目次

変更履歴

Version	Date	Changes	Resp.
1.00	2022/3/29	New release	TMC Kurashige
1.01	2022/6/30	Appendix Cに鍵を更新	TMC Kurashige
1.02	2022/7/29	Appendix D S001 S013を個別から共通に変更 [DC24-4144] Appendix D S004 A005の削除 [DC24-4144] Appendix D S902 対象鍵スペア2(AES128鍵)からOEM Apps保護用 に変更 [DC24-4144] Appendix C 表のA902 A904 A905 A906の4096を3072に変更 [DC24-4071] Appendix Dの4096を3072に変更 [DC24-4071] Appendix C、DのGoogle Fast Pairの鍵であるS015、A910、911を削除 Appendix C、DのS011のYARD MODEをUSBリプロに修正 Appendix C、DのS012を削除 [DC24-7484] Appendix C、DのS005を削除 Appendix C、DのS006をECIES CMAC用に修正 Appendix C、DにS016、S017、S018、A017を追加 Appendix CにS019を追加 [DC24-6893] Appendix CにA018を追加 [DC24-5014] Appendix DからA006、A007を削除 Appendix Dの誤記修正 Appendix D-1にデフォルト値を追加 Appendix DをAppendix Cの表に合わせて更新 Appendix CのS014の説明の誤記修正(リプロ保護用→汎用) Appendix C、DにAuthSession用の鍵としてS020、S021、S022、S023を追加[DC24-5209]	TMC Sakurada
1.03	2022/10/14	Appendix D-1. 鍵フォーマットのチップシリアルNo.を10桁から12桁に変更	TMC Kitamura
1.04	2022/11/11	S24としてDEM(Data Encapsulation Mechanism)用鍵を記載[AGLSD-2844] S013、S018について開発用と商用の鍵があり、商用ソフトで開発用の鍵を削除することを記載[AGLSD-3630] S902はCP/AAのOEM Appは仕様ドロップしたため「スペア」	TMC Kitamura

		に変更[AGLSD-3670] S901をCP/AAの開発用鍵から商用鍵への切り替え時のデータ保護用に使用する旨を記載 [AGLSD-3670] S901をDolby Atmosプログラム保護鍵の暗号化用に使用する旨を記載[AGLSD-3308]	
1.05	2023/5/22	S006について、ECIESで不要になったものの、OTA4.0対応でOTAマスタ用鍵、A021、S027、S028を暗号化から復号し、TEE環境で利用するための鍵として修正[AGLSD-5472] [AGLSD-6030] A001について、誤記修正で「トヨタ生成」を「○」に修正[AGLSD-5472] S013、S018、S025、S026は「24MM_Security-HAL_IF仕様書_v1.70」でのログ暗号化API削除に伴い削除[AGLSD-5472] A012について、OEM Appが仕様ドロップとなったためスペア鍵に修正[AGLSD-6030] S027、S028、A021～A039をOTA4.0対応で追加[AGLSD-6030] S006、S017、A015についてAppendixDの誤記を修正[AGLSD-6138] S902をスペアからOTAマスターのサービスキーに修正[AGLSD-6138] S020～S023の更新可能をYes→Noに修正[AGLSD-6138] A016をShare Key Root Publicに修正[AGLSD-6138] 表D-xxに番号を付与 [AGLSD-6138] S029としてMaster Auth Key Rootを追加[AGLSD-6138] A040としてdm-verityのcstm ROM用を追加[AGLSD-6138]	TMC Kitamura

Appendix C. 暗号鍵

24CYでは、下記を基準として、HUが保有する暗号鍵（対称鍵・非対称鍵）と証明書の一覧を以下に示す。リプログラミング機能によってアップデートされ得る鍵は、「更新可能」列によって示す。

(1) 対称鍵

ID	名前	説明	アルゴリズム	サイズ [bit]	個体別	HSM 保管	トヨタ 生成	更新 可能
S001	リプロデータ保護用	センタから配信する際の、リプロのデータ暗号化用。	AES	128	No	○	○	Yes
S002	プライバシーデータ保護用_HSM内	保護が必要なデータを不揮発メモリに保存する際の、暗号化用。HSM内で暗号処理を行うもの。	AES	128	Yes	○	○	Yes
S003	プライバシーデータ保護用_HSM外	S002と同じ目的で利用するが、HSM外で暗号処理を行うもの。	AES	128 or above	Yes	–	– (Tier1 or HSM vendor)	–
S006	対称鍵_ OTAマスタ用鍵	OTAマスタ用鍵、A021、S027、S028を暗号化から復号し、TEE環境で利用させるための鍵	AES	128	No	○	○	Yes
S007	汎用HMAC用	HUが不揮発メモリにデータを保存する際に、改竄を防止する目的で利用される。HU内で閉じて利用されるもので、他の機器やサーバと共有される鍵ではない。	HMAC-SHA	256	No	○	○	Yes
S008	セキュリティパラメータ更新用	HSM保護下のセキュリティパラメータ更新時の、パラメータ復号用。	AES	128	No	○	○	Yes
S011	リプロデータ保護用（USBリプロ）	USBリプロにおける復号鍵。	AES	128	No	○	○	Yes
S014	汎用CMAC用	汎用で利用するCMAC用の鍵	AES	128	No	○	○	Yes
S016	デバッグ機能再有効化認証データ保護用	デバッグ機能再有効化のための認証データの保護用。	AES	128	No	○	○	Yes
S017	デバッグ機能再有効化認証データ検証用(H/U→サーバ)	デバッグ機能再有効化のための認証データ(H/U→サーバ)検証用。	HMAC-SHA	256	No	○	○	Yes
S019	UIEによるモジュール保護用	セキュアブートにおいてUIEによるモジュール保護用	AES	128	No	–	–	–
S020	AuthSession用鍵1	AuthSession用鍵1	AES	128	No	○	○	–
S021	AuthSession用鍵2	AuthSession用鍵2	AES	128	No	○	○	–
S022	AuthSession用鍵3	AuthSession用鍵3	AES	128	No	○	○	–
S023	AuthSession用鍵4	AuthSession用鍵4	AES	128	No	○	○	–
S024	DEM(Data Encapsulation Mechanism)用鍵	データ保護用のDEM(Data Encapsulation Mechanism)用鍵。	AES	128	Yes	–	–	–

S027	対称鍵_PKG暗号鍵(UO向け)	PKG暗号鍵(UO向け)。OTA4.0仕様におけるOTA042。保護資産は下記。 ・UO向けメタデータ	AES	128	No	– (S006を使ったKEM-DEM)	○	Yes
S028	対称鍵_PKG暗号鍵(DC向け)	PKG暗号鍵(DC向け)。OTA4.0仕様におけるOTA043。保護資産は下記。 ・DC向けメタデータ	AES	128	No	– (S006を使ったKEM-DEM)	○	Yes
S029	Master Auth Key Root	Root key for HKDF of individual derived auth keys of TA100	HMAC-SHA	256	No	–	○	–
S901	・Dolby Atmosプログラム保護鍵の暗号化用 ・CP/AAの開発用鍵から商用鍵への切り替え時の保護用	・Dolby Atmosプログラム保護鍵の暗号化用。 ・CarPlayおよびAndroid Autoの開発用鍵から商用鍵への切り替え時の保護用。	AES	128	No	○	○	Yes
S902	サービスキー	OTAマスタのツール認証用サービスキー。	AES	128	No	○	○	Yes
S903	対称鍵_スペア３	汎用のスペア対称鍵３。	HMAC-SHA	256	No	○	○	Yes
S904	対称鍵_スペア４	汎用のスペア対称鍵４。	HMAC-SHA	256	No	○	○	Yes
S905	対象鍵 スペア5	汎用のスペア対象鍵5	AES	128	No	○	○	Yes

非対称鍵

ID	名前	説明	アルゴリズム	サイズ [bit]	個体別	HSM保管	トヨタ生成	更新可能
A001	秘密鍵_クライアント証明用	クライアント証明に利用する秘密鍵。	ECDSA	256	Yes	○	○	No
A002	公開鍵_リプロデータ署名用	センタから配信する際の、リプロデータの署名検証用。	ECDSA	256	No	○	○	Yes
A003	公開鍵_トヨタルートCA用１	トヨタサーバに接続する際の、サーバ認証に用いる公開鍵。	ECDSA	256	No	○	○	Yes
A004	公開鍵_トヨタルートCA用２	トヨタサーバ用のルートCA公開鍵のサブ。「A003」が漏洩した際のスペア。	ECDSA	256	No	○	○	Yes
A006	公開鍵_セキュアブート用１	セキュアブートの際に、最初の検証に利用する鍵。	RSA	4096	No	–	–	–
A007	公開鍵_セキュアブート用２	A006の次に、検証に利用する鍵。	RSA	4096	No	–	–	–
A008	公開鍵_セキュアブート用３	A007の次に、検証に利用する鍵。（OS起動後の検証に利用）バックグラウンド検証用。	ECDSA	256	No	○	○	Yes
A010	公開鍵_ルートCA証明書検証用	一般サーバ向けのルートCA証明書自体に、トヨタが署名したときの、署名検証用。これ以外のデータも	ECDSA	256	No	○	○	Yes

ID	名前	説明	アルゴリズム	サイズ [bit]	個体別	HSM 保管	トヨタ 生成	更新 可能
		署名がなされる場合は、この鍵にて検証される。						
A012	公開鍵_ スペア3	汎用のスペア公開鍵。	ECDSA	256	No	○	○	Yes
A013	公開鍵_スクリーンロック	スクリーンロック機能におけるチャレンジ・レスポンス用。	ECDSA	256	No	○	○	Yes
A014	公開鍵_鍵更新用	リプロパッケージの中に入った暗号化鍵束をTA100内で復号するための公開鍵。	ECDSA	256	No	○	○	Yes
A015	秘密鍵_ECIES用	ECIES受信者秘密鍵 _secp256r1	ECDH	256	No	○	○	Yes
A016	Share Key Root Public	Public key for authenticating Share Key sequence for TA100 reprogramming.	ECDH	256	No	○	○	–
A017	公開鍵_デバッグ機能再有効化認証データ検証用(サーバ→H/U)	デバッグ機能再有効化のための認証データ(サーバ→H/U)検証用。	ECDSA	256	No	○	○	Yes
A018	公開鍵_サブマイコンリプロ用	サブマイコン用のリプロデータの署名検証用。	ECDSA	256	No	–	○	Yes
A019	公開鍵_Linux kernel module検証用	Linux kernel moduleの署名検証用。	RSA	4096	No	–	– (Tier1)	–
A020	公開鍵_セキュアブート用４	A007の次に、検証に利用する鍵。（OS起動後の検証に利用）dm-verity用。	RSA	2048 or 4096	No	–	– (Tier1)	–
A021	秘密鍵_Uptane向けECU鍵	Uptane向けECU鍵。OTA4.0仕様におけるOTA001。保護資産は下記。 ・マスタECU→配信センタへのHTTP POSTメッセージのBody部	ECDSA	256	No	– (S006を使ったKEM-DEM)	○	Yes
A022	公開鍵_Director Root鍵(初期鍵)	Director Root鍵(初期鍵)。OTA4.0仕様におけるOTA006。保護資産は下記。 ・Director Root Metadata	ECDSA	256	No	–	○	Yes
A023	公開鍵_Director Targets鍵(初期鍵)	Director Targets鍵(初期鍵)。OTA4.0仕様におけるOTA008。保護資産は下記。 ・Director Targets Metadata ・Augmented Meta Data ・OTA Action取得応答(C_03_Res) ・キャンペーン有効性確認応答(C_18_Res) ・OTA コマンド取得応答(C_36_Res)	ECDSA	256	No	–	○	Yes
A024	公開鍵_Director Snapshot鍵(初期鍵)	Director Snapshot鍵(初期鍵)。OTA4.0仕様におけるOTA010。保護資産は下記。 ・Director Shapshot Metadata	ECDSA	256	No	–	○	Yes

ID	名前	説明	アルゴリズム	サイズ [bit]	個体別	HSM 保管	トヨタ 生成	更新 可能
A025	公開鍵_Director Timestamp鍵(初期鍵)	Director Timestamp鍵(初期鍵)。OTA4.0仕様における OTA012。保護資産は下記。 ・Director Timestamp Metadata	ECDSA	256	No	–	○	Yes
A026	公開鍵_Director Root鍵(更新鍵)	Director Root鍵(更新鍵)。OTA4.0仕様におけるOTA014。保護資産は下記。 ・Director Root Metadata	ECDSA	256	No	–	○	Yes
A027	公開鍵_Director Targets鍵(更新鍵)	Director Targets鍵(更新鍵)。OTA4.0仕様におけるOTA016。保護資産は下記。 ・Director Targets Metadata ・Augmented Meta Data ・OTA Action取得応答 (C_03_Res) ・キャンペーン有効性確認応答 (C_18_Res) ・OTA コマンド取得応答 (C_36_Res)	ECDSA	256	No	–	○	Yes
A028	公開鍵_Director Snapshot鍵(更新鍵)	Director Snapshot鍵(更新鍵)。OTA4.0仕様における OTA018。保護資産は下記。 ・Director Shapshot Metadata	ECDSA	256	No	–	○	Yes
A029	公開鍵_Director Timestamp鍵(更新鍵)	Director Timestamp鍵(更新鍵)。OTA4.0仕様における OTA020。保護資産は下記。 ・Director Timestamp Metadata	ECDSA	256	No	–	○	Yes
A030	公開鍵_Image Root鍵(初期鍵)	Image Root鍵(初期鍵)。OTA4.0仕様におけるOTA022。保護資産は下記。 ・Image Root Metadata	ECDSA	256	No	–	○	Yes
A031	公開鍵_Image Targets鍵(初期鍵)	Image Targets鍵(初期鍵)。OTA4.0仕様におけるOTA024。保護資産は下記。 ・Image Targets Metadata ・Augmented Meta Data ・OTA Action取得応答 (C_03_Res) ・キャンペーン有効性確認応答 (C_18_Res) ・OTA コマンド取得応答 (C_36_Res)	ECDSA	256	No	–	○	Yes
A032	公開鍵_Image Snapshot鍵(初期鍵)	Image Snapshot鍵(初期鍵)。OTA4.0仕様におけるOTA026。保護資産は下記。 ・Image Shapshot Metadata	ECDSA	256	No	–	○	Yes

ID	名前	説明	アルゴリズム	サイズ [bit]	個体別	HSM 保管	トヨタ 生成	更新 可能
A033	公開鍵_Image Timestamp鍵(初期鍵)	Image Timestamp鍵(初期鍵)。OTA4.0仕様における OTA028。保護資産は下記。 ・Image Timestamp Metadata	ECDSA	256	No	–	○	Yes
A034	公開鍵_Image Root鍵(更新鍵)	Image Root鍵(更新鍵)。 OTA4.0仕様におけるOTA030。 保護資産は下記。 ・Image Root Metadata	ECDSA	256	No	–	○	Yes
A035	公開鍵_Image Targets鍵(更新鍵)	Image Targets鍵(更新鍵)。 OTA4.0仕様におけるOTA032。 保護資産は下記。 ・Image Targets Metadata	ECDSA	256	No	–	○	Yes
A036	公開鍵_Image Snapshot鍵(更新鍵)	Image Snapshot鍵(更新鍵)。 OTA4.0仕様におけるOTA034。 保護資産は下記。 ・Image Shapshot Metadata	ECDSA	256	No	–	○	Yes
A037	公開鍵_Image Timestamp鍵(更新鍵)	Image Timestamp鍵(更新鍵)。OTA4.0仕様における OTA036。保護資産は下記。 ・Image Timestamp Metadata	ECDSA	256	No	–	○	Yes
A038	公開鍵_PKG署名鍵(UO向け)	PKG署名鍵(UO向け)。OTA4.0 仕様におけるOTA046。保護資産は下記。 ・UO向けメタデータ	ECDSA	256	No	–	○	Yes
A039	公開鍵_PKG署名鍵(DC向け)	PKG署名鍵(DC向け)。OTA4.0 仕様におけるOTA048。保護資産は下記。 ・DC向けメタデータ	ECDSA	256	No	–	○	Yes
A040	公開鍵_dm-verityの cstm ROM用	dm-verityのcstm ROMの署名検証用。	RSA	2048 or 4096	No	–	○)	–
A901	公開鍵_スペア１	汎用のスペア公開鍵。	ECDSA	256	No	○	○	Yes
A902	公開鍵_スペア２	汎用のスペア公開鍵。	RSA	3072	No	○	○	Yes
A903	秘密鍵_スペア１	汎用のスペア秘密鍵。	ECDSA	256	No	○	○	Yes
A904	秘密鍵_スペア2	汎用のスペア秘密鍵。	RSA	3072	No	○	○	Yes
A905	公開鍵_トヨタルート CA用スペア１	トヨタサーバに接続する際の、サーバ証明書に用いる公開鍵スペア。	RSA	3072	No	○	○	Yes
A906	公開鍵_トヨタルート CA用スペア２	トヨタサーバに接続する際の、サーバ証明書に用いる公開鍵スペア。	RSA	3072	No	○	○	Yes

(2) 証明書

	名前	説明	アルゴリズム	個体別	HSM 保管	トヨタ 生成	更新 可能
C001	トヨタルートCA証明書 1	A003に対応する、トヨタルートCA 証明書。	X.509v3	No	○	○	Yes
C002	トヨタルートCA証明書 2	A004に対応する、トヨタルートCA 証明書。	X.509v3	No	○	○	Yes
C003	クライアント証明書	クライアント証明用の証明書。	X.509v3	Yes	○	○	No

C004	第三者サーバ用ルートCA証明書	トヨタ管理外のサーバに直接接続する際に、サーバ証明書を認証するための証明書。	(採用する証明書に依存)	No	–	– (Depends on the CA)	Yes
C901	トヨタルートCA証明書スペア1	A905に対応する、トヨタルートCA証明書。	X.509v3	No	○	○	Yes
C902	トヨタルートCA証明書スペア2	A906に対応する、トヨタルートCA証明書。	X.509v3	No	○	○	Yes

Appendix D. 鍵フォーマット

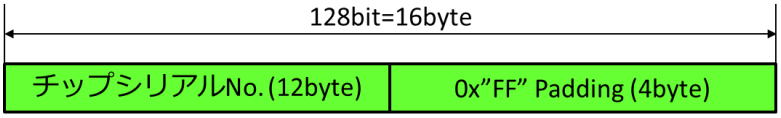
Appendix D-1. 鍵フォーマット

以下、鍵コードは、ASCII文字列(例えば、”S001”)でパディングは0x00で行う。バージョンは、初期値を0x00000000(ALL 0)とする。

■①IDデータフォーマット

●データタイプ　：　テキスト(char)16 Byte

●データサイズ　：　16 Byte / 組



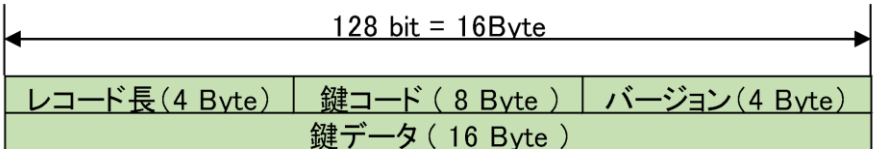
チップシリアルNo.の先頭は'C'固定、2文字目は'C' or 'Y' or 'Z'、3文字目は'A' or 'B'、4文字目は'A' or 'B' or 'C' or 'D'、5文字目は'A'固定、6文字目以降は'AAAAAAA'からインクリメントされる

チップシリアルNo.+"FFFF"が鍵束のファイル名の一部となる

■③AES128鍵データフォーマット

●データタイプ　：　バイナリ(bin)4 Byte + テキスト(char)8 Byte + バイナリ(bin)4 Byte + バイナリ(bin)16 Byte

●データサイズ　：　32 Byte / 組



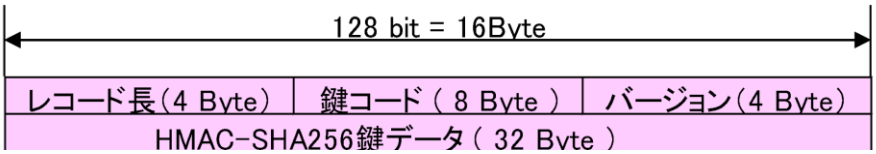
レコード長は自身の長さを含める、AES128鍵の場合は0x00000020を格納

鍵コードは「24CY_情報セキュリティ要求仕様書」Appendix.A 各表のID欄に準拠（例：S001）

■④HMAC-SHA256鍵データフォーマット

●データタイプ　：　バイナリ(bin)4 Byte + テキスト(char)8 Byte + バイナリ(bin)4 Byte + バイナリ(bin)32 Byte

●データサイズ　：　48 Byte / 組



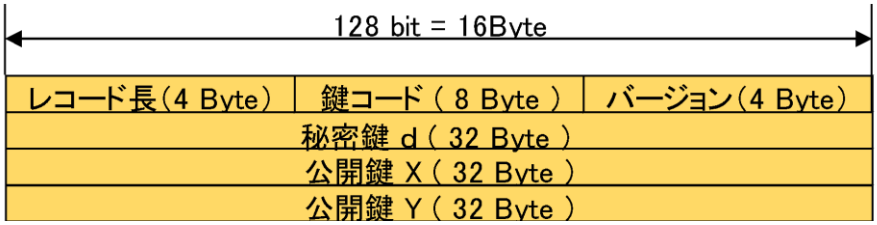
レコード長は自身の長さを含める、HMAC-SHA256鍵の場合は0X00000030を格納

鍵コードは「24CY_情報セキュリティ仕様書」Appendix.A 各表のID欄に準拠（例：S006）

■⑤ECDSA-P256鍵ペアデータフォーマット

●データタイプ　：　バイナリ(bin)4 Byte + テキスト(char)8 Byte + バイナリ(bin)4 Byte + バイナリ(bin)96 Byte

●データサイズ　：　112 Byte / 組



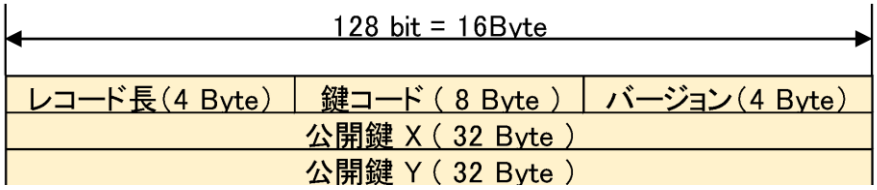
レコード長は自身の長さを含める、ECDSA-P256鍵ペアの場合は0x00000070を格納

鍵コードは「24CY_情報セキュリティ仕様書」Appendix.A 各表のID欄に準拠(例：A901)

■⑥ECDSA-P256公開鍵データフォーマット

●データタイプ　：　バイナリ(bin)4 Byte + テキスト(char)8 Byte + バイナリ(bin)4 Byte + バイナリ(bin)64 Byte

●データサイズ　：　80 Byte / 組



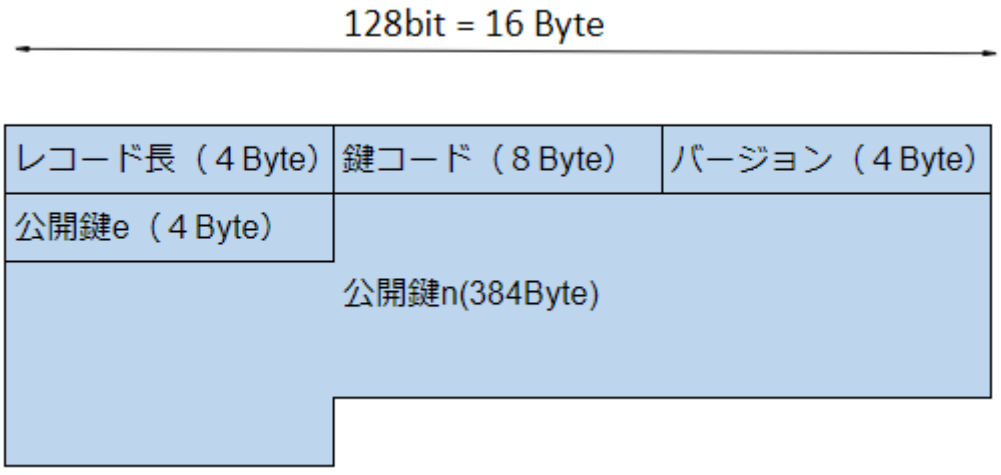
レコード長は自身の長さを含める、ECDSA-P256公開鍵の場合は0x000050を格納

鍵コードは「24CY_情報セキュリティ仕様書」Appendix.A 各表のID欄に準拠（例：A002）

■⑦RSA3072公開鍵データフォーマット

●データタイプ　：　バイナリ(bin)4 Byte + テキスト(char)8 Byte + バイナリ(bin)4 Byte + バイナリ(bin)388 Byte

●データサイズ　：　404 Byte / 組



レコード長は自身の長さを含める、RSA3072公開鍵の場合は0x00000194を格納

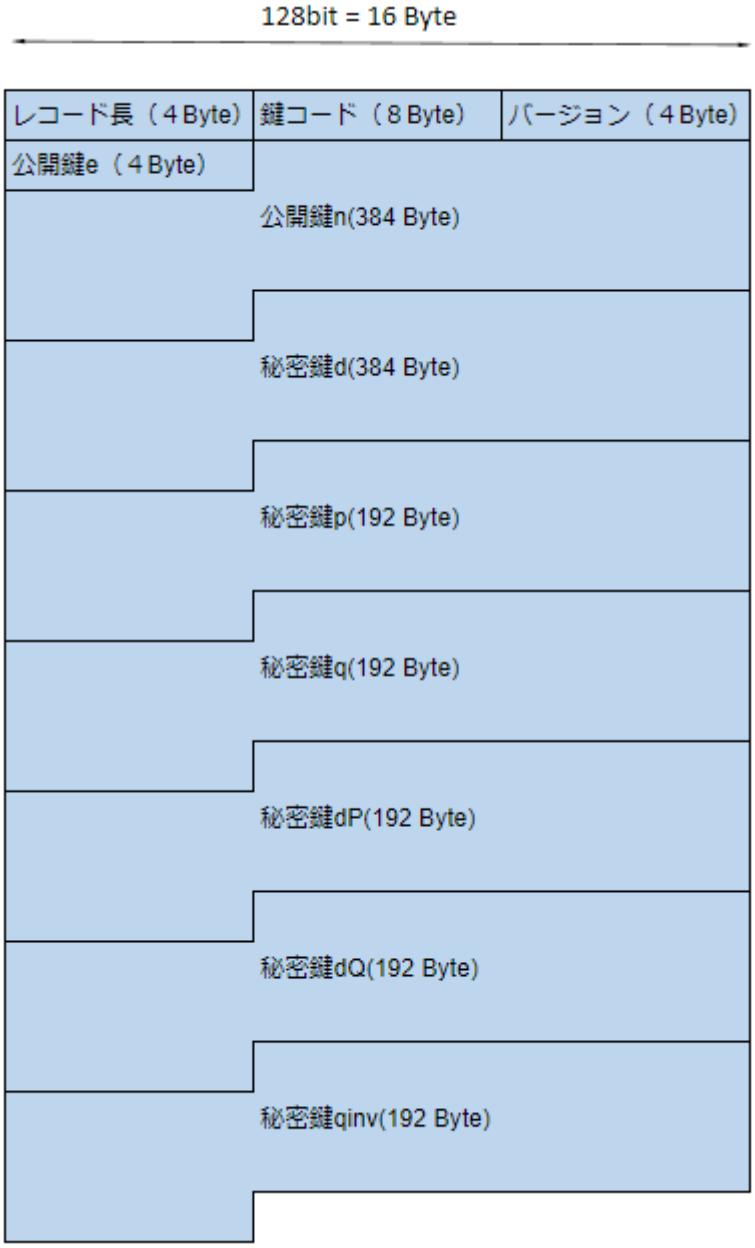
鍵コードは「24CY_情報セキュリティ仕様書」Appendix.A 各表のID欄に準拠（例：A005）

公開鍵eは0x00010001を設定のこと

■ ⑨RSA3072鍵ペアデータフォーマット

●データタイプ ： バイナリ(bin)4 Byte + テキスト(char)8 Byte + バイナリ(bin)4 Byte + バイナリ(bin)1732 Byte

●データサイズ ： 1748 Byte / 組



レコード長は自身の長さを含める、RSA3072鍵ペアの場合は0x000006D4を格納

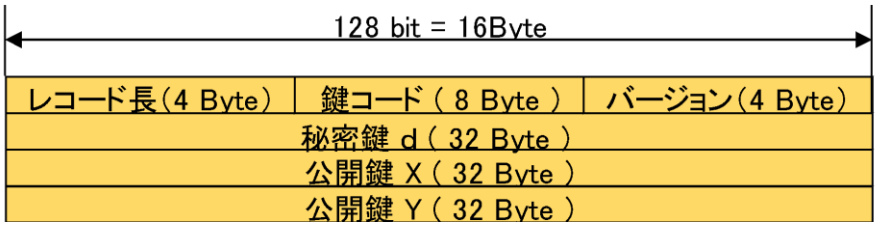
鍵コードは「24CY_情報セキュリティ仕様書」Appendix.A 各表のID欄に準拠（例：A902）

公開鍵eは0x00010001を設定のこと

■ ⑩ECDH-P256鍵ペアデータフォーマット

●データタイプ ： バイナリ(bin)4 Byte + テキスト(char)8 Byte + バイナリ(bin)4 Byte + バイナリ(bin)96 Byte

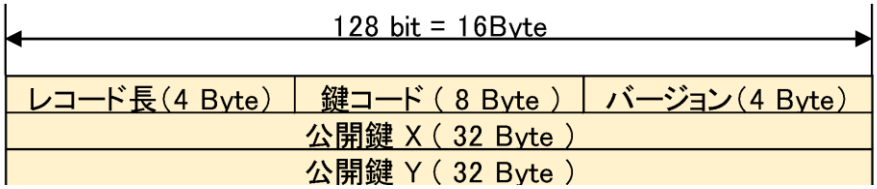
●データサイズ ： 112 Byte / 組



レコード長は自身の長さを含める、ECDH-P256鍵ペアの場合は0x00000070を格納
鍵コードは「24CY_情報セキュリティ仕様書」Appendix.A 各表のID欄に準拠(例：A901)

■⑪ECDH-P256公開鍵データフォーマット

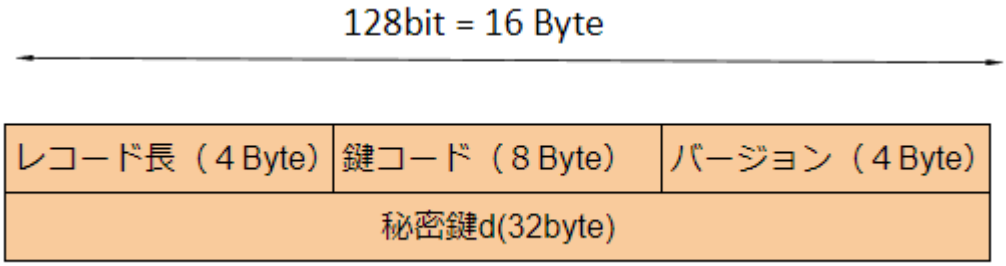
●データタイプ ： バイナリ(bin)4 Byte + テキスト(char)8 Byte + バイナリ(bin)4 Byte + バイナリ(bin)64 Byte
●データサイズ ： 80 Byte / 組



レコード長は自身の長さを含める、ECDH-P256公開鍵の場合は0x000050を格納
鍵コードは「24CY_情報セキュリティ仕様書」Appendix.A 各表のID欄に準拠（例：A002）

■⑫ECDH-P256秘密鍵データフォーマット

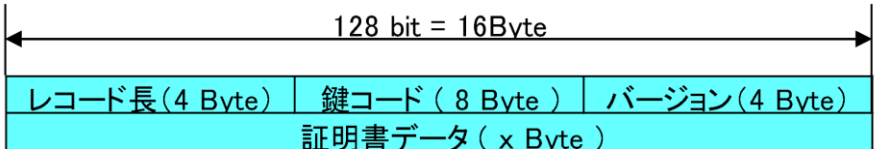
●データタイプ ： バイナリ(bin)4 Byte + テキスト(char)8 Byte + バイナリ(bin)4 Byte + バイナリ(bin)32 Byte
●データサイズ ： 48 Byte / 組



レコード長は自身の長さを含める、ECDH-P256秘密鍵の場合は0x000050を格納
鍵コードは「24CY_情報セキュリティ仕様書」Appendix.A 各表のID欄に準拠（例：A015）

■ⒶⒷⒸⒹⒺ各種証明書データフォーマット

●データタイプ ： バイナリ(bin)4 Byte + テキスト(char)8 Byte + バイナリ(bin)4 Byte + バイナリ(bin)α Byte
●データサイズ ： 16+ x Byte / 組



レコード長は自身の長さを含める
鍵コードは「24CY_情報セキュリティ仕様書」Appendix.A 各表のID欄に準拠（例：C001）
バージョンの表現形式はT.B.D
証明書データはDER形式(バイナリ)で格納する

■24CY鍵データフォーマット（step1：チップベンダー→OEM）

●データサイズ ：502 Byte

128 bit = 16 Byte	個別/共通	データサイズ[Byte]
クライアント証明書作成用CSR ・ECDSA-P256鍵ペアより生成 、x509v3仕様に準拠 ・Subject ″C=JP,O=TOEJA,OU=microchip,OU=Japan, CN=チップシリアルNo.の先頭10文字″ を指定 ・keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment を指定	個別	502

黄色部はチップベンダーで作成するレコード

ECDSA鍵ペアからCSRを生成、チップシリアルNo.単位で鍵ペアのユニーク性を保証する。

秘密鍵を4バイト単位の区間に区切り、区間内で連続した'0'または'1'のビットがないことを保証する。

チップシリアルNo.をCSRのファイル名の一部とする。(例：CCAAAAAAAAAAFFFF.csr.pem)

1件1ファイルとして作成する。

最大1M件まで1フォルダに格納する。

■24CYインストール鍵データフォーマット（step2：OEM→チップベンダ―）

●データサイズ ： (4608+α)*n + 4Byte/鍵束 （α：証明書のサイズ、n：鍵束本数）

24CYでは下記を基準とする。

	← 128bit = 16Byte →		個別/共通	データサイズ[Byte]
	チップシリアル No		個別	16
①	S001	リプロデータ保護用（AES128 鍵）	共通	32
③	S002	プライバシーデータ保護用（AES128 鍵）	個別	32
③	S006	対称鍵_ OTA マスタ用鍵	共通	32
④	S007	汎用 HMAC 用（HMAC-SHA256 鍵）	共通	48
③	S008	セキュリティパラメータ更新用（AES128 鍵）	共通	32
③	S011	リプロデータ保護用(USB リプロ)（AES128 鍵）	共通	32
③	S014	汎用 CMAC 用	共通	32
③	S016	デバッグ機能再有効化認証データ保護用	共通	32
④	S017	デバッグ機能再有効化認証データ検証用(H/U→サーバ)	共通	48
③	S901	対象鍵 スペア 1（AES128 鍵）	共通	32
③	S902	サービスキー	共通	32
④	S903	対象鍵 スペア 3（HMAC-SHA256 鍵）	共通	48
④	S904	対象鍵 スペア 4（HMAC-SHA256 鍵）	共通	48
③	S905	対象鍵 スペア 5（AES128 鍵）	共通	32
⑩	A001	秘密鍵_クライアント証明用	個別	112
⑥	A002	公開鍵 リプロデータ署名用（ECDSA-P256 公開鍵）	共通	80
⑥	A003	公開鍵 トヨタルート CA 用 1（ECDSA-P256 公開鍵）	共通	80
⑥	A004	公開鍵 トヨタルート CA 用 2（ECDSA-P256 公開鍵）	共通	80
⑥	A008	公開鍵 セキュアブート用 3（ECDSA-P256 公開鍵）	共通	80
⑥	A010	公開鍵 ルート CA 証明書検証用（ECDSA-P256 公開鍵）	共通	80
⑥	A012	公開鍵_OEM Apps における署名検証鍵（ECDSA-P256 公開鍵）	共通	80
⑥	A013	公開鍵_スクリーンロック（ECDSA-P256 公開鍵）	共通	80
⑥	A014	公開鍵_セキュリティパラメータ更新用（ECDSA-P256 公開鍵）	共通	80
⑩	A015	秘密鍵_ECIES 用	共通	112
⑥	A017	デバッグ機能再有効化認証データ検証用(サーバ→H/U)	共通	80
⑥	A901	スペア公開鍵 1（ECDSA-P256 公開鍵）	共通	80
⑦	A902	スペア公開鍵 2（RSA 3072 公開鍵）	共通	404
⑤	A903	スペア秘密鍵 1（ECDSA-P256 鍵ペア）	共通	112
⑨	A904	スペア秘密鍵 2（RSA 3072 鍵ペア）	共通	1748
⑦	A905	公開鍵トヨタルート CA 用スペア 1（RSA 3072 公開鍵）	共通	404
⑦	A906	公開鍵トヨタルート CA 用スペア 2（RSA 3072 公開鍵）	共通	404
A	C001	証明書 トヨタルート CA 証明書 1（x.509v3 DER 形式）	共通	α
B	C002	証明書 トヨタルート CA 証明書 2（x.509v3 DER 形式）	共通	
C	C003	証明書_クライアント証明書（x.509v3 DER 形式）	個別	
D	C901	証明書_トヨタルート CA 証明書スペア 1（x.509v3 DER 形式）	共通	
E	C902	証明書_トヨタルート CA 証明書スペア 2（x.509v3 DER 形式）	共通	
⑩		CRC-32 値	-	4

			合計	(4708+α)*n+4

黄色部はチップベンダーで作成するレコード
鍵束および証明書をｎ本分セット + CRC-32値を付加した状態で１ファイル構成とする。
配送時はフォルダに格納(max100万ファイル)後、zip圧縮した後でPGP暗号化を行う。

Appendix D-2. 更新用データフォーマット

24CYでは、下記を基準とする。

◆ 更新用CSPデータ束のデータフォーマット

※鍵と証明書のフォーマットは共通であるが、CSP更新APIに渡すデータはそれぞれに分かれる。

図 D-1 CSP更新API

32bit
CSP更新データ 件数 (4byte)
CSP更新データ[0] データタイプ (4byte)
CSP更新データ[0] データ長 (4byte)
CSP更新データ[0]
CSP更新データ[1] データタイプ (4byte)
CSP更新データ[1] データ長 (4byte)
CSP更新データ[1]
:
CSP更新データ[n] データタイプ (4byte)
CSP更新データ[n] データ長 (4byte)
CSP更新データ[n]

データタイプ：CSP更新データを識別するフィールド

鍵更新データ = 0

証明書更新データ = 1

図 D-2 更新用CSPデータ (AES 128bit Key)

128bit			
32bit	32bit	32bit	32bit
Random IV			
更新データ種(=0)	鍵グループID(=1)	鍵ID	Reserved
カウンタ	鍵プロパティ	Reserved	
AES128鍵 (128bit)			
Signature： r (ECDSA Secp256r1 256bit)			
Signature： s (ECDSA Secp256r1 256bit)			

Signature target

AES128 CBC Encryption

- Reservedのフィールドには0を設定
- 鍵IDおよび鍵プロパティはAppendix D-3参照
- カウンタは鍵のバージョン番号を表す。初期値は0で更新する度にインクリメントした値を設定

図 D-3 更新用CSPデータ (RSA 3072bit Pair-Key)

128bit			
32bit	32bit	32bit	32bit
RandomIV			
更新データ種(=0)	鍵グループID(=4)	鍵ID	Reserved
カウンタ	鍵プロパティ	Reserved	
Public-Key n (3072bit)			
Private-Key d (3072bit)			
Private-Key (p-1)(q-1) (3072bit)			
Signature r (ECDSA secp256r1 256bit)			
Signature s (ECDSA secp256r1 256bit)			

- Reservedのフィールドには0を設定
- 鍵IDおよび鍵プロパティはAppendix D-3参照
- カウンタは鍵のバージョン番号を表す。初期値は0で更新する度にインクリメントした値を設定
- RSA公開鍵指数 e は65537固定

図 D-4 更新用CSPデータ (RSA 3072bit Pair-Key for MicroChip)

128bit			
32bit	**32bit**	**32bit**	**32bit**
RandomIV			
更新データ種(=0)	**鍵グループID(=6)**	**鍵ID**	**Reserved**
カウンタ	**鍵プロパティ**	**Reserved**	
Public-Key n (3072bit)			
Private-Key d (3072bit)			
Private-Key p (1536bit)			
Private-Key q (1536bit)			
Private-Key dp (1536bit)			
Private-Key dq (1536bit)			
Private-Key qInv (1536bit)			
Signature r (ECDSA secp256r1 256bit)			
Signature s (ECDSA secp256r1 256bit)			

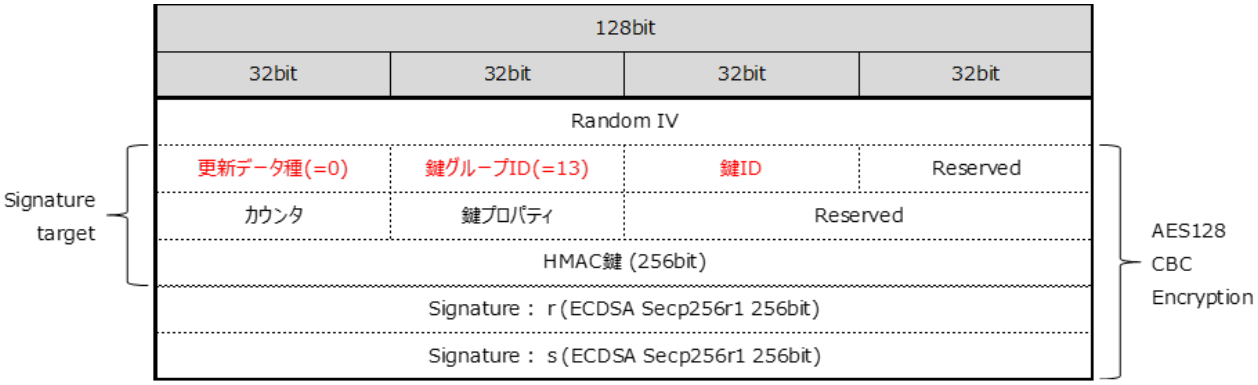
- Reservedのフィールドには0を設定
- 鍵IDおよび鍵プロパティはAppendix D-3参照
- カウンタは鍵のバージョン番号を表す。初期値は0で更新する度にインクリメントした値を設定

図 D-5 更新用CSPデータ (RSA 3072bit Public-Key)

128bit			
32bit	32bit	32bit	32bit
RandomIV			
更新データ主(=0)	鍵グループID(=5)	鍵ID	Reserved
カウンタ	鍵プロパティ	Reserved	
Public-Key n (3072bit)			
Public-Key e (32bit)	Reserved		
Signature r (ECDSA secp256r1 256bit)			
Signature s (ECDSA secp256r1 256bit)			

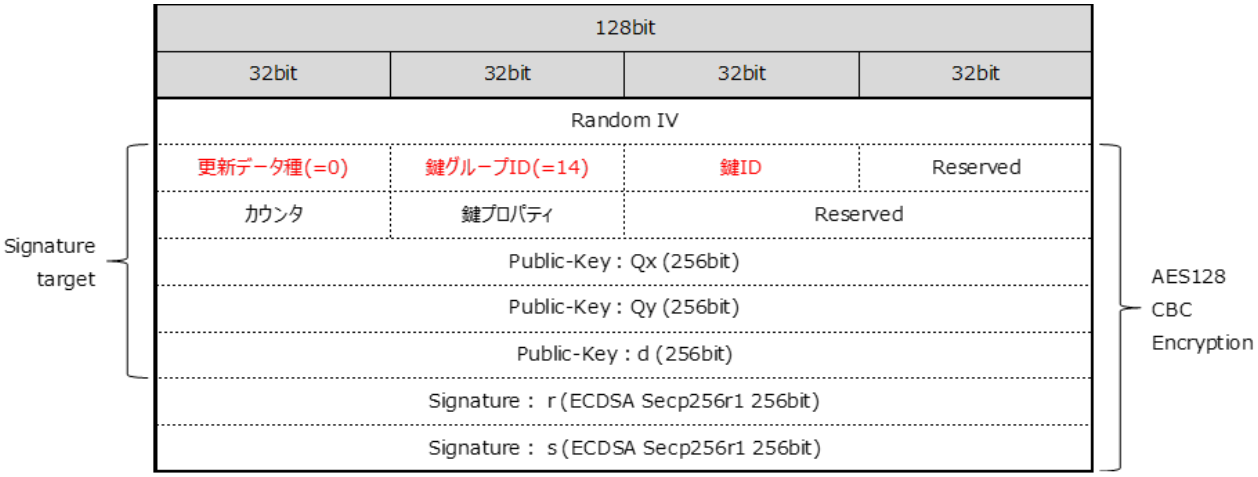
- Reservedのフィールドには0を設定
- 鍵IDおよび鍵プロパティはAppendix D-3参照
- カウンタは鍵のバージョン番号を表す。初期値は0で更新する度にインクリメントした値を設定

図 D-6 更新用CSPデータ (HMAC SHA256 Key)



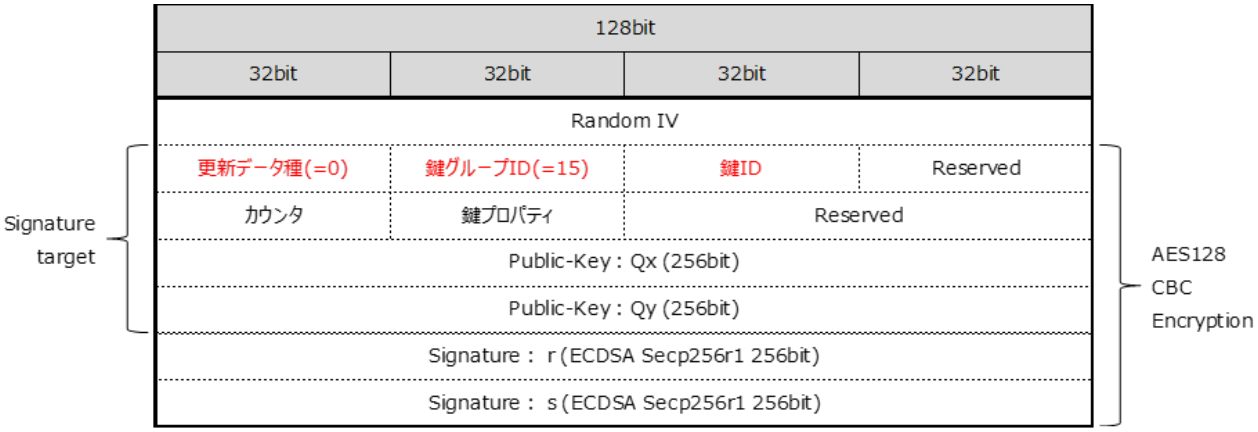
- Reservedのフィールドには0を設定
- 鍵IDおよび鍵プロパティはAppendix D-3参照
- カウンタは鍵のバージョン番号を表す。初期値は0で更新する度にインクリメントした値を設定

図 D-7 更新用CSPデータ (ECC P-256 Pair-Key)



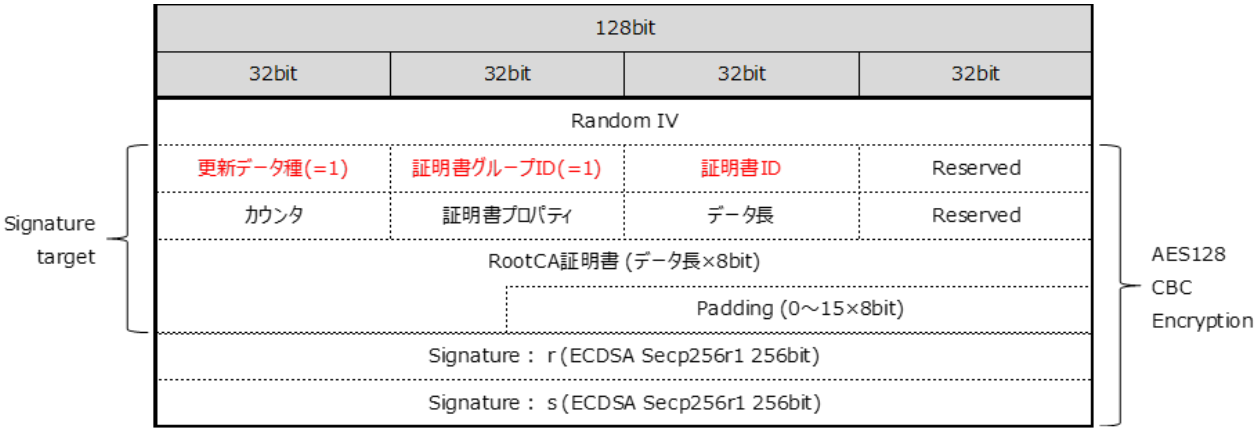
- Reservedのフィールドには0を設定
- 鍵IDおよび鍵プロパティはAppendix D-3参照
- カウンタは鍵のバージョン番号を表す。初期値は0で更新する度にインクリメントした値を設定

図 D-8 更新用CSPデータ (ECC P-256 Public Key)



- Reservedのフィールドには0を設定
- 鍵IDおよび鍵プロパティはAppendix D-3参照
- カウンタは鍵のバージョン番号を表す。初期値は0で更新する度にインクリメントした値を設定

図 D-9 更新用CSPデータ (RootCA証明書)



- ReservedおよびPaddingのフィールドには0を設定
- Paddingデータ長はRootCA証明書＋Paddingのデータ長が16バイトでアラインされるように設定
- 証明書IDおよび証明書プロパティはAppendix D-4参照
- カウンタは証明書のバージョン番号を表す。初期値は0で更新する度にインクリメントした値を設定
- データ長はクライアント証明書データのデータ長を設定

Appendix D-3. HSMで扱う鍵のID等

24CYでは、下記を基準とする。

表 D-10 プロパティー覧 (対称鍵)

ID	名前	鍵グループID	鍵ID	鍵プロパティ
S001	リプロデータ保護用	0x00000001	0x00000000	0x80000080
S002	プライバシーデータ保護用_HSM内	0x00000001	0x00000001	0x80030000
S006	対称鍵_ OTAマスタ用鍵	0x00000001	0x00000011	0x800C0000
S007	汎用HMAC用	0x0000000d	0x00000001	0x800C0000
S008	セキュリティパラメータ更新用	0x00000001	0x00000004	0x80000020
S011	リプロデータ保護用（USBリプロ）	0x00000001	0x00000006	0x80000080
S014	汎用CMAC用	0x00000001	0x0000000A	0x00000000
S016	デバッグ機能再有効化認証データ保護用	0x00000001	0x0000000B	0x00000000
S017	デバッグ機能再有効化認証データ検証用(H/U→サーバ)	0x0000000d	0x00000005	0x00000000
S901	対称鍵_スペア１	0x00000001	0x00000008	0x800F0000
S902	サービスキー	0x00000001	0x00000009	0x800F0000
S903	対称鍵_スペア３	0x0000000d	0x00000003	0x800C0000
S904	対称鍵_スペア４	0x0000000d	0x00000004	0x800C0000
S905	対象鍵 スペア5（AES128鍵）	0x00000001	0x0000000D	0x00000000

表 D-11 プロパティー覧 (非対称鍵)

ID	名前	鍵グループID	鍵ID	鍵プロパティ
A002	公開鍵_リプロデータ署名用	0x0000000f	0x00000000	0x81000080
A003	公開鍵_トヨタルートCA用１	0x0000000f	0x00000001	0x81000000
A004	公開鍵_トヨタルートCA用２	0x0000000f	0x00000002	0x81000000
A008	公開鍵_セキュアブート用３	0x0000000f	0x00000003	0x81000000
A010	公開鍵_ルートCA証明書検証用	0x0000000f	0x00000005	0x81000000
A012	公開鍵_OEM Appsにおける署名検証鍵	0x0000000f	0x00000006	0x81000000
A013	公開鍵_スクリーンロック	0x0000000f	0x00000007	0x81000000
A014	公開鍵_鍵更新用	0x0000000f	0x00000008	0x80000020
A015	秘密鍵_ECIES用	0x0000000e	0x00000002	0x00000000
A017	デバッグ機能再有効化認証データ検証用(サーバ→H/U)	0x0000000f	0x0000000C	0x00000000
A901	公開鍵_スペア１	0x0000000f	0x00000009	0x81000000
A902	公開鍵_スペア２	0x00000005	0x00000001	0x89000000
A903	秘密鍵_スペア１	0x0000000e	0x00000001	0x83000000
A904	秘密鍵_スペア2	0x00000006	0x00000001	0x8F000000
A905	公開鍵_トヨタルートCA用スペア１	0x00000005	0x00000002	0x81000000
A906	公開鍵_トヨタルートCA用スペア２	0x00000005	0x00000003	0x81000000

Appendix D-4. HSMで扱う証明書のID等

24CYでは、下記を基準とする。

表 D-12 プロパティ一覧 (証明書)

ID	名前	証明書グループID	証明書ID	証明書プロパティ
C001	トヨタルートCA証明書 1	0x00000001	0x00000000	0x80000000
C002	トヨタルートCA証明書 2	0x00000001	0x00000001	0x80000000
C901	トヨタルートCA証明書スペア 1	0x00000001	0x00000002	0x80000000
C902	トヨタルートCA証明書スペア 2	0x00000001	0x00000003	0x80000000