Chip Parameters Guide

Version: 1.0
24 January 2025
Publication number: CPG-1.0-1/24/2025

For the latest technical documentation, see the Documentation Portal.

Thredd, Kingsbourne House, 229-231 High Holborn, London, WC1V 7DA
Support Email: occ@thredd.com
Support Phone: +44 (0) 203 740 9682

Copyright

To the maximum extent permitted by law, Thredd Ltd shall not be liable to any person or organisation, in any manner whatsoever from the use, construction or interpretation of, or the reliance upon, all or any of the information or materials contained on this website.

To the maximum extent permitted by law, Thredd Ltd shall not be liable to any person or organisation, in any manner whatsoever from the use, construction or interpretation of, or the reliance upon, all or any of the information or materials contained in this guide.

The information in these materials is subject to change without notice and Thredd Ltd. assumes no responsibility for any errors.

About this Guide

This guide is intended as a reference document, to provide information on how to set chip parameters in order for the cards to work successfully with the Thredd platform.

Note: This guide covers both Visa and Mastercard chip parameters relevant to Thredd.

Target Audience

This guide is aimed at Issuers or Program Managers who need to configure the card chip parameters.

Out of Scope

This guide is focused only on interoperability with Thredd platform, and as a result it does not advise on any of the following:

- Best practice
- Settings recommended by Visa or Mastercard
- Settings to ensure a sensible risk profile
- Settings to prevent fraud or lots of unlimited offline spending

What's Changed?

If you want to find out what's changed since the previous release, see the Document History section.

Conventions used in this Guide

- **MUST** – Indicates that this setting is required to work with the Thredd platform
- **SHOULD** – Thredd strongly advise that this setting is set as advised. This is generally on the basis of not restricting card functionality and future proofing. However, the card will work with Thredd if you want to select the non-advised option.
- **ANY** – Program Manager choice – any setting can be used, Thredd does not recommend any value. You can choose as they please (refer to other guidance on what to set it to if not sure).

Tip: For the latest technical documentation, see the Documentation Portal.

1 Introduction

This guide describes the Card Scheme chip card personalisation settings and provide the specific parameters that configure the card functionality.

Parameters generally fall into the following categories:

Mastercard

- Mastercard Chip and PIN Application (MCHIPA). These are generally items where the MCHIPA/EMV specifications give a choice to the issuer/program manager. For example, Card Issuer Action Code - Decline.

Visa

- Visa Integrated Specifications (VIS). These are generally items where the VIS/VCPS/EMV specifications give a choice to the issuer/program manager. For example, Application Default Action.
- Visa Contactless Payment Specification (VCPS). For example, Application Default Action.

General

- Parameters relevant for the chip setup, defined by the program manager. For example, what MAC length for issuer script commands is supported by the card.
- EMV parameters. For example, Issuer Action Code - Decline.
- Parameters that will vary per card (not per profile). This guide will not mention these items unless relevant to profile setup. For example, PAN.
- Parameters that will vary per transaction (not per card or profile). For example, Amount Transaction or Application Cryptogram. This guide does not mention these items unless relevant to profile setup.

Chip Management on the Thredd Platform

For information on recommended chip settings for cards on the Thredd Platform, see Chip Management on the Thredd Platform.

2 Notation

It is important to be clear on the difference between binary, decimal and hexadecimal notation.

For consistency, Thredd follows EMV notation. https://www.emvco.com/. For a full list, refer to *EMV book 4.3 section 4 'Abbreviations, Notations, Conventions and Terminology'*.

The following table summarises the notation used by Thredd:

Notation	Description
0 to 9	Decimal digits
'0' to '9' and 'A' to 'F'	Hexadecimal characters. These will always be in single quotes
AC	Application Cryptogram. Defined by EMV, and in EMV tag '9F26'.
00000000	8 binary bits. Most significant bit is on the left, least significant on the right. In accordance with EMV: • Bit 8 = Most significant (top) bit in the byte • Bit 1 = Least significant (bottom) bit in the byte
0	A single binary bit, value 0
1	A single binary bit, value 1
Byte numbers	If a parameter is made up of bytes, then: • Byte 1 is the first byte • Byte 2 is the second byte, and so on.
Profile	This describes one particular complete set of configuration settings for a chip card. For example, if all the chip cards pre-configured data was the same for all your cards, you would only need 1 Profile.
RFU	Reserved for Future Use
TLV	Tag Length Value
Tag	The tag part of TLV
Template	Some tags are held inside Templates. There can be many templates holding different values of the same items. For example, the tag '5F2D' (language preference) is held inside the FCI Proprietary Template 'A5', which is held inside the FCI Template '6F'. There may be many different FCI Templates on the card, hence many different '5F2D' values, one for each different template. See *EMV Book1 section 11.3.4* (SELECT command response APDU data)

3 Converting Hexadecimal Values to Bit Values

The Visa/Mastercard profile information may contain values in hexadecimal only. However, the table below may refer to particular bytes and bits.

To convert **8C01F21C1693** to bytes and bits, do the following:

1. Each byte is 2 hexadecimal digits. therefore, ‘8C’ is the first byte, and ‘01’ the second byte.
2. Each byte of 2 hexadecimal digits can be converted to 8 binary bits as follows:
    a. First hexadecimal digit = bits 8 to 5 of this byte
    b. Second hexadecimal digit = bits 4 to 1 of this byte
    c. Convert hexadecimal digits to 4 bits as follows:

Hexadecimal character	Binary bits equivalent	Decimal value
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
A	1010	10
B	1011	11
C	1100	12
D	1101	13
E	1110	14
F	1111	15

    d. For example, ‘8C’ is in binary *b*10001100
    e. Therefore ‘8C’ is: bit8=1, bit7=0, bit6=0, bit5=0, bit4=1, bit3=1, bit2=0, bit1=0

3. For the example **8C01F21C1693**:

Byte	Hex value	Binary (bit8 (leftmost) to bit1 (rightmost)
1	8C	10001100
2	01	00000001
3	F2	11110010
4	1C	00011100
5	16	00010110
6	93	10010011

For example: Byte 3 bit 8 =1, and Byte 5 bit1=0

4 Mastercard MCHIPA and EMV Settings

The following table describes the Mastercard Chip and PIN Application (MCHIPA) settings relevant to Thredd.

Note: The M/Chip Advance application supports both Contact and Contactless interfaces.

The Tag values are as described in the *EMV MCHIPA Chapter 26 "Data Dictionary"*.

Note: This table only includes the parameter/tag settings that are relevant to Thredd.

Tag & Name	Byte / Bit (s)	Description	Thredd comment

Accumulator 1 Control (Contact)
'DF11'
[MCHIPA]
(Len = 1 byte)
	Byte 1
	bits 2-1
		Include in Issuer Application Data
		Values:
		b00 = Do not include
		b01 = Include Accumulator as Value
		b10 = Include as Balance
		b11 = RFU
			You can set this to ANY.
			However, Thredd recommend that, unless you have a specific reason why not, they SHOULD set the value to b01 (Include Accumulator as Value), in order for the "Plaintext/Encrypted Counters" field in tag '9F10' to be similar to M/Chip 4.1, to keep consistency where possible.

Accumulator 1 Control (Contactless) 'DF12' [MCHIPA] (Len = 1 byte)	Byte 1 bits 2-1	Same values as Accumulator 1 Control (Contact) tag 'DF11'	Same comment as 'DF11' above.
Accumulator 1 Currency Conversion Table 'D1' [MCHIPA] (Len = 25 bytes)	All	Holds a table of currency conversion values in order to convert the transaction amount from the transaction currency to the currency of Accumulator 1.	You can set this to ANY. **Note:** An Issuer Script is required to update this. To update many cards with a new conversion rate table, please raise a Thredd request (this may be chargeable). Our suggestion is to choose sensible values that can remain on the card throughout the card's lifetime. For example, by being conservative on the rate values.
Accumulator 2 Control (Contact) 'DF14' [MCHIPA] (Len = 1 byte)	Byte 1 bits 2-1	Same values as Accumulator 1 Control (Contact) tag 'DF11'	You can set this to ANY.
Accumulator 2 Control (Contactless) 'DF15' [MCHIPA] (Len = 1 byte)	Byte 1 bits 2-1	Same values as Accumulator 1 Control (Contact) tag 'DF11'	You can set this to ANY.
Accumulator 2 Currency Conversion Table 'DF17'	All	Holds a table of currency conversion values in order to convert the transaction amount from the transaction currency to	Same comment as (Accumulator 1 Currency Conversion Table 'D1') above.

Tag & Name	Byte / Bit (s)	Description	Thredd comment
[MCHIPA] (Len = 25 bytes)		the currency of Accumulator 2.	
Application Control (Contact) 'D5' [MCHIPA] (Len = 6 bytes)	Byte 1 bit 8	Accept Online Transactions without ARPC	Thredd recommend this SHOULD be set to b0 to ensure that only valid ARPC values are accepted (Although you can set to ANY).
	Byte 1 Bit 7	Skip CIAC-Default On CAT3	You can set this to ANY. However, care should be taken when setting this, as if set (value b1) it enables limitless offline transactions in some offline-only terminals

	Byte 1
	bit 2
		Session Key Derivation Algorithm:
		b0 = Mastercard Proprietary SKD
		b1 = EMV CSK
			This can be set to any value, and values can be mixed across cards in the same Thredd Card Product.

	Byte 1 bit 1	b1 = Encrypt Offline Counters	Thredd recommend that this SHOULD be set to b0, since Thredd currently do not support decrypting the counters. However, Thredd currently ignore the counter values, so it is possible to set to b1.
	Byte 2 bit 1	b1 = Include Counters in AC	This can be set to ANY.

	Byte 3
	bits 8-7
		Compute Cryptographic Checksum command support.Indicates whether the card supports Magnetic Stripe Contactless.
		Values:
		b00 = RFU
		b01 = Compute Cryptographic Checksum Supported
		b10 = Compute Cryptographic Checksum Not Supported
		b11 = RFU
			Thredd currently do not support verifying the CVV3. This means that Thredd cannot detect fraudulent Mastercard Magnetic Stripe Contactless transactions. Therefore, Thredd recommend this SHOULD be set to b10 (Not supported.)
			Note: Magnetic Stripe Contactless is being phased out.

	Byte 3 bit 3	b1 = Use M/Chip 4 CDOL 1	Thredd recommend this SHOULD be set to 0. This therefore permits the Transaction Time and Merchant Custom Data to be set to the card in 1st GENERATE AC, and thus sent to the Issuer.
	Byte 5 bits 4-2	Issuer Host Backwards Compatibility Values:	Thredd recommend this SHOULD be set to b000. This enables the full M/Chip Advance data to be used and sent to Thredd (the Issuer).

Tag & Name	Byte / Bit (s)	Description	Thredd comment

		b000 = No host backwards compatibility
		b001 = M/Chip v2.1 and M/Chip v2.2 host backwards compatibility
		b010 = M/Chip v2.0.5 host backwards compatibility
		b011 = M/Chip 4 v1.1 and M/Chip 4 v1.3 Host backwards compatibility
		b1xx = RFU
			This MUST be set to either b000 or b011, otherwise AC validation and CVR decoding will fail, causing transaction declines.

	Byte 6 bit 2	b1 = Reset Script Counter With Online Response	Thredd recommend this SHOULD be set to b1. This means the script counter in the CVR will behave as it did for M/Chip 4.1 (counting the number of script commands received since the last valid ARPC.)
Application Control (contactless) 'D7' [MCHIPA] (Len = 6 bytes)	Byte 1 bit 8	Accept Online Transactions without ARPC	Thredd recommend this SHOULD be set to b0 (Although you can set to ANY).
	All other bits and bytes	All the bits have the same meaning as Application Control (contact) - see 'D5' above.	Except for Byte 1 bit 8 (see directly above), the same Thredd comments apply for the contactless setting the same way they do for the contact setting (see Application Control (contact) tag 'D5' above.)
Application Interchange Profile Tag '82' [EMV] (Len = 2 bytes)	Byte 1 bit 1	b1 = CDA is supported	You can set this to ANY. **Note:** Thredd recommend it SHOULD be set to b1 if the card supports this, in order to avoid man-in-the-middle wedge attacks on chip transactions.
Card Issuer Action Code (Contact) - Decline 'C3' [MCHIPA] (Len = 3 bytes)	Byte 1 bit 8	b1 = Last Online Transaction Not Completed	Thredd recommend this SHOULD be set to b0. Otherwise (if b1), then if the Last Online Transaction was not completed, the card will decline all contact transactions offline, effectively blocking the card.
	Byte 1 bit 4	b1 = PIN Try Limit Exceeded	Thredd recommend this SHOULD be set to b0. Otherwise (if b1), then if the offline PIN is blocked on the card, then the card will decline all contact transactions offline,

Tag & Name	Byte / Bit (s)	Description	Thredd comment
			effectively blocking the card.
	Byte 2 bit 8	b1 = Lower Consecutive Counter 1 Limit Exceeded	Thredd recommend this SHOULD be set to b0. Otherwise (if b1), then once this limit is exceeded, then the card will decline all contact transactions offline, effectively blocking the card.
	Byte 2 bit 7	b1 = Upper Consecutive Counter 1 Limit Exceeded	Thredd recommend this SHOULD be set to b0. Otherwise (if b1), then once this limit is exceeded, then the card will decline all contact transactions offline, effectively blocking the card.
	Byte 2 bit 6	b1 = Lower Cumulative Accumulator 1 Limit Exceeded	Thredd recommend this SHOULD be set to b0. Otherwise (if b1), then once this limit is exceeded, then the card will decline all contact transactions offline, effectively blocking the card.
	Byte 2 bit 5	b1 = Upper Cumulative Accumulator 1 Limit Exceeded	Thredd recommend this SHOULD be set to b0. Otherwise (if b1), then once this limit is exceeded, then the card will decline all contact transactions offline, effectively blocking the card.
	Byte 2 bit 4	b1 = Go Online On Next Transaction was set	Thredd recommend this SHOULD be set to b0. Otherwise (if b1), then once this situation happens, then the card will decline all contact transactions offline, effectively blocking the card.
	Byte 2 bit 3	b1 = Issuer Authentication Failed	Thredd recommend this SHOULD be set to b0. Otherwise (if b1), then once this situation happens, then the card will decline all contact transactions offline, effectively blocking the card.
	Byte 2 bit 2	b1 = Script Received	Thredd recommend this SHOULD be set to b0. Otherwise (if b1), then once this situation happens, then the card will decline all contact transactions offline, effectively blocking the card.
	Byte 2 bit 1	b1 = Script Failed	Thredd recommend this SHOULD be set to b0. Otherwise (if b1), then once this situation happens, then the card will decline all contact transactions offline, effectively blocking the card.
	Byte 3 bit 8	b1 = Lower Consecutive Counter 2 Limit Exceeded	Thredd recommend this SHOULD be set to b0. Otherwise (if b1), then once this limit is exceeded, then the card will decline all contact transactions offline, effectively blocking the card.
	Byte 3 bit 7	b1 = Upper Consecutive Counter 2 Limit Exceeded	Thredd recommend this SHOULD be set to b0. Otherwise (if b1), then once this limit is exceeded, then the card will decline all contact transactions offline, effectively blocking the card.

Tag & Name	Byte / Bit (s)	Description	Thredd comment
	Byte 3 bit 6	b1 = Lower Cumulative Accumulator 2 Limit Exceeded	Thredd recommend this SHOULD be set to b0. Otherwise (if b1), then once this limit is exceeded, then the card will decline all contact transactions offline, effectively blocking the card.
	Byte 3 bit 5	b1 = Upper Cumulative Accumulator 2 Limit Exceeded	Thredd recommend this SHOULD be set to b0. Otherwise (if b1), then once this limit is exceeded, then the card will decline all contact transactions offline, effectively blocking the card.
	Byte 3 bit 3	1 = Number of Days Offline Limit Exceeded	Thredd recommend this SHOULD be set to b0. Otherwise (if b1), then once this situation happens, then the card will decline all contact transactions offline, effectively blocking the card.
Card Issuer Action Code (Contactless) - Decline 'CF' [MCHIPA] (Len = 3 bytes)	All	Indicates whether the card should decline an offline contactless transaction	You can set this to ANY. **Note:** If a contactless transaction is declined offline, the cardholder will generally try a contact transaction instead (if possible.) Therefore, where above for the Card Issuer Action Code (contact) - Decline ('C3') a bit is recommended to be b0, the same is not necessarily true for the contactless equivalent.
Card Issuer Action Code (Contact) - Online 'C5' (Len = 3 bytes)	All		ANY. Care should be taken in setting this.
Card Issuer Action Code (Contactless) - Online 'CE' [MCHIPA] (Len = 3 bytes)	All		ANY. Care should be taken in setting this.
Card Issuer Action Code (Contact) - Default 'C4' (Len = 3 bytes)	All		ANY. Care should be taken in setting this.
Card Issuer Action Code	All		ANY. Care should be taken in setting this.

Tag & Name	Byte / Bit (s)	Description	Thredd comment
(Contactless) - Default 'CD' [MCHIPA] (Len = 3 bytes)			
Common Currency conversion Table 'D2' [MCHIPA] (v1.2.3) (Len = 100 bytes)	All	A currency conversion table, which can be used for at least the following: Accumulator 1 Accumulator 2 Maximum Transaction Amount check (possibly others)	Same comment as Accumulator 1 Currency Conversion Table 'D1'

Counter 1 Control (Contact)
'DF1A'
[MCHIPA]
(Len = 1 byte)
	Byte 1
	bits 2-1
		Include in Issuer Application Data
		Values:
		b00 = Do not include
		b01 = Include counter as value
		b10 = Include as balance
		b11 = RFU
			You can set this to ANY.
			However, Thredd recommend that, unless you have a specific reason why not, they SHOULD set the value to b01 (Include Counter as Value), in order for the "Plaintext/Encrypted Counters" field in tag '9F10' to be similar to M/Chip 4.1, to keep consistency where possible.

Counter 1 Control (contactless) 'DF1B' [MCHIPA] (Len = 1 byte)	Byte 1 bits 2-1	Same as Counter 1 Control (Contact) 'DF1A', but for contactless.	Same comment as Counter 1 Control (Contact) 'DF1A'
Cryptogram Version Number Part of '9F10' [MCHIPA] (Len = 1 byte)	All	Arrives in transactions only, not configured in profile.	This is not configured, and you should not see it in the profile. Therefore, nothing to do. (The values for Cryptogram Version Number received in part of '9F10' in a transaction are set from the relevant bits in the Application Control (Contact or Contactless as applicable for the transaction.))
CVM List Tag '8E' [EMV] (Len= 10-252 bytes)	All	List of Cardholder Verification Methods	You can set this to ANY. However, if Issuer Action Code - Denial (Tag '9F0E') byte 3 bit 8 (cardholder verification) is '1', then it is very important that if Offline PIN CV fails, the CVM list will try online PIN.
CVR Issuer Discretionary Data (Contact) Tag 'DF3C'	Byte 1	Issuer discretionary data object of which the two least significant bits are copied in the Card Verification Results when the	SHOULD be set to hex '00'. This is because non-zero values can be used to indicate Biometric sensor-on-card tests as per M/Chip Advance Biometric specification.

Tag & Name	Byte / Bit (s)	Description	Thredd comment
(Len = 1 byte)		contact interface is active.	
CVR Issuer Discretionary Data (Contactless) Tag 'DF3D' (Len = 1 byte)	Byte 1	Issuer discretionary data object of which the two least significant bits are copied in the Card Verification Results when the contactless interface is active.	SHOULD be set to hex '00'. This is because non-zero values can be used to indicate Biometric sensor-on-card tests as per M/Chip Advance Biometric specification.
Issuer Action Code - Denial '9F0E' [EMV] (Len = 5 bytes)	Bytes 1 to 5	Compared against the TVR by the terminal - any bits in common will result in transaction being declined offline.	You can set this to ANY. But note that they should set this with care, since if a test would always be TRUE for all transactions, the card is effectively useless, and a new one may need to be issued.
Issuer Action Code - Denial '9F0E' [EMV] (the value used for the contact interface) (Len = 5 bytes)	Byte 3 bit 8, for the contact interface only	Cardholder verification failed	For the contact interface value: You can set this to ANY, but if set to '1' (decline offline if cardholder verification failed), then they should ensure that this will not prevent the card coming online to receive a new offline PIN. If this set to '1', then the CVM list (tag '8E') must be setup to ensure there that a blocked offline PIN does not permanently prevent the card going online to retrieve a new offline PIN. (See CVM list Tag '8E' above.)
Issuer Action Code - Online '9F0F' [EMV] (Len = 5 bytes)	Bytes 1 to 5	Compared against the TVR by the terminal - any bits in common will result in transaction being sent online.	ANY. Care should be taken in setting this.
Issuer Action Code - Default '9F0D' [EMV] (Len = 5 bytes)	Bytes 1 to 5	Compared against the TVR by the terminal - any bits in common will result in transaction being declined offline if: online was requested but not possible.	ANY. Care should be taken in setting this.
Log Entry Tag '9F4D' [EMV] (Len = 2 bytes)	Byte 2	Maximum number of records in the transaction log file	You can set this to ANY. The transaction log can be useful: • for cardholders (if offline transactions are supported, and you provide a way of reading the transaction log available to the cardholder) • for the issuer or program manager if you physically possess the card, and have a reader, to diagnose what happened on previous transactions.

5 Visa Contact VIS and EMV Settings

This section describes the Visa Integrated Specifications (VIS) settings relevant to Thredd for the Visa Contact application.

The Tag values are as mentioned in the *EMV VIS table A-1 "Data Element Descriptions*".

Note: This table only includes the parameter/tag settings that are relevant to Thredd.

Tag & Name	Byte / Bit (s)	Description	Thredd comment
Application Default Action '9F52' [VIS]	Byte 1 bit 7	b1 = If Issuer Authentication performed and failed, decline transaction.	You can set this to ANY, however you should consider the following: Visa currently recommend that this SHOULD be set to b0, in case an acquirer error causes the ARPC to be altered when sent to the card. (However, this makes it difficult to verify the ARPC is correct.) HOWEVER, there are advantages to setting this to b1, so that an invalid ARPC will decline the transaction. This ensures that ARPC is working, and also prevents fake online responses (as Thredd and Visa will always send a valid ARPC.) So Thredd recommend you consider setting this to b1.
	Byte 1 bit 6	b1 = If Issuer Authentication is mandatory and no ARPC received, decline transaction.	We recommend that this SHOULD be set to b1, for the same reasons as above.
	Byte 2 bit 8	b1 = If PIN Try limit exceeded on current transaction, block application.	You can set this to ANY. But if setting to b1, understand that a new card must be issued if the offline PIN is blocked.
	Byte 2 bit 7	b1 = If PIN Try limit exceeded on previous transaction, decline transaction	You can set this to ANY. But if setting to b1, this might prevent the offline PIN being reset by Thredd if the offline PIN is blocked on the chip.
	Byte 2 bit 4	b1 = If Issuer Script failed on a previous transaction, transmit transaction online	You can set this to ANY. However, having set to b1 will assist in diagnosing any Issuer Script failures.
	Byte 2 bit 3	b1 = If PIN Try Limit exceeded on previous transaction, decline and block application	You can set this to ANY. But if setting to b1, if the offline PIN is blocked, a new card must be issued.
	Byte 3 bit 3	b1 = Use Issuer Script MAC Chaining Option	This MUST be set to b0. Thredd does support Issuer Script MAC Chaining
	Byte 3 bit 2	b1 = Issuer Script Command Counter is cyclic.	Thredd recommend it SHOULD be set to b0, to retain backwards compatibility with the standard way the Visa Card script results work, so that anyone manually looking at the values is not confused. However, there is no automated Thredd process for checking the "script failed" or script command counter, so you can set this to ANY.

<table>
<tr><th>Tag &amp; Name</th><th>Byte / Bit (s)</th><th>Description</th><th>Thredd comment</th></tr>
<tr><td></td><td>Byte 4
bit 5</td><td>b1 = Padding method ‘80’ supported for IDD MACing</td><td>You can set this to ANY.
However, note that Thredd does not currently support validation of the IDD MAC.</td></tr>
<tr><td></td><td>Byte 5
bit 1</td><td>b1 = Secure Messaging uses EMV Session-key based derivation</td><td>You can set this to ANY.
(This bit will be sent in the CVR and Thredd will inspect it to determine the Secure Messaging key derivation method.)</td></tr>
<tr><td>Application Interchange Profile
Tag ‘82’
[EMV]</td><td>Byte 1
bit 1</td><td>b1 = CDA is supported</td><td>You can set this to ANY.
Note however that Thredd recommends it SHOULD be set to b1 if the card supports this, in order to avoid man-in-the-middle wedge attacks on chip transactions.</td></tr>
<tr><td>CVM List
Tag ‘8E’</td><td></td><td>List of Cardholder Verification Methods</td><td>You can set this to ANY.
However, if Issuer Action Code - Denial (Tag ‘9F0E’) byte 3 bit 8 (cardholder verification) is ‘1’, then it is very important that if Offline PIN CV fails, the CVM list will try online PIN.</td></tr>
<tr><td>Cryptogram Version Number
Part of ‘9F10’
[VIS]</td><td>Byte 1</td><td>Upper nibble: ‘9F10’ format (including Secure messaging algorithm in VIS 1.6.1)
Lower nibble: Application Cryptogram algorithm</td><td>This MUST be set to one of the following:
<table>
<tr><th>Hex value</th><th>Decimal value</th></tr>
<tr><td>‘0A’</td><td>10</td></tr>
<tr><td>‘12’</td><td>18</td></tr>
<tr><td>‘22’</td><td>34</td></tr>
</table>
Thredd also supports Cryptogram version hex ’11’ (decimal 17), but this is only for contactless only.
See Appendix 1: Mastercard Cryptogram Version Number Values.
Any other cryptogram version number will result in a decline.</td></tr>
<tr><td>Issuer Action Code - Denial
‘9F0E’
[EMV]</td><td>Bytes 1 to 5</td><td>Compared against the TVR by the terminal - any bits in common will result in transaction being declined offline.</td><td>You can set this to ANY.
But note that they should set this with care, since if a test would always be TRUE for all transactions, the card is effectively useless, and a new one may need to be issued.</td></tr>
<tr><td>Issuer Action Code - Denial
‘9F0E’
[EMV]</td><td>Byte 3
bit 8</td><td>Cardholder verification failed</td><td>If set to ‘1’ (decline offline if cardholder verification failed), then they should ensure that this will not prevent the card coming online to receive a new offline PIN.
If this set to ‘1’, then the CVM list (tag ‘8E’) must be setup to ensure there that a blocked offline PIN does not permanently prevent the card going online to retrieve a new offline PIN. (See CVM list Tag ‘8E’ above.)</td></tr>
</table>

Tag & Name	Byte / Bit (s)	Description	Thredd comment
Issuer Action Code - Online ‘9F0F’ [EMV]	Bytes 1 to 5	Compared against the TVR by the terminal - any bits in common will result in transaction being sent online.	You can set this to ANY. But note that care should be taken when deciding how to set this.
Issuer Action Code - Default ‘9F0D’ [EMV]	Bytes 1 to 5	Compared against the TVR by the terminal - any bits in common will result in transaction being declined offline if: online was requested but not possible.	You can set this to ANY. But note that care should be taken when deciding how to set this.
Issuer Application Data Tag ‘9F10’ [VIS] [EMV]	All bytes	as defined in [VIS] to be sent to the issuer online.	First byte MUST be ‘06’ or ‘1F’. Any other value will result in transactions being declined. See Appendix 1: Mastercard Cryptogram Version Number Values. See also “Derivation Key Index” and “Cryptogram Version Number” above.
Issuer Authentication Data Tag ‘91’ [VIS] [EMV]	All bytes	Data from the Issuer (Thredd here) to be sent back to the card in an online transaction response.	Note that Thredd does not currently support sending “proprietary authentication data”.
Log Entry Tag ‘9F4D’ [EMV]	Byte 2	Maximum number of records in the transaction log file	You can set this to ANY. The transaction log can be useful: • for cardholders (if offline transactions are supported, and you provide a way of reading the transaction log available to the cardholder) • for the Issuer or Program Manager if you physically possess the card, and have a reader, to diagnose what happened on previous transactions.
Profile Control “x” Tags ‘DF1x’ in Template ‘BF59’	Various	Configures the application data and behaviour to be used for transactions conducted using the profile.	See comments for “Application Default Action” for bits which have the same meaning.

6 Visa Contactless EMV Settings

This section describes the Visa Contactless Payment Specification (VCPS) settings relevant to Thredd for the Visa Contactless application.

The Tag values are as mentioned in the *VIS table A-1 "Data Element Descriptions"*.

Additionally, for each tag, as per [VCPS] manual, each tag will be noted as:

- **Shared** – shared with [VIS]. This means the parameter exists once on the card, and is used for both Contact and Contactless.
- **Independent** – value independent to [VIS]. This means the parameter exists twice: once for contact, and once for contactless. Values are separate, (but they can be configured to have the same value if desired.)
- **Exclusive to VCPS** – value does not exist for [VIS]. Parameter only exists for contactless.

Note: This table only includes the parameter/tag settings that are relevant to Thredd.

Tag & Name	Byte / Bit (s)	Description	Thredd comment
Application Default Action '9F52' [VCPS] and [VIS] (Shared)	All Bytes	This is shared with VIS.	See VIS comments above.
Application Interchange Profile '82' [EMV], [VCPS], [VIS] (Independent)	Byte 2 bit 8	1b = Is Contactless Magnetic Stripe supported?	Thredd recommend You SHOULD set this to b0. This is because Thredd does not support validation of the dCVV, which is required to validate genuine contactless magnetic stripe transactions. You can set this to ANY, but should be aware that fraudulent contactless magnetic stripe transactions could be approved.
Card Additional Processes '9F68' (Shared)	All	Indicates card processing requirements and preferences (for contactless application).	You can set this to ANY.
Card CVM Limit '9F6B' [VCPS] (Exclusive to VCPS)	all	Visa proprietary data element indicating that for domestic contactless transactions where this value is exceeded, a CVM is required by the card. Online PIN and Signature are the CVMs supported by cards compliant to this specification.	You can set this to ANY (including not personalising it, which is Visa's recommendation.) Note that Thredd would need to assist (via Issuer Script) if you need the value changed for a large number of cards (for example, if the limit changed.)
Card Transaction Qualifiers '9F6C' [VCPS] (Exclusive to VCPS)	All	Indicates card CVM requirements, issuer preferences, and card capabilities.	You can set this to ANY.
Cryptogram Version Number Part of '9F10'	Byte 1	(See [VIS] above)	See Appendix 1: Mastercard Cryptogram Version Number Values. It MUST only be set to an algorithm in Appendix

Tag & Name	Byte / Bit (s)	Description	Thredd comment
[VCPS] (Independent)			A.1 where "Thredd Supported = Yes". (Any other CVN value will result in a decline.) **Note:** '11' is normally used for contactless (but Thredd does not require this.)
Issuer Application Data Tag '9F10' [VIS], [EMV], [VCPS]	All bytes	Data from the card as defined in [VIS]/[VCPS] to be sent to the issuer online.	See comment in [VIS]
Issuer Authentication Data Tag '91' [VIS], [EMV], [VCPS]	All bytes	Data from the Issuer (Thredd here) to be sent back to the card in an online transaction response.	See comment in [VIS]
Log Entry Tag '9F4D' [EMV]	Byte 2	Maximum number of records in the transaction log file.	See comment in [VIS]

7 Non-profile Settings

Some settings for the cards are not normally mentioned in the Card Profile, either because:

- Settings are outside the scope of the particular Card Specification
- Settings are card-specific

Note: This table only includes the parameter/tag settings that are relevant to Thredd.

Tag & Name	Byte / Bit (s)	Description	Thredd comment
Issuer Script Command MAC length(no tag) [PERSO] (Len = may vary)	All bytes	A value on the end of each script command to prove integrity and authentication of the command	This **MUST** be set to 8 bytes. Thredd only support generating an Issuer Script MAC of 8 bytes. Current understanding is that M/Chip Advance cards always use a MAC of 8 bytes. However, if the card manufacturer has a setting to configure the length, it MUST be set to 8.
Application Primary Account Number Sequence Number Tag '5F34' [EMV] (Len = 1 byte)	Byte 1 (BCD)	PAN sequence number, 00 to 99 (BCD coded)	This is set in the <PAN_SEQ> field of the Thredd card production export file. Thredd will always set the <PAN_SEQ> to zero in the card export file, unless specifically requested otherwise. **Note:** Thredd currently does not record the PAN sequence number, however Thredd will use it in the ARQC validation. Thredd will: • Use any value from 00 to 99 for <PAN_SEQ> in card export file • Record PAN sequence in CARDS_PHYSICAL database table (for ATC tracking and replay detection.)
Derivation Key Index (or Key Derivation Index) Part of '9F10' [MCHIPA] [VIS] (Len = 1 byte)	Byte 1	Key index to select the Issuer EMV AC/MAC/ENC keys with.	**Note:** Thredd do not currently support more than 1 key set for a sub-bin range, and we currently ignore this value. In future Thredd are looking to support this. However, the Card Scheme (Visa, Mastercard) STIP system needs to know this, and it must match what was placed on the card. You can set this to ANY, however we recommend 0 or 1, unless a good reason why not.

8 Chip Management on the Thredd Platform

Although the chip card profile defines a card's behaviour, the host system has some limited capability to change chip transaction outcomes or chip card behaviour. See below for a list of Thredd Platform features that affect chip card transaction flows:

- CVM result check
- Contactless Magstripe
- ARC (ARPC Response Code) instructions

CVM (Cardholder Verification Method) Result Check

If a Cardholder Verification Method (CVM) is disabled on card's usage group, any online transaction with that CVM will be declined. Those methods are listed on Usage Group settings:

CVM Check	Description
Chip PAN Entry - Offline PIN verification	Normally, this setting is checked for almost all chip cards. Please refer to your chip card profile (CPV report) to ensure Offline PIN is among the CVM methods supported.
Chip PAN Entry - Online PIN verification	The Online PIN verification setting is normally checked for almost all chip cards. Please refer to your chip card profile (CPV report) to ensure Online PIN is among the CVM methods supported.
Chip PAN Entry - Signature verification	Transactions with signature could be disallowed with this setting. This is not recommended because the terminal might not support PIN Entry at all, the PIN pad might be broken, or the PIN on the card might be blocked. Most common usage of this setting could be to restrict the card usage with PIN based transactions only.
Chip PAN Entry - No CVM Required	Occasionally, CVM cannot be applied when there is no common CVM method between card and terminal. These transactions might be considered as risky.
Chip PAN Entry - No verification	This setting can be used to decline chip transactions without any valid CVM check result.

Contactless Magstripe

Contactless Magstripe is the inferior method for performing contactless transactions. Usage of this technology is generally restricted, but may be allowed or required in certain regions and countries. Please check with your Thredd account manager to enable this feature.

ARC (ARPC Response Code) Instructions

ARC is a field that is sent in response messages to provide the card's instructions for current and next transactions. This feature is currently enabled for Mastercard cards only. The following instructions can be submitted to chip cards:

CVM Check	Description
If declined, force next transaction online	The card will not be able to do offline transactions until a transaction is approved online.
Force next transaction online	This is a mechanism to disable offline transactions. Not recommended to set if the cards are expected to do offline transactions.
If zero or negative balance, force next	This setting also prevents offline transactions, but only if the balances on the Thredd host side is not positive. It is useful setting to prevent offline transactions for risky customers.

CVM Check	Description
transaction online	
Reset EMV counters to offline limits	This is another mechanism to prevent offline transactions. Available funds on the card for doing Offline transactions effectively becomes zero. This setting is not recommended if the cards are intended for offline usage.

Appendix 1: Mastercard Cryptogram Version Number Values

CVN Bit Positions

This table summarises all the CVN bit positions:

CVN bit position (hex)	Meaning	Value (binary)	Value meaning	Thredd supported?
8-5	Cryptogram Version	0001	Fixed for M/Chip 4 and M/Chip Advance	Yes
4-4	RFU	0	Reserved for future use	Yes
3-2	Session key algorithm	00	Mastercard SKD	Yes
		10	EMV CSK	Yes
1-1	Counters included in AC data?	0	No	Yes
		1	Yes	Yes

CVN Values

This table summarises the resultant CVN values:

CVN (hex)	CVN (binary)	CVN (decimal)	Value meaning	Thredd supported?
‘10’	00010000	16	Mastercard SKD, counters not in AC data	Yes
‘11’	00010001	17	Mastercard SKD, counters in AC data	Yes
‘14’	00010100	20	EMV CSK, counters not in AC data	Yes
‘15’	00010101	21	EMV CSK, counters in AC data	Yes
All other values	All other values	All other values	Reserved for Future Use	No

Appendix 2 Visa Cryptogram Version Number Values

[VIS] version 1.6 redefined the Cryptogram Version Number to simplify the structure of it, by allocating different information to each nibble, as follows:

- Upper nibble: ‘What is the Format of the Issuer Application Data’ and Issuer Scripting algorithm
- Lower nibble: ‘ARQC algorithm’

This table summarises all the CVN values for Visa cards up to and including VIS 1.6, VCPS 2.2 and VCP 1.8.2, showing which ones Thredd supports. (If a value is used which is not supported, all EMV transactions will be declined.)

CVN (hex)	CVN (decimal)	9F10 format	ARQC algorithm	Thredd supported?	Comment
0A	10	0/1/3	‘A’	Yes	Original Visa standard for VIS contact chip transactions
0C	12	0/1/3	Issuer proprietary	No	Issuer proprietary cryptogram processing
11	17	0/1/3	‘1’	Yes	Original Visa standard for VIS contactless chip transactions
12	18	0/1/3	‘2’	Yes	New VIS 1.6 ARQC algorithm
22	34	2	‘2’	Yes	New VIS 1.6 ARQC algorithm, with new ‘9F10’ format ‘2’
2C	44	2	Issuer proprietary	No	Issuer proprietary cryptogram processing, with new ‘9F10’ format ‘2’
32 to 3B	50 to 59	0/1/3	Issuer proprietary	No	Issuer proprietary cryptogram processing
43	67	4	‘3’	No	For Visa Cloud-Based Token Payments New ‘9F10’ format ‘4’
Other	Other	Undefined	Undefined	No	RFU by Visa

Visa Issuer Application Data (tag ‘9F10’) Formats

[VIS] version 1.6 standardised the ‘9F10’ Issuer Application data formats, which vary depending on the first byte.

See EMV [VIS] version 1.6 appendix F for extra information if needed.

This table summarises the formats, based on the first byte which determines it:

9F10 first byte (hex)	9F10 first byte (decimal)	9F10 format	Thredd supported?	Comment
06	6	0/1/3	Yes	Original Visa 9F10 format
1F	31	2 or 4	Yes	New in VIS 1.6
Other	Other	Unknown	No	Not supported by Thredd

Glossary

This page provides a list of glossary terms used in this guide.

A

Acquirer

The merchant acquirer or bank that offers the merchant a trading account, to enable the merchant to take payments in store or online from cardholders.

Application Authentication Cryptogram (AAC)

Cryptogram created when a transaction is declined, helping issuers validate their risk management processes. See also: Application Cryptogram.

Application Cryptogram

The Application Cryptogram is an encrypted value generated by the EMV chip card during a transaction. It is used for transaction validation, fraud prevention and data security. here are several types of application cryptograms used in EMV transactions: ARQC, ARPC and AAC.

Authentication

This includes checks to confirm the cardholder identity, such as PIN, CVV2 and CAVV.

Authorisation

Stage where a merchant requests approval for a card payment by sending a request to the card issuer to check that the card is valid, and that the requested authorisation amount is available on the card. At this stage the funds are not deducted from the card.

Authorization Request Cryptogram (ARQC)

Cryptogram generated by the card when a transaction is initiated and sent to the issuer for authorization. It validates that the transaction details match what is expected and confirms that the card is legitimate. See also: Application Cryptogram.

Authorization Response Cryptogram (ARPC)

Cryptogram generated by the issuer in response to an ARQC. It indicates whether the transaction has been approved or declined and provides additional verification. See also: Application Cryptogram.

B

BIN

The Bank Identification Number (BIN) is the first six to eight numbers on a payment card, which identifies the institution that issues the card.

C

Card Manufacturer

Thredd has relationships with existing card manufacturers, who we can instruct to print your cards. We use Secure FTP (sFTP) to send the card manufacturer a generated bulk XML file containing card details. This is sent on a daily basis, or at a frequency that can be customised for your service. The card manufacturer prints the cards and sends to the cardholder.

Card Scheme (Network)

Card network, such as MasterCard, Visa and Discover, responsible for managing transactions over the network and for arbitration of any disputes.

Cardholder Verification Method (CVM)

The card chip provides a list of permitted methods that can be used by the terminal or device to verify the identity of the cardholder. Common methods include: PIN verification (offline and online), signature verification and no verification.

Cryptogram Version Number (CVN)

A proprietary data element that specifies which cryptographic algorithm is employed during transaction processing. The CVN is included in the Issuer Application Data (IAD) and can influence how cryptographic keys are derived and how transaction data is processed. Different versions of CVN correspond to different processing methods and security protocols used by various card schemes, such as Visa or MasterCard.

E

EMV

A payment card chip standard, to ensure all EMV cards work in all EMV terminals. Derived from the names of the three payment systems that wrote it: Europay, Mastercard and Visa. See www.emvco.com for more information

I

Issuer (BIN Sponsor)

The card issuer, typically a financial organisation authorised to issue cards. The issuer has a direct relationship with the relevant card scheme (payment network).

M

MAC length

The MAC length typically refers to the size of a MAC (Message Authentication Code) in cryptographic contexts. The length of a MAC can vary depending on the specific algorithm being used. Common MAC lengths are 128, 160, and 256 bits depending on the specific method used.

Mastercard Chip and PIN Application (MCHIPA)

Mastercard Chip and PIN Application, is a specification developed by MasterCard for the secure processing of transactions using EMV (Europay, Mastercard, and Visa) chip cards. It outlines the protocols and standards for card authentication, transaction processing, and data security in environments where chip-and-PIN is used.

Merchant

The shop or store providing a product or service that the cardholder is purchasing. A merchant must have a merchant account, provided by their acquirer, in order to trade. Physical stores use a terminal or card reader to request authorisation for transactions. Online sites provide an online shopping basket and use a payment service provider to process their payments.

Merchant Category Code (MCC)

A unique identifier of the merchant, to identity the type of account provided to them by their acquirer.

P

PCI Compliance

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organisations that handle credit cards from the major card schemes (payment networks). All Program Managers who handle customer card data must be compliant with this standard. See: https://www.pcisecuritystandards.org/pci_security/

Primary Account Number (PAN)

The PAN is the long number (typically 16-19 digits) that is either printed or embossed on the card.

Product Setup Form (PSF)

The Product Setup Form is a spreadsheet that provides details of your Thredd account setup. The details are used to configure your Thredd account.

Program Manager

A Thredd customer who manages a card program. The program manager can create branded cards, load funds and provide other card or banking services to their end customers.

Public Token

The 9-digit token is a unique reference for the PAN. This is used between and clients to remove the need for clients to hold actual PANs.

V

Validation

Checks to confirm the card is valid, such as CHIP cryptograms, mag-stripe data (if available) and expiry date

Visa Contactless Payment Specification (VCPS)

Outlines the requirements for conducting secure contactless transactions at point-of-sale (POS) devices.

Visa Integrated Specifications (VIS)

A set of standards covering aspects of transaction processing such as security protocols, data formats, and communication methods between payment devices and networks.

Document History

This section provides details of what has changed since the previous document release.

Version	Date	Reason	Revised by
1.0	13/01/2024	Added a new chapter describing Chip Management on the Thredd Platform.	WS
	12/11/2024	First version	PC

Contact Us

Please contact us if you have queries relating to this document. Our contact details are provided below.

Thredd UK Ltd.

Company registration number 09926803

Support Email: occ@thredd.com

Telephone: +44 (0) 203 740 9682

Our Head Office

Kingsbourne House
229-231 High Holborn
London
WC1V 7DA

Technical Publications

If you want to contact our technical publications team directly, for queries or feedback related to this guide, you can email us at: docs@thredd.com.