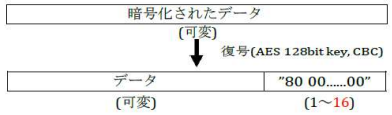
特定在留カード等仕様書（一般公開用）_Ver 1.1　新旧対照表

<table>
<tr><th>頁</th><th>該当箇所</th><th>新</th><th>旧</th></tr>
<tr><td>7</td><td>図3-2 Tの長さ</td><td>(1～2)
<table><tr><th>T</th><th>L</th><th>V</th></tr><tr><td>3.3.4 参照</td><td>“00”～”7F”
“81 00”～”81FF”
“82 00 00”～”82 FF FF”</td><td>値</td></tr><tr><td>(1～2)</td><td>(1～3)</td><td>(L)</td></tr></table></td><td>(1)
<table><tr><th>T</th><th>L</th><th>V</th></tr><tr><td>3.3.4 参照</td><td>“00”～”7F”
“81 00”～”81FF”
“82 00 00”～”82 FF FF”</td><td>値</td></tr><tr><td>(1)</td><td>(1～3)</td><td>(L)</td></tr></table></td></tr>
<tr><td>8</td><td>3.3.1 ファイル構成
表 3-1 特定在留カードファイル構成
DF1/EF02：券面記載事項 の ファイル容量(byte)</td><td>73</td><td>76</td></tr>
<tr><td>8</td><td>3.3.1 ファイル構成
表 3-2 特定特別永住者証明書ファイル構成
DF1/EF02：券面記載事項 の ファイル容量(byte)</td><td>46</td><td>73</td></tr>
<tr><td>9</td><td>表3-3　在留 APのAID</td><td>“D3 92 F0 00 4F 01 00 00 00 00 00 00 00 00 00</td><td>“D3 92 F0 00 4F 01 00 00 00 00 00 00 00 00 00</td></tr>
<tr><td>9</td><td>表3-3　DF1のAID</td><td>“D3 92 F0 00 4F 02 00 00 00 00 00 00 00 00 00</td><td>“D3 92 F0 00 4F 02 00 00 00 00 00 00 00 00 00</td></tr>
<tr><td>9</td><td>表3-3　DF2のAID</td><td>“D3 92 F0 00 4F 03 00 00 00 00 00 00 00 00 00</td><td>“D3 92 F0 00 4F 03 00 00 00 00 00 00 00 00 00</td></tr>
<tr><td>9</td><td>表3-3　DF3のAID</td><td>“D3 92 F0 00 4F 04 00 00 00 00 00 00 00 00 00</td><td>“D3 92 F0 00 4F 04 00 00 00 00 00 00 00 00 00</td></tr>
<tr><td>11</td><td>3.3.4.4
「国籍」の内容</td><td>国籍・地域</td><td>国籍</td></tr>
<tr><td>11</td><td>3.3.4.4
「国籍」の詳細</td><td>国籍・地域コード</td><td>国籍コード</td></tr>
<tr><td>11</td><td>3.3.4.4
「在留資格」の詳細</td><td>在留資格期間コード</td><td>在留資格コード(3 桁)+YYMMDDD</td></tr>
<tr><td>11</td><td>3.3.4.4
「在留期間」の詳細</td><td>無期限でない場合：YYMM もしくは DDD
無期限の場合(永住者など)：0000</td><td>YYMM もしくは DDD
永住者の場合**年**月、
特定活動の場合***日と格納</td></tr>
<tr><td>11</td><td>3.3.4.4
「許可の種類」の詳細</td><td>許可の種類コード(2 桁)
特別永住者証明書は項目無し</td><td>在留資格許可コード(2 桁)
特別永住者証明書は項目無し</td></tr>
<tr><td>11</td><td>3.3.4.4「就労制限の有無」の詳細</td><td>1:就労制限なし
2:在留資格に基づく就労活動のみ可
4:指定書により指定された就労活動のみ可
9:就労不可
特別永住者証明書は項目無し</td><td>0:無し
1:有り(在留資格に基づく就労活動のみ可)
2:有り(就労不可)
3:有り(指定書により指定された就労活動のみ可)
特別永住者証明書は項目無し</td></tr>
<tr><td>11</td><td>3.3.4.5 氏名イメージ・顔画像 (DF1/EF02)</td><td>3.3.4.5 氏名イメージ・顔画像 (DF1/EF03)</td><td>3.3.4.5 氏名イメージ・顔画像 (DF1/EF02)</td></tr>
</table>

特定在留カード等仕様書（一般公開用）_Ver 1.1　新旧対照表

頁	該当箇所	新	旧
11	3.3.4.5 「氏名印字イメージ」	氏名イメージ	氏名印字イメージ
11	3.3.4.6 住居地イメージ (DF1/EF03)	3.3.4.6 住居地イメージ (DF1/EF04)	3.3.4.6 住居地イメージ (DF1/EF03)
12	3.3.4.6 「住居地印字イメージ」	住居地イメージ	住居地印字イメージ
12	3.3.4.7 「包括許可欄」の最大データ長（バイト）	7 ※実際に書き込まれるデータは1バイト	7
12	3.3.4.7 「包括許可欄」の詳細	0:無し 1:許可(週28時間以内・風俗営業不可) 2:許可(週28時間以内・教育等の活動)	在留資格コード
13	3.3.4.10 チェックコード、公開鍵証明書 (DF3/EF01) チェックコード(署名値)の最大データ長(バイト)	96	104
13	3.3.4.10 チェックコード、公開鍵証明書 (DF3/EF01) チェックコード(署名値)の最大データ長(バイト)	602	594
13	3.3.4.10 チェックコード、公開鍵証明書 (DF3/EF01) 公開鍵証明書の詳細	X.509（ver.3）形式 ECDSA(NIST P-384 SHA256)を想定 ※最大データ長としては602バイトだが、実際に書き込まれるデータは598もしくは599バイト	X.509（ver.3）形式 ECDSA(NIST P-384 SHA256)を想定
13	3.3.5 1 歳未満の在留カード及び特別永住者証明書のデータ取り扱いについて	（※1を顔写真の注釈とした上で） *1 DF1/EF02には「Tag1バイト(0xD1)・Length1バイト(0x00)・以降 Null値(0x00)埋め」が格納される。 *2 DF3/EF01には「Tag1バイト(0xDC)・Length1バイト(0x00)・Tag1バイト(0xDD)・Length1バイト(0x00)・以降 Null値(0x00)埋め」が格納される。	*1 DF3/EF01 には「Tag1 バイト(0xDC)・Length1 バイト(0x00)・Tag1 バイト(0xDD)・Length1 バイト(0x00)・以降 Null 値(0x00)埋め」が格納される。 *2 チェックコード、公開鍵証明書なしの場合、DF3/EF01には「Tag1バイト(0xDC)・Length1バイト(0x00)・以降 Null 値(0x00)埋め」が格納される。
15	3.4.3.1 署名検証方法 図3-4 署名検証方法　公開鍵証明書のバイト数	598もしくは599	594
15	3.4.3.1 署名検証方法	ドメインパラメータについては、secp384r1とする。 楕円曲線鍵長：384bit 楕円曲線ドメインパラメータ：secp384r1 署名アルゴリズム：SHA256WithECDSA 図 3-4追加	ドメインパラメータについては、発行事業者と決定する。
21	在留AP選択の「データ」の長さ	16	2
21	EF選択の「データ」の長さ	2	16

特定在留カード等仕様書(一般公開用)_Ver 1.1　新旧対照表

頁	該当箇所	新	旧
23	4.2.2 VERIFY コマンド (i) 暗号化された簡易認証コードの生成方法 IVの設定	IVは以下の手順にて導出する。 (1)セッション開始時(SET SESSION KEYコマンド実行後)の場合、メッセージカウンターNを初期化(N=1)する。 (2) Nをセキュアメッセージング用セッション鍵で暗号化し、得られた結果をIVとする。 暗号アルゴリズムは AES 128bit key CBC モード、initialization vectorは"00 00 … 00"とする。	IV="00 00 …. 00"とする。
23	4.2.2 VERIFY コマンド (i) 暗号化された簡易認証コードの生成方法	③ Nを1加算する(N=N+1)	記載なし
27	4.2.4 READ BINARY コマンド パラメータ「Le」の意味	"XX XX"が"00 00"以外の場合は"XX XX"以下のサイズで読み出せるだけ読出し。 ただし、指定可能な値は、各 EF のファイル容量までとする。	"XX XX"が"00 00"以外の場合は"XX XX"以下のサイズで読み出せるだけ読出し。
29	4.2.4 READ BINARY コマンド パディング("80 00.....00")の長さ	(1～16) 	(1～8) 
29	4.2.4 READ BINARY コマンド (ii) 暗号化されたデータの復号方法 IVの設定	IVは以下の手順にて導出する。 (1) セッション開始時(SET SESSION KEY コマンド実行後)の場合、メッセージカウンターNを初期化(N=1)する (2) Nをセキュアメッセージング用セッション鍵で暗号化し、得られた結果をIVとする。 暗号アルゴリズムは AES 128bit key CBC モード、initialization vectorは"00 00 … 00"とする。	IV="00 00 …. 00"とする。
29	4.2.4 READ BINARY コマンド (ii) 暗号化されたデータの復号方法	③ Nを1加算する(N=N+1)	記載なし
31	別添 1 セキュアメッセージングセッション鍵配送 Step1. セッション鍵の元鍵の生成 鍵の生成方法	Kenc, Kmac は端末のみが知り得る16バイトの値とする。これらの値は、セッションごとに異なる値とすることを推奨する。	Kenc, Kmac は共に在留カード等番号(12 バイト)を SHA-1 でハッシュ化した値の先頭 16 バイトとする。
32	別添 2 読出しシーケンス コマンド例	在留カード等番号= "41 41 31 32 33 34 35 36 37 38 42 42" h(在留カード等番号) = "65 22 B4 E1 71 19 5B B2 18 22 3A 97 6C 04 01 11 BD C4 AA 25" ※1 Kenc = Kmac = "65 22 B4 E1 71 19 5B B2 18 22 3A 97 6C 04 01 11" ※2 ※1 h は SHA-1 とする ※2 本例示では、Kenc, Kmac は在留カード等番号を基に設定しているが、運用時は端末のみが知り得るセッションごとに異なる値とすることを推奨する。	在留カード等番号= "41 41 31 32 33 34 35 36 37 38 42 42" h(在留カード等番号) = "65 22 B4 E1 71 19 5B B2 18 22 3A 97 6C 04 01 11 BD C4 AA 25" Kenc = Kmac = "65 22 B4 E1 71 19 5B B2 18 22 3A 97 6C 04 01 11" ※ h は SHA-1 とする
35	別添 2 読出しシーケンス コマンド例 13. 電子署名の読出し	Send -> 00 B0 82 00 00 00 00 Recv <- DC 60 [チェックコード 96 バイト] DD 82 02 56 [公開鍵証明書 598 バイト] [00 パディング x 4] 90 00 注) 公開鍵証明書は599バイトになる場合もある。その場合は、[00パディング x3]とすること	Send -> 00 B0 82 00 00 00 00 Recv <- DC 68 [チェックコード 104バイト] DD 82 02 52 [公開鍵証明書 594 バイト] 90 00