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　/

車載個人・プライバシー情報対策要求仕様書 **Requirements of Personal and Privacy 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 4G E/E Architecture Development Div System network & architecture development dept 4G			
	No. SEC-ePF-PPI-REQ-SPEC-a00-01-a			
	承認 Approved 河井	調査 Checked 松井	作成 Created 玉樹	2021/11/25 Omission of signature (approved electronically)

適用 Scope	個人・プライバシー情報を取り扱う ECU に適用する Applies to ECUs that process personal and privacy information..
変更内容 **Revision Record**	【主な変更点　Major changes】 (SEC-ePF-PPI-REQ-SPEC-a00-00-a ⇒ SEC-ePF-PPI-REQ-SPEC-a00-01-a) ・要求変更　Change requirements
特記 **Special note**	【入手先　Source】 本文書は iSpirit からダウンロードしてください。 This document can be downloaded from iSpirit. [Folder]/Repository/Electronics_Spec/Cybersecurity[サイバーセキュリティ]/Standard[標準]/PPI[プライバシー]/仕様書 ALL 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
a00-00-a	・gnsecppir-a00-03-a,と gnsecmms-a00-05-a を元に要件の追加、修正（以下参照） 3、4章 ・全ての要件に要求番号を付与 3 章 ・同意/撤回機能の導入時期を修正 4 章 ・個人・プライバシ情報の消去機能要件を修正 5 章 ・gnsecmms-a00-05-a 内の個人・プライバシー情報対策要件を追加 6 章 ・同意/撤回機能の制御信号要件を TBD に修正 ・消去機能に関する制御信号要件を削除	2021/05/20	46F 河合，垣屋
a00-01-a	全般 ・章構成の変更 2.3 節 ・関連文書の変更 3.1 節 ・要求一覧の追加 3 章、5.1 節、5.4 節、6 章 ・同意/撤回機能の要求を削除 4.1.1 項 ・ディーラ作業で個人・プライバシー情報を消去する場合の要件を追加	2021/11/25	46F 早川

目次

2. はじめに

2.1. 本書の目的

本書は上位文書[1]に基づき、各 ECU において実施しなければならない要件を示す。なお、MM 個別の要件については、4.2 参照のこと

2.2. 要求事項の記載

【要求事項：PPIREQ_*****】と記載されている部分が本書の要件とする。ただし、（補足）と記載されているものは補足事項のため要件ではない。

2.3. 関連文書

本書の上位文書を以下に示す。

表 1　上位文書

No	仕様書	Ver(最新版を適用ください)	主管
1	車載個人・プライバシー情報対策基準書	SEC-ePF-PPI-STD-***-**-*	46F

本書の関連仕様書を以下に示す。

表 2　関連仕様書

No	仕様書	Ver(最新版を適用ください)	主管
1	TOYOTA Phase6 Diagnostics Communication and Reprogramming standard specifications	Cover_TOYOTA Phase6_Ver***	BRF
2	Phase5 ダイアグシステム標準通信仕様書	DIAGSTD-04-Phase5-02-COVER_****	BRF

3. 要求概要

3.1. 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 3-1 に示す。要求事項の詳細については、4 章以降を参照。

表 3-1 要求事項対応表

要求事項番号	MM(マルチメディア) ECU	MM(マルチメディア) 以外の ECU
PPIREQ_00001	(欠番)	(欠番)
PPIREQ_00002	(欠番)	(欠番)
PPIREQ_00003	(欠番)	(欠番)
PPIREQ_01001	○	○
PPIREQ_01002	○ ※1	○ ※1
PPIREQ_01003	○ ※1	○ ※1
PPIREQ_01004	○ ※1	○ ※1
PPIREQ_01005	○ ※1	○ ※1
PPIREQ_01006	○ ※1	○ ※1
PPIREQ_01007	○ ※1	○ ※1
PPIREQ_01008	○ ※1	○ ※1
PPIREQ_01009	○ ※1	○ ※1
PPIREQ_01010	○ ※1	○ ※1
PPIREQ_01011	○ ※1	○ ※1
PPIREQ_01012	○ ※1	○ ※1
PPIREQ_01013	○ ※1	○ ※1
PPIREQ_01014	○ ※1	○ ※1
PPIREQ_02001	(欠番)	(欠番)
PPIREQ_02002	(欠番)	(欠番)
PPIREQ_02003	(欠番)	(欠番)
PPIREQ_02004	○	-
PPIREQ_02005	○	-
PPIREQ_02006	○	-

要求事項番号	MM(マルチメディア) ECU	MM(マルチメディア) 以外の ECU
PPIREQ_02007	○	-
PPIREQ_02008	○	-
PPIREQ_02009	○	-
PPIREQ_02010	○	-
PPIREQ_02011	○	-
PPIREQ_02012	○	-
PPIREQ_02013	○	-
PPIREQ_02014	○	-
PPIREQ_02015	(欠番)	(欠番)

※1　既に本書とは別の手段でディーラ作業による消去機能を実装している場合や、お客様操作による消去機能のみを実装する場合は、対応不要。詳細は 4.1 節参照。

4. 機能要求詳細

4.1. 個人・プライバシー情報の消去機能要件

＜対象 ECU＞

・個人・プライバシー情報を保持・保存している ECU の内、『車載個人・プライバシー情報対策基準』表４．１．の消去対象外にできるものにあたらない情報を保持・保存する ECU

＜導入時期＞

・19PF Ver.2 以降での ECU 開発の新設、または改良等の変更のタイミング

・Post19PF 以降の車両開発のタイミング

＜要件＞

【要求事項：PPIREQ_01001】

・対象 ECU は、下記 1,2 の少なくとも 1 つの機能を実装し、保持している個人・プライバシー情報を完全消去できること。ただし、消去対象の情報が上位文書[1]に記載の低レベルの情報に該当する場合は、完全消去でなくても可。

個人・プライバシー情報の消去要件は、上位文書[1]参照。

１．お客様操作による消去機能（HMI 操作、スイッチ操作など）

２．ディーラ作業による消去機能（サービスツールでのダイアグコマンド指示など）※1

※1：ディーラでの操作による消去を実装する場合、お客様に対し、ディーラで消去可能な旨をオーナーズマニュアル等で連絡すること

（補足）お客様、またはディーラにて、個人・プライバシー情報を完全消去できる別の手段が実装されている場合、新たに消去機能を実装する必要なし

4.1.1. ディーラ作業による消去機能を実装する場合の要件

本項では、【要求事項：PPIREQ_01001】にてディーラ作業による消去機能を実装する場合の要件を規定する。既に本節とは別の手段でディーラ作業による消去機能を実装している場合や、お客様操作による消去機能のみを実装する場合は、本節の要求事項は対応不要である。

4.1.1.1. 機能要件

【要求事項：PPIREQ_01002】

ディーラ作業による個人・プライバシー情報の消去機能を実装する ECU は、表 4-1 に示す機能を有すること。コマンドを受け付けるセッション、およびセキュリティアクセス解除の要否についても表 4-1 に従うこと。

表 4-1　個人・プライバシー情報消去機能

機能名	概要	ID	受付ｾｯｼｮﾝ		ｾｷｭﾘﾃｨ
			ﾃﾞﾌｫﾙﾄ	拡張	ｱｸｾｽ解除
個人・プライバシー情報消去機能	ツールからの要求に対し、保持する個人・プライバシー情報を消去する。	SID$31 RID$1016(Phase5) RID$D906(Phase6)	○	○	不要

【要求事項：PPIREQ_01003】
IG-ON 中にツールから個人・プライバシー情報消去の subFunction - startRoutine リクエストを受信した場合、保持している個人・プライバシー情報を消去すること。

【要求事項：PPIREQ_01004】
個人・プライバシー情報消去中に、IG OFF となった場合、個人・プライバシー情報の消去を中止すること。

【要求事項：PPIREQ_01005】
個人・プライバシー情報消去中に、個人・プライバシー情報消去の subFunction - startRoutine リクエストを受信した場合は、個人・プライバシー情報の消去処理を継続すること。

【要求事項：PPIREQ_01006】
subFunction - requestRoutineResults のリクエストを受信した場合は、4.1.1.2 に示す状態遷移の制御ステータスを応答すること。

【要求事項：PPIREQ_01007】
subFunction - stopRoutine は非対応とする。stopRoutine のリクエストを受信した場合は、ネガティブレスポンス(NRC 0x12)を応答すること。個人・プライバシー情報を消去中であれば、個人・プライバシー情報の消去処理を継続すること。

【要求事項：PPIREQ_01008】
セッション移行は処理継続とする。状態遷移は実施せず、個人・プライバシー情報消去中であれば、個人・プライバシー情報の消去処理を継続すること。

4.1.1.2.　状態遷移

【要求事項：PPIREQ_01009】
個人・プライバシー情報消去機能の状態遷移は、図 4-1 および表 4-2 に従うこと。

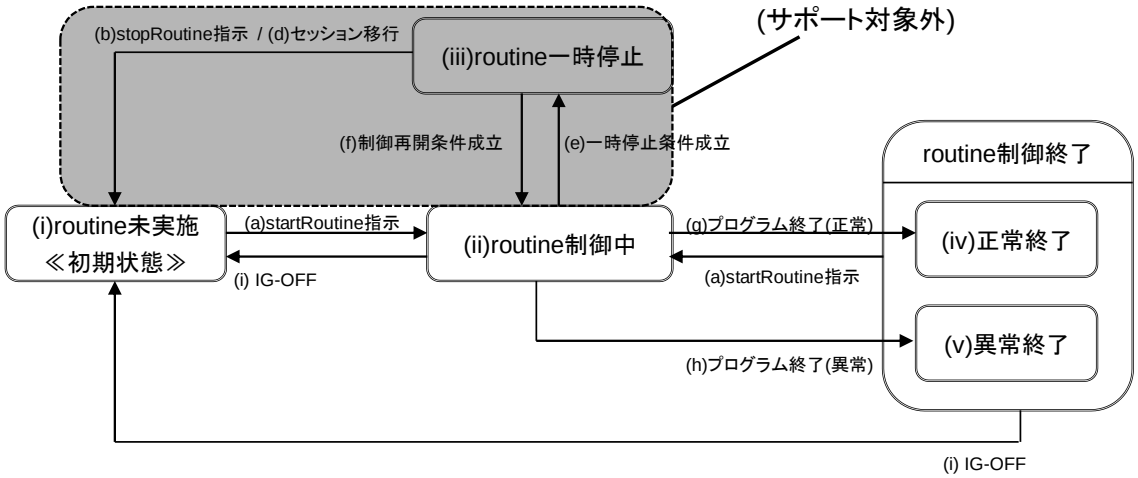

図 4-1　個人・プライバシー情報消去の状態遷移図

各ステータスの動作は以下の通り。

<u>各ステータスでの動作</u>

(i)　routine 未実施

実施処理なし。

(ii)　routine 制御中

個人・プライバシー情報の消去を実施する。

(iii)　routine 一時停止

本機能ではサポートしない。

(iv)　正常終了

実施処理なし。

(v)　異常終了

実施処理なし。

表 4-2　個人・プライバシー情報消去の状態遷移表

				状態			
				S1	S2	S3	S4
				routine未実施(0x00)	routine制御中(0x01)	正常終了(0x02)	異常終了(0x03)
イベント	(a)	startRoutine指示	アクション	* ポジティブレスポンスを応答する * 個人・プライバシー情報消去を開始する (PPIREQ_01003)	* ネガティブレスポンス(NRC24)を送信する * 個人・プライバシー情報消去を継続する (PPIREQ_01005)	* ポジティブレスポンスを応答する * 個人・プライバシー情報消去を開始する (PPIREQ_01003)	* ポジティブレスポンスを応答する * 個人・プライバシー情報消去を開始する (PPIREQ_01003)
			遷移先	S2	S2	S2	S2
	(b)	stopRoutine指示 →サポート対象外	アクション	* ネガティブレスポンス(NRC12)を送信する (PPIREQ_01007)	* ネガティブレスポンス(NRC12)を送信する * 個人・プライバシー情報消去を継続する (PPIREQ_01007)	* ネガティブレスポンス(NRC12)を送信する (PPIREQ_01007)	* ネガティブレスポンス(NRC12)を送信する (PPIREQ_01007)
			遷移先	S1	S2	S3	S4
	(c)	強制終了条件成立 →サポート対象外	アクション	N/A(Not Applicable)	N/A	N/A	N/A
			遷移先				
	(d)	セッション移行	アクション	* 何もしない(PPIREQ_01008) ※1	* 個人・プライバシー情報消去を継続する (PPIREQ_01008)	* 何もしない(PPIREQ_01008) ※1	* 何もしない(PPIREQ_01008) ※1
			遷移先	S1	S2	S3	S4
	(e)	一時停止条件成立 →サポート対象外	アクション	N/A	N/A	N/A	N/A
			遷移先				
	(f)	制御再開条件成立 →サポート対象外	アクション	N/A	N/A	N/A	N/A
			遷移先				
	(g)	プログラム終了(正常)	アクション	N/A	* 何もしない ※1	N/A	N/A
			遷移先		S3		
	(h)	プログラム終了(異常)	アクション	N/A	* 何もしない ※1	N/A	N/A
			遷移先		S4		
	(i)	IG OFF	アクション	* 何もしない ※1	* 個人・プライバシー情報消去を中止する (PPIREQ_01004)	* 何もしない ※1	* 何もしない ※1
			遷移先	S1	S1	S1	S1
	(x)	request Routine Results指示	アクション	* ポジティブレスポンス(routineStatus#1=0x00) を送信する(PPIREQ_01006)	* ポジティブレスポンス(routineStatus#1=0x01) を送信する(PPIREQ_01006) * 個人・プライバシー情報消去を継続する	* ポジティブレスポンス(routineStatus#1=0x02) を送信する(PPIREQ_01006)	* ポジティブレスポンス(routineStatus#1=0x03) を送信する(PPIREQ_01006)
			遷移先	S1	S2	S3	S4

※1 個人・プライバシー情報消去機能の処理に関わるもののみ記載している。

4.1.1.3. 通信コマンド

【PPIREQ_01010】

個人・プライバシー情報消去機能は物理アドレスに対応すること。

(1) startRoutine 指示

【PPIREQ_01011】

個人・プライバシー情報消去機能の startRoutine 指示は、表 4-3 に従うこと。

表 4-3 個人・プライバシー情報消去のリクエストメッセージフォーマット(startRoutine)

A_Data byte	Parameter	Byte Value		Scaling/Bit
		Phase5	Phase6	
#1	RoutineControl Request SID	0x31		hexadecimal
#2	subFunction = startRoutine, suppressPosRspMsgIndicationBit = FALSE/TRUE	0x01/0x81		hexadecimal
	routineIdentifier[] = 個人・プライバシー情報削除[			
#3	byte#1(MSB)	0x10	0xD9	hexadecimal
#4	byte#2]	0x16	0x06	hexadecimal

※routineControlOptionRecord はなし。

【要求事項：PPIREQ_01012】

個人・プライバシー情報消去機能の startRoutine のレスポンスは表 4-4 に従うこと。

表 4-4 個人・プライバシー情報消去のレスポンスメッセージフォーマット(startRoutine)

A_Data byte		Parameter	Byte Value		Scaling/Bit
Phase5	Phase6		Phase5	Phase6	
#1		RoutineControl Response SID	0x71		hexadecimal
#2		subFunction = startRoutine	0x01		hexadecimal
		routineIdentifier[] = 個人・プライバシー情報削除[			
#3		byte#1(MSB)	0x10	0xD9	hexadecimal
#4		byte#2]	0x16	0x06	hexadecimal
-	#5	routineInfo	NA	0x03	hexadecimal

※routineStatusRecord はなし。

ポジティブレスポンスおよびネガティブレスポンスの詳細は Phase6 の場合は関連文書[1]の Diagnostic design specification UDS Protocol、Phase5 の場合は関連文書[2]の RoutineControl service 標準仕様書(sid31-rd***)に準拠する。

(2) stopRoutine 指示

未サポート

(3) requestRoutineResults

【要求事項：PPIREQ_01013】

個人・プライバシー情報消去機能の requestRoutineResults 指示は、表 4-5 に従うこと。

表 4-5 個人・プライバシー情報消去のリクエストメッセージフォーマット(requestRoutineResults)

A_Data byte	Parameter	Byte Value		Scaling/Bit
		Phase5	Phase6	
#1	RoutineControl Request SID	0x31		hexadecimal
#2	subFunction = requestRoutineResults, suppressPosRspMsgIndicationBit = FALSE/TRUE	0x03/0x83		hexadecimal
	routineIdentifier[] = 個人・プライバシー情報削除[			
#3	byte#1(MSB)	0x10	0xD9	hexadecimal
#4	byte#2]	0x16	0x06	hexadecimal

※routineControlOptionRecord はなし。

【要求事項：PPIREQ_01014】

個人・プライバシー情報消去機能の requestRoutineResults のレスポンスは、表 4-6 に従うこと。

表 4-6 個人・プライバシー情報消去のレスポンスメッセージフォーマット(requestRoutineResults)

A_Data byte		Parameter	Byte Value		Scaling/Bit
Phase5	Phase6		Phase5	Phase6	
#1		RoutineControl Response SID	0x71		hexadecimal
#2		subFunction = requestRoutineResults	0x03		hexadecimal
		routineIdentifier[] = 個人・プライバシー情報削除[			
#3		byte#1(MSB)	0x10	0xD9	hexadecimal
#4		byte#2]	0x16	0x06	hexadecimal
-	#5	routineInfo	NA	0x03	hexadecimal
		routineStatusRecord[] = [			
#5	#6	routineStatus#1]	0xXX		hexadecimal

※routineStatusRecord の応答値は以下の通り。

0x00 = routine 未実施

0x01 = routine 制御中

0x02 = 正常終了

0x03 = 異常終了

4.2. MM（マルチメディア）向け個人・プライバシー対策要件

本節では、MM 個別の要件を規定する。本章で記載する要件は、下記対象 ECU と対象導入時期に適用される。

＜対象 ECU＞

・MM

＜導入時期＞

-MM：21CY 以降

4.2.1. MM（マルチメディア）向け個人・プライバシー情報の機密保護要件

本項では、MM 向けの個人・プライバシー情報の機密保護要件を規定する。

【要求事項：PPIREQ_02004】

・MM の UI を介したユーザ操作により＋B 電源 ON 時にユーザ認証を設定可能なこと。＋B 電源 ON 時からユーザ認証が成功するまでの間は、MM の UI およびユーザが使用するデータ出力 I/F に個人・プライバシー情報を出力・表示しないこと。

【要求事項：PPIREQ_02005】

・MM の UI を介したユーザ認証により、MM の個人・プライバシー情報の出力・表示を許可/禁止する設定が可能なこと。

【要求事項：PPIREQ_02006】

・MM は、無線 I/F 経由で個人・プライバシー情報を出力する際は、通信路を暗号化すること

【要求事項：PPIREQ_02007】

・MM において個人認証（例：FIDO 認証）の機能を提供する場合は、あるユーザが入力した情報をその他のユーザが MM の UI を介して閲覧できないようにすること。ただし、この事項は推奨とする。

【要求事項：PPIREQ_02008】

・MM は、不揮発メモリ上に上位文書[1]で定義される暗号化保存の対象情報を保存する際は、暗号化して保存すること。耐タンパ性を持つセキュリティチップを暗号鍵の保護および暗号化処理に利用すること。

【要求事項：PPIREQ_02009】

・MM は、車載 LAN 通信用コネクタから個人・プライバシー情報を出力する際は、アクセス制御かつ暗号化をすること（個人財産情報は必須、その他は推奨）

【要求事項：PPIREQ_02010】

・MM は、外部記録媒体等のユーザが容易に取出し・読出し可能な領域に個人・プライバシー情報を出力する際は、暗号化すること。ただし、出力の目的が、自宅 PC での閲覧のように、ユーザが車両外部に情報を持出すことを想定したサービスである場合は、暗号化しなくてもよい。

【要求事項：PPIREQ_02011】

・MM の UI を介して個人財産情報を出力・表示しないこと。

【要求事項：PPIREQ_02012】

・MM は、DLC 経由で個人財産情報を出力しないこと。

【要求事項：PPIREQ_02013】

・MM は、外部記録媒体等のユーザが容易に取出し・読出しが可能な領域に個人財産情報を出力しないこと。

4.2.2. MM（マルチメディア）向け個人・プライバシー情報の消去機能要件

本項では、MM 向けの個人・プライバシー情報の消去機能要件を規定する。

【要求事項：PPIREQ_02014】

・MM は、メモリ上に上位文書[1]で定義されるデータ消去の対策情報を保存するときは、ユーザによる MM の UI を介した消去操作により、完全消去が可能なこと。

1. Revision Record

Version	Revision contents	Data	Revised
a00-00-a	Modify the following contents based on gnsecppir-a00-03-a and gnsecmms-a00-05-a Chapter3, 4. ・Add the requirement ID to all requirements in this document. Chapter3. ・ Modify the implementation timing of the Consent/Withdrawal function Chapter4. ・Modify the requirements of erasing function Chapter5. ・ Add the requirements of Personal and Privacy information countermeasure described in gnsecmms-a00-05-a. Chapter6. ・ Modify the requirements of control signals of Consent/Withdrawal function. ・Delete the requirements of control signals of erasing function.	May, 20, 2021	46F Kawai, Kakiya
a00-01-a	Overall ・Change chapter structure Section2.3 ・Change reference documents Section3.1 ・Add requirement list Chapter3, Section5.1, Section5.4, Chapter6 ・Delete the requirements of the Consent/Withdrawal function Subsection4.1.1 ・ Add the requirements for erasing Personal and Privacy information by dealer operation	Nov. 25, 2021	46F Hayakawa

Table of Contents

2. Introduction

2.1. Purpose of this document

This document will indicate the requirements that have to be fulfilled at the individual ECUs based on Upper-level Document[1].

Refer to chapter 4.2 for MM-specific requirements.

2.2. Description of Requirements

A requirements in this document shall be labeled as 【Requirement : PPIREQ_*****】.

Provided, however, that what is labeled as (Supplement) in this document is a supplementary item and therefore it is not a requirement.

2.3. Reference Documents

Upper-level Documents of this document are shown in Table 1.

Table 1. Upper-level Documents

No	Document Nama	Ver(Applied to the latest version)	Issued
1	Standards of Personal and Privacy Information	SEC-ePF-PPI-STD-***-**-*	46F

Related Documents of this document are shown in Table 2.

Table 2. Related Documents

No	Document Name	Ver(Applied to the latest version)	Issued
1	TOYOTA Phase6 Diagnostics Communication and Reprogramming standard specifications	Cover_TOYOTA Phase6_Ver***	BRF
2	Phase 5 Diagnostics System Standard Communication Specifications	DIAGSTD-04-Phase5-02-COVER_****	BRF

3. Requirement List

Table 3-1 shows a list of requirements that are met by each entity. For more details of the requirement, see Chapter 4 and later.

Table 3-1 Requirement Table

Requirement	MM(MultiMedia) ECU	The ECUs other than MM that process personal and privacy information
PPIREQ_00001	(deleted)	(deleted)
PPIREQ_00002	(deleted)	(deleted)
PPIREQ_00003	(deleted)	(deleted)
PPIREQ_01001	○	○
PPIREQ_01002	○ *1	○ *1
PPIREQ_01003	○ *1	○ *1
PPIREQ_01004	○ *1	○ *1
PPIREQ_01005	○ *1	○ *1
PPIREQ_01006	○ *1	○ *1
PPIREQ_01007	○ *1	○ *1
PPIREQ_01008	○ *1	○ *1
PPIREQ_01009	○ *1	○ *1
PPIREQ_01010	○ *1	○ *1
PPIREQ_01011	○ *1	○ *1
PPIREQ_01012	○ *1	○ *1
PPIREQ_01013	○ *1	○ *1
PPIREQ_01014	○ *1	○ *1
PPIREQ_02001	(deleted)	(deleted)
PPIREQ_02002	(deleted)	(deleted)
PPIREQ_02003	(deleted)	(deleted)
PPIREQ_02004	○	-
PPIREQ_02005	○	-
PPIREQ_02006	○	-

Requirement	MM(MultiMedia) ECU	The ECUs other than MM that process personal and privacy information
PPIREQ_02007	○	-
PPIREQ_02008	○	-
PPIREQ_02009	○	-
PPIREQ_02010	○	-
PPIREQ_02011	○	-
PPIREQ_02012	○	-
PPIREQ_02013	○	-
PPIREQ_02014	○	-
PPIREQ_02015	○	-

*1 If erasing function by dealer operation using a different method this document has already implemented on the target ECU, or if only erasing function by user operation is implemented on the target ECU, the requirements need not be satisfied. For more details, see section 4.1.be satisfied. For more details, see section 4.1.

4. Functional Requirements

4.1. Functional Requirements for Erasing of Personal and Privacy Information

<Target ECUs>

Of the ECUs retaining and/or storing personal and privacy information, the target ECUs are the ECUs that retain and/or store the information that does not fall under the information that can be exempted from erasing as indicated in Table 4.1. of Upper-level Document[1] .

＜Target timing of implementation＞

・Changing including new adoption or improvement of ECU development for 19PF Ver. 2 and later

・Developing vehicles for Post19PF and later

<Requirements>

【Requirement: PPIREQ_01001】

・Target ECU shall be implemented at least one function in the following two functions and perform complete erasing of personal and privacy information of itself by the erasing function.

However, if the information to be erased falls under “Low privacy” information described in Upper-level Document[1], complete erasing does not have to be performed. See Upper-level Document[1] for the erasing requirements(including requirements of complete erasing).

1．Erasing function by user operation（Operating HMI、Pushing button, etc.）

2．Erasing function by dealer operation (Erasing request from diagnostic tool, etc.）*1

*1：If erasing function by dealer operation is implemented, the ECU design department shall inform user by owner’s manual etc. that Personal and Privacy information is able to be erased at dealer.

（Supplement）Additional implementation of erasing functions is not required if users or dealers have been provided other means to performed complete erasing for Personal and Privacy information of the ECU.

4.1.1. Requirements for Implementing Erasing function by Dealer Operation

This subsection indicates the requirements for implementing erasing function by dealer operation in 【Requirement: PPIREQ_01001】. If erasing function by dealer operation using a different method from in this section has already implemented on the target ECU, or if only erasing function by user operation is implemented on the target ECU, the requirements in this section need not be satisfied.

4.1.1.1. Functional Requirements

【Requirement: PPIREQ_01002】

The target ECU that implements erasing function by dealer operation shall have the function as indicated in Table 4-1. A session in which a command is accepted, and the necessity of cancellation of security access shall also comply with Table 4-1.

Table 4-1 Personal and Privacy Information Erasing Function

Function name	Outline	ID	Acceptance session		Cancellation of security access
			Default	Extension	
Personal and privacy information erasing function	In response to request from the tool, the target ECU erase the personal and privacy information of itself.	SID$31 RID$1016(Phase5) RID$D906(Phase6)	○	○	Not required

【Requirement: PPIREQ_01003】

If the target ECU receives the subFunction - startRoutine request of personal and privacy information erasing from the tool during IG-ON, the target ECU shall erase personal and privacy information of itself.

【Requirement: PPIREQ_01004】

If IG is turned OFF during erasing personal and privacy information, the target ECU shall stop erasing personal and privacy information.

【Requirement: PPIREQ_01005】

If the target ECU receives the subFunction - startRoutine request of personal and privacy information erasing during erasing personal and privacy information, the target ECU shall continue the erasing process of personal and privacy information.

【Requirement: PPIREQ_01006】

If the target ECU receives the subFunction - requestRoutineResults request, the target ECU shall respond with the control status of the state transition as indicated in 4.1.1.2.

【Requirement: PPIREQ_01007】

subFunction - stopRoutine shall not be supported. If the target ECU receives the stopRoutine request, the target ECU shall respond with a negative response (NRC 0x12). If personal and privacy information is being erased, the target ECU shall continue the erasing process of personal and

privacy information.

【Requirement: PPIREQ_01008】

If the session transfer occurs, the process shall be continued. The target ECU shall not execute the state transition, and if personal and privacy information is being erased, the target ECU shall continue the erasing process of personal and privacy information.

4.1.1.2. State Transition

【Requirement: PPIREQ_01009】

The state transition in the personal and privacy information erasing function shall comply with Fig. 4-1 and Table 4-2.

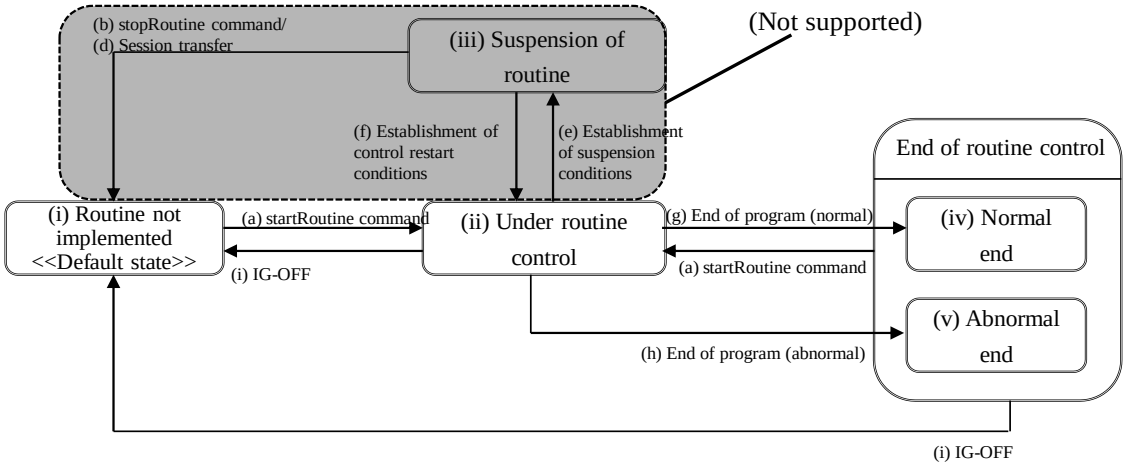

Fig. 4-1 State Transition Diagram of Personal and Privacy Information Erasing

The operation in each state shall be as follows:

<u>Operation in each state</u>

(i) Routine not implemented

No processing is implemented.

(ii) Under routine control

The target ECU shall execute erasing of personal and privacy information.

(iii) Suspension of routine

This is not supported by this function.

(iv) Normal end

No processing is implemented.

(v) Abnormal end

No processing is implemented.

Table 4-2 State Transition Table of Personal and Privacy Information Erasing

				Status			
				S1	S2	S3	S4
				Routine not implemented (0x00)	Routine being controlled (0x01)	Normal end (0x02)	Abnormal end (0x03)
Event	(a)	startRoutine command	Action	* Responds with a positive response. * Starts erasing of personal and privacy information. (PPIREQ_01003)	* Transmits a negative response (NRC24). * Continues erasing of personal and privacy information. (PPIREQ_01005)	* Responds with a positive response. * Starts erasing of personal and privacy information. (PPIREQ_01003)	* Responds with a positive response. * Starts erasing of personal and privacy information. (PPIREQ_01003)
			Transition to	S2	S2	S2	S2
	(b)	stopRoutine command → Not supported	Action	* Transmits a negative response (NRC12). (PPIREQ_01007)	* Transmits a negative response (NRC12). * Continues erasing of personal and privacy information. (PPIREQ_01007)	* Transmits a negative response (NRC12). (PPIREQ_01007)	* Transmits a negative response (NRC12). (PPIREQ_01007)
			Transition to	S1	S2	S3	S4
	(c)	Establishment of forced termination conditions	Action	N/A (Not Applicable)	N/A	N/A	N/A
			Transition to				
	(d)	Session transfer	Action	* Takes no action. (PPIREQ_01008) *1	* Continues erasing of personal and privacy information. (PPIREQ_01008)	* Takes no action. (PPIREQ_01008) *1	* Takes no action. (PPIREQ_01008) *1
			Transition to	S1	S2	S3	S4
	(e)	Establishment of suspension condition	Action	N/A	N/A	N/A	N/A
			Transition to				
	(f)	Establishment of control restart condition	Action	N/A	N/A	N/A	N/A
			Transition to				
	(g)	End of program (normal)	Action	N/A	* Takes no action. *1	N/A	N/A
			Transition to		S3		
	(h)	End of program (abnormal)	Action	N/A	* Takes no action. *1	N/A	N/A
			Transition to		S4		
	(i)	IG OFF	Action	* Takes no action. *1	* Stops erasing of personal and privacy information. (PPIREQ_01004)	* Takes no action. *1	* Takes no action. *1
			Transition to	S1	S1	S1	S1
	(x)	request Routine Results command	Action	* Transmits a positive response (routineStatus#1=0x00). (PPIREQ_01006)	* Transmits a positive response (routineStatus#1=0x01). (PPIREQ_01006) * Continues erasing of personal and privacy information.	* Transmits a positive response (routineStatus#1=0x02). (PPIREQ_01006)	* Transmits a positive response (routineStatus#1=0x03). (PPIREQ_01006)
			Transition to	S1	S2	S3	S4

*1 This action is described only the processing regarded to Personal and Privacy Information Erasing Function

4.1.1.3. Communication Commands

【Requirement: PPIREQ_01010】

A command for the personal and privacy information erasing function shall support physical addresses.

(1) startRoutine command

【Requirement: PPIREQ_01011】

The startRoutine command for the personal and privacy information erasing function shall comply with Table 4-3.

Table 4-3 Format of Request Message for Personal and Privacy Information Erasing (startRoutine)

A_Data byte	Parameter	Byte Value		Scaling/Bit
		Phase5	Phase6	
#1	RoutineControl Request SID	0x31		hexadecimal
#2	subFunction = startRoutine, suppressPosRspMsgIndicationBit = FALSE/TRUE	0x01/0x81		hexadecimal
	routineIdentifier[] = personal and privacy information erasing[			
#3	byte#1(MSB)	0x10	0xD9	hexadecimal
#4	byte#2]	0x16	0x06	hexadecimal

* There is no routineControlOptionRecord.

【Requirement: PPIREQ_01012】

The response to startRoutine for the personal and privacy information erasing function shall comply with Table 4-4.

Table 4-4 Format of Response Message for Personal and Privacy Information Erasing (startRoutine)

A_Data byte		Parameter	Byte Value		Scaling/Bit
Phase5	Phase6		Phase5	Phase6	
#1		RoutineControl Response SID	0x71		hexadecimal
#2		subFunction = startRoutine	0x01		hexadecimal
		routineIdentifier[] = personal and privacy information erasing[			
#3		byte#1(MSB)	0x10	0xD9	hexadecimal
#4		byte#2]	0x16	0x06	hexadecimal
-	#5	routineInfo	NA	0x03	hexadecimal

*There is no routineStatusRecord.

The details of the positive response and the negative response shall comply with Diagnostic design specification UDS Protocol in Related Document [1] or RoutineControl service standard specifications (sid31-rd***) in Related Document [2].

(2) stopRoutine command

Not supported

(3) requestRoutineResults

【Requirement: PPIREQ_01013】

The requestRoutineResults command for the personal and privacy information erasing function shall comply with Table 4-5.

Table 4-5 Format of Request Message for Personal and Privacy Information Erasing (requestRoutineResults)

A_Data byte	Parameter	Byte Value		Scaling/Bit
		Phase5	Phase6	
#1	RoutineControl Request SID	0x31		hexadecimal
#2	subFunction = requestRoutineResults, suppressPosRspMsgIndicationBit = FALSE/TRUE	0x03/0x83		hexadecimal
	routineIdentifier[] = personal and privacy information erasing[			
#3	byte#1(MSB)	0x10	0xD9	hexadecimal
#4	byte#2]	0x16	0x06	hexadecimal

* There is no routineControlOptionRecord.

【Requirement: PPIREQ_01014】

The response to requestRoutineResults of the MAC key verification information transmission function shall comply with Table 4-6.

Table 4-6 Format of Response Message for Personal and Privacy Information Erasing (requestRoutineResults)

A_Data byte		Parameter	Byte Value		Scaling/Bit
Phase5	Phase6		Phase5	Phase6	
#1		RoutineControl Response SID	0x71		hexadecimal
#2		subFunction = requestRoutineResults	0x03		hexadecimal
		routineIdentifier[] = personal and privacy information erasing [			

#3 #4		byte#1(MSB) byte#2]	0x10 0x16	0xD9 0x06	hexadecimal hexadecimal
-	#5	routineInfo	NA	0x03	hexadecimal
#5	#6	routineStatusRecord[] = [routineStatus#1]	0xXX		hexadecimal

The response values of routineStatusRecord are as follows.

0x00 = Routine not implemented

0x01 = Under routine control

0x02 = Normal end

0x03 = Abnormal end

4.2. MM(Multi-Media)-specific requirements for Personal and Privacy information

This section indicates the requirements for MM. The requirements described in this chapter are applied to target ECU and target timing of implementation bellow.

<Target ECU>

・MM

<Target timing of implementation>

・MM：21CY and later

4.2.1. Security protection Requirements of Personal and Privacy information for MM

This subsection indicates Security protection Requirements of Personal and Privacy information for MM.

【Requirement: PPIREQ_02004】

・User authentication shall be able to be set by user operation via the UI of the MM when the +B power is ON. During the period from when the +B power is turned ON until the user authentication is successfully completed, MM shall not output/display personal and privacy information to the UI of MM or Data Output I/F of MM for user.

【Requirement: PPIREQ_02005】

・Permission and prohibition of outputting/displaying of personal and privacy information of the MM shall be set by user authentication via the UI of the MM.

【Requirement: PPIREQ_02006】

・When personal and privacy information is outputted via wireless I/F, the communication path shall be encrypted.

【Requirement: PPIREQ_02007】

・If personal authentication function (e.g., FIDO authentication) is provided to the MM, information entered by a certain user should not be able to be viewed by other users via the UI of the MM. However, this is a recommended item.

【Requirement: PPIREQ_02008】

・When MM stores the information is subject to saving with encryption defined in Upper-level Document[1] in a non-volatile memory, the information shall be saved after being encrypted. A

tamper-resistant security chip shall be used for protection of an encryption key and encryption processing.

【Requirement: PPIREQ_02009】

・Personal and privacy information shall be authenticated and encrypted in case of outputting via In-vehicle LAN communication connector (Personal property information：Mandatory , other than Personal property information：Recommendation).

【Requirement: PPIREQ_02010】

・When personal and privacy information is outputted in an area of an external storage medium etc., where it is easily retrievable and readable by the user, the data shall be encrypted.

However, in the case where the service assumes that the information is taken out to the outside of the vehicle by the user, such as when browsing the information via home computer, it doesn't not have to be encrypted.

【Requirement: PPIREQ_02011】

・Personal property information shall not be outputted/displayed via the UI of the MM.

【Requirement: PPIREQ_02012】

・Personal property information shall not be outputted via the DLC.

【Requirement: PPIREQ_02013】

・Personal property information shall not be outputted to an area of an external storage medium, etc., where it is easily retrievable and readable by the user.

4.2.2. Erasing Requirements of Personal and Privacy information for MM

This subsection indicates erasing Requirements of Personal and Privacy information for MM.

【Requirement: PPIREQ_02014】

・When the information subject to data erasing defined in Upper-level Document[1] is stored in the memory, the data shall be able to be erased using a method of complete erasing by user operation via the UI of the MM. See Upper-level Document[1] for the erasing requirements(including requirements of complete erasing).