EMV Contactless Setting Manual for VEGA3000

Version 0.94

August 2014

http://www.castech.com.tw

CASTLES TECHNOLOGY

Table of Contents

Revision History

Version	Date	Description
V0.9	2014/06/09	Release
V0.91	2014/06/17	Add Tag DF23, DF24 information
V0.92	2014/07/24	1. Add Upload DOL Tags (DF8F49, DF8F45, DF8F4C, DF8F4E) 2. Add Forced Transaction Online Tag DF9F01
V0.93	2014/08/04	Add Exception File Check Enable Indicator Tag (DF27)
V0.94	2014/08/06	1. Add Visa Issuer Script Results Tag information (9F5B) 2. Add Application Prefer Order Tag (DF9F02)

WARNING

Information in this document is subject to change without prior notice.

ABOUT THIS MANUAL

1 Purpose

When the terminal with contactless exporting to the vendors, it is required to be preloaded with some settings, such as Terminal Tags, Scheme ID, and the CA Public Keys. Each of them may be used for different applications, like PayWave, PayPass. These settings are very important in transaction.

It is very important to re-design and plan the suitable settings for your projects.

You should have each application's books in hand to understand every setting's meaning.

2 Terminal Tag

For different types of transaction (PayWave, PayPass) the setting may be various. Mandatory tags must be set for specific transaction type.

2.1 EMV Tags

Some EMV Tags are needed for the contactless kernel, please refer to EMV Book 3 Annex A to see the description. The EMV tags are set for all the payments which contactless kernel supports.

2.1.1 9F1A Terminal Country Code

Data Format	N4 (2 Bytes)
Value	0158h - Taiwan [Default] Others - Please refer to the ISO 3166 for the currency code

2.1.2 9F1B Floor Limit

Data Format	B (4 Bytes)
Value	00030D40 [Default] $2000.00 (In the case the currency exponent is 2)

2.1.3 9F1E Interface Device(IFD) Serial Number

Data Format	AN8 (8 Bytes)
Value	Tag Absent [Default]

2.1.4 9F15 Merchant Category Code

Data Format	N4 (2 Bytes)
Value	Tag Absent [Default]

2.1.5 9F16 Merchant Identifier

Data Format	ANS15 (15 Bytes)
Value	Tag Absent [Default]

2.1.6 9F4E Merchant Nameand Location

Data Format	ANS (var. Bytes)
Value	Tag Absent [Default]

2.1.7 9F1C Terminal Identification

Data Format	AN8 (8 Bytes)
Value	Tag Absent [Default]

2.1.8 9F35 Terminal Type

Data Format	N2 (1 Byte)
Value	01h [Default]

2.1.9 5F2A Transaction Currency Code

Data Format	N3 (2 Bytes)
Value	0901h - Taiwan Dollar (NT) [Default] Others - Please refer to the ISO 4217 for the currency code

2.1.10 9C Transaction Type

Data Format	N2 (1 Byte)
Value	00h - Sale(Purchase) Transaction [Default] Others - Please refer to each payment specification.

2.1.11 9F33 Terminal Capability

Data Format	B3 (3 Bytes)
Value	0008C8 [Default]

2.1.12 9F40 Additional Terminal Capability

Data Format	B5 (5 Bytes)
Value	6F00002001 [Default]

2.2 Mandatory Tags for Visa PayWave

Please refer to Visa Contactless Payment Specification(VCPS) v2.1 for the detail description.

2.2.1 9F66 Terminal Transaction Qualifiers

Please set the BYTE 1 corresponding to the settings in the Scheme ID supported by the contactless kernel.
For example, if the contactless kernel supports the qVSDC in Scheme ID setting, the BYTE 1 bit 6 (Contactless qVSDC Supported Bit) should be set to 1.

Data Format	B32 (4 Bytes)
Value	
Byte 1 20h [Default]	Bit 8 '1' – Contactless MSD supported '0' – Contactless MSD not supported [Default] Bit 7 RFU (should be 0)

	Bit 6 '1' – Contactless qVSDC supported [Default] '0' – Contactless qVSDC not supported Bit 5 (***Do not set to '1'***) '1' – Contact VSDC supported '0' – Contact VSDC not supported [Default] Bit 4 '1' – Reader is Offline Only '0' – Reader is Online Capable [Default] Bit 3 (***Please set to '1' if terminal supports***) '1' – Online PIN supported '0' – Online PIN not supported [Default] Bit 2 (***Please set to '1' if terminal supports***) '1' – Signature supported '0' – Signature not supported [Default] Bit 1 RFU
Byte 2 00 [Default]	Bit 8 **(*If qVSDC supported, this bit will be varied by contactless kernel. Recommend to set to '0' if qVSDC supported.***) '1' – Online cryptogram required '0' – Online cryptogram not required Bit 7 **(*If qVSDC supported, this bit will be varied by contactless kernel. Recommend to set to '0' if qVSDC supported.***) '1' – CVM required '0' – CVM not required Other Bit RFU
Byte 3 00 [Default]	Bit 8 '1' – Issuer Update Processing supported '0' –Issuer Update Processing not supported Bit 7 '1' – Consumer Device CVM supported '0' –Consumer Device CVM not supported Other Bit RFU
Byte 4 00 [Default]	RFU

2.3 Optional Visa PayWave Tags

Please refer to VCPS v2.1 and Visa AP Spec. for the detail description.

2.3.1 DF00 Reader Contactless Transaction Limit

It is a Visa AP tag and used for all Visa Paywave Payment (qVSDC/MSD/Wave2).

Data Format	N12 (6 Bytes)
Value	Tag Absent - Bypass this check [Default] FFh - Bypass this check Others - Ex : 000000300000 If the amount is equal to or large than 3000, this transaction can't use the contactless interface. (In the case the currency exponent is 2)

2.3.2 DF01 Reader CVM Required Limit

It is a Visa AP tag and used for all Visa Paywave Payment (qVSDC/MSD/Wave2).

Data Format	N12 (6 Bytes)
Value	Tag Absent - Bypass this check [Default] FFh - Bypass this check Others - Ex : 000000200000 If the amount is equal to or large than 2000, this transaction shall perform the CVM. (In the case the currency exponent is 2)

2.3.3 DF02 Reader Contactless Floor Limit

It is a Visa AP tag and used for all Visa Paywave Payment (qVSDC/MSD/Wave2).

Data Format	N12 (6 Bytes)
Value	Tag Absent - Bypass this check [Default] FFh - Bypass this check Others - Ex : 000000100000 If the amount is large than 1000, this transaction shall go online (In the case the currency exponent is 2)

2.3.4 DF05 Display Offline Funds Indicator

It is a Visa AP tag and used for all Visa Paywave Payment (qVSDC/MSD/Wave2).

Data Format	N2 (1 Byte)
Value	Tag Absent - Do not display offline funds. [Default] 00h - Do not display offline funds. 01h - Display offline funds.

2.3.5 DF25 Status Check (Contactless Kernel Proprietary Tag)

Please refer to VCPS v2.1 Req 5.31 Status Check (qVSDC/MSD).

Data Format	N2 (1 Byte)
Value	Tag Absent - Status Check is disable. [Default] FFh - Status Check is disable. 01h - Status Check is enable.

2.3.6 DF8F4B Amount 0 Check (Contactless Kernel Proprietary Tag)

Please refer to VCPS v2.1 Req 5.32 Amount, Authorozed of Zero Check (qVSDC/MSD).

Data Format	N2 (1 Byte)
Value	FFh - Amount 0 Check is disable. 00h - Option 1 : Indicate Online Cryptogram Required (set TTQ byte 2 bit 8 to 1b). [Default] 01h - Option 2 : Set the Contactless Application Not

	Allowed indicator for Visa AIDs to 1.

2.3.7 DF20 Terminal Entry Capability (Contactless Kernel Proprietary Tag)

This tag will be returned in chip data response for Visa transaction (qVSDC/MSD).
Please refer to VCPS v2.1 K Online Message and Clearing Records

Data Format	N2 (1 Byte)
Value	A value of 5 (for readers that also support VSDC contact chip) or a value of 8 (for readers that do not also support VSDC contact chip). Check with your Visa regional representative.

2.3.8 DF21 Visa MSD Track1 Enable Indicator (Contactless Kernel Proprietary Tag)

Please refer to VCPS v2.1 Req 5.72 Constructing Track 1 Data (MSD).

Data Format	N2 (1 Byte)
Value	Tag Absent - Constructing Track 1 Data is enable. [Default] 00h - Constructing Track 1 Data is disable. 01h - Constructing Track 1 Data is enable.

2.3.9 DF22 Visa MSD Track2 Enable Indicator (Contactless Kernel Proprietary Tag)

Please refer to VCPS v2.1 Req 5.71 Formatting Track 2 Data (MSD).

Data Format	N2 (1 Byte)
Value	Tag Absent - Formatting Track 2 Data is enable. [Default] 00h - Formatting Track 2 Data is disable. 01h - Formatting Track 2 Data is enable.

2.3.10 DF29 Visa MSD CVN17 Enable Indicator (Contactless Kernel Proprietary Tag)

Please refer to VCPS v2.1 Req 5. 9 Disable MSD CVN17 Functionality (MSD).

Data Format	N2 (1 Byte)
Value	Tag Absent - MSD CVN17 functionality is enable. [Default] 00h - MSD CVN17 functionality is disable. 01h - MSD CVN17 functionality is enable.

2.3.11 DF24 Dynamic Reader Limit (DRL) Enable Indicator (Contactless Kernel Proprietary Tag)

DRL functionality allows the reader to apply different Reader Limit Sets for different card applications (even if they have the same AID), allowing the reader to vary Reader Risk Parameters on a transaction by transaction basis. Please refer to VCPS v2.1 Req 5. 5. 4 DRL Functionality (qVSDC).

Data Format	N2 (1 Byte)
Value	Tag Absent – DRL functionality is disable. [Default] 00h - DRL functionality is disable. 01h - DRL functionality is enable.

2.3.12 DF23 Dynamic Reader Limit DRL Overwrite Tag (Contactless Kernel Proprietary Tag)

This tag is used to set each Limit Set for each Application Program ID. When DRL functionality is enable and a matching Application Program ID is returned by card, the kernel will overwrite the limit data set in this tag and determine the Reader Risk Parameters.

The format of the data is as below

APID1 Len + APID1 + data length + data (in TLV) +
APID2 Len + APID2 + data length + data (in TLV) + ...
APIDn Len + APIDn + data length + data (in TLV)

***APID : Application Program ID

Example : if APID = 0102 , then status check is disable, amount 0 check is disable, cl transaction limit = 30.00, cl cvm limit = 10.00 and cl floor limit = 20.00

The value of DRL overwrite tag is
02010224DF2501FFDF8F4B01FFDF00060000000003000DF0106000000001000DF0206000000002000

If the Application Program ID returned from card is 0102, kernel will use the limit data above to determine the Reader Risk Parameters

Please refer to VCPS v2.1 Req 5. 5. 4 DRL Functionality (qVSDC).

Data Format	B (var. Bytes)
Value	Tag Absent –No DRL overwrite

2.3.13 DF27 Exception File Check Enable Indicator

Please refer to VCPS v2.1 Req 5.75 Terminal Exception File Check.(qVSDC).

Data Format	N2 (1 Byte)
Value	Tag Absent –Terminal Exception File Check is configurable to be disabled. [Default] 00h - Terminal Exception File Check is configurable to be disabled. 01h - Terminal Exception File Check is configurable to be enabled.

2.3.14 9F5B Visa Issuer Script Results

Please refer to VCPS v2.1 Table D-1: VCPS Data Elements.(qVSDC).
This tag is not used for configuration. This is a transaction output data and it can be got from transaction response. Indicates the results of Issuer Script Processing.
The data format is Script 1 Result + Script 2 Result + …+ Script n Result
The format of Script x Result is below.

Data Format	(Var Bytes)
Value	

Byte 1	Script Result Bits 8-5: Result of the Issuer Script processing performed by the reader: '0' = Issuer Script not performed '1' = Issuer Script processing failed '2' = Issuer Script processing successful Bits 4-1: Sequence number of the Issuer Script Command: '0' = Not specified '1'–'E' = Sequence number 1-14 'F' = Sequence number 15 or above
Byte 2-5	Issuer Script Identifier): Issuer Script Identifier received by the reader, if available; zero filled if not available. Mandatory if more than one Issuer Script Template was received by the reader-terminal.

2.4 Mandatory Tags for PayPass 3.x

Please refer to paypass – Mchip Reader Spec v3.0.x for the detail description.

2.4.1 5F57 Account Type

Indicates the type of account selected on the Terminal, coded as specified in Annex G of [EMV Book 3]

Data Format	N2 (1 Byte)
Value	Tag Absent [Default]

2.4.2 9F01 Acquirer Identifier

Uniquely identifies the acquirer within each payment system.

Data Format	N6-11 (6 Bytes)
Value	Tag Absent [Default]

2.4.3 9F09 Application Version Number

Version number assigned by the payment system for the Kernel application.

Data Format	B (2 Bytes)
Value	0002h [Default]

2.4.4 DF8117 Card Data Input Capability

Indicates the card data input capability of the Terminal and Reader. The Card Data Input Capability is coded according to Annex A.2 of [EMV Book 4].

Data Format	B (1 Byte)
Value	00h [Default] Byte 1 b8 : Manual key entry b7 : Magnetic stripe b6 : IC with contacts b5-1 : RFU

2.4.5 DF8118 CVM Capability – CVM Required

Indicates the CVM capability of the Terminal and Reader when the transaction amount is greater than the Reader CVM Required Limit.
The CVM Capability – CVM Required is coded according to Annex A.2 of [EMV Book 4].

Data Format	B (1 Byte)
Value	60h [Default] Byte 1 b8 : Plaintext PIN for ICC verification b7 : Enciphered PIN for online verification b6 : Signature (paper) b5 : Enciphered PIN for offline verification b4 : No CVM required b3-1 : RFU

2.4.6 DF8119 CVM Capability – No CVM Required

Indicates the CVM capability of the Terminal and Reader when the transaction amount is less than or equal to the Reader CVM Required Limit.
The CVM Capability – No CVM Required is coded according to Annex A.2 of [EMV Book 4].

Data Format	B (1 Byte)
Value	08h [Default] Byte 1 b8 : Plaintext PIN for ICC verification b7 : Enciphered PIN for online verification b6 : Signature (paper) b5 : Enciphered PIN for offline verification b4 : No CVM required b3-1 : RFU

2.4.7 DF811A Default UDOL

The Default UDOL is the UDOL to be used for constructing the value field of the COMPUTE CRYPTOGRAPHIC CHECKSUM command if the UDOL in the Card is not present. The Default UDOL must contain as its only entry the tag and length of the Unpredictable Number (Numeric) and has the value: '9F6A04

Data Format	B (3 Bytes)
Value	9F6A04h [Default]

2.4.8 DF811B Kernel Configuration

Indicates the Kernel configuration options

Data Format	B1 (1 Bytes)
Value	20h [Default] Byte1 b8 : Only EMV mode transactions supported b7 : Only mag-stripe mode transactions supported b6 : On device cardholder verification supported b5-1 : RFU

2.4.9 DF810C Kernel ID

Contains a value that uniquely identifies each Kernel. There is one occurrence of this data object for each Kernel in the Reader

Data Format	B (1 Byte)
Value	02h [Default]

2.4.10 9F6D Mag-srtipe Application Version Number (Reader)

Version number assigned by the payment system for the specific mag-stripe mode functionality of the Kernel.

Data Format	B (2 Bytes)
Value	0001h [Default]

2.4.11 DF811E Mag-stripe CVM Capability – CVM Required

Indicates the CVM capability of the Terminal/Reader in the case of a mag-stripe mode transaction when the Amount, Authorized (Numeric) is greater than the Reader CVM Required Limit.

Data Format	B (1 Byte)
Value	10h [Default] Byte 1 b8-5 : 0000 : NO CVM 0001 : OBTAIN SIGNATURE 0010 : ONLINE PIN 1111 : N/A Other values : RFU B4-1 : RFU

2.4.12 DF812C Mag-stripe CVM Capability – No CVM Required

Indicates the CVM capability of the Terminal/Reader in the case of a mag-stripe mode transaction when the Amount, Authorized (Numeric) is less than or equal to the Reader CVM Required Limit

Data Format	B (1 Byte)
Value	00h [Default]

	Byte 1 b8-5 : 0000 : NO CVM 0001 : OBTAIN SIGNATURE 0010 : ONLINE PIN 1111 : N/A Other values : RFU B4-1 : RFU

2.4.13 DF811C Max Lifetime of Torn Transaction Log Record

Maximum time, in seconds, that a record can remain in the Torn Transaction Log

Data Format	B (2 Byte)
Value	0000h [Default]

2.4.14 DF811D Max Number of Torn Transaction Log Record

Indicates the maximum number of records that can be stored in the Torn Transaction Log.

Data Format	B (1 Byte)
Value	00h [Default]

2.4.15 9F7E Mobile Support Indicator

The Mobile Support Indicator informs the Card that the Kernel supports extensions for mobile and requires on-device cardholder verification.

Data Format	B (1 Byte)
Value	Tag Absent [Default] Byte 1 b8-3 : RFU b2 : Offline PIN Required b1 : Mobile supported

2.4.16 DF8123 Reader Contactless Floor Limit

Indicates the transaction amount above which transactions must be authorized online.

Data Format	N12 (6 Bytes)
Value	000000100000 [Default]

2.4.17 DF8124 Reader Contactless Transaction Limit (No On-device CVM)

Indicates the transaction amount above which the transaction is not allowed. This data object is instantiated with Reader Contactless Transaction Limit (On-device CVM) if on-device cardholder verification is supported by the Card and with Reader Contactless Transaction Limit (No On-device CVM) otherwise.

Data Format	N12 (6 Bytes)
Value	000000300000 [Default]

2.4.18 DF8125 Reader Contactless Transaction Limit (On-device CVM)

Indicates the transaction amount above which the transaction is not allowed, when on-device cardholder verification is supported.

Data Format	N12 (6 Bytes)
Value	000000500000 [Default]

2.4.19 DF8126 Reader CVM Required Limit

Indicates the transaction amount above which the Kernel instantiates the CVM capabilities field in Terminal Capabilities with CVM Capability – CVM Required.

Data Format	N12 (6 Bytes)
Value	000000500000 [Default]

2.4.20 DF811F Security Capability

Indicates the security capability of the Kernel.
The Security Capability is coded according to Annex A.2 of [EMV Book 4].

Data Format	B (1 Byte)
Value	08h [Default]

	Byte 1 b8 : SDA b7 : DDA b6 : Card capture b5 : RFU b4 : CDA b3-1 : RFU

2.4.21 DF8120 Terminal Action Code - Default

Specifies the acquirer's conditions that cause a transaction to be rejected on an offline only Terminal.

Data Format	B (5 Bytes)
Value	0000000000h [Default]

2.4.22 DF8121 Terminal Action Code - Denial

Specifies the acquirer's conditions that cause the denial of a transaction without attempting to go online.

Data Format	B (5 Bytes)
Value	0000000000h [Default]

2.4.23 DF8122 Terminal Action Code - Online

Specifies the acquirer's conditions that cause a transaction to be transmitted online on an online capable Terminal.

Data Format	B (5 Bytes)
Value	0000000000h [Default]

2.5 Optional Proprietary Tags

2.5.1 Upload DOL Tags

The Upload DOL tags are used to get the required data objects which are returned in the Chip (or Additional) data of transaction response after

performing a transaction.
The template for this DOL is “FFC3”. Please always pack the DOL with this template.
The format of Tag Upload DOL is (FFC3 + DOL Data Length + DOL Data).
The format of DOL Data is (Tag1 + 0x00 + Tag2 + 0x00 + …. + Tagn + 0x00).

For example, if developer would like to get TVR(Tag 95) and CID(Tag 9F27) in Chip data of transaction response, please set this tag with the values “FFC3 0595009F2700”

There are three Upload DOL Tags that data bojects will be returned in Chip data of transaction response.

Tag DF8F49 is used for PayPass transaction.
Tag DF8F45 is used for payWave CVN10 transaction.
Tag DF8F4C is used for payWave CVN17 transaction.

There is one Upload DOL Tag that data objects will be returned in Additional data of transaction response.

Tag DF8F4E is used for all payments.

2.5.1.1. DF8F49 Upload DOL

This tag is used for PayPass transaction. The Contactless Kernel will respond data objects set in this tag.

Data Format	B (var. Bytes)
Value	Tag Absent [Default] – kernel will return default data objects to Chip data field.

2.5.1.2. DF8F45 Visa payWave Cryptogram Version 10 Upload DOL

This tag is used for payWave transaction. The Contactless Kernel will respond data objects set in this tag when card indicates that its Cryptogram Version is 10 (CVN10).

Data Format	B (var. Bytes)
Value	Tag Absent [Default] – kernel will return default data objects to Chip data field.

2.5.1.3. DF8F4C Visa payWave Cryptogram Version 17 Upload DOL

This tag is used for payWave transaction. The Contactless Kernel will respond data objects set in this tag when card indicates that its Cryptogram Version is 17 (CVN17).

Data Format	B (var. Bytes)
Value	Tag Absent [Default] – kernel will return default data objects to Chip data field.

2.5.1.4. DF8F4E Additional TLV response in Additional Data

This tag is used for all payments. Specify which data will be returned in the additional data field.

Data Format	B (var. Bytes)
Value	Tag Absent [Default] – kernel will return default data objects to Additional data field.

2.5.2 DF9F01 Forced Transaction Online

This tag is used to force the transaction online or not.

Data Format	B (1 Byte)
Value	Tag Absent – Forced transaction online functionality is disable. [Default] 00h - Forced transaction online functionality is disable. 01h - Forced transaction online

2.5.3 DF9F02 Application Prefer Order

If there are more applications in one card, normally the order of performing application is following the Application Priority Indicator. This Tag is used to change the order of the applications which user prefers to use.

The format is (1^{st} PreferAIDLen + 1^{st} PreferAID + 2^{nd} PreferAIDLen + 2^{nd} PreferAID + … + n^{th} PreferAIDLen + n^{th} PreferAID)

Ex : if applications A0000000031010 and A0000000132020 are perfered to perform transaction, please add data DF9F021007A0000000031010 07A0000000132020

Data Format	B (var. Bytes)
Value	Tag Absent – application order is following Application Priority Indicator. [Default] Tag Present –application order is changed to higher priority if the application is matched with prefer order setting.