex. Area #n, n=3)

6.1.2. Encryption Processing of Binary format

This section clarifies the encryption processing of binary format in the Reprogramming Key Management and Encryption System

(1) Take out the area

Extract the target area from the offset from the beginning of the input data and data length specified by the screen input. If no area is specified, the entire input data area is treated as the target data.

(2) Generate signature

The Reprogramming Key Management and Encryption System generates signature. Range of subject to signature generation, see 4.3.2.

(3) Padding

After (1), data to be encrypted is padded with PKCS#7.

(4) Encrypt

The Reprogramming Key Management and Encryption System encrypts the data that was processed (3).

(5) Output Signature and Encrypted Writing Program

The Reprogramming Key Management and Encryption System outputs signature in (2) and encrypted writing program in (4).

6.2. Overall Flow of Reprogramming Security

Figure 6-2 shows overall flow of reprogramming security.

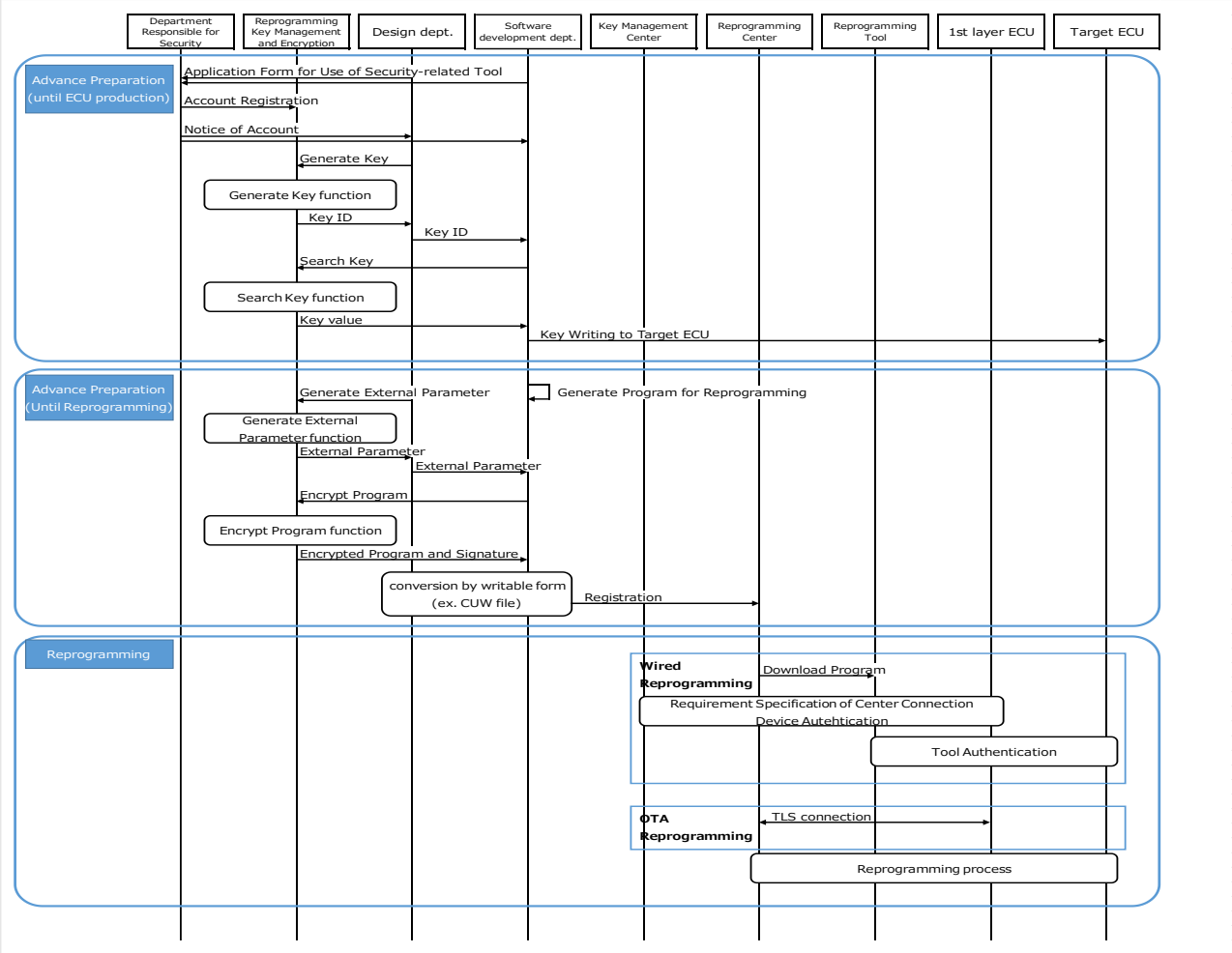


Figure 6-2 Overall Flow of Reprogramming Security

6.2.1. Item to be Implemented before ECU Shipment

Item to be implemented before ECU shipment is below.

- Create account of the Reprogramming Key Management and Encryption System
- Generate cryptographic key(Figure 6-3)
- Search cryptographic key(Figure 6-4), implement cryptographic key to ECU

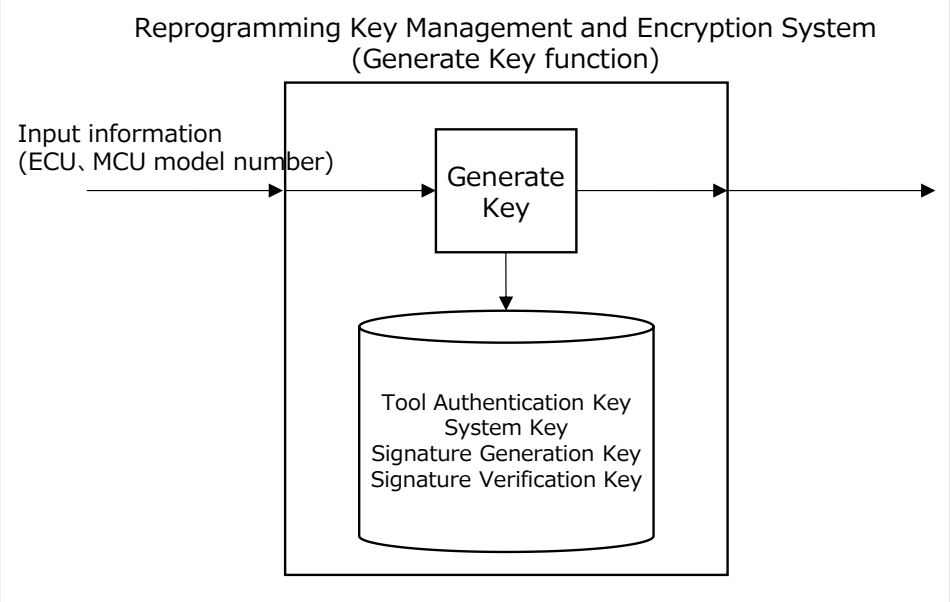


Figure 6-3 Generate Key Function

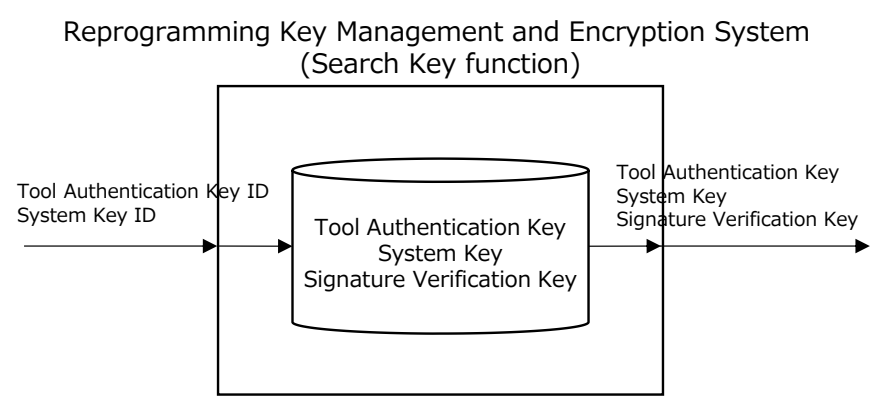


Figure 6-4 Search Key Function

6.2.2. Item to be Implemented before Reprogramming

Item to be implemented before reprogramming is below.

- Generate external parameter(Figure 6-5)
- Encrypt program and generate signature(Figure 6-6)

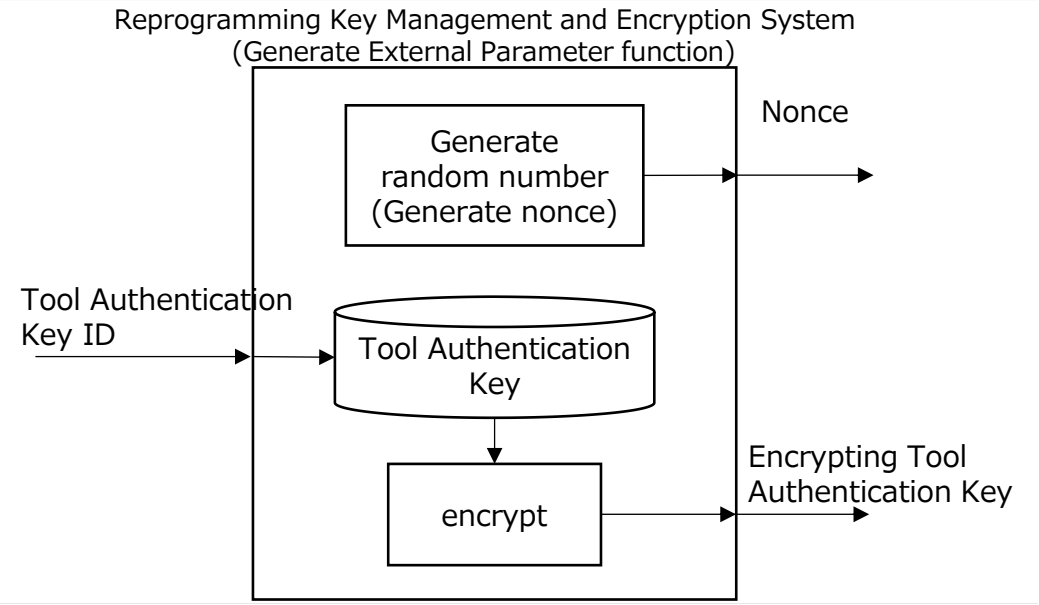


Figure 6-5 External Parameter Generate Function

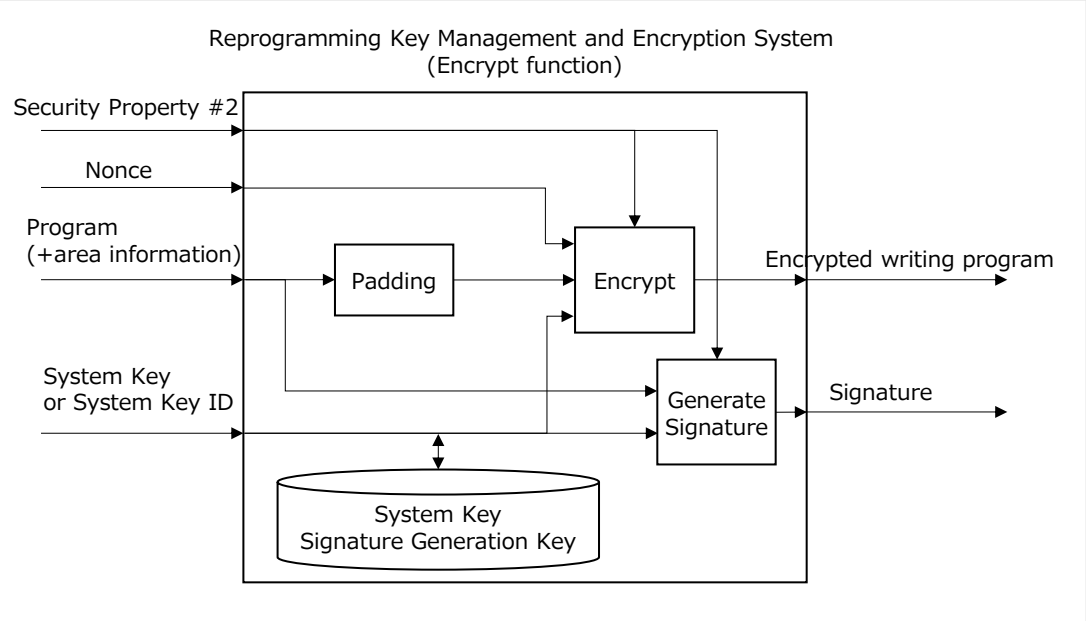


Figure 6-6 Encryption Function

6.2.3. Operation during Reprogramming

Operation during reprogramming is below. However, in this document, only the actions related to reprogramming security will be described. See Related Document [2] for overall reprogramming operation.

- Authenticate Reprogramming Tool using the Encrypting Tool Authentication Key (Figure 6-7)
- Decrypt program (Figure 6-8)
- Tamper detection using signature (Figure 6-8)
- Validate version information (Figure 6-8)

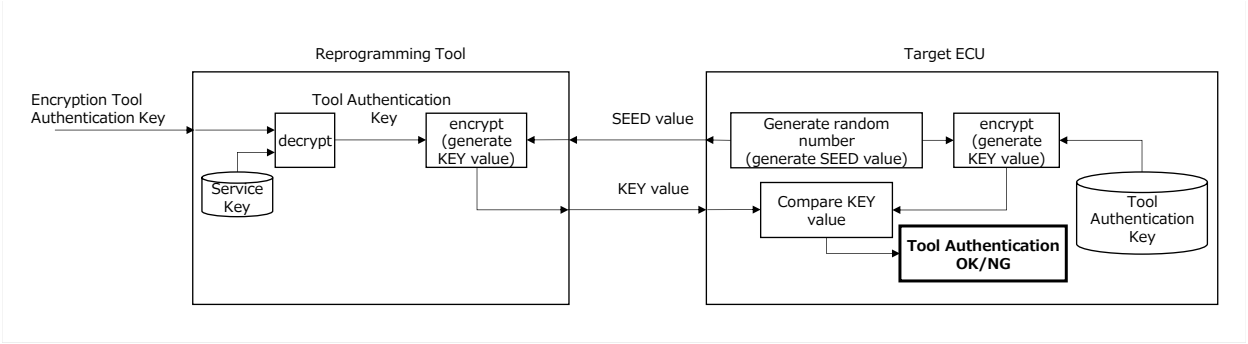


Figure 6-7 Tool Authentication Process

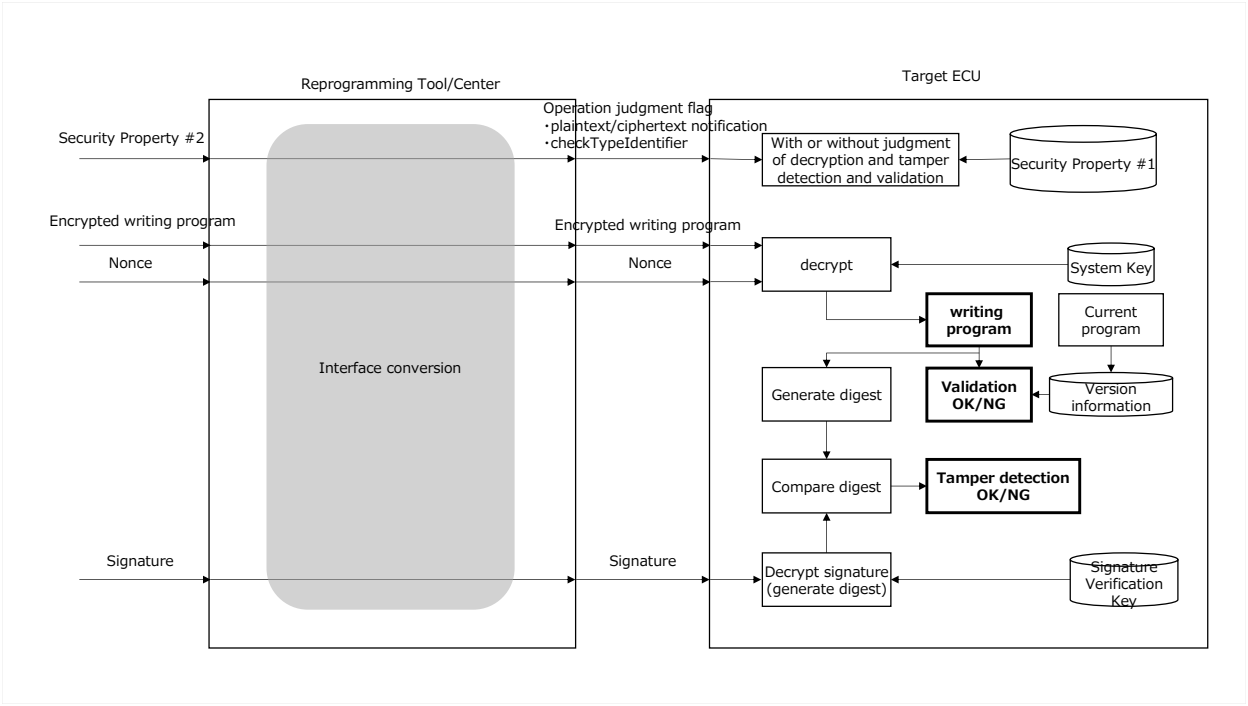


Figure 6-8 Decryption, Tamper Detection and Validation Process

6.3. Countermeasure for case sub-microcontroller/slave ECU configuration

This section will describe the concept of countermeasure in case sub-microcontroller/slave ECU configuration.

- If sub-microcontroller/slave ECU can be reprogramming from Untrusted zone, sub-microcontroller/slave ECU implements standard reprogramming security countermeasures in this document.
- If sub-microcontroller/slave ECU cannot be reprogramming from Untrusted zone. sub-microcontroller/slave ECU or main-microcontroller/master ECU implements standard reprogramming security countermeasures in this document.

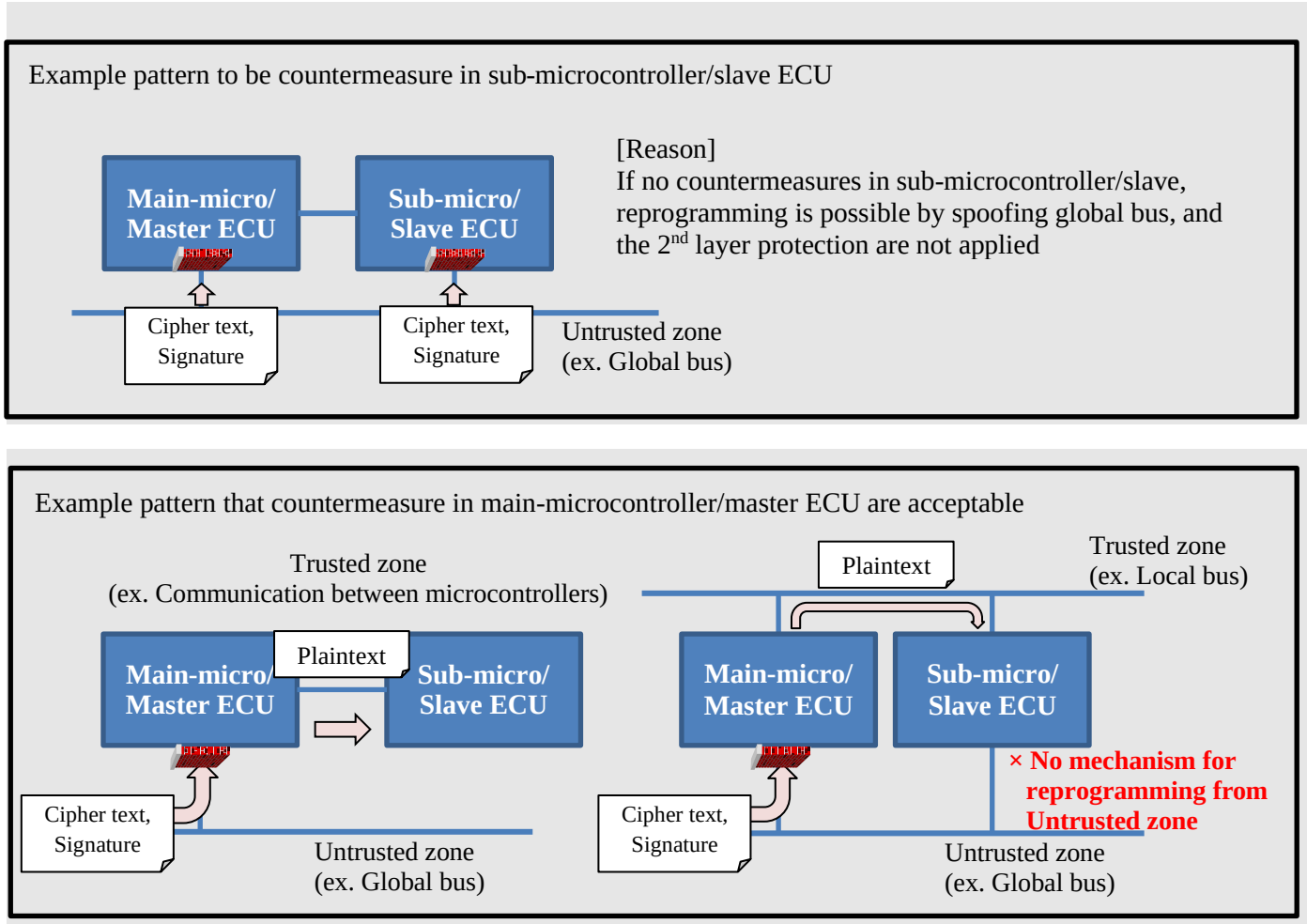


図 6-9 Concept of countermeasure in case sub-microcontroller/slave ECU configuration

6.4. Change Conditions of Cryptographic Keys (Tool Authentication Key, System Key, Signature Verification Key)

This section will describe change conditions of cryptographic keys (Tool Authentication Key, System Key Signature Verification Key) to be written to the ECU for the Reprogramming Security usage.
In case impact increases due to software changes, change cryptographic keys based on the Table 6-1 .

Table 6-1 Change conditions of keys

#	Assumed case	soft ware	micro controller	supplier	ECU node	Vehicle	Key change	Remarks
0	[Basic condition]	○	○	○	○	○	–	[Basic condition]
1	Microcontroller change (backup support, etc.)	●	●	–	–	–	**Recommended**	・With software changes ・Expanding impact on multiple ECUs with different microcontrollers
2	Supplier change (Differences by vehicle models, etc.)	●	–	●	–	–	**Recommended**	・With software changes ・Expanding impact on multiple ECUs with different suppliers
3	ECU change (Software diversion to different ECU, etc.)	●	–	–	●	–	**Recommended**	・With software changes ・Expanding impact on multiple ECUs
4	Vehicle change New development (New ECU development with different vehicle, etc.)	●	–	–	–	●	**Recommended**	・With software changes ・Expanding impact on multiple vehicles
5	Vehicle change ECU diversion (ECU diversion to different vehicle, etc.)	○	○	○	○	●	**Optional**	・Without software changes ・Expanding impact on multiple vehicles
6	Software part number change (rewriting/Reprogramming software, etc.)	●	○	○	○	○	**Optional**	・With software changes ・No change of impact scope because of software rewriting

● : With changes　○ : Without changes

*Notes

-A software change refers to a case where there is a logic change. If only the constant is changed, it can be interpreted as no software change.

-A Vehicle change refers to a case where there is a change to vehicle type (Vehicle code)

-If it is difficult to change the key in a case where key change is recommended, the design department shall decide whether or not to change the key after considering the risk of key leakage.