AN 6797 Supporting ISO Format 4 PIN Blocks

Type:
Switching release announcement

Audience:
Acquirer
Issuer
Processor
Network enablement partner

Region:
Global

Brand:
Mastercard®
Debit Mastercard®
Maestro®
Cirrus®

Release:
23.Q4

Action indicator:
Program or service requirement: acquirer, issuer
Attention warranted (network related): acquirer, issuer
Testing recommended: acquirer, issuer

System:
Authorization
Single Message System

Published:
8 August 2023

Effective:
7 November 2023

Executive overview

Mastercard is supporting the International Standards Organization (ISO) Format 4 PIN Blocks by introducing a data element usage layout to provide customers with increased security of PIN data encryption.

Effective date details

Date	Details
7 November 2023	Dual Message System (Authorization) and Single Message System

Customer benefit

This enhancement provides increased security for data encryption. ISO Format 4 PIN Blocks uses Advanced Encryption Standard (AES) encryption, which uses a longer block size, making it more secure than the Data Encryption Standard (DES) cipher.

What Mastercard is doing

Mastercard is supporting the International Standards Organization (ISO) Format 4 PIN Blocks by introducing a data element usage layout, Data Element (DE) 110 (Encryption Data) to support ISO Format 4 PIN Blocks. The additional usage layout will follow the DE 110 specifications in ISO/DIS 13492 and for both Authorization and Single Message System.

The new usage layout does not impact the existing DE 110 (Additional Data-2). However, the modifications outlined in *AN 5543 Enhancements to DE 110 (Additional Data-2) for the Single Message System* are a prerequisite to this announcement.

Version history

Each customer must determine the impact on its operations.

Date	Description of change
8 August 2023	Updated data representation attribute for DE 110, Dataset 4, TAG 88 for both Authorization and Single Message System.
6 June 2023	Added Other media to Related documentation
23 May 2023	Corrected impacted systems listed in Enhancements section.
18 April 2023	Initial publication date

Customer impact

This section provides high-level information about customer impact. Refer to the Enhancements section for more details.

Program or service requirement: acquirer, issuer

Acquirers and issuers should migrate to ISO Format 4 PIN Blocks and use AES key blocks for all Host Security Module (HSM) processing.

Acquirers and issuers should complete the enhancements outlined in *AN 5543 Enhancements to DE 110 (Additional Data-2) for the Single Message System* before completing the format changes outlined in this announcement.

Effective with this announcement, acquirers and issuers determine when to support ISO Format 4 PIN Blocks. When prepared to support the format changes in this announcement customers should contact Mastercard Customer Implementation Services (CIS).

Attention warranted (program/service-related): acquirer, issuer

Mastercard recommends that customers implement the DE 110 layout changes using a two-step process:

1. Migrate to the DE 110 layout and continue to use the existing ISO Format 0 PIN Block or ISO Format 1 PIN Block, and current key.
2. Once successfully migrated to the DE 110 layout, implement the AES keys and ISO 4 PIN Block.

Completing the migration this way may help with a rollback if there are unforeseen issues.

Testing recommended: acquirer, issuer

Mastercard recommends testing for acquirers and issuers to support this release announcement.

Transaction message flow impact

The manner in which a customer is connected to Mastercard determines the group of message flows that apply and the transaction message types they send or receive within that group. Customers can interface to the Mastercard Dual Message System, Single Message System, or both, as applicable. This announcement affects the message flows marked in the Transaction message flow impact table.

Transaction message flow impact

Acquirer to Mastercard	Mastercard to issuer	Impacted
Dual Message System	Dual Message System	√

Acquirer to Mastercard	Mastercard to issuer	Impacted
Dual Message System	Single Message System	√
Single Message System	Single Message System	√
Single Message System	Dual Message System	√

Examples of message types within the Dual Message System and Single Message System are:

- Authorization Request/0100 and First Presentment/1240 messages
- Financial Transaction Request/0200 and Financial Transaction Advice/0220 messages

Enhancements

Mastercard will introduce changes to support this announcement.

Dual Message System (Authorization) and Single Message System

Mastercard will introduce a data element usage layout, DE 110 (Encryption Data) to support ISO Format 4 PIN Blocks. The usage layout will contain Tag and Dataset fields.

Sample data for Dataset 01

An example of ISO Format 4 PIN Blocks data for DE 110, Dataset 01 with a dataset length of 51 is as follows:

- Tags:
  8001018108000000000000000082050001234567830101840200248601018701108810 0A145698011267AA0A145698011267AA
- Dataset 01:
  0100338001018108000000000000000082050001234567830101840200248601018701148810 0A145698011267AA0A145698011267AA
- DE 110, Dataset 01:
  F0F5F4010033800101810800000000000000082050001234567830101840200248601018701148810 0A145698011267AA0A145698011267AA

Related documentation

Information relevant to this release announcement can be found in the documents available on Mastercard Connect™. Mastercard updates manuals with necessary changes after release implementation. Depending on timing, information provided in this release announcement may not be reflected in a manual until it is updated.

Announcements

Refer to these previously published announcements for more information:

- *AN 5543 Enhancements to DE 110 (Additional Data-2) for the Single Message System*
- *AN 2944 Update to the Announced Cryptographic Key Block Changes Supporting Phase 2 of PCI Mandates*

Reference manuals

For information about the current state of Mastercard processing refer to the:

- *Authorization Manual*
- *Customer Interface Specification*
- *Single Message System Specifications*

Other media

The PCI Security Standards Council Information Supplement: Implementing ISO Format 4 PIN Blocks is available for more information.

Statements made in videos presented at the Customer Technical Conference are current when the video was recorded. Videos are currently available only for those announcements presented at the Customer Technical Conference. Mastercard may update announcements without updating the corresponding video. Refer to the most recent version of the announcement for the most up-to-date information.

AN 6797 Supporting ISO Format 4 PIN Blocks, Customer Technical Conference, May 2023

Platform impact

The Platform impact table lists the impact of this announcement. For items that are marked √ (Yes), details are available in the corresponding topics.

Platform impact

Topic	Dual Message System (Authorization)	Dual Message System (Clearing)	Single Message System
Message flows			
Message layouts	√		√
Data element definitions	√		√
IPM MPE			
Interchange			
CAB programs, descriptions, and associated MCCs			
Edits	√		√
Error numbers			
Alternate processing			
Interchange compliance			
Pricing and fees			
Reports			
Bulk files			
Forms			
Quarterly Mastercard reporting			
Transaction Investigator			
SAFE			
Single Message Transaction Manager			
250-byte Batch Data File			
80-byte Financial Institution Table File			

Authorization

Mastercard will introduce changes to the Authorization Platform to support this announcement.

Message layouts

Mastercard will add the DE fields listed below as applicable for the noted message types. Whether the data element is mandatory, conditional, optional, system provided, or not required is noted for each applicable message.

Authorization Request/0100

DE ID	Data element name	Org	Sys	Dst	Comments
110	Encryption Data	C	X	C	Includes PIN encryption data

Network Management Request/0800: PEK Exchange

DE ID	Data element name	Org	Sys	Dst	Comments
110	Encryption Data	•	O	C	Includes key management encryption data

Network Management Request/0800: Sign-On/Sign-Off

DE ID	Data element name	Org	Sys	Dst	Comments
110	Encryption Data	C	C	•	Includes key management encryption data

Network Management Advice/0820: PEK Exchange

DE ID	Data element name	Org	Sys	Dst	Comments
110	Encryption Data	•	M	M	Includes key management encryption data

CIS data element definitions

Mastercard will update data elements to support this announcement.

DE 110 (Encryption Data)

DE 110 (Encryption Data) is used in PIN encryption data and key management encryption data.

Attributes

Attribute	Description
Data representation	Mastercard Standard: b...999; LLLVAR
	ISO Standard: b...9999; LLLLVAR
Data element length	n...999 (EBCIDIC)
Dataset ID	1 byte binary value
Dataset length	2 byte binary value
Data field	Dataset Tags
Tag contents	Values
Justification	N/A

Usage

Whether the data element is mandatory, conditional, optional, system-provided, or not required is noted for each applicable message.

Message	Org	Sys	Dst
Authorization Request/0100	C	X	C
Network Management Request/0800: PEK Exchange	•	O	C
Network Management Advice/0820: PEK Exchange	•	M	M
Network Management Request/0800: Sign-On/Sign-Off	C	C	•

Application notes

The length fields in the Tag Length Value (TLV) is coded according to ISO 8825. If the TLV-coded version of a dataset is used the length of the dataset itself is always coded as a two byte binary value.

- The Dataset ID is the first component in a dataset.
- Dataset ID is a one byte binary identifier given to each dataset within a DE 110 field.

- Dataset length is a two byte binary subfield that contains the total length of the TLV element(s) within the dataset.
- The Tag field contains one byte length hexadecimal code that identifies the content of the Value field.
- The Tag length field follows the ISO 8825 spec. n-byte field that defines the length of the Value field.
- The Value field is a variable-length field that will contain the data specified by the Tag field.

DE 110 layout

DE 110 (Encryption Data) is a usage layout to support the PCI Standards Security Council's mandate for ISO Format 4 PIN Blocks. The layout follows DE 110 specifications in ISO/DIS 13492.

Hierarchy of DE 110 for PIN encryption data and key exchange data

DE 110 contains:

- Dataset ID
- Dataset length
- Tags

Each Tag contains:

- Tag ID
- Tag length
- Tag value

Entity	Description
Dataset ID	A one byte hex value specific for each data set Example: 0x01
Dataset length	A two byte hex value. Example: If the length is 24 it will be represented as 0x00 18. This length is the accumulation of all Tags.
Tag ID	A one byte hex specific for each Tag: for example, 0x80

Entity	Description

Tag length	The length field is coded according to ISO 8825. The Dataset length is always coded as a two byte binary value. ISO 8825 defines two forms length octets.
	• Definite form
	• Indefinite form (not supported by Mastercard)
	The definite form has a short and long form.
	Short form: Tag length consists of a single octet or byte. This from can only be used if the number of octets in the Tag data is less than or equal to 127 bytes. It is encoded as:
	• Bit 8 is zero
	• Bits 7 to 1 encode the number of octets or bytes in the contents octets (Tag data) as an unsigned binary integer with bit 7 as the most significant bit.
	Example: If the Tag data is 38 bytes the Tag length is encoded as:
	`00100110`
	Long form: the Tag length consists of an initial octet and one or more additional octets.
	The initial octet will be encoded as:
	• Bit 8 is one
	• Bits 7 to 1 shall encode the number of additional octets in the length octets, as an unsigned binary integer with bit 7 as the most significant bit the value 11111111 must not be used.
	Coding for additional octets:
	1. First additional octet bits 8 to 1
	2. Second additional octet bits 8 to 1
	3. Each additional octet bits 8 to 1
	Octets will be encoded as unsigned binary integer equal to the number of octets in the Tag data, with bit 8 of the first additional octet as the most significant bit.
	Examples:
	• If the Tag data is 201 bytes the Tag length would be encoded as
	`10000001 11001001`
	– 10000001: Initial byte which tells how many additional length bytes.
	– 11001001: The actual length byte.
	• If the tag data is 402 bytes the Tag length would be encoded as
	`10000010 00000001 10010010`

Entity	Description
Tag value	If the data representation is *b* it is binary • b-1 is a value of 21 specified by 0x15 • b-2 is a value of 21 specified by 0x0015 • b-8 is a value of 21 specified by 0x0000000000000015
	If the data representation is *n*, only right padded Binary-Coded Decimal (BCD) is allowed and only values 0 to 9. • n-4 is a value of 112 stored in BCD as 0x01, 0x12 • n-8 is a value of 112 stored in BCD as 0x00, 0x00, 0x01, 0x12

Dataset 01 (PIN Encryption)
DE 110, Dataset 01 (PIN Encryption) contains the personal identification number (PIN), a unique identifier used by the cardholder at the point-of-interaction (POI).

Attribute	Description	Value
Dataset ID	b-1	01
Dataset length	b-2	
Data representation	b...999; LLLVAR	
Data field contains	cryptogram	
Number of tags	7	
	TAG 80 (Control), Mandatory TAG 81 (Key-set Identifier), Mandatory TAG 83 (Algorithm), Conditional TAG 86 (Key Index), Conditional TAG 87 (PIN Block Format), Mandatory TAG 88 (Encrypted PIN Block), Mandatory TAG 89 (Additional Encrypted PIN Block [New PIN Data]), Conditional	

TAG 80 (Control)
DE 110, Dataset 01, TAG 80 (Control) field identifies the key management scheme and associated structure of the remainder of the data element.

Attributes

Attribute	Description
Tag ID	80
Tag length	b-1
Data representation	b-1
Justification	N/A
Required	Mandatory

Values

Value	Description
00	Default value for the Dual Message System

TAG 81 (Key-set Identifier)
DE 110, Dataset 01, TAG 81 (Key-set Identifier) Key-set identifier field is used with DUKPT key management exclusively. The key-set identifier uniquely identifies the base derivation key as defined in the *American National Standard for Financial Services ...Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques (ANSI X9.24 Part 1)*.

Attributes

Attribute	Description
Tag ID	81
Tag length	b-1
Data representation	b-8
Justification	N/A
Required	Mandatory

Values

Value	Description
0000000000000000	Default value for the Dual Message System

TAG 83 (Algorithm)
DE 110, Dataset 01, TAG 83 (Algorithm) selects the encryption algorithm used to encipher the keys contained in the associated key management data element.

Attributes

Attribute	Description
Tag ID	83
Tag length	b-1
Data representation	n-2 (Packed binary coded decimal)
Justification	N/A
Required	Conditional

Values

Value	Description
01	Data Encryption Algorithm (DEA)
03	Triple Data Encryption Algorithm (TDEA)
05	Advanced Encryption Standard (AES)

Application notes

TAG 83 is for online PIN transactions performed on the Authorization Platform for acquirers and issuers in the Europe region. It is not a requirement for acquirers outside of the Europe region.

TAG 86 (Key Index)
DE 110, Dataset 01, TAG 86 (Key Index) indicates the specific PIN key to be used when more than one key is available in a PIN key set.

Attribute	Description
Tag ID	86
Tag length	b-1
Data representation	n-2 (Packed binary coded decimal)
Justification	N/A
Required	Conditional

Values

Value	Description
00-99	PIN key index value for the Dual Message System

Application notes

TAG 86 is for online PIN transactions performed on the Authorization Platform for acquirers and issuers in the Europe region. It is not a requirement for acquirers outside of the Europe region.

TAG 87 (PIN Block Format)
DE 110, Dataset 01, TAG 87 (PIN Block Format) is the format of the PIN Block defined in ISO 9564-1.

Attributes

Attribute	Description
Tag ID	87
Tag length	b-1
Data representation	n-2 (Packed binary coded decimal)
Justification	N/A
Required	Mandatory

Values

Value	Description
10	ISO PIN Block Format 0
11	ISO PIN Block Format 1
14	ISO PIN Block Format 4

TAG 88 (Encrypted PIN Block)
DE 110, Dataset 01, TAG 88 (Encrypted PIN Block) contains PIN block encryption as defined in ISO 9564-1.

Attributes

Attribute	Description
Tag ID	88
Tag length	b-1
Data representation	b-8 or b-16
Justification	N/A

Attribute	Description
Required	Mandatory

Values

Value	Description
8 byte of PIN Block	Format 0
16 bytes of PIN Block	Format 4

TAG 89 (Additional Encrypted PIN Block)
DE 110, Dataset 01, TAG 89 (Additional Encrypted PIN Block) is used for PIN change transaction.

Attributes

Attribute	Description
Tag ID	89
Tag length	b-1
Data representation	b-8 or b-16
Justification	N/A
Required	Conditional

Values

Value	Description
8 bytes of additional PIN Block	Format 0
16 bytes of additional PIN Block	Format 4

Dataset 04 (Key Exchange)
Dataset 04 (Key Exchange) is a method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm.

Attributes

Attribute	Description	Value
Dataset ID	b-1	04
Dataset length	b-2	
Data representation	b...999; LLLVAR	
Data field contains	cryptogram	
Number of tags	6	
	TAG 80 (Control), Mandatory	
	TAG 81 (Key-set Identifier), Mandatory	
	TAG 83 (Algorithm), Mandatory	
	TAG 86 (Key Index), Mandatory	
	TAG 87 (Encrypted Data), Conditional	
	TAG 88 (Key Checksum Value), Conditional	

Usage

Whether the data element is mandatory, conditional, optional, system-provided, or not required is noted for each applicable message.

Message	Org	Sys	Dst
Network Management Request/0800: PEK Exchange	•	O	C
Network Management Request/0800: Sign-On/ Sign-Off	C	C	•
Network Management Advice/0820: PEK Exchange	•	M	M

TAG 80 (Control)
DE 110, Dataset 04, TAG 80 (Control) field identifies the key management scheme and associated structure of the remainder of the data element.

Attributes

Attribute	Description
Tag ID	80
Tag length	b-1
Data representation	b-1
Justification	N/A
Required	Mandatory

Values

Value	Description
00	Default value for the Dual Message System

TAG 81 (Key-set Identifier)
DE 110, Dataset 04, TAG 81 (Key-set Identifier) is a number that uniquely identifies a key-set.

Attributes

Attribute	Description
Tag ID	81
Tag length	b-1
Data representation	b-8
Justification	N/A
Required	Mandatory

Values

Value	Description
0000000000000000	Default value for the Dual Message System

TAG 83 (Algorithm)
DE 110, Dataset 04, TAG 83 (Algorithm) defines the encryption algorithm used to encipher the keys contained in the associated key management data element.

Attributes

Attribute	Description
Tag ID	83
Tag length	b-1
Data representation	n-2 (Packed binary coded decimal)
Justification	N/A
Required	Mandatory

Values

Value	Description
01	Data Encryption Algorithm (DEA)
03	Triple Data Encryption Algorithm (TDEA)
05	Advanced Encryption Standard (AES)

TAG 86 (Key Index)
DE 110, Dataset 04, TAG 86 (Key Index) is used when multiple keys are identified with the same key set identifier; for example, key rotation.

Attribute	Description
Tag ID	86
Tag length	b-1
Data representation	n-2 (Packed binary coded decimal)
Justification	N/A
Required	Mandatory

Values

Value	Description
00	Network Management Request/0800: PEK Exchange Network Management Request/0820: PEK Exchange

Value	Description
00-99	Network Management Request/0800: Sign-on/Sign-off

TAG 87 (Encrypted Data)
DE 110, Dataset 04, TAG 87 (Encrypted Data) uses a structure within it before encryption to identify the data.

Attributes

Attribute	Description
Tag ID	87
Tag length	n-byte
Data representation	b-8 to b-999; LLLVAR
Justification	N/A
Required	Conditional

Values

Hexadecimal values 0-9 and A-F, of the 64 bits of the new encryption key, encrypted under the current communications key.

TAG 88 (Key Checksum Value)
DE 110, Dataset 04, TAG 88 (Key Checksum Value) contains a value used to verify a conveyed key.

Attributes

Attribute	Description
Tag ID	88
Tag length	n-byte
Data representation	b-2 or b-3; LLLVAR
Justification	N/A
Required	Conditional

Values

The key check value consists of the hexadecimal characters, 0-9 and A-F, of the calculated check value.

Edits

Mastercard will add new edits, modify existing edits, or remove existing edits to support this announcement.

Authorization Request/0100 message

Authorization Platform edits for DE 110 (Encryption Data) are as follows:

When...	Then the Authorization Platform...
DE 110, Dataset 01 (PIN Encryption), and TAG 80 (Key Management scheme) is not present in Dataset 01	will return to the acquirer an Authorization Request Response/0110 message where: • DE 39 (Response Code) is 30 (Format error) • DE 44 (Additional Response Data) is 110 (indicating DE 110 is in error).
DE 110, Dataset 01, and TAG 81 (Key Set Identifier) is not present in Dataset 01	will return to the acquirer an Authorization Request Response/0110 message where: • DE 39 (Response Code) is 30 (Format error) • DE 44 (Additional Response Data) is 110 (indicating DE 110 is in error).
DE 110, Dataset 01, and TAG 87 (PIN Block Format Code) is not present in Dataset 01	will return to the acquirer an Authorization Request Response/0110 message where: • DE 39 (Response Code) is 30 (Format error) • DE 44 (Additional Response Data) is 110 (indicating DE 110 is in error).
DE 110, Dataset 01, and TAG 88 (Encrypted PIN Block) is not present in Dataset 01	will return to the acquirer an Authorization Request Response/0110 message where: • DE 39 (Response Code) is 30 (Format error) • DE 44 (Additional Response Data) is 110 (indicating DE 110 is in error).
an Authorization Request/0100 message contains DE 110, Dataset 01 and DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode) is not 02, 05, 07, 80, 81, 82, 90, or 91	will return to the acquirer an Authorization Request Response/0110 message where: • DE 39 (Response Code) is 30 (Format error) • DE 44 (Additional Response Data) is 110 (indicating DE 110 is in error).
an Authorization Request/0100 message of DE 03 (Processing Code), is 92 (PIN Change) and does not contain DE 110, Dataset 01, TAG 89 (New PIN Data)	will return to the acquirer an Authorization Request Response/0110 message where: • DE 39 (Response Code) is 30 (Format error) • DE 44 (Additional Response Data) is 110 (indicating DE 110 is in error).
an Authorization Request/0100 message with DE110, Dataset 01, Tag 88 is present and acquirer keys managed by Authorization, TAG 83 or TAG 86 not present	will return to the acquirer an Authorization Request Response/0110 message where: • DE 39 (Response Code) is 30 (Format error) • DE 44 (Additional Response Data) is 110 (indicating DE 110 is in error).

When...	Then the Authorization Platform...
an Authorization Request/0100 message DE 110, Dataset 01, TAG 87 is not 10 or 14	will return to the acquirer an Authorization Request Response/0110 message where: • DE 39 (Response Code) is 30 (Format error) • DE 44 (Additional Response Data) is 110 (indicating DE 110 is in error).
an Authorization Request/0100 message contains both: • DE 22 (Point-of-Service [POS] Entry Mode), subfield 1 (POS Terminal PAN Entry Mode), value 03 (PAN auto-entry via barcode reader) and • DE 52 (Personal ID Number [PIN] Data) or DE 110, Dataset 01, TAG 88	rejects the message and sends the acquirer an Authorization Request Response/0110 message where DE 39 (Response Code) is 58 (Transaction not permitted to acquirer/terminal).
an Authorization Request/0100 message for a Mastercard Electronic card contains: DE 22, subfield 1, value 02, 03, 05, 07, 09, 80, 90, or 91, and DE 18 (Merchant Type) MCC value is 5542 (Fuel Dispensers, Automated), and DE 52 (Personal ID Number [PIN] Data), and DE 110, Dataset 01, TAG 88 or DE 55 (Integrated Circuit Card [ICC] System-related Data) is not present, and DE 61 (Point-of-Service [POS] Data), subfield 10 (Cardholder Activated Terminal Level) is not a value of 1 (Authorized Level 1 CAT: Automated dispensing machine with a PIN)	sends an Authorization Request Response/0110 message to the acquirer with DE 39 (Response Code), value 58 (Transaction not permitted to acquirer/terminal).
DE 61, subfield 10, value 1 and DE 52 and DE 110, Dataset 01, TAG 88 is not present and DE 55 is not present	sends an Authorization Request Response/0110 message to the acquirer where DE 39 is 30 and DE 44 is 52.
an Authorization Request/0100 message for a Cardless ATM transaction: • Contains DE 18 (Merchant Type), value 6011 (Member Financial Institution: Automated Cash Disbursements), and • DE 48 (Additional Data: Private Data), Transaction Category Code (TCC), value Z (ATM), and • DE 22, subfield 1 (POS Terminal PAN Entry Mode) is present and contains a value other than 09 (PAN/Token entry via electronic commerce containing DSRP cryptogram in DE 55), but DE 52 , and • DE 110, Dataset 01, TAG 88 is not present	rejects the message and sends the acquirer an Authorization Request Response/0110 message where: • DE 39 (Response Code) is 30 (Format error) • DE 44 (Additional Response Data) is 52 (indicating the data element in error).

When...	Then the Authorization Platform...
an Authorization Request/0100 message if • DE 3, subfield 1 contains value 91 (PIN unblock) or 92 (PIN Change) and • DE 52 and DE 110, Dataset 01, TAG 88 is not present	sends the acquirer an Authorization Request Response/0110 message where: • DE 39 (Response Code) is 30 (Format error) • DE 44 (Additional Response Data) is 52 (indicating the data element in error).
the Authorization Request/0100 message contains • DE 61, subfield 10, value 1 and • DE 52 and DE 110, Dataset 01, TAG 88 is not present and • DE 55 is present	forwards the Authorization Request/0100 message to the issuer.
the Authorization Request/0100 message contains • DE 61, subfield 10, value 1 and • DE 52 or DE 110, Dataset 01, TAG 88 is present and • DE 55 is present	forwards the Authorization Request/0100 message to the issuer.
the Authorization Request/0100 message contains • DE 61, subfield 10, value 1 and • DE 52 or DE 110, Dataset 01, TAG 88 is present and • DE 55 is not present	forwards the Authorization Request/0100 message to the issuer.
an authorization Request/0100 message, DE 3, subfield 1 contains value 92 (PIN Change) and DE 125 (New PIN Data) and DE 110, Dataset 01, TAG 89 is not present	sends the acquirer an Authorization Request Response/0110 message where: • DE 39 (Response Code) is 30 (Format error) • DE 44 (Additional Response Data) is 125 (indicating the data element in error).

Single Message System

Mastercard will introduce changes to the Single Message System to support this announcement.

Message layouts

Mastercard will add the DE fields listed below as applicable for the noted message types. Whether the data element is mandatory, conditional, optional, system provided, or not required is noted for each applicable message.

Financial Transaction Request/0200

DE ID	Data element name	Org	Sys	Dst
110	Encryption Data	C	X	C

Network Management Request/0800: PEK Exchange

DE ID	Data element name	Org	Sys	Dst
110	Encryption Data	•	X	C

Network Management Advice/0820: PEK Exchange

DE ID	Data element name	Org	Sys	Dst
110	Encryption Data	•	X	C

Single Message System data element definitions

Mastercard will update data elements to support this announcement.

DE 110 (Encryption Data)

DE 110, Dataset 01 (PIN Encryption), is used in PIN encryption data and key management encryption data.

Attributes

Attribute	Description
Data representation	Mastercard Standard: b...999; LLLVAR ISO Standard: b...9999; LLLLVAR
Data element length	n...999 (EBCIDIC)
Dataset ID	1 byte binary value
Dataset length	2 byte binary value
Data field	Dataset Tags
Tag contents	Values
Justification	N/A

Usage

Whether the data element is mandatory, conditional, optional, system-provided, or not required is noted for each applicable message.

Message	Org	Sys	Dst
Financial Transaction Request/0200	C	X	C
Network Management Request/0800: PEK Exchange	•	X	C

Message	Org	Sys	Dst
Network Management Advice/0820: PEK Exchange	•	X	C

Application notes

The length fields in the Tag Length Value (TLV) are coded according to ISO 8825 if the TLV-coded version of a dataset is used, while the length of the dataset itself is always coded as a 2-byte binary value.

- The dataset ID is the first component in a dataset.
- Dataset ID is a one-byte binary identifier given to each dataset within a DE 110 field.
- Dataset length is two bytes binary subfield that contains the total length of the TLV element(s) within the dataset.
- The Tag field contains a variable-length hexadecimal code that identifies the content of the Value field.
- The Tag length field should follow the ISO 8825 spec. n-byte field that defines the length of the Value field.
- The Value field is a variable-length field that will contain the data specified by the Tag field.

DE 110 layout

DE 110 (Encryption Data) is a usage layout to support the PCI Standards Security Council's mandate for ISO Format 4 PIN Blocks. The layout follows DE 110 specifications in ISO/DIS 13492.

Hierarchy of DE 110 for PIN encryption data and key exchange data

DE 110 contains:

- Dataset ID
- Dataset length
- Tags

Each Tag contains:

- Tag ID
- Tag length
- Tag value

Entity	Description
Dataset ID	A one byte hex value specific for each data set Example: 0x01
Dataset length	A two byte hex value. Example: If the length is 24 it will be represented as 0x00 18. This length is the accumulation of all Tags.
Tag ID	A one byte hex specific for each Tag: for example, 0x80

Entity	Description

Tag length	The length field is coded according to ISO 8825. The Dataset length is always coded as a two byte binary value. ISO 8825 defines two forms length octets.
	• Definite form
	• Indefinite form (not supported by Mastercard)
	The definite form has a short and long form.
	Short form: Tag length consists of a single octet or byte. This from can only be used if the number of octets in the Tag data is less than or equal to 127 bytes. It is encoded as:
	• Bit 8 is zero
	• Bits 7 to 1 encode the number of octets or bytes in the contents octets (Tag data) as an unsigned binary integer with bit 7 as the most significant bit.
	Example: If the Tag data is 38 bytes the Tag length is encoded as:
	`00100110`
	Long form: the Tag length consists of an initial octet and one or more additional octets.
	The initial octet will be encoded as:
	• Bit 8 is one
	• Bits 7 to 1 shall encode the number of additional octets in the length octets, as an unsigned binary integer with bit 7 as the most significant bit the value 11111111 must not be used.
	Coding for additional octets:
	1. First additional octet bits 8 to 1
	2. Second additional octet bits 8 to 1
	3. Each additional octet bits 8 to 1
	Octets will be encoded as unsigned binary integer equal to the number of octets in the Tag data, with bit 8 of the first additional octet as the most significant bit.
	Examples:
	• If the Tag data is 201 bytes the Tag length would be encoded as
	`10000001 11001001`
	– 10000001: Initial byte which tells how many additional length bytes.
	– 11001001: The actual length byte.
	• If the tag data is 402 bytes the Tag length would be encoded as
	`10000010 00000001 10010010`

Entity	Description
Tag value	If the data representation is *b* it is binary • b-1 is a value of 21 specified by 0x15 • b-2 is a value of 21 specified by 0x0015 • b-8 is a value of 21 specified by 0x0000000000000015
	If the data representation is *n*, only right padded Binary-Coded Decimal (BCD) is allowed and only values 0 to 9. • n-4 is a value of 112 stored in BCD as 0x01, 0x12 • n-8 is a value of 112 stored in BCD as 0x00, 0x00, 0x01, 0x12

Dataset 01 (PIN Encryption)
DE 110, Dataset 01 (PIN Encryption) contains the personal identification number (PIN), a unique identifier used by the cardholder at the point-of-interaction (POI).

Attributes

Attribute	Description	Value
Dataset ID	b-1	01
Dataset length	b-2	
Data representation	b...999; LLLVAR	
Data field contains	cryptogram	
Number of tags	5	
	TAG 80 (Control), Mandatory	
	TAG 81 (Key-set Identifier), Mandatory	
	TAG 87 (PIN Block Format), Mandatory	
	TAG 88 (Encrypted PIN Block), Mandatory	
	TAG 89 (Additional Encrypted PIN Block [New PIN Data]), Conditional	

Usage

Whether the data element is mandatory, conditional, optional, system-provided, or not required is noted for each applicable message.

Message	Org	Sys	Dst
Financial Transaction Request/0200	C	X	C

TAG 80 (Control)
DE 110, Dataset 01, TAG 80 (Control) field identifies the key management scheme and associated structure of the remainder of the data element.

Attributes

Attribute	Description
Tag ID	80
Tag length	b-1
Data representation	b-1
Justification	N/A
Required	Mandatory

Values

Value	Description
00	Default value for the Single Message System

TAG 81 (Key-set Identifier)
DE 110, Dataset 01, TAG 81 (Key-set Identifier) is a number that uniquely identifies a key-set.

Attributes

Attribute	Description
Tag ID	81
Tag length	b-1
Data representation	b-8
Justification	N/A
Required	Mandatory

Values

Value	Description
0000000000000000	Default value for the Single Message System

TAG 87 (PIN Block Format)
DE 110, Dataset 01, TAG 87 (PIN Block Format) contains the format for PIN block as defined in ISO 9564-1.

Attributes

Attribute	Description
Tag ID	87
Tag length	n-byte
Data representation	n-2 (Packed binary coded decimal)
Justification	N/A
Required	Mandatory

Values

Value	Description
10	ISO PIN Block Format 0
14	ISO PIN Block Format 4

TAG 88 (Encrypted PIN Block)
DE 110, Dataset 01, TAG 88 (Encrypted PIN Block) contains PIN block encryption as defined in ISO 9564-1.

Attributes

Attribute	Description
Tag ID	88
Tag length	n-byte
Data representation	b-8 or b-16
Justification	N/A
Required	Mandatory

Values

Value	Description
8 bytes of PIN Block	Format 0
16 bytes of PIN Block	Format 4

TAG 89 (Additional Encrypted PIN Block)
DE 110, Dataset 01, TAG 89 (Additional Encrypted PIN Block) is used for PIN change transaction.

Attributes

Attribute	Description
Tag ID	89
Tag length	b-1
Data representation	b-8 or b-16
Justification	N/A
Required	Conditional

Values

Value	Description
8 bytes of additional PIN Block	Format 0
16 bytes of additional PIN Block	Format 4

Dataset 04 (Key Exchange)
Dataset 04 (Key Exchange) is a method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm.

Attributes

Attribute	Description	Value
Dataset ID	b-1	04
Dataset length	b-2	
Data representation	b...999; LLLVAR	
Data field contains	cryptogram	
Number of tags	6	
	TAG 80 (Control), Mandatory	
	TAG 81 (Key-set Identifier), Mandatory	
	TAG 83 (Algorithm), Mandatory	
	TAG 86 (Key Index), Mandatory	
	TAG 87 (Encrypted Data), Conditional	
	TAG 88 (Key Checksum Value), Mandatory	

Usage

Whether the data element is mandatory, conditional, optional, system-provided, or not required is noted for each applicable message.

Message	Org	Sys	Dst
Network Management Request/0800: PEK Exchange	•	X	C
Network Management Advice/0820: PEK Exchange	•	X	C

Application notes

Upon receipt of a network management advice message from the Single Message System, processors may begin to use the new working key delivered in the network management request message. The length fields in the TLV coding of the subfield is coded according to ISO 8825 if the TLV coded version of a dataset is used. The length of the dataset is always coded as a two byte binary value.

The check digit is in DE 110, Dataset 04, TAG 88 in the Network Management Advice/0820: PEK Exchange messages. Its presence is confirmation the key is loaded and ready for use.

TAG 80 (Control)
DE 110, Dataset 04, TAG 80 (Control) identifies the key management scheme and associated structure of the remainder of the data element.

Attributes

Attribute	Description
Tag ID	80
Tag length	b-1
Data representation	b-1
Justification	N/A
Required	Mandatory

Values

Value	Description
00	Default value for the Single Message Message System

TAG 81 (Key-set Identifier)
DE 110, Dataset 04, TAG 81 (Key-set Identifier) is a number that uniquely identifies a key-set.

Attributes

Attribute	Description
Tag ID	81
Tag length	b-1
Data representation	b-8
Justification	N/A
Required	Mandatory

Values

Value	Description
0000000000000000	Default value for the Single Message System

TAG 83 (Algorithm)
DE 110, Dataset 04, TAG 83 (Algorithm) defines the encryption algorithm used to encipher the keys contained in the associated key management data element.

Attributes

Attribute	Description
Tag ID	83
Tag length	b-1
Data representation	n-2 (Packed binary coded decimal)
Justification	N/A
Required	Mandatory

Values

Value	Description
01	Data Encryption Algorithm (DEA)
03	Triple Data Encryption Algorithm (TDEA)
05	Advanced Encryption Standard (AES)

TAG 86 (Key Index)
DE 110, Dataset 04, TAG 86 (Key Index) is used when multiple keys are identified with the same key set identifier; for example, key rotation.

Attribute	Description
Tag ID	86
Tag length	b-1
Data representation	n-2 (Packed binary coded decimal)
Justification	N/A
Required	Mandatory

Values

Value	Description
00	Default value for the Single Message System

TAG 87 (Encrypted Data)
DE 110, Dataset 04, TAG 87 (Encrypted Data) uses a structure within it before encryption to identify the data.

Attribute	Description
Tag ID	87
Tag length	n-byte
Data representation	b-8 to b-999; LLLVAR
Justification	N/A
Required	Conditional

Values

Hexadecimal values 0-9 and A-F, of the 64 bits of the new encryption key, encrypted under the current communications key.

TAG 88 (Key Checksum Value)
DE 110, Dataset 04, TAG 88 (Key Checksum Value) contains a value used to verify a conveyed key.

Attributes

Attribute	Description
Tag ID	88
Tag length	n-byte
Data representation	b-2 or b-3; LLLVAR
Justification	N/A
Required	Mandatory

Values

The key check value consists of the hexadecimal characters, 0-9 and A-F, of the calculated check value.

Edits

Mastercard will add new edits, modify existing edits, or remove existing edits to support this announcement.

Financial Transaction Request/0200
Single Message System edits for DE 110 (Encryption Data) are as follows:

When...	Then the Single Message System...
DE 110, Dataset 01 (PIN Encryption), TAG 89 (Additional Encrypted PIN Block) is not present for PIN change transaction	will decline the transaction with: • DE 39 (Response Code) is 30 (Format Error) • DE 44 (Additional Response Data) is 110 (indicating DE 110 is in error)

When...	Then the Single Message System...
DE 110, Dataset 01, TAG 89 is present for non-PIN change transaction	will decline the transaction with: • DE 39 (Response Code) is 30 (Format Error) • DE 44 (Additional Response Data) is 110 (indicating DE 110 is in error).
DE 110, Dataset 01, TAG 88 (Encrypted PIN Block) is not present for EBT transaction	will decline the transaction with: • DE 39 (Response Code) is 30 (Format Error) • DE 44 (Additional Response Data) is 110 (indicating DE 110 is in error).
DE 110, Dataset 01, TAG 88 is not present for PIN change transaction	will decline the transaction with: • DE 39 (Response Code) is 30 (Format Error) • DE 44 (Additional Response Data) is 110 (indicating DE 110 is in error).
DE 110, Dataset 01, TAG 88 is present, DE 22 (Point of Service Entry Mode) subfield 1 (POS Terminal PAN Entry Mode) is 09 and not a Cardless ATM transaction	will decline the transaction with: • DE 39 (Response Code) is 30 (Format Error) • DE 44 (Additional Response Data) is 110 (indicating DE 110 is in error)
DE 110, Dataset 01, TAG 88 is present and DE 22, subfield 1 (POS Terminal PAN Entry Mode) 03 and POS transaction	will decline the transaction with DE 39 (Response Code) is 58 (Transaction not permitted to acquirer or terminal).
the transaction is India domestic: • DE 22, subfield 1 is 91, requested amount is greater than 5000 INR, and • DE 110, Dataset 01, TAG 88 is not present	will decline the transaction with DE 39 (Response Code) is 05 (Do not honor).
the transaction is India domestic: • DE 22, subfield 1 is 07, requested amount is greater than 5000 INR, • CVM TAG 9F34 in DE 55 (Integrated Circuit Card [ICC] System-Related Data) is invalid, and • DE 110 Dataset 01, TAG 88 is not present	will decline the transaction with DE 39 (Response Code) is 05 (Do not honor).
the transaction is India domestic: • DE 22, subfield 1 is 02, 80, or 90, and • DE 110, Dataset 01, TAG 88 is not present	will decline the transaction with DE 39 (Response Code) is 05 (Do not honor).
the transaction is India domestic: • DE 22, subfield 1 is 05, • CVM TAG 9F34 in DE 55 is invalid, and • DE 110, Dataset 01, TAG 88 is not present	will decline the transaction with DE 39 (Response Code) is 05 (Do not honor).