EMV® Specification Bulletin No. 185
Second Edition October 2018

Biometric Terminal Specification

This Specification Bulletin updates the EMV ICC books to add optional biometric verification functionality.

The 2nd edition of this Specification Bulletin:

- ***Corrects the length of the Enciphered Biometric Key Seed.***
- ***Clarifies that there are no padding bytes before, between, or after data objects in the Biometric Verification Data Template.***
- ***Corrects the length of the Biometric Verification Data Template.***
- ***Clarifies the contents of the VERIFY command data field when sending offline biometric verification data.***
- ***Clarifies that a terminal without biometric support may choose whether to recognize or not recognize the Biometric CVM Codes.***
- ***Corrects the template to which the Card BIT Group Template belongs.***
- ***Clarifies that the BIT in a terminal shall not contain the level 2 BHT 1 nor BHT 2.***

Changes made in this 2nd edition are shown in red text.

Effective Date and Approval Readiness Date

January 1, 2018

Applicability

This Specification Bulletin applies to:

- *EMV Integrated Circuit Card Specifications for Payment Systems Version 4.3 Book 2*
- *EMV Integrated Circuit Card Specifications for Payment Systems Version 4.3 Book 3*
- *EMV Integrated Circuit Card Specifications for Payment Systems Version 4.3 Book 4*

Related Documents

- *ISO/IEC 7816-4 Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange*
- *ISO/IEC 7816-11 Identification cards – Integrated circuit cards – Personal verification through biometric methods*
- *ISO/IEC 9797-2 Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function*
- *ISO/IEC 18033-2 Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers*
- *ISO/IEC 18033-3 Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*
- *ISO/IEC 19785-3 Information technology – Common Biometric Exchange Formats Framework – Patron format specifications*
- *ISO/IEC 19794 Information technology – Biometric data interchange formats*
- *ISO/IEC 19794-2 Information technology – Biometric data interchange formats – Part 2: Finger minutiae data*

Description

This bulletin introduces biometric verification functionality to the EMV Integrated Circuit Card Specifications for Payment Systems to support the Biometric Cardholder Verification Method (CVM) solution in chip-based contact card transactions.

Changes to the EMV ICC books are shown using underlined text.
Specification Change

EMV Book 2

In Section 2 Normative References, add the following reference before the reference for ISO/IEC 18033-3:

ISO/IEC 18033-2 — Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers

Add the following reference after the reference for ISO/IEC 9797-1:2011:

ISO/IEC 9797-2 — Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function

---

In Section 3 Definitions, add the following terms:

Biometric Data Block — A block of data with a specific format that contains information captured from a biometric capture device and that could be used as follows:

- stored in the card as part of the biometric reference template
- sent to the ICC in the data field of the PIN CHANGE/UNBLOCK command
- sent to the ICC in the data field of the VERIFY command for offline biometric verification
- sent online for verification

The format of the BDB is outside the scope of this specification.

biometric reference template — Biometric data stored in the card as reference. Data provided by a biometric capture device would be compared against the biometric reference template to determine a match.

DEM1 — A family of data encapsulation mechanisms defined in ISO/IEC 18033-2

I2OSP — An integer to octet string conversion primitive function defined in ISO/IEC 18033-2

RSA-KEM — A family of key encapsulation mechanisms defined in ISO/IEC 18033-2

RSATransform — The RSA exponentiation that is used for encryption and decryption, and generating and verifying a signature

---

In Section 4.1 Abbreviations, add the following entries:

BDB	Biometric Data Block
BEK	Biometric Encryption Key
BMK	Biometric MAC Key
HMAC	Keyed-hash Message Authentication Code
KDF	Key Derivation Function
SHA-256	Secure Hash Algorithm 256

In Section 7 Personal Identification Number Encipherment, update the section as shown below:

7. Personal Identification Number and Biometric Data Encipherment

If supported, Personal Identification Number (PIN) encipherment for offline PIN verification is performed by the terminal using an asymmetric based encipherment mechanism in order to ensure the secure transfer of a PIN from a secure tamper-evident PIN pad to the ICC.

More precisely, the ICC shall own a public key pair associated with PIN encipherment. The public key is then used by the PIN pad or a secure component of the terminal (other than the PIN pad) to encipher the PIN, and the private key is used by the ICC to decipher the enciphered PIN for verification.
The PIN block used in the data field to be enciphered shall be 8 bytes as shown in section 6.5.12 of Book 3.

If offline Biometric CVM is supported, the biometric data encipherment is performed by the terminal using both symmetric and asymmetric based encipherment mechanisms in order to ensure the secure transfer of biometric data from the biometric capture device to the ICC.

More precisely, the ICC shall own a public/private key pair associated with biometric data encipherment. The public key is then used by the Biometric Processing Application, as shown in Figure 6a of Book 4, or a secure component of the terminal (other than Biometric Processing Application) to encipher a seed, which generates the AES-128 key used to encrypt the biometric data, and the private key is used by the ICC to decipher the seed, which generates the AES-128 key used to decrypt the Enciphered Biometric Data for verification.

7.1 Keys and Certificates

If offline PIN encipherment or offline biometric data encipherment is supported, the ICC shall own a unique public/private key pair consisting of a public encipherment key and the corresponding private decipherment key. This specification allows the following two possibilities.

1. The ICC owns a specific ICC PIN Encipherment Private and Public Key. The ICC PIN Encipherment Public Key shall be stored on the ICC in a public key certificate in exactly the same way as for the ICC Public Key for offline dynamic data authentication as specified in section 6.[31]
   The ICC PIN encipherment public key pair has an ICC PIN Encipherment Public Key Modulus of N_{PE} bytes, where $N_{PE} \leq N_I \leq N_{CA} \leq 248$, N_I being the length of the Issuer Public Key Modulus (see section 6.1). If $N_{PE} > (N_I - 42)$, the ICC PIN Encipherment Public Key Modulus is divided into two parts, one part consisting of the $N_I - 42$ most significant bytes of the modulus (the Leftmost Digits of the ICC PIN Encipherment Public Key) and a second part consisting of the remaining $N_{PE} - (N_I - 42)$ least significant bytes of the modulus (the ICC PIN Encipherment Public Key Remainder).

   The ICC PIN Encipherment Public Key Exponent shall be equal to 3 or $2^{16} + 1$.

   The ICC PIN Encipherment Public Key Certificate is obtained by applying the digital signature scheme as specified in Annex A2.1 on the data in Table 23 using the Issuer Private Key.

   The terminal shall use the ICC PIN Encipherment key pair also for biometric data encipherment.

Field Name	Length	Description	Format
Certificate Format	1	Hex Value '04'	b
Application PAN	10	PAN (padded to the right with Hex 'F's)	cn 20
Certificate Expiration Date	2	MMYY after which this certificate is invalid	n 4

[31] In the case that the ICC owns a specific ICC PIN Encipherment Public Key, the format of the data recovered from the certificate is exactly the same as for dynamic data authentication (see Table 14 in section 6.4) however the data that is input to the hash algorithm when computing the certificate (see Table 23) does not include the Static Data to be Authenticated. Hence all the verification steps specified in section 6.4 are performed except in step 5 the static data to be authenticated is not included in the concatenation of data elements to be hashed in step 6.

Certificate Serial Number	3	Binary number unique to this certificate assigned by the issuer	b
Hash Algorithm Indicator	1	Identifies the hash algorithm used to produce the Hash Result in the digital signature scheme [32]	b
ICC PIN Encipherment Public Key Algorithm Indicator	1	Identifies the digital signature algorithm to be used with the ICC PIN Encipherment Public Key [32]	b
ICC PIN Encipherment Public Key Length	1	Identifies the length of the ICC PIN Encipherment Public Key Modulus in bytes	b
ICC PIN Encipherment Public Key Exponent Length	1	Identifies the length of the ICC PIN Encipherment Public Key Exponent in bytes	b
ICC PIN Encipherment Public Key or Leftmost Digits of the ICC PIN Encipherment Public Key	$N_I – 42$	If $N_{PE} \leq N_I – 42$, consists of the full ICC PIN Encipherment Public Key padded to the right with $N_I – 42 – N_{PE}$ bytes of value 'BB' If $N_{PE} > N_I – 42$, consists of the $N_I – 42$ most significant bytes of the ICC PIN Encipherment Public Key[33]	b
ICC PIN Encipherment Public Key Remainder	0 or $N_{PE} – N_I + 42$	Present only if $N_{PE} > N_I – 42$ and consists of the $N_{PE} – N_I + 42$ least significant bytes of the ICC PIN Encipherment Public Key	b
ICC PIN Encipherment Public Key Exponent	1 or 3	ICC PIN Encipherment Public Key Exponent equal to 3 or $2^{16} + 1$	b

Table 23: ICC PIN Encipherment Public Key Data to be Signed by Issuer (i.e. input to the hash algorithm)

2. The ICC does not own a specific ICC PIN encipherment public key pair, but owns an ICC public key pair for offline dynamic data authentication as specified in section 6.1. This key pair can then be used for PIN encipherment and biometric data encipherment. The ICC Public Key is stored on the ICC in a public key certificate as specified in section 6.1.

The first step of PIN encipherment or biometric data encipherment shall be the retrieval of the public key to be used by the terminal for the encipherment of the PIN or biometric data. This process takes place as follows.

1. If the terminal has obtained all the data objects specified in Table 24 from the ICC, then the terminal retrieves the ICC PIN Encipherment Public Key in exactly the same way as it retrieves the ICC Public Key for offline dynamic data authentication (see section 6).

2. If the terminal has not obtained all the data objects specified in Table 24, but has obtained all the data objects specified in Table 12, then the terminal retrieves the ICC Public Key as described in section 6.

3. If the conditions under points 1 and 2 above are not satisfied or if as described in Section 6.1.2 for dynamic data authentication, the Issuer Public Key Certificate has been revoked, then PIN encipherment has failed and the Offline Enciphered PIN CVM has failed, or biometric data encipherment has failed and the Offline Biometric CVM has failed.

[32] See Annex B for specific values assigned to approved algorithms.

[33] As can be seen in Annex A2.1, $N_I − 22$ bytes of the data signed are retrieved from the signature. Since the length of the first through the eighth data elements in Table 23 is 20 bytes, there are $N_I − 22 − 20 = N_I − 42$ bytes left for the data to be stored in the signature.

Tag	Length	Value	Format
—	5	Registered Application Provider Identifier (RID)	b
'8F'	1	Certification Authority Public Key Index	b
'90'	N_{CA}	Issuer Public Key Certificate	b
'92'	$N_I – N_{CA} + 36$	Issuer Public Key Remainder, if present	b
'9F32'	1 or 3	Issuer Public Key Exponent	b
'9F2D'	N_I	ICC PIN Encipherment Public Key Certificate	b
'9F2E'	1 or 3	ICC PIN Encipherment Public Key Exponent	b
'9F2F'	$N_{PE} – N_I + 42$	ICC PIN Encipherment Public Key Remainder, if present	b

Table 24: Data Objects Required for Retrieval of ICC PIN Encipherment Public Key

After Section 7.2 PIN Encipherment and Verification, add the following new section:

7.3 Biometric Data Encipherment and Recovery

The exchange and decipherment of Enciphered Biometric Data between terminal and ICC takes place in the following steps, as illustrated in Book 3 Figure 12a.

1. The biometric template is captured on a biometric capture device and the Biometric Data Block (BDB) is constructed by the Biometric Processing Application.

2. The terminal issues a GET CHALLENGE command to the ICC to obtain an 8-byte unpredictable number from the ICC. When the response to the GET CHALLENGE command is anything other than an 8 byte data value with SW1 SW2 = '9000', then the terminal considers that the Offline Biometric CVM has failed.

3. Using the public key specified above, the terminal shall generate the Enciphered Biometric Data, as follows:
    a) The public key recovered, as described in section 7.1, has exponent e and modulus n.
    b) The terminal generates a random number r, which has the same number of bits as n, and shall be less than n, i.e. r < n. Then the terminal converts r into a byte string R as defined in ISO/IEC 18033-2: R = I2OSP(r, Len(n)).
    c) The random number R is then used to generate K using the key derivation function KDF1 defined in ISO/IEC 18033-2 with SHA-256 as the hash function: K= KDF1 (R, 48).
    d) Split K from step c into two keys K = (BEK || BMK), where the 16 most significant bytes of K are the Biometric Encryption Key BEK used to encrypt the biometric data, and the 32 least significant bytes of K are the Biometric MAC Key BMK used to generate the MAC in step g.
    e) The random number R shall be enciphered using the RSA Transform algorithm as defined in ISO/IEC 18033-2: C = RSATransform (R, e, n). The result is the Enciphered Biometric Key Seed.
    f) Encrypt the data specified in Table 25a using the DEM1 mechanism as defined in ISO/IEC 18033-2, with the Biometric Encryption Key BEK generated in step d, in order to generate the Enciphered Biometric Data.
    The symmetric cipher (SC) used in the DEM1 mechanism shall be the SC1 defined in ISO/IEC 18033-2 with the block cipher being the AES-128 defined in ISO/IEC 18033-3.
    g) Use the Biometric MAC Key BMK generated in step d to generate an 8-byte MAC on the Enciphered Biometric Data according to the DEM1 mechanism as defined in ISO/IEC 18033-2.

The MAC algorithm used in the DEM1 mechanism shall be HMAC, as defined in ISO/IEC 9797-2 using SHA-256 as the hash function. Note that the label L defined in DEM1 shall be null, and thus according to DEM1 the HMAC is computed over the Enciphered Biometric Data appended with 8 zero bytes.

Field Name	**Length**	**Description**	**Format**
ICC Unpredictable Number	8	Unpredictable number obtained from the ICC with the GET CHALLENGE command	b
Biometric Solution ID Length	1	Length of Biometric Solution ID	b
Biometric Solution ID	value of Biometric Solution ID Length	As defined in Book 3 Table 43a	b
Biometric Type Length	1	Length of Biometric Type data element	b
Biometric Type	value of Biometric Type Length	As defined in Book 3 Table 43b	b
Biometric Subtype	1	As defined in Book 3 Table 43c	b
Biometric Data Block (BDB) Length	2	Length of BDB data element	b
Biometric Data Block (BDB)	value of BDB Length	A block of data with a specific format that contains information captured from a biometric capture device	b

Table 25a: Data to be enciphered for Biometric Encipherment

Note: The length bytes in Table 25a are simple binary bytes, and are *not* coded as BER-TLV length fields.

4. The terminal shall construct the Biometric Verification Data Template, and order the data elements as indicated in Table 25b.
    a) The value of Biometric Type is set as the plaintext value referenced in step 3-f
    b) The value of Biometric Solution ID is set as the plaintext value referenced in step 3-f
    c) The value of Enciphered Biometric Key Seed is set as the value generated in step 3-e
    d) The value of Enciphered Biometric Data is set as the value generated in step 3-f
    e) The value of MAC of Enciphered Biometric Data is set as the value generated in step 3-g.

Tag	**Length**	**Field Name**
'81'	var.	Biometric Type
'90'	var.	Biometric Solution ID
'DF50'	N_{PE} or N_{IC}	Enciphered Biometric Key Seed
'DF51'	var.	Enciphered Biometric Data
'DF52'	8	MAC of Enciphered Biometric Data

Table 25b: Biometric Verification Data Template

Note: The data objects in Table 25b are BER-TLV coded. The length of all TLV coded data objects are coded on the minimum number of bytes (that is, on 1 byte if < 128, on 2 bytes if in the range 128 to 255, and so on). See Book 3 Annex B.2 for BER-TLV coding rules. There shall be no '00' padding bytes before, between, or after the BER-TLV coded data objects."

5. The terminal shall construct and issue VERIFY command(s) as following:
   a) If the length of the value field of the Biometric Verification Data Template is no more than 255 bytes, the terminal shall set the value field of the Biometric Verification Data Template as the data field of the single VERIFY command.
   b) If the length of the value field of the Biometric Verification Data Template is more than 255 bytes, the terminal shall divide the value field of the Biometric Verification Data Template into 255 byte data blocks. The last data block may be 1 to 255 bytes in length. Then the terminal shall set these data blocks as the data fields of the commands and chain the commands using command chaining defined in Book 3 Section 6.5.13.
   c) The terminal shall issue the VERIFY command(s).

6. With the ICC Private key, the ICC decrypts the Enciphered Biometric Data in the following way:
   a) The private key owned by the ICC has exponent d and modulus n.
   b) The ICC decrypts the Enciphered Biometric Key Seed using the RSA Transform algorithm as defined in ISO/IEC 18033-2: R = RSATransform (C, d, n), where C is Enciphered Biometric Key Seed (tag 'DF50').
   c) The ICC generates two keys using the key derivation function KDF1 as defined in ISO/IEC 18033-2 with SHA-256 as the hash function: K = KDF1 (R, 48). The 16 most significant bytes of K is the Biometric Encryption Key BEK and the 32 least significant bytes of K is the Biometric MAC Key BMK.
   d) The ICC uses the BMK generated in step c to generate an 8-byte MAC on the Enciphered Biometric Data according to the DEM1 mechanism as defined in ISO/IEC 18033-2.
      The MAC algorithm used in the DEM1 mechanism shall be HMAC, as defined in ISO/IEC 9797-2 using SHA-256 as the hash function. Note that the label L defined in DEM1 shall be null, and thus according to DEM1 the HMAC is computed over the Enciphered Biometric Data appended with 8 zero bytes.
      If the generated MAC is not equal to the MAC of Enciphered Biometric Data (tag 'DF52') included in the Biometric Verification Data Template, Offline Biometric CVM has failed.
   e) The ICC decrypts the Enciphered Biometric Data using the DEM1 mechanism as defined in ISO/IEC 18033-2, with the Biometric Encryption Key BEK generated in step c.
      The symmetric cipher (SC) used in the DEM1 mechanism shall be the SC1 defined in ISO/IEC 18033-2 with the block cipher being the AES-128 defined in ISO/IEC 18033-3.

7. The ICC verifies whether the ICC Unpredictable Number recovered in step 6-e is equal to the ICC Unpredictable Number generated by the ICC with the GET CHALLENGE command. If they are not the same, Offline Biometric CVM has failed.

8. The ICC verifies whether the Biometric Solution ID recovered in step 6-e is equal to the Biometric Solution ID (tag '90') included in the Biometric Verification Data Template. If they are not the same, Offline Biometric CVM has failed.

9. The ICC verifies whether the Biometric Type recovered in step 6-e is equal to the Biometric Type (tag '81') included in the Biometric Verification Data Template. If they are not the same, Offline Biometric CVM has failed.

The ordering of steps 1 and 2 is representative, not mandatory. Key retrieval as described in Section 7.1 and steps 1 and 2 can be conducted in any order, provided they are all completed before the terminal applies the RSA-KEM algorithm (as described in step 3).

EMV Book 3

In Section 2 Normative References, add the following reference after the reference for ISO/IEC 7816-6:

ISO/IEC 7816-11	Identification cards – Integrated circuit cards – Personal verification through biometric methods

Add the following references as the new last three rows:

ISO/IEC 19785-3	Information technology – Common Biometric Exchange Formats Framework – Patron format specifications
ISO/IEC 19794	Information technology – Biometric data interchange formats
ISO/IEC 19794-2	Information technology – Biometric data interchange formats – Part 2: Finger minutiae data

In Section 3 Definitions, add the following terms:

Biometric Data Block — A block of data with a specific format that contains information captured from a biometric capture device and that could be used as follows:

- stored in the card as part of the biometric reference template
- sent to the ICC in the data field of the PIN CHANGE/UNBLOCK command
- sent to the ICC in the data field of the VERIFY command for offline biometric verification
- sent online for verification

The format of the BDB is outside the scope of this specification.

biometric reference template — Biometric data stored in the card as reference. Data provided by a biometric capture device would be compared against the biometric reference template to determine a match.

biometric verification — The process of determining that the biometrics presented, such as finger, palm, iris, voice or facial, are valid.

command chaining — A mechanism where consecutive command-response pairs can be chained.

facial verification — The process of determining that the face presented is valid.

finger verification — The process of determining that the finger presented is valid.

iris verification — The process of determining that the iris presented is valid.

palm verification — The process of determining that the palm presented is valid.

voice verification — The process of determining that the voice presented is valid.

In Section 4.1 Abbreviations, add the following entries:

BDB	Biometric Data Block
BEK	Biometric Encryption Key
BHT	Biometric Header Template
BIT	Biometric Information Template
BMK	Biometric MAC Key
CBEFF	Common Biometric Exchange Formats Framework
CCYYMMDD	Year (4 digits), Month, Day
SHA-256	Secure Hash Algorithm 256

In Section 4.2 Notations, add the following notation:

MIN (x, y)	The smaller of values x and y.

In Section 6.3.5 Coding of the Status Bytes, add the following entries to Table 4, after "Checking errors":

'68'	'00'	Command chaining failed
'68'	'83'	Last command of chain was expected but not received
'68'	'84'	Command chaining not supported

Add the following entries to Table 5:

'68'	'00'													X
'68'	'83'													X
'68'	'84'													X

Update Section 6.5.7 GET DATA Command-Response APDUs as shown below:

6.5.7 GET DATA Command-Response APDUs

6.5.7.1 Definition and Scope

The GET DATA command is used to retrieve a primitive or constructed data object not encapsulated in a record within the current application.

The usage of the GET DATA command in this specification is limited to the retrieval of the following primitive or constructed data objects that are defined in Annex A and interpreted by the application in the ICC:

- ATC (tag '9F36')
- Last Online ATC Register (tag '9F13')
- PIN Try Counter (tag '9F17')
- Log Format (tag '9F4F')
- Biometric Try Counters Template ('BF4C')
- Preferred Attempts Template ('BF4D')

6.5.7.2 Command Message

The GET DATA command message is coded as shown in Table 16:

Code	Value
CLA	'80'
INS	'CA'
P1 P2	'9F36', '9F13', '9F17', '9F4F', 'BF4C' and 'BF4D'
Lc	Not present
Data	Not present
Le	'00'

Table 16: GET DATA Command Message

6.5.7.3 Data Field Sent in the Command Message

The data field of the command message is not present.

6.5.7.4 Data Field Returned in the Response Message

The data field of the response message contains the primitive or constructed data object referred to in P1 P2 of the command message (in other words, including its tag and its length).

6.5.7.5 Processing State Returned in the Response Message

'9000' indicates a successful execution of the command.

Update Section 6.5.10 PIN CHANGE/UNBLOCK Command-Response APDUs as shown below:

6.5.10 PIN CHANGE/UNBLOCK Command-Response APDUs

6.5.10.1 Definition and Scope

The PIN CHANGE/UNBLOCK command is a post-issuance command. Its purpose is to provide the issuer the capability either to unblock the PIN or to simultaneously change and unblock the reference PIN. It also provides the issuer the capability either to unblock the specified Biometric Type, or to simultaneously update the specified biometric reference template and unblock the associated Biometric Type, or to store the biometric reference templates in the card during enrollment.

If the PIN CHANGE/UNBLOCK command is used either to unblock the PIN or to simultaneously change and unblock the reference PIN, upon successful completion of the PIN CHANGE/UNBLOCK command, the card shall perform the following functions:

- The value of the PIN Try Counter shall be reset to the value of the PIN Try Limit.
- If requested, the value of the reference PIN shall be set to the new PIN value.

If PIN data is transmitted in the command it shall be enciphered for confidentiality.

Note: The reference PIN, which is stored within the card, is the one that is associated with the application and which the card uses to check the Transaction PIN Data transmitted within the VERIFY command.

If the PIN CHANGE/UNBLOCK command is used either to unblock the specified Biometric Type, or to simultaneously enroll or update the specified biometric reference template and unblock the associated Biometric Type, then upon successful completion of the command the card shall perform the following functions:

- In order to unblock the Biometric Type, the value of the Biometric (Facial, Finger, Iris, Palm, or Voice) Try Counter for the Biometric Type being updated shall be reset to the value of the associated Biometric (Facial, Finger, Iris, Palm, or Voice) Try Limit.

- If requested, the biometric reference templates in the card shall be set to or replaced by the new template in the Biometric Data Block (BDB), received in the PIN CHANGE/UNBLOCK command.

The BDB transmitted in the PIN CHANGE/UNBLOCK command shall be enciphered for confidentiality.

Due to the large size of the BDB, multiple PIN CHANGE/UNBLOCK commands are typically required, as described in Section 6.5.13.

Note: The biometric reference template, which is stored within the card, is the one that is associated with the application and which the card uses to check the template captured by the biometric capture device and transmitted within the VERIFY command.

6.5.10.2 Command Message

The PIN CHANGE/UNBLOCK command message is coded as shown in Table 19:

Code	Value
CLA	'8C','84', '9C' or '94'; coding according to the secure messaging specified in Book 2 and command chaining specified in Section 6.5.13
INS	'24'
P1	'00'
P2	'00', '01', '02', '03', '04'
Lc	Number of data bytes
Data	If P2 = '00', then the data field contains the MAC data component coded according to the secure messaging specified in Book 2. If P2 = '03', then the data field contains the Biometric Type, as shown in Table 43b, and the MAC data component coded according to the secure messaging specified in Book 2. The P2 values '01', '02', and '04' are reserved for the payment systems, but the data field should contain one of the following: • Enciphered PIN data component, if present, and MAC data component; coding according to the secure messaging specified in Book 2 • The following enciphered biometric data: o Biometric Type, as shown in Table 43b o Biometric Subtype, as shown in Table 43c o Biometric Solution ID, as shown in Table 43a o Biometric Data Block (BDB) followed by the MAC data component coded according to the secure messaging specified in Book 2. If the length of the enciphered biometric data plus MAC is greater than 255 bytes, then the data should be sent to the card over several PIN CHANGE/UNBLOCK commands. The data encipherment and MACing should be applied to each command.
Le	Not present

Table 19: PIN CHANGE/UNBLOCK Command Message

P2: If P2 is equal to '00', the reference PIN is unblocked and the PIN Try Counter is reset to the PIN Try Limit. There is no PIN update, since the PIN CHANGE/UNBLOCK command does not contain a new PIN value.

If P2 is equal to '03', the try counter associated with the Biometric Type specified in the data field of the command is reset to the try limit of the specified Biometric Type. There is no biometric update, since the PIN CHANGE/UNBLOCK command does not contain a new BDB.

The usage of P2 equal to '01', '02', '04' is reserved for payment systems.

Any other value of P2 allowing PIN/Biometric Type unblocking and/or PIN/biometric reference template changing is out of the scope of this specification and shall be described for each payment system individually.

6.5.10.3 Data Field Sent in the Command Message

The data field of the command message contains one of the following:

- The PIN data component, if present, followed by the MAC data component coded according to the secure messaging format specified in Book 2.

- The Biometric Type, Biometric Subtype, Biometric Solution ID and BDB followed by the MAC data component coded according to the secure messaging format specified in Book 2.

- The Biometric Type followed by the MAC data component coded according to the secure messaging format specified in Book 2.

6.5.10.4 Data Field Returned in the Response Message

No data field is returned in the response message.

6.5.10.5 Processing State Returned in the Response Message

'9000' indicates a successful execution of the command.

Update Section 6.5.12 VERIFY Command-Response APDUs as shown below:

6.5.12 VERIFY Command-Response APDUs

6.5.12.1 Definition and Scope

If the CVM chosen from the CVM List is an offline PIN, as described in section 10.5, the VERIFY command initiates in the ICC the comparison of the Transaction PIN Data sent in the data field of the command with the reference PIN data associated with the application. The manner in which the comparison is performed is proprietary to the application in the ICC.

If the CVM chosen from the CVM List is any of the offline biometric verification methods, the VERIFY command initiates in the ICC the comparison of the biometric template captured by the biometric capture device and sent in the data field of the command with the biometric reference template(s) associated with the application. The manner in which the comparison is performed is proprietary to the application in the ICC.

The biometric data to be sent in the VERIFY command shall be enciphered for confidentiality, as described in Book 2 Section 7.3.

Due to the large size of the biometric data to be sent in the VERIFY command, command chaining is typically required, as described in Book 3 Section 6.5.13.

6.5.12.2 Command Message

The VERIFY command message is coded as shown in Table 22:

Code	Value
CLA	'00' or '10'; coding according to the command chaining specified in Book 3 Section 6.5.13
INS	'20'
P1	'00'
P2	Qualifier of the reference data (see Table 23)
Lc	Var.

Data	Transaction PIN Data or Biometric Verification Data Template
Le	Not present

Table 22: VERIFY Command Message

Table 23 defines the qualifier of the reference data (P2):

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	As defined in ISO/IEC 7816-4
1	0	0	0	0	0	0	0	Plaintext PIN, format as defined below
1	0	0	0	0	x	x	x	RFU for this specification
1	0	0	0	1	0	0	0	Enciphered PIN, format as defined in Book 2
1	0	0	0	1	0	0	1	Enciphered Biometric
1	0	0	0	1	0	1	x	RFU for this specification
1	0	0	0	1	1	x	x	RFU for the individual payment systems
1	0	0	1	x	x	x	x	RFU for the issuer

Table 23: VERIFY Command qualifier of reference data (P2)

The processing of the VERIFY command in the ICC will be defined in combination with the CVM rules as specified in section 10.5.
The plaintext offline PIN block shall be formatted as follows:

C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

where:

	Name	Value
C	Control field	4 bit binary number with value of 0010 (Hex '2')
N	PIN length	4 bit binary number with permissible values of 0100 to 1100 (Hex '4' to 'C')
P	PIN digit	4 bit binary number with permissible values of 0000 to 1001 (Hex '0' to '9')
P/F	PIN/filler	Determined by PIN length
F	Filler	4 bit binary number with a value of 1111 (Hex 'F')

Table 24: Plaintext Offline PIN Block Format

P2 = '00' indicates that no particular qualifier is used. The processing of the VERIFY command in the ICC should know how to find the PIN data unambiguously.

6.5.12.3 Data Field Sent in the Command Message

If the Transaction PIN Data is sent in the VERIFY command, then the data field of the command message contains the value field of tag '99' (Transaction PIN Data).

If offline biometric verification data is sent in the VERIFY command, then the data field of the command message contains the value field of tag 'BF4E' (Biometric Verification Data Template).

6.5.12.4 Data Field Returned in the Response Message

No data field is returned in the response message.

6.5.12.5 Processing State Returned in the Response Message

'9000' indicates a successful execution of the command.

If command chaining is required, when the VERIFY command has CLA = '10' and the SW1 SW2 ≠ '9000', the terminal shall discontinue sending the remainder of the chained VERIFY commands.

When the VERIFY command has CLA = '10' and command chaining fails, the ICC shall return SW1 SW2 = '6800' to indicate command chaining failed (due to a failure other than the specific error conditions described in 6.5.13).

For the VERIFY command with CLA = '00', when for the currently selected application the comparison between the Transaction PIN Data and the reference PIN data, or the comparison between the biometric template captured on the biometric capture device and contained in the command and the biometric reference template stored on the card, performed by the VERIFY command fails, the ICC shall return SW2 = 'Cx', where 'x' represents the number of retries still possible. When the card returns 'C0', no more retries are left, and the CVM shall be blocked. Any subsequent VERIFY command applied in the context of that application shall then fail with SW1 SW2 = '6983'.

After Section 6.5.12 VERIFY Command-Response APDUs, add the following new section:

6.5.13 Command Chaining

When more than one command is required to perform a function, multiple VERIFY or PIN CHANGE/UNBLOCK commands need to be sent to the card, in which case the consecutive command-response pairs can be chained. As defined in ISO/IEC 7816-4, bit 5 of the class byte CLA of the command is used to indicate command chaining, as shown in Table 24a.

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	x	-	-	-	-	Command chaining control
-	-	-	0	-	-	-	-	– The command is the last or only command of a chain
-	-	-	1	-	-	-	-	– The command is not the last command of a chain

Table 24a: Values of CLA in command chaining

As defined in ISO/IEC 7816-4, in response to a command that is not the last command of a chain, SW1 SW2 is set to '9000', meaning that the process has been completed so far. Moreover, the following specific error conditions may occur.

- If SW1 SW2 is set to '6883', then the last command of the chain was expected but was not received.
- If SW1 SW2 is set to '6884', then command chaining is not supported.

Update Section 10.5 Cardholder Verification as shown below:

10.5 Cardholder Verification

Purpose:

Cardholder verification is performed to ensure that the person presenting the ICC is the person to whom the application in the card was issued.

Conditions of Execution:

Ability of the ICC to support at least one cardholder verification method is indicated in the Application Interchange Profile, as shown in Annex C1. If this bit is set to 1, the terminal shall use the cardholder verification related data in the ICC to determine whether one of the issuer-specified cardholder verification methods (CVMs) shall be executed. This process is described below.

Sequence of Execution:

This function may be performed any time after Read Application Data and before completion of the terminal action analysis.
Description:

The CVM List (tag '8E') is a composite data object consisting of the following:

1. An amount field (4 bytes, binary format), referred to as 'X' in Table 40: CVM Condition Codes. 'X' is expressed in the Application Currency Code with implicit decimal point. For example, 123 (hexadecimal '7B') represents £1.23 when the currency code is '826'.

2. A second amount field (4 bytes, binary format), referred to as 'Y' in Table 40. 'Y' is expressed in Application Currency Code with implicit decimal point. For example, 123 (hexadecimal '7B') represents £1.23 when the currency code is '826'.

3. A variable-length list of two-byte data elements called Cardholder Verification Rules (CV Rules). Each CV Rule describes a CVM and the conditions under which that CVM should be applied (see Annex C3).

If the CVM List is not present in the ICC, the terminal shall terminate cardholder verification without setting the 'Cardholder verification was performed' bit in the TSI.

Note: A CVM List with no Cardholder Verification Rules is considered to be the same as a CVM List not being present.

If the CVM List is present in the ICC, the terminal shall process each rule in the order in which it appears in the list according to the following specifications. Cardholder verification is completed when any one CVM is successfully performed or when the list is exhausted.

If the terminal encounters formatting errors in the CVM List such as a list with an odd number of bytes (that is, with an incomplete CVM Rule), the terminal shall terminate the transaction as specified in Book 3 section 7.5.

If any of the following is true:

- the conditions expressed in the second byte of a CV Rule are not satisfied, or

- data required by the condition (for example, the Application Currency Code or Amount, Authorised) is not present, or

- the CVM Condition Code is outside the range of codes understood by the terminal (which might occur if the terminal application program is at a different version level than the ICC application),

then the terminal shall bypass the rule and proceed to the next. If there are no more CV Rules in the list, cardholder verification has not been successful, and the terminal shall set the 'Cardholder verification was not successful' bit in the TVR to 1.

If the conditions expressed in the second byte of the CV Rule are satisfied, the terminal next checks whether it recognises the CVM coded in the first byte of the CV Rule and proceeds according to the following steps:

1. If the CVM is recognised, the terminal next checks to determine whether it supports the CVM.
   - If the CVM is supported, the terminal shall attempt to perform it.

        - If the CVM is performed successfully, cardholder verification is complete and successful. If the CVM just processed was ‘Fail CVM Processing’, the terminal shall set the ‘Cardholder verification was not successful’ bit in the TVR (b8 of byte 3) to 1 and no further CVMs shall be processed regardless of the setting of b7 of byte 1 in the first byte of the CV Rule.
        - If the CVM is not performed successfully, processing continues at step 2.
    - If the CVM is not supported, processing continues at step 2. In addition, the terminal shall perform the following:
        - Set the ‘PIN entry required and PIN pad not present or not working’ bit (b5 of byte 3) of the TVR to 1 for the following cases:
            - The CVM was online PIN and online PIN was not supported
            - The CVM included any form of offline PIN, and neither form of offline PIN was supported.
        - Set the ‘A selected Biometric Type not supported’ bit (b2 of byte 4) of the TVR to 1 for the following case:
            - The CVM included any Biometric Type, and no common Biometric Type was supported.

    If the CVM is not recognised, the terminal shall set the ‘Unrecognised CVM’ bit in the TVR (b7 of byte 3) to 1 and processing continues at step 2.

2. If cardholder verification was not completed in step 1 (that is, the CVM was not recognised, was not supported, or failed), the terminal examines b7 of byte 1 of the CV Rule.
    - If b7 is set to 1, processing continues with the next CV Rule, if one is present.
    - If b7 is set to 0, or there are no more CV Rules in the list, cardholder verification is complete and unsuccessful. The terminal shall set the ‘Cardholder verification was not successful’ bit in the TVR (b8 of byte 3) to 1.

When cardholder verification is completed, the terminal shall:

- set the CVM Results according to Book 4 section 6.3.4.5
- set the ‘Cardholder verification was performed’ bit in the TSI to 1.

After Section 10.5.5 CVM Processing Logic, add the following new section:

10.5.6 Offline Biometric Verification Processing

This section applies to the verification by the ICC of an enciphered biometric template presented by the terminal. The offline biometric verification methods include offline facial, finger, iris, palm, and voice.

If any of the offline biometric verification methods is the selected CVM, offline biometric verification processing may not be successfully performed for any of the following reasons:

- The terminal does not support the selected offline Biometric CVM. In this case, the terminal shall set the ‘A selected Biometric Type not supported’ bit in the TVR to 1.
- The terminal supports the selected offline Biometric CVM, but the biometric capture device is malfunctioning. In this case, the terminal shall set the ‘Biometric required but Biometric capture device not working’ bit in the TVR to 1.
- The terminal bypassed the selected offline Biometric Subtype entry at the direction of either the merchant or the cardholder. In this case, the terminal shall set the ‘Biometric required, Biometric capture device present, but Biometric Subtype entry was bypassed’ bit in the TVR to 1.
- The selected offline Biometric CVM is blocked upon initial use of the VERIFY command or if recovery of the Enciphered Biometric Data has failed (the ICC returns SW1 SW2 = '6983' or '6984'

in response to the final VERIFY command). In this case, the terminal shall set the ‘Biometric Try Limit exceeded’ bit in the TVR to 1.

- The number of remaining tries of the selected offline Biometric CVM is reduced to zero (indicated by an SW1 SW2 of '63C0' in the response to the final VERIFY command). In this case, the terminal shall set the ‘Biometric Try Limit exceeded’ bit in the TVR to 1.

- The terminal does not support the format specified in any of the Biometric Information Templates (BITs), as specified in Annex C7, retrieved from the card for the selected Biometric Type. In this case, the terminal shall set 'Biometric template format not supported' bit in the TVR to 1.

When the VERIFY command is chained, the SW1 SW2 in response to the final VERIFY command indicates the outcome of biometric verification processing. If SW1 SW2 = '6800', '6883' or '6884', the terminal shall consider this CVM unsuccessful and shall continue cardholder verification processing in accordance with the card’s CVM List.

The only case in which the selected offline biometric verification processing is considered successful is when the ICC returns an SW1 SW2 of '9000' in response to a single or all of multiple VERIFY command(s). In this case, the terminal shall set 'Biometric performed and successful' bit in the TVR to 1.

As shown in Figure 12a, the terminal shall determine if tag '87' and '88' (format owner and format type) of the BIT in the Card BIT Group Template, as specified in Annex C8, match tag '87' and '88' of any BIT in the Terminal BIT Group Template, as specified in Annex C8, using the following procedures:

- If the BIT in the Card BIT Group Template does not contain level 2 Biometric Header Template (BHT) 1 and BHT 2, as shown in Table 43a, and if the values of tag '87' and '88' of the BIT in the Card BIT Group Template are equal to the values of tag '87' and '88' (respectively) of any BIT in the Terminal BIT Group Template, the terminal shall determine that there is a match.

- If the BIT in the Card BIT Group Template contains level 2 BHT 1 and BHT 2, as shown in Table 43a, and if the values of tag '87' and '88' in the BHT 1 of the BIT in the Card BIT Group Template are equal to the values of tag '87' and '88' (respectively) of any BIT in the Terminal BIT Group Template, the terminal shall determine that there is a match.

- Otherwise, the terminal shall determine that there is no match.

Moreover, the terminal shall use the sequence of BITs in the Card BIT Group Template and the Preferred Attempts Template (tag 'BF4D') to determine which Biometric Subtype the terminal shall ask the user to present for verification.

As an example, if the Preferred Finger Attempts is configured as 3 and the Card BIT Group Template is configured as following:

- BIT 1 – right index finger
- BIT 2 – right middle finger

Then, if Finger is selected by the terminal as the CVM, the terminal shall ask the user to present the right index finger first since it is first in the list. If the verification of the right index finger fails after 3 tries and the Finger Try Counter is not zero, the terminal shall move to the next finger on the list and ask the user to present the right middle finger up to 3 tries. The process continues until either the ICC returns SW1 SW2 = '9000' or the Finger Try Counter is zero.

After Section 10.5.5 CVM Processing Logic, add the following new section:

10.5.7 Online Biometric Verification Processing

If online biometric verification is a required CVM as determined by the process described in Figure 8, the processing may not be successfully performed for any one of the following reasons:

- The terminal does not support the selected online Biometric CVM. In this case, the terminal shall set the 'A selected Biometric Type not supported' bit in the TVR to 1.

- The terminal supports the selected online Biometric CVM, but the biometric capture device is malfunctioning. In this case, the terminal shall set the 'Biometric required but Biometric capture device not working' bit in the TVR to 1.

- The terminal bypassed the selected online Biometric Subtype entry at the direction of either the merchant or the cardholder. In this case, the terminal shall set the 'Biometric required, Biometric capture device present, but Biometric Subtype entry was bypassed' bit in the TVR to 1.

- The terminal does not support the format specified in any of the BITs retrieved from the card for the selected Biometric Type. In this case, the terminal shall set 'Biometric template format not supported' bit in the TVR to 1.

If the online biometric verification is successfully captured, the terminal shall set the 'Online CVM captured' bit in the TVR to 1. In this case, cardholder verification is considered successful and complete.

Update Figure 8 CVM Processing (Part 1 of 5) as shown below:

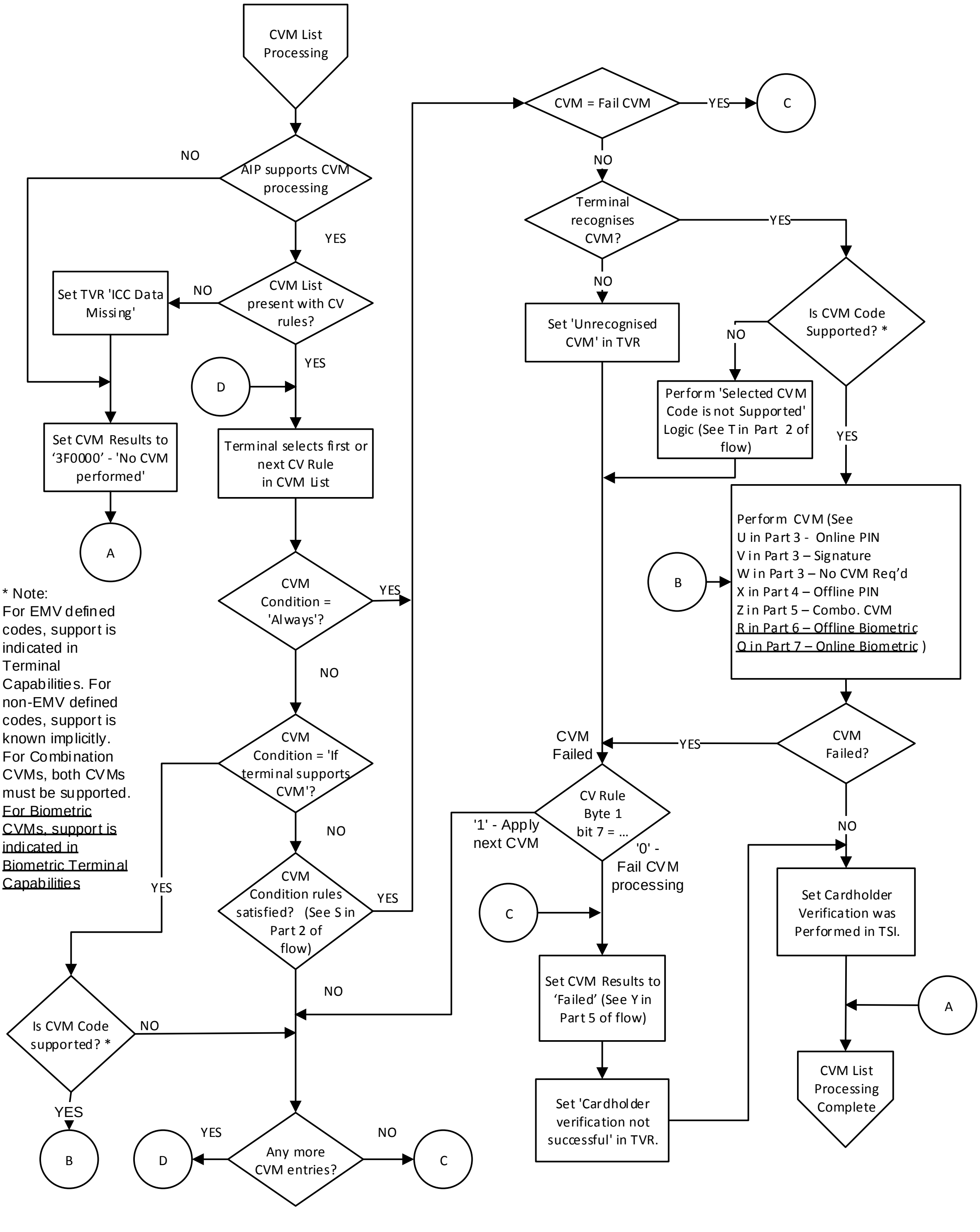

CVM List Processing
AIP supports CVM processing
NO
YES
CVM List present with CV rules?
NO
Set TVR 'ICC Data Missing'
YES
D
Set CVM Results to '3F0000' - 'No CVM performed'
A
Terminal selects first or next CV Rule in CVM List
* Note:
For EMV defined codes, support is indicated in Terminal Capabilities. For non-EMV defined codes, support is known implicitly. For Combination CVMs, both CVMs must be supported. For Biometric CVMs, support is indicated in Biometric Terminal Capabilities
CVM Condition = 'Always'?
YES
NO
CVM Condition = 'If terminal supports CVM'?
YES
NO
CVM Condition rules satisfied? (See S in Part 2 of flow)
YES
NO
Is CVM Code supported? *
NO
YES
B
D
YES
Any more CVM entries?
NO
C
CVM = Fail CVM
YES
C
NO
Terminal recognises CVM?
YES
NO
Set 'Unrecognised CVM' in TVR
Is CVM Code Supported? *
NO
Perform 'Selected CVM Code is not Supported' Logic (See T in Part 2 of flow)
YES
Perform CVM (See
U in Part 3 - Online PIN
V in Part 3 – Signature
W in Part 3 – No CVM Req'd
X in Part 4 – Offline PIN
Z in Part 5 – Combo. CVM
R in Part 6 – Offline Biometric
Q in Part 7 – Online Biometric)
B
CVM Failed?
YES
CVM Failed
NO
CV Rule Byte 1 bit 7 = …
'1' - Apply next CVM
'0' - Fail CVM processing
C
Set CVM Results to 'Failed' (See Y in Part 5 of flow)
Set 'Cardholder verification not successful' in TVR.
Set Cardholder Verification was Performed in TSI.
A
CVM List Processing Complete

Figure 8: CVM Processing (Part 1 of 7)

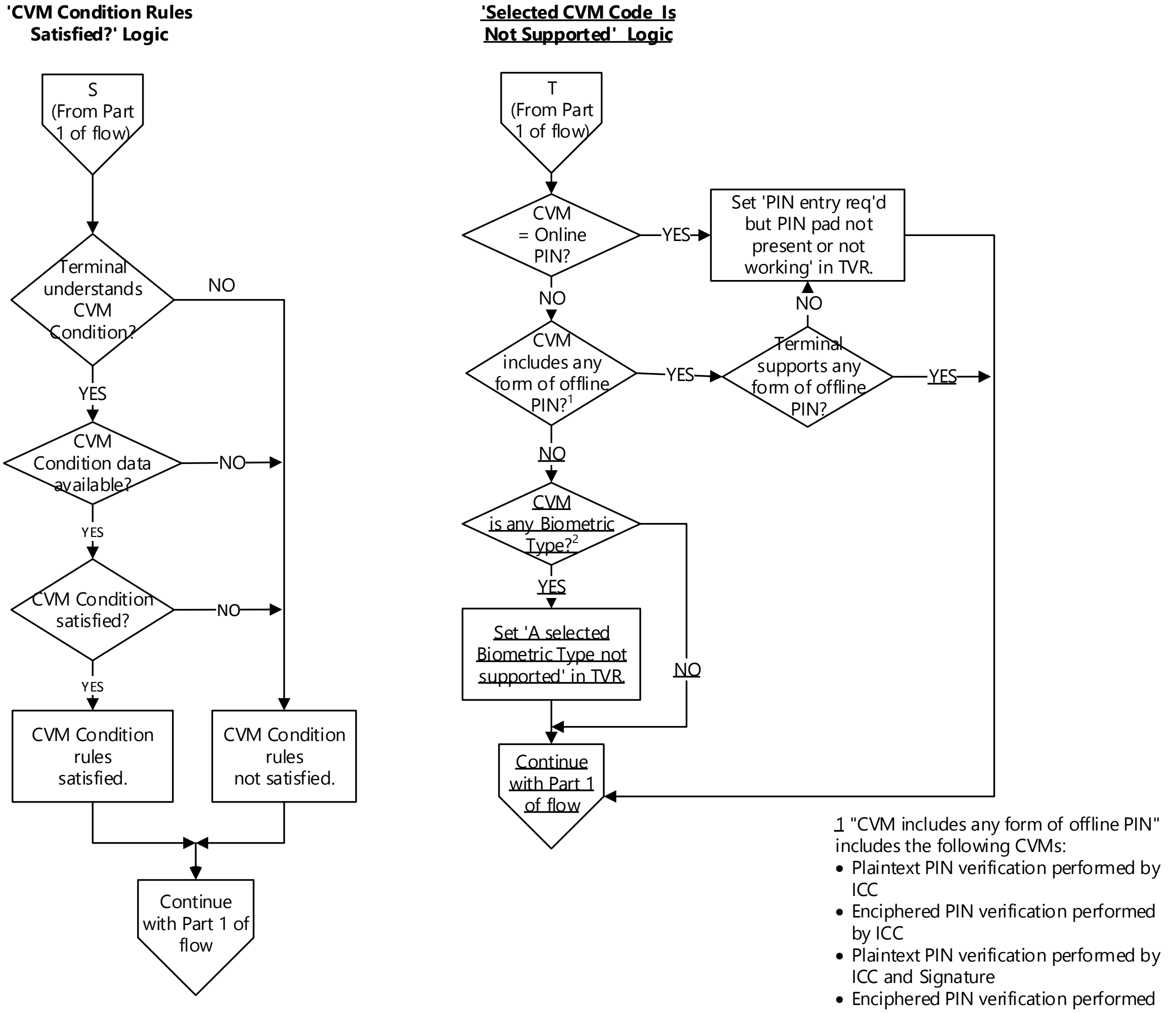
Add the following under Figure 8:

Note: When a biometric card is presented to a terminal without biometric support, the Biometric CVM Code is either not recognized or recognized but not supported by the terminal. As described in Book 3 Section 10.5, the terminal will process the next CVM if CVM Code Byte 1 bit 7 has the value 1b, or will complete cardholder verification, set CVM Results to 'Failed' and set 'Cardholder verification not successful' bit in TVR, if CVM Code Byte 1 bit 7 has the value 0b.

A terminal without biometric support may choose whether to recognize or not recognize the Biometric CVM Codes. If the terminal without biometric support chooses to recognize the Biometric CVM Codes, then the terminal shall implement the biometric cardholder verification processing in Book 3 Section 10.5 and shall treat biometric data objects as recognized data objects.

When a non-biometric card is presented to a terminal with biometric support, the terminal will not select a Biometric CVM Code, as described in Book 3 Section 10.5.

Update Figure 9 CVM Processing (Part 2 of 5) as shown below:


'CVM Condition Rules Satisfied?' Logic
S (From Part 1 of flow)
Terminal understands CVM Condition?
NO
YES
CVM Condition data available?
NO
YES
CVM Condition satisfied?
NO
YES
CVM Condition rules satisfied.
CVM Condition rules not satisfied.
Continue with Part 1 of flow
'Selected CVM Code Is Not Supported' Logic
T (From Part 1 of flow)
CVM = Online PIN?
YES
Set 'PIN entry req'd but PIN pad not present or not working' in TVR.
NO
NO
CVM includes any form of offline PIN?1
YES
Terminal supports any form of offline PIN?
YES
NO
CVM is any Biometric Type?2
YES
Set 'A selected Biometric Type not supported' in TVR.
NO
Continue with Part 1 of flow

[1] "CVM includes any form of offline PIN" includes the following CVMs:

- Plaintext PIN verification performed by ICC
- Enciphered PIN verification performed by ICC
- Plaintext PIN verification performed by ICC and Signature
- Enciphered PIN verification performed by ICC and Signature

[2] "CVM is any biometric type" includes the following CVMs:

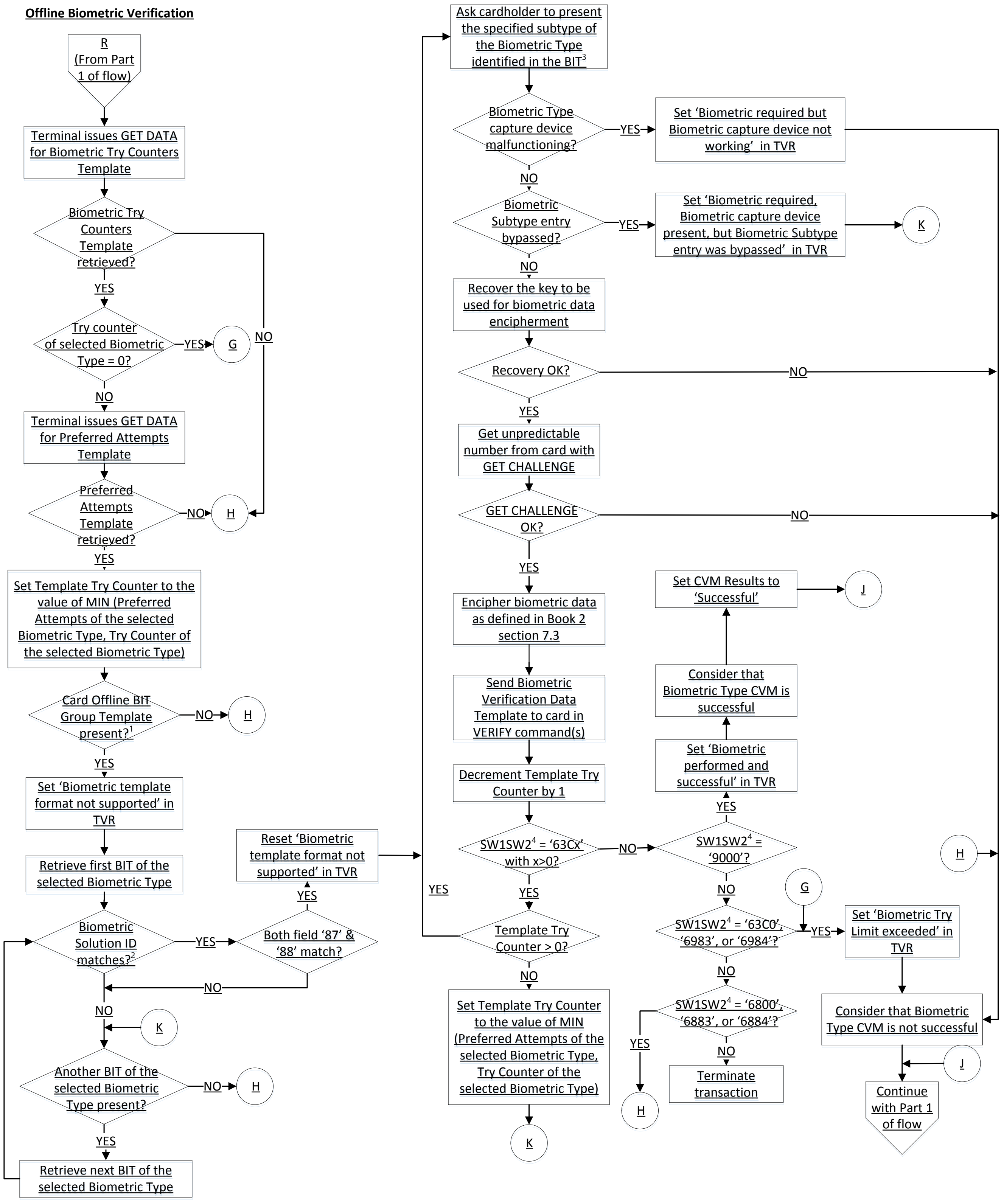
- Online or offline facial
- Online or offline finger
- Online or offline iris
- Online or offline palm
- Online or offline voice

Figure 9: CVM Processing (Part 2 of 7)

Update the titles of Figure 10, 11 and 12 as shown below:

Figure 10: CVM Processing (Part 3 of 7)
Figure 11: CVM Processing (Part 4 of 7)
Figure 12: CVM Processing (Part 5 of 7)

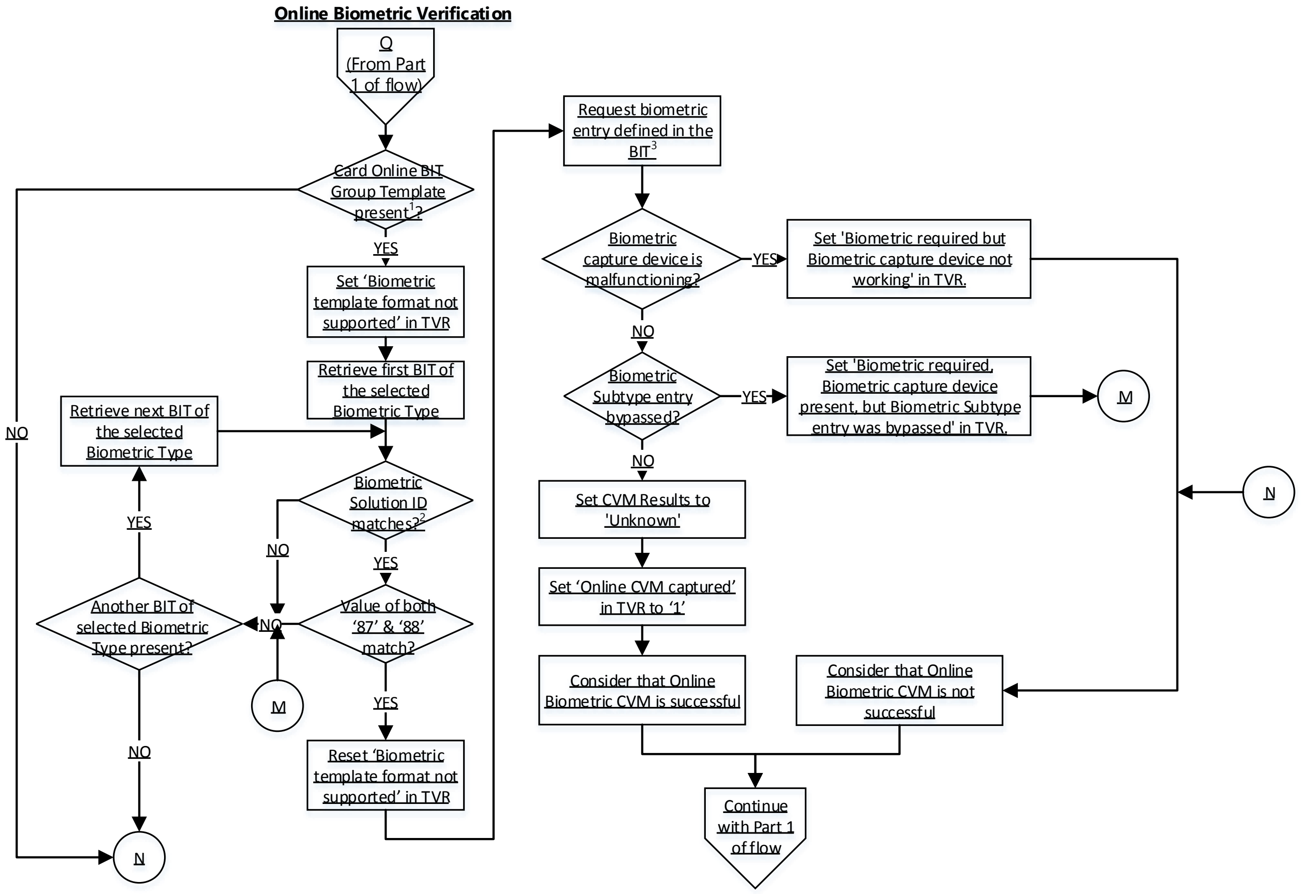
After Figure 12 CVM Processing (Part 5 of 5), add the following new figure:


Offline Biometric Verification
R (From Part 1 of flow)
Terminal issues GET DATA for Biometric Try Counters Template
Biometric Try Counters Template retrieved?
YES
NO
Try counter of selected Biometric Type = 0?
YES
G
NO
Terminal issues GET DATA for Preferred Attempts Template
Preferred Attempts Template retrieved?
NO
H
YES
Set Template Try Counter to the value of MIN (Preferred Attempts of the selected Biometric Type, Try Counter of the selected Biometric Type)
Card Offline BIT Group Template present?1
NO
H
YES
Set 'Biometric template format not supported' in TVR
Retrieve first BIT of the selected Biometric Type
Biometric Solution ID matches?2
YES
Both field '87' & '88' match?
YES
Reset 'Biometric template format not supported' in TVR
NO
NO
K
Another BIT of the selected Biometric Type present?
NO
H
YES
Retrieve next BIT of the selected Biometric Type
Ask cardholder to present the specified subtype of the Biometric Type identified in the BIT3
Biometric Type capture device malfunctioning?
YES
Set 'Biometric required but Biometric capture device not working' in TVR
NO
Biometric Subtype entry bypassed?
YES
Set 'Biometric required, Biometric capture device present, but Biometric Subtype entry was bypassed' in TVR
K
NO
Recover the key to be used for biometric data encipherment
Recovery OK?
NO
YES
Get unpredictable number from card with GET CHALLENGE
GET CHALLENGE OK?
NO
YES
Encipher biometric data as defined in Book 2 section 7.3
Send Biometric Verification Data Template to card in VERIFY command(s)
Decrement Template Try Counter by 1
SW1SW2^4 = '63Cx' with x>0?
NO
YES
YES
Template Try Counter > 0?
NO
Set Template Try Counter to the value of MIN (Preferred Attempts of the selected Biometric Type, Try Counter of the selected Biometric Type)
K
SW1SW2^4 = '9000'?
YES
Set 'Biometric performed and successful' in TVR
Consider that Biometric Type CVM is successful
Set CVM Results to 'Successful'
J
NO
G
SW1SW2^4 = '63C0', '6983', or '6984'?
YES
Set 'Biometric Try Limit exceeded' in TVR
NO
SW1SW2^4 = '6800', '6883', or '6884'?
YES
H
NO
Terminate transaction
H
Consider that Biometric Type CVM is not successful
J
Continue with Part 1 of flow

[1] The Offline BIT Group Template shall be present and contain at least one BIT.
[2] The terminal shall determine if the Biometric Solution ID of the BIT being processed equals to the Biometric Solution ID of any BIT in Terminal BIT Group Template.
[3] It is assumed that the biometric template is captured after the cardholder is advised on which Biometric Subtype is required, and the BDB is obtained from the Biometric Processing Application.
[4] The SW1 SW2 shall be in response to the final VERIFY command.

Figure 12a: CVM Processing (Part 6 of 7)

After Figure 12 CVM Processing (Part 5 of 5), add the following new figure:


Online Biometric Verification
Q (From Part 1 of flow)
Card Online BIT Group Template present¹?
YES
NO
Set 'Biometric template format not supported' in TVR
Retrieve first BIT of the selected Biometric Type
Retrieve next BIT of the selected Biometric Type
Biometric Solution ID matches?²
YES
NO
Value of both '87' & '88' match?
YES
NO
Another BIT of selected Biometric Type present?
YES
NO
M
N
Reset 'Biometric template format not supported' in TVR
Request biometric entry defined in the BIT³
Biometric capture device is malfunctioning?
YES
NO
Set 'Biometric required but Biometric capture device not working' in TVR.
Biometric Subtype entry bypassed?
YES
NO
Set 'Biometric required, Biometric capture device present, but Biometric Subtype entry was bypassed' in TVR.
M
N
Set CVM Results to 'Unknown'
Set 'Online CVM captured' in TVR to '1'
Consider that Online Biometric CVM is successful
Consider that Online Biometric CVM is not successful
Continue with Part 1 of flow

[1] The Online BIT Group Template shall present and contain at least one BIT.
[2] The terminal shall determine if the Biometric Solution ID of the BIT being processed equals to the Biometric Solution ID of any BIT in Terminal BIT Group Template.
[3] It is assumed that the biometric template is captured after the cardholder is advised on which Biometric Subtype is required, and the BDB is obtained from the Biometric Processing Application.

Figure 12b: CVM Processing (Part 7 of 7)

Add the following entries to Table 33 of Annex A1 Data Elements by Name:

A1 Data Elements by Name

Name	Description	Source	Format	Template	Tag	Length
Biometric Encryption Key (BEK)	An AES-128 key generated from the Biometric Key Seed, that is used to encrypt/decrypt the BDB constructed on the Biometric Processing Application	Terminal	b	—	—	16
Biometric MAC Key (BMK)	A key generated from the Biometric Key Seed, that is used to ensure the integrity of the BDB	Terminal	b	—	—	32
Biometric Key Seed	A random number generated by the terminal, that is used as the seed to generate the Biometric Encryption Key (BEK) and Biometric MAC Key (BMK)	Terminal	b	—	—	N_{PE} or N_{IC}
Biometric Header Template (BHT)	A template defined in ISO/IEC 19785-3, that is nested under the BIT.	Card, Terminal	b	'7F60'	'A1'	var.
Biometric Information Template (BIT)	A template defined in ISO/IEC 19785-3, that describes information regarding the biometric format and solution supported in a card.	Card	b	'BF4A', 'BF4B'	'7F60'	var.
Biometric Information Template (BIT)	A template defined in ISO/IEC 19785-3, that describes information regarding the biometric format and solution supported in a terminal.	Terminal	b	—	'7F60'	var.
Biometric Solution ID	A unique identifier assigned by EMVCo that is used to identify a biometric program, regional or global, supported by the card or terminal. The Biometric Solution ID is referred to within ISO/IEC 19785-3 as the "Index".	Terminal, Card	b	'A1' 'BF4E'	'90'	var.
Biometric Subtype	A data element defined in ISO/IEC 19785-3, that describes the subtype of the Biometric Type supported by the card or terminal, as shown in Table 43c.	Terminal, Card	b	'A1'	'82'	1
Biometric Terminal Capabilities	A data element that identifies the Biometric CVM capabilities of the terminal	Terminal	b	—	'9F30'	3

Name	Description	Source	Format	Template	Tag	Length
Biometric Try Counters Template	A template that contains one or more of the following Biometric Try Counters: • Facial Try Counter • Finger Try Counter • Iris Try Counter • Palm Try Counter • Voice Try Counter	Card	b	—	'BF4C'	var.
Biometric Type	A data element defined in ISO/IEC 19785-3, that describes the type of biometrics supported by the card or terminal among facial, finger, iris, palm and voice, as shown in Table 43b.	Terminal, Card	b	'A1' 'BF4E'	'81'	var.
Biometric Verification Data Template	A template that contains the TLV-coded values for the data to be included in the VERIFY command. The Biometric Verification Data Template contains Biometric Type ('81'), Biometric Solution ID ('90'), Enciphered Biometric Key Seed ('DF50'), Enciphered Biometric Data (tag 'DF51'), and MAC of Enciphered Biometric Data (tag 'DF52').	Terminal	b	—	'BF4E'	var.
Card BIT Group Template	A template in the card that contains one or more Biometric Information Templates (BITs)	Card	b	'70'	'9F31'	var.
Enciphered Biometric Data	The enciphered data sent in the VERIFY command	Terminal	b	'BF4E'	'DF51'	var.
Enciphered Biometric Key Seed	The Biometric Key Seed enciphered using the public key from the ICC	Terminal	b	'BF4E'	'DF50'	N_{PE} or N_{IC}
Facial Try Counter	Identifies the number of facial verification tries remaining	Card	b	'BF4C'	'DF50'	1
Finger Try Counter	Identifies the number of finger verification tries remaining	Card	b	'BF4C'	'DF51'	1
Iris Try Counter	Identifies the number of iris verification tries remaining	Card	b	'BF4C'	'DF52'	1
MAC of Enciphered Biometric Data	An HMAC generated on the Enciphered Biometric Data to ensure integrity	Terminal	b	'BF4E'	'DF52'	8

Name	Description	Source	Format	Template	Tag	Length
Offline BIT Group Template	A template, defined in ISO/IEC 7816-11, that is nested under the Card BIT Group Template, as shown in Table 43d, and contains one or more multiple Biometric Information Templates (BITs) for offline biometric verification supported by card	Card	b	'9F31'	'BF4A'	var.
Online BIT Group Template	A template, defined in ISO/IEC 7816-11, that is nested under the Card BIT Group Template, as shown in Table 43d, and contains one or more multiple Biometric Information Templates (BITs) for online biometric verification supported by card	Card	b	'9F31'	'BF4B'	var.
Palm Try Counter	Identifies the number of palm verification tries remaining	Card	b	'BF4C'	'DF53'	1
Preferred Attempts Template[4]	A template that contains the TLV-coded values for the preferred attempts of any BIT of a Biometric Type. It contains one or more of the following: • Preferred Facial Attempts • Preferred Finger Attempts • Preferred Iris Attempts • Preferred Palm Attempts • Preferred Voice Attempts	Card	b		'BF4D'	var.
Preferred Facial Attempts	Number of preferred attempts for any BIT of the facial Biometric Type stored in the card.	Card	b	'BF4D'	'DF50'	1
Preferred Finger Attempts	Number of preferred attempts for any BIT of the finger Biometric Type stored in the card.	Card	b	'BF4D'	'DF51'	1
Preferred Iris Attempts	Number of preferred attempts for any BIT of the iris Biometric Type stored in the card	Card	b	'BF4D'	'DF52'	1
Preferred Palm Attempts	Number of preferred attempts for any BIT of the palm Biometric Type stored in the card.	Card	b	'BF4D'	'DF53'	1
Preferred Voice Attempts	Number of preferred attempts for any BIT of the voice Biometric Type stored in the card.	Card	b	'BF4D'	'DF54'	1

[4] The preferred attempts for each Biometric Type are used to define how many attempts the issuer allows the terminal to verify using a single BIT. It is different from any biometric try limit used within the card to limit how many tries are allowed by the issuer for a Biometric Type.
For example, an issuer may set a finger try limit in the card (associated with the Finger Try Counter) to five, and set the Preferred Finger Attempts to three, allowing three attempts to verify the primary finger before two additional attempts are allowed using a secondary finger.

Name	Description	Source	Format	Template	Tag	Length
Template Try Counter	Identifies the number of biometric verification tries remaining for a specific BIT	Terminal	b	—	—	1
Terminal BIT Group Template	A template in the terminal, defined in ISO/IEC 7816-11, that contains one or more Biometric Information Templates (BITs)	Terminal	b	—	—	var.
Voice Try Counter	Identifies the number of voice verification tries remaining	Card	b	'BF4C'	'DF54'	1

Add the following entries to Table 34 of Annex A2 Data Elements by Tag:

Name	Template	Tag
Biometric Information Template (BIT), card	'BF4A' or 'BF4B'	'7F60'
Biometric Information Template (BIT), terminal	–	'7F60'
Biometric Type	'A1' or 'BF4E'	'81'
Biometric Subtype	'A1'	'82'
Biometric Solution ID	'A1' or 'BF4E'	'90'
Biometric Terminal Capabilities	–	'9F30'
Card BIT Group Template	'70'	'9F31'
Biometric Header Template (BHT)	'7F60'	'A1'
Offline BIT Group Template	'9F31'	'BF4A'
Online BIT Group Template	'9F31'	'BF4B'
Biometric Try Counters Template	–	'BF4C'
Preferred Attempts Template	–	'BF4D'
Biometric Verification Data Template	–	'BF4E'
Facial Try Counter	'BF4C'	'DF50'
Preferred Facial Attempts	'BF4D'	'DF50'
Enciphered Biometric Key Seed	'BF4E'	'DF50'
Finger Try Counter	'BF4C'	'DF51'
Preferred Finger Attempts	'BF4D'	'DF51'
Enciphered Biometric Data	'BF4E'	'DF51'
Iris Try Counter	'BF4C'	'DF52'
Preferred Iris Attempts	'BF4D'	'DF52'
MAC of Enciphered Biometric Data	'BF4E'	'DF52'
Palm Try Counter	'BF4C'	'DF53'
Preferred Palm Attempts	'BF4D'	'DF53'
Voice Try Counter	'BF4C'	'DF54'
Preferred Voice Attempts	'BF4D'	'DF54'

Update Table 39 CVM Codes as shown below:

CV Rule Byte 1 (Leftmost): Cardholder Verification Method (CVM) Codes

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0								RFU
	0							Fail cardholder verification if this CVM is unsuccessful
	1							Apply succeeding CV Rule if this CVM is unsuccessful
		0	0	0	0	0	0	Fail CVM processing
		0	0	0	0	0	1	Plaintext PIN verification performed by ICC
		0	0	0	0	1	0	Enciphered PIN verified online
		0	0	0	0	1	1	Plaintext PIN verification performed by ICC and signature
		0	0	0	1	0	0	Enciphered PIN verification performed by ICC
		0	0	0	1	0	1	Enciphered PIN verification performed by ICC and signature
		0	0	0	1	1	0	Facial biometric verified offline (by ICC)
		0	0	0	1	1	1	Facial biometric verified online
		0	0	1	0	0	0	Finger biometric verified offline (by ICC)
		0	0	1	0	0	1	Finger biometric verified online
		0	0	1	0	1	0	Palm biometric verified offline (by ICC)
		0	0	1	0	1	1	Palm biometric verified online
		0	0	1	1	0	0	Iris biometric verified offline (by ICC)
		0	0	1	1	0	1	Iris biometric verified online
		0	0	1	1	1	0	Voice biometric verified offline (by ICC)
		0	0	1	1	1	1	Voice biometric verified online
		0	x	x	x	x	x	Values in the range 010000-011101 reserved for future use by this specification
		0	1	1	1	1	0	Signature
		0	1	1	1	1	1	No CVM required
		1	0	1	x	x	x	Values in the range 100000-101111 reserved for use by the individual payment systems
		1	1	x	x	x	x	Values in the range 110000-111110 reserved for use by the issuer
		1	1	1	1	1	1	This value is not available for use

Table 39: CVM Codes

Update Table 42 Terminal Verification Results as shown below:

TVR Byte 1: (Leftmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Offline data authentication was not performed
x	1	x	x	x	x	x	x	SDA failed
x	x	1	x	x	x	x	x	ICC data missing
x	x	x	1	x	x	x	x	Card appears on terminal exception file
x	x	x	x	1	x	x	x	DDA failed
x	x	x	x	x	1	x	x	CDA failed
x	x	x	x	x	x	1	x	SDA Selected
x	x	x	x	x	x	x	0	RFU

TVR Byte 2:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	ICC and terminal have different application versions
x	1	x	x	x	x	x	x	Expired application
x	x	1	x	x	x	x	x	Application not yet effective
x	x	x	1	x	x	x	x	Requested service not allowed for card product
x	x	x	x	1	x	x	x	New card
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	1	x	Biometric performed and successful
x	x	x	x	x	x	x	1	Biometric template format not supported

TVR Byte 3:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Cardholder verification was not successful
x	1	x	x	x	x	x	x	Unrecognised CVM
x	x	1	x	x	x	x	x	PIN Try Limit exceeded
x	x	x	1	x	x	x	x	PIN entry required and PIN pad not present or not working
x	x	x	x	1	x	x	x	PIN entry required, PIN pad present, but PIN was not entered
x	x	x	x	x	1	x	x	Online CVM captured
x	x	x	x	x	x	1	x	Biometric required but Biometric capture device not working
x	x	x	x	x	x	x	1	Biometric required, Biometric capture device present, but Biometric Subtype entry was bypassed

Table 42: Terminal Verification Results

TVR Byte 4:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Transaction exceeds floor limit
x	1	x	x	x	x	x	x	Lower consecutive offline limit exceeded
x	x	1	x	x	x	x	x	Upper consecutive offline limit exceeded
x	x	x	1	x	x	x	x	Transaction selected randomly for online processing
x	x	x	x	1	x	x	x	Merchant forced transaction online
x	x	x	x	x	1	x	x	Biometric Try Limit exceeded
x	x	x	x	x	x	1	x	A selected Biometric Type not supported
x	x	x	x	x	x	x	0	RFU

Table 42: Terminal Verification Results, continued

TVR Byte 5 (Rightmost):

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Default TDOL used
x	1	x	x	x	x	x	x	Issuer authentication failed
x	x	1	x	x	x	x	x	Script processing failed before final GENERATE AC
x	x	x	1	x	x	x	x	Script processing failed after final GENERATE AC
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Table 42: Terminal Verification Results, continued

After Annex C6 Transaction Status Information, add the following two new annexes:

C7 Biometric Information Template (BIT)

The BIT provides descriptive information regarding the biometric formats and solutions supported in a card or in a terminal.

The format of the BIT is defined in ISO/IEC 19785-3 with TLV-encoded patron format, as shown in Table 43a.

The Biometric Solution ID is present to ensure that a biometric card certified by a program will only perform biometric verification on the terminal that is certified by the same program, and a terminal certified by a program will only perform biometric CVM on the biometric card that is certified by the same program. The terminals and cards certified by the same program shall contain the same Biometric Solution ID. Such program can be global or regional.

If the Biometric Subtype is not applicable to a Biometric Type or biometric solution, the Biometric Subtype shall be set to all binary zeros.

The biometric reference template stored in the card may consist of a template that is completely in standardized format, completely in proprietary format, or a combination of partially standardized format and partially proprietary format. If the template is partially in standardized format and partially in proprietary format, then the level 2 Biometric Header Template (BHT) 1 and BHT 2, as shown in Table

43a, shall be present within the BIT in the card; otherwise the level 2 BHT 1 and BHT 2 shall not be present within the BIT in the card.

If the BIT in the Card BIT Group Template contains level 2 BHT 1 and BHT 2, the terminal compares the terminal BIT tags '87' and '88' against the level 2 BHT 1 tags '87' and '88'.

Note that if the level 2 BHT 2 on the card is needed for complementary matching by the terminal, then this is based on proprietary data. This proprietary data may be stored in the terminal in a proprietary way, but it is not stored in the terminal template. Ideally, BHT 2 should be used to prioritize different solutions, and not to determine whether there is a match or not. However, this is proprietary.

The BIT in a terminal shall not contain the level 2 BHT 1 ~~and~~ nor BHT 2. A single BIT in the terminal presents only one format owner and one format type.

Tag	**L**	**Value**			**Presence**
'A1'	Var.	Biometric Header Template (BHT) in compliance with CBEFF. The contents within this template are TLV-encoded and may appear in any order within the template.			Mandatory
		Tag	L	Value	
		'80'	2	Patron header version (default '0101')	Mandatory
		'90'	Var.	Biometric Solution ID, a unique identifier used for referencing this biometric data set in an application context outside the card	Mandatory
		'81'	1-3	Biometric Type, as shown in Table 43b	Mandatory
		'82'	1	Biometric Subtype, as shown in Table 43c	Mandatory
		'83'	7	Creation date and time of the reference template (CCYYMMDDhhmmss)	Optional
		'84'	Var.	Creator	Optional
		'85'	8	Validity period (from CCYYMMDD, to CCYYMMDD)	Optional
		'86'	2	Identifier of product (PID) that created the reference template, value assigned by IBIA, see www.ibia.org	Optional
		'91'or 'B1'	Var.	Biometric matching algorithm parameters	Conditional Only present if it is in the Card BIT Group Template and required by the standard or the specification which defines the format of the BDB[5]

[5] For example, if the format of BDB is compliant with ISO/IEC 19794-2, the biometric matching algorithm parameters, including the maximum number of minutiae and the minutiae ordering scheme, shall be present as defined in ISO/IEC 19794-2.

Tag	L	Value					Presence
		'87'	2	Format owner, value assigned by IBIA, see www.ibia.org			Conditional Only present if the template contains no level 2 BHT 1 and BHT 2
		'88'	2	Format type, specified by format owner			Conditional Only present if the template contains no level 2 BHT 1 and BHT 2
		'A1'	Var.	BHT 1 (level 2). The contents within this template are TLV-encoded and may appear in any order within the template.			Optional
				Tag	L	Value	
				'87'	2	Format owner, e.g. format owner identifier of ISO/IEC JTC1/SC37	Mandatory
				'88'	2	Format type, specified by format owner	Mandatory
		'A2'	Var.	BHT 2 (level 2). The contents within this template are TLV-encoded and may appear in any order within the template.			Optional
				Tag	L	Value	
				'87'	2	Format owner, e.g. a card manufacturer	Mandatory
				'88'	2	Format type, specified by format owner	Mandatory

Table 43a: Biometric Information Template (BIT)

Note: The data object tags used within the Biometric Header Template (tag 'A1') only have the specified meaning within template 'A1'. For example, tag '90' is the Biometric Solution ID only within template 'A1', and tag '90' is the Issuer Public Key Certificate outside of template 'A1'.

Name of Biometric Type	Value
Facial	'02'
Finger[6]	'08'
Iris	'10'
Palm	'020000'
Voice	'04'

Table 43b: Biometric Type

[6] The Biometric Type "Finger" is used for both fingerprint and finger vein. The Format Type (tag '88') contained in BIT (tag '7F60') then identifies whether it represents fingerprint or finger vein.

b8	b7	b6	b5	b4	b3	b2	b1	Biometric Subtype
0	0	0	0	0	0	0	0	No information given
x	x	1	x	x	x	0	1	Right
x	x	1	x	x	x	1	0	Left
x	0	1	0	0	0	x	x	No meaning
x	0	1	0	0	1	x	x	Thumb
x	0	1	0	1	0	x	x	Index finger
x	0	1	0	1	1	x	x	Middle finger
x	0	1	1	0	0	x	x	Ring finger
x	0	1	1	0	1	x	x	Little finger
x	1	1	0	0	1	x	x	Palm
x	1	1	0	1	0	x	x	Back of hand
x	1	1	0	1	1	x	x	Wrist
All other values								RFU

Table 43c: Biometric Subtype

C8 BIT Group Template

The BIT Group Template contains one or more BITs. There are two BIT Group Templates defined in this specification: Card BIT Group Template and Terminal BIT Group Template.

The Card BIT Group Template is provided by the card in records that are read by the terminal using the READ RECORD command prior to a biometric verification process.

The sequence of BITs in a Card BIT Group Template identifies the sequence in which different Biometric Subtypes shall be requested for verification.

The Terminal BIT Group Template contains one or more BITs, which are used to identify matching BITs supported by both the card and terminal.

The Card BIT Group Template is structured as shown in Table 43d, and the Terminal BIT Group Template is structured as shown in Table 43e.

Tag	L	Value				
'9F31'	var.	Card BIT Group Template				
		Tag	L	Value		
		'BF4A'	var.	Offline BIT Group Template		
				'02'	1	Number of BITs in the group
				'7F60'	Var.	BIT 1, see Table 43a
				'7F60'	Var.	BIT 2, see Table 43a
				…	…	…
				'7F60'	Var.	BIT n, see Table 43a
		'BF4B'	var.	Online BIT Group Template		
				'02'	1	Number of BITs in the group
				'7F60'	Var.	BIT 1, see Table 43a
				'7F60'	Var.	BIT 2, see Table 43a
				…	…	…
				'7F60'	Var.	BIT n, see Table 43a

Table 43d: Card BIT Group Template

Tag	L	Value
'02'	1	Number of BITs in the group

'7F60'	Var.	BIT 1, see Table 43a
'7F60'	Var.	BIT 2, see Table 43a
…	…	…
'7F60'	Var.	BIT n, see Table 43a

Table 43e: Terminal BIT Group Template

EMV Book 4

In Section 2 Normative References, add the following references as the new last two rows:

ISO/IEC 19794 Information technology – Biometric data interchange formats

ISO/IEC 19794-2 Information technology – Biometric data interchange formats – Part 2: Finger minutiae data

---

In Section 3 Definitions, add the following terms:

Biometric Data Block A block of data with a specific format that contains information captured from a biometric capture device and that could be used as follows:

- stored in the card as reference
- sent to the ICC in the data field of the PIN CHANGE/UNBLOCK command
- sent to the ICC in the data field of the VERIFY command for offline biometric verification
- sent online for verification

The format of the BDB is outside the scope of this specification.

biometric verification The process of determining that the biometrics presented, such as finger, palm, iris, voice or facial, are valid.

In Section 6.3.4 Cardholder Verification Processing, update the first bullet point as shown below:

- For EMV-defined CVM codes, support is indicated in Terminal Capabilities and Biometric Terminal Capabilities.

In Section 6.3.9 Issuer-to-Card Script Processing, add the following after the Note in the second paragraph:

Note: A terminal or special device used for biometric enrollment or update, i.e. to store a biometric template in the card as the biometric reference template or later update the biometric reference template, shall be able to support one or more Issuer Scripts, where the total length of all Issuer Scripts is more than 128 bytes. The maximum size is dependent on the program(s) supported by the terminal.

After Section 8.5 Plugs and Sockets, add the following new section:

8.6 Biometric Terminal

Figure 6a shows the high level architecture of the Biometric Terminal and Card.

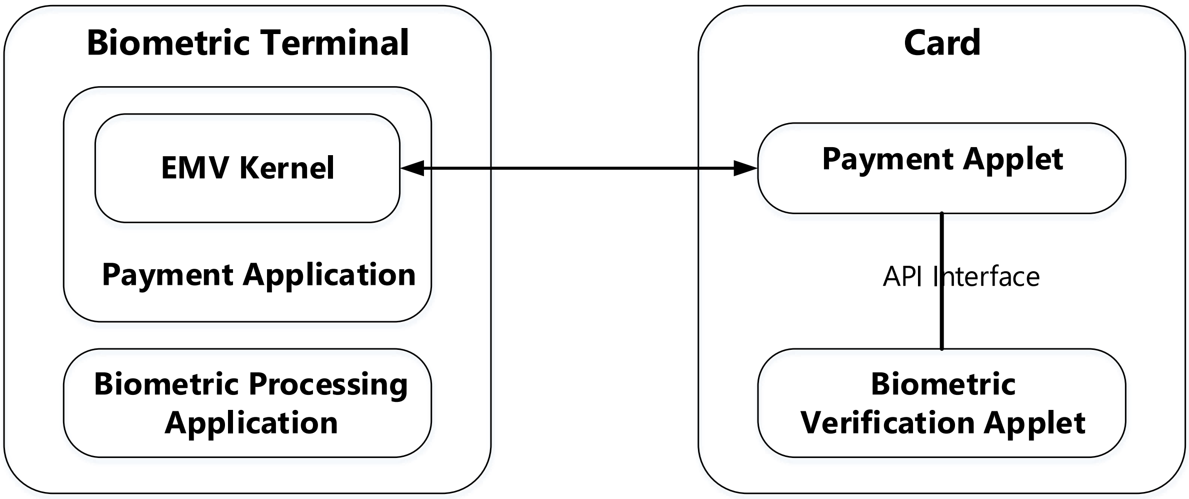


Figure 6a: Architecture of Biometric Terminal and Card

Note: The Biometric Processing Application could be implemented as an integrated part of or as a separate component from the Biometric Terminal. Figure 6a shows one example of the Biometric Terminal and Card implementation.

As shown in Figure 6a, the Biometric Terminal has a Biometric Processing Application, which supports at least one biometric verification method among facial, finger, iris, palm and voice verifications.

If the Biometric Processing Application supports finger verification, it shall be able to support the capture of any of the ten fingers. Similarly, if it supports palm verification it shall be able to support the capture of both left and right palms; and if it supports iris verification, it shall be able to support the capture of both left and right irises.

For each supported biometric verification method, the Biometric Processing Application shall support at least one ISO format specified in ISO/IEC 19794 for interoperability and may support others to satisfy the business requirements, such as performance, liveness detection, etc.

Note: When the Biometric Processing Application supports one ISO format specified in ISO/IEC 19794, it shall support all possible values of the mandatory biometric comparison algorithm parameters defined in the standard. For example, if the Biometric Processing Application supports ISO/IEC 19794-2, it shall support all possible values of the minutiae order indication defined in ISO/IEC 19794-2.

The Biometric Processing Application shall be able to construct the Biometric Data Block (BDB) using the biometric template captured by the biometric capture device and communicate the BDB to the EMV Kernel.

The mechanism on how the biometric capture device captures the biometric template and transmits it to the Biometric Processing Application, and how the Biometric Processing Application transmits the BDB to the EMV Kernel is not in the scope of this specification bulletin.

Update Table 26 Terminal Capabilities Byte 2 - CVM Capability as shown below:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Plaintext PIN for ICC verification
x	1	x	x	x	x	x	x	Enciphered PIN for online verification
x	x	1	x	x	x	x	x	Signature
x	x	x	1	x	x	x	x	Enciphered PIN for offline verification
x	x	x	x	1	x	x	x	No CVM Required
x	x	x	x	x	1	x	x	Online Biometric
x	x	x	x	x	x	1	x	Offline Biometric
x	x	x	x	x	x	x	0	RFU

Table 26: Terminal Capabilities Byte 2 - CVM Capability

After Annex A6 Authorisation Response Code, add the following new annex:

A7 **Biometric Terminal Capabilities**

This section provides the coding for Biometric Terminal Capabilities:

- Byte 1: Offline Biometric Capabilities
- Byte 2: Online Biometric Capabilities
- Byte 3: RFU

If any of the Offline Biometric Capabilities is supported in Biometric Terminal Capabilities, then the 'Offline Biometric' bit of the Terminal Capabilities shall be set to 1. If any of the Online Biometric Capabilities is supported in Biometric Terminal Capabilities, then the 'Online Biometric' bit of the Terminal Capabilities shall be set to 1.

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Facial biometric for offline verification
x	1	x	x	x	x	x	x	Finger biometric for offline verification
x	x	1	x	x	x	x	x	Iris biometric for offline verification
x	x	x	1	x	x	x	x	Palm biometric for offline verification
x	x	x	x	1	x	x	x	Voice biometric for offline verification
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Table 35a: Biometric Terminal Capabilities Byte 1 - Offline Biometric Capabilities

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Facial biometric for online verification
x	1	x	x	x	x	x	x	Finger biometric for online verification
x	x	1	x	x	x	x	x	Iris biometric for online verification
x	x	x	1	x	x	x	x	Palm biometric for online verification
x	x	x	x	1	x	x	x	Voice biometric for online verification
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Table 35b: Biometric Terminal Capabilities Byte 2 - Online Biometric Capabilities

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	x	x	x	x	x	x	x	RFU
x	0	x	x	x	x	x	x	RFU
x	x	0	x	x	x	x	x	RFU
x	x	x	0	x	x	x	x	RFU
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Table 35c: Biometric Terminal Capabilities Byte 3 - RFU

Legal Notice

The EMV® Specifications are provided "AS IS" without warranties of any kind, and EMVCo neither assumes nor accepts any liability for any errors or omissions contained in these Specifications. EMVCO DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AS TO THESE SPECIFICATIONS.

EMVCo makes no representations or warranties with respect to intellectual property rights of any third parties in or in relation to the Specifications. EMVCo undertakes no responsibility to determine whether any implementation of the EMV® Specifications may violate, infringe, or otherwise exercise the patent, copyright, trademark, trade secret, know-how, or other intellectual property rights of third parties, and thus any person who implements any part of the EMV® Specifications should consult an intellectual property attorney before any such implementation.

Without limiting the foregoing, the Specifications may provide for the use of public key encryption and other technology, which may be the subject matter of patents in several countries. Any party seeking to implement these Specifications is solely responsible for determining whether its activities require a license to any such technology, including for patents on public key encryption technology. EMVCo shall not be liable under any theory for any party's infringement of any intellectual property rights in connection with the EMV® Specifications