AN 2117—Introducing Cryptographic Key Block Changes to Support Phase 2 of PCI Mandates

Generated on 25 October 2018

This PDF was created from content on the Mastercard Technical Resource Center, which is updated frequently. For the most current documentation, go to Mastercard Connect > Support.

AN 2117—Introducing Cryptographic Key Block Changes to Support Phase 2 of PCI Mandates

Mastercard is introducing changes to key exchange information to support recent Payment Card Industry (PCI) mandates.

Version History

The version history of this announcement is as follows.

Date	Description of Change	Where to Look
23 Oct 2018	Initial publication date	

At-A-Glance

The At-a-Glance table provides key information about the systems and groups affected by this announcement, action indicators that specify the appropriate action, and the required implementation date or dates.

Type:	Switching Release Announcement
Audience:	Acquirer, Issuer, Processor
	Each customer must determine the impact on its operations.
Brands:	Mastercard®, Debit Mastercard®, Maestro®, Cirrus®, Visa®, Mastercard Electronic™, U.K. Domestic Maestro, Plus®, Pulse®, NYCE®, STAR®, Interlink®
Release:	19.Q2
Region:	All
System:	Authorization, Single Message System
Action Indicator:	
	Network Mandate—Acquirer, Issuer
	Testing required—Acquirer, Issuer
Effective Date:	Dual Message System (Authorization): 12 April 2019 Single Message System: 12 April 2019

Overview

This overview provides information about the current environment and any applicable background information as it relates to this enhancement. This section also provides a brief explanation of what Mastercard is going to do to address this opportunity and the business drivers behind the enhancement.

The Payment Card Industry (PCI) Council mandated enforcement of new requirements pertaining to the storing of keys for later retrieval, for example, key cryptograms. The new restrictions stipulate customers must begin using structures called key blocks, which are immune to specific types of attacks and also restrict further key usage, in order to enhance security. The mandate stipulates customers must be fully compliant by June 2021.

©2018 MasterCard. Proprietary. All rights reserved.

Background

PCI PIN Security Requirements v2.0, published December 2014, introduced a new requirement to increase security for encrypted keys. Implementation of key blocks—sometimes referred to as "key bundling"—greatly improves the security of symmetric keys that are shared among payment participants to protect PINs and other sensitive data.

What Mastercard Is Currently Doing

Mastercard currently sends dynamic key exchange information to customers in DE 48 (Additional Data), subelement 11 (Key Exchange Data Block).

What Mastercard Is Going to Do

Mastercard is announcing changes to support the PCI mandate involving key exchange information storage using key blocks. In Release 19.Q2, Mastercard is introducing new values for DE 70 (Network Management Information Code) to allow customers to exchange keys for the new key block structure. In addition, Mastercard will begin using DE 110 (Additional Data -2) and two new subelements, 9 (ANSI X9 TR-31 Key Block Key) and 10 (Key Check Value) for customers to receive the new key block format information.

Why Mastercard Is Implementing These Enhancements

These enhancements will assist customers to be compliant with the PCI Council mandate by June 2021.

Related Documentation

Information relevant to this release announcement can be found in the following documents available on Mastercard Connect™.

Reference Materials

Refer to these reference manuals for information about the current state of Mastercard processing:

- X9 TR-31 Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms
- Cryptographic Key Blocks, June 2017
- Customer Interface Specification
- Single Message System Specifications

Note:

Manuals are updated with necessary changes after release implementation. Depending on timing, information provided in this release announcement may not yet be reflected in the manuals.

Customer Impact

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

©2018 MasterCard. Proprietary. All rights reserved.

Is Customer Action Required?

Attention warranted (Network mandate)—Acquirers and issuers must support the new subelements and values in the Network Management Request/0800—PEK Exchange, Network Management Response/0810—PEK Exchange and Network Management Advice/0820 messages by June 2021.

Prior to June 2021, customers can contact their Customer Implementation Support representative when they are prepared to receive the new PCI PIN encryption key exchange information in DE 110, subelements 9 and 10 or they can submit a Network Management Request/0800—PEK Exchange in DE 70 containing a value 163 (Solicitation for Encryption Key Exchange - TR-31 Keyblock).

Note:

Customers can continue receiving DE 48, subelement 11 (Key Exchange Data Block) until June 2021. Beginning in June 2021, only DE 110, subelements 9 and 10 will be used for PIN encryption key exchange processing.

Testing required—Mastercard requires that acquirers and issuers perform testing to support the enhancements in this announcement.

Transaction Message Flow Impacts

This announcement does not impact any transaction message flows.

Enhancements

Mastercard will introduce the following changes to support this announcement.

©2018 MasterCard. Proprietary. All rights reserved.

Dual Message System (Authorization)—Acquirer, Issuer

Mastercard will make the following changes to support this mandate:

- DE 70 (Network Management Information Code)
  - Add new value 163 (Solicitation for Encryption Key Exchange - TR-31 Keyblock) to the Network Management Request/0800—PEK Exchange and the Network Management Request Response/0810—PEK Exchange messages. Customers will use this value to indicate they are prepared to receive the PCI Key Exchange information.
  - Add new value 164 (Encryption Key Exchange Confirmation of Success) to the Network Management Advice/0820—PEK Exchange message for confirmation of a successful Key Exchange completion.
  - Add new value 165 (Encryption Key Exchange Advice of Failure) to the Network Management Advice/0820—PEK Exchange message for notification of a failed key exchange attempt.
- Add and define DE 110 (Additional Data—2) **which is currently reserved for ISO use**, with the following:
  - Add subelement 9 (ANSI X9 TR-31 Key Block Key)
  - Add subelement 10 (Key Check Value)

Single Message System—Acquirer, Issuer

Mastercard will make the following changes to support this mandate:

- DE 70 (Network Management Information Code)
  - Add new value 163 (Solicitation for Encryption Key Exchange - TR-31 Keyblock) to the Network Management Request/0800—PEK Exchange message and the Network Management Request Response/0810—PEK Exchange messages. Issuers will use this value to indicate they are prepared to receive the PCI Key Exchange information.
  - Add new value 164 (Encryption Key Exchange Confirmation of Success) to the Network Management Advice/0820—PEK Exchange message for confirmation of a successful Key Exchange completion.
  - Add new value 165 (Encryption Key Exchange Advice of Failure) to the Network Management Advice/0820—PEK Exchange message for notification of a failed key exchange attempt.
- Existing DE 110 (Additional Data—2)
  - Expand DE 110 to the ISO Standard: ans...999; LLLVAR
  - Add subelement 9 (ANSI X9 TR-31 Key Block Key)
  - Add subelement 10 (Key Check Value)

Implementation Scenarios

The following scenarios describe the different time frames and criteria to implement the PCI key exchange information mandate.

Implementation Scenarios

Three scenarios will be supported for this PCI mandate.

©2018 MasterCard. Proprietary. All rights reserved.

Scenario 1: Prior to Release 19.Q2:

- A customer can initiate the PIN encryption key exchange sequence by sending a Network Management Request/0800 message where DE 70 (Network Management Information Code) contains the value 162 (Solicitation for Encryption Key Exchange).
- Mastercard responds with a Network Management response/0810 message.
- Mastercard originates a Network Management Request/0800 message to initiate a PIN encryption key (sometimes referred to as the "working key") change with the customer. The message contains the following data:
  - DE 70 contains value 161 (Encryption Key Exchange)
  - DE 48, subelement 11 (Key Exchange Data Block) contains the Key Exchange Data Block
- The customer responds with a Network Management Request Response/0810 message, which contains the following data:
  - DE 39 contains value 00 if the response is an approval (if there is a problem then DE 39 contains value 96 indicating a denial)
  - DE 70 contains value 161 (Encryption Key Exchange)
  - DE 48 subelement 11 may be returned at customer's discretion,
- Mastercard completes the sequence by sending a Network Management Advice/0820 message to the customer, indicating confirmation of the PIN encryption key change. This message contains the following data:
  - DE 70 contains value 161 (Encryption Key Exchange)
  - DE 48 subelement 11 contains the first characters of the original subelement 11 up to the beginning of the actual key.

Note:

If the Network Management Request Response/0810 message indicated a denial, then the Network Management Advice/0820 message will not contain DE 48 and DE 70.

Scenario 2: After Release 19.Q2, but prior to June 2021:

- When the customer wants to initiate the PIN encryption key exchange sequence for the new PCI Key Block Structure Exchange Information, the customer sends a Network Management Request/0800 message where DE 70 (Network Management Information Code) contains value 163 (Solicitation for Encryption Key Exchange - TR-31 Keyblock).
- Mastercard responds with a Network Management Response/0810 message.
- Mastercard originates a Network Management Request/0800 message to initiate the PIN encryption key (this is sometimes referred to as the "working key"). The message contains the following data:
  - DE 70 contains value 161 (Encryption Key Exchange)
  - DE 110, subelement 9 (ANSI X9 TR-31 Key Block Key)
  - DE 110, subelement 10 (Key Check Value)
- The customer responds with a Network Management Request Response/0810 message, which contains the following data:
  - DE 39 contains value 00 if the response is an approval (if there is a problem then DE 39 contains 96 indicating a denial).
  - DE 70 contains value 161 (Encryption Key Exchange)
  - DE 110, subelement 10 may be returned at the customer's discretion

©2018 MasterCard. Proprietary. All rights reserved.

- Mastercard completes the sequence by sending a Network Management Advice/0820 message to the customer, indicating confirmation of the working key change. This message contains the following data:
  - DE 70 contains value 164 (Encryption Key Exchange Confirmation of Success) or value 165 (Encryption Key Exchange Advice of Failure)
  - DE 110 subelement 10 (Key Check Value)

Note:

Customers should begin using the new keys after they receive the Network Management Advice/0820 message. However, if the Network Management Advice/0820 message contains DE 70 value 165 (Encryption Key Exchange Advice of Failure), the customer must continue to use the current key.

Scenario 3: After implementation of Release 19.Q2 and prior to June 2021 the customer can revert back to receiving the key exchange information through DE 48, subelement 11 by sending a Network Management Request/0800 where DE 70 (Network Management Information Code) contains the value 162 (Solicitation for Encryption Key Exchange).

Refer to Scenario 1 for details on processing for scenario 3.

Platform Impact

The following table lists the impact of this announcement. For items that are marked √ (Yes), details are provided below.

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/Fees			
Reports			
Bulk Files			
Forms			
Quarterly Mastercard Reporting			
Transaction Investigator			
SAFE			

©2018 MasterCard. Proprietary. All rights reserved.

Topic	Dual Message System (Authorization)	Dual Message System (Clearing)	Single Message System
Single Message Transaction Manager			
250-byte Batch Data File			
80-byte Financial Institution Table File			

Authorization

Mastercard will update the Authorization Platform as follows.

CIS Data Element Definitions

Mastercard will update the following data elements to support this announcement.

DE 70—Network Management Information Code

DE 70 (Network Management Information Code) identifies network status.

Network Management Request/0800—PEK Exchange and Network Management Request

The following values apply to this message.

Code		Financial Network	MC	NP	VI	TE	MS	CI
163	=	Solicitation for Encryption Key Exchange - TR-31 Keyblock	√	√	√	√	√	√

Network Management Request Response/0810—PEK Exchange and Network Management Request Response

The following values apply to this message.

Code		Financial Network	MC	NP	VI	TE	MS	CI
163	=	Solicitation for Encryption Key Exchange - TR-31 Keyblock	√	√	√	√	√	√

Network Management Advice/0820—PEK Exchange

The following values apply to this message.

Code		Financial Network	MC	NP	VI	TE	MS	CI
164	=	Encryption Key Exchange Confirmation of Success	√	√	√	√	√	√
165	=	Encryption Key Exchange Advice of Failure	√	√	√	√	√	√

DE 110—Additional Data–2

DE 110 (Additional Data-2) is reserved for use based on product type.

©2018 MasterCard. Proprietary. All rights reserved.

Attributes

Data Representation:	ISO Standard: ans...999; LLLVAR Mastercard Standard: ans...999; LLLVAR
Length Field:	3 positions, value =...999
Data Field:	Contents of subelements 9-10
Subelements:	2
Justification:	See "Subelements"

Usage

Following is the usage of DE 110 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages.

Message	Org	Sys	Dst
Network Management Request/0800—PEK Exchange and Network Management Request	•	M	M
Network Management Request Response/0810—PEK Exchange and Network Management Response	O	M	•
Network Management Advice/0820—PEK Exchange	•	M	M

Application Notes

DE 110 provides supplemental data in a message when a specific ISO-designated data element is not available. It is a free-format, variable-length alphanumeric data element that may be used for multiple purposes. This data element's content may vary by program and service.

The following tables provide formats and descriptions for the subelements in DE 110. Currently, there are two subelements but as subelements are added, the subelement sequence will not have to be in the order of ID value.

Subelement 9—ANSI X9 TR-31 Key Block Key (128-bit Key Block Protection Key)

DE 110, subelement 9 (ANSI X9 TR-31 Key Block Key [128-bit Key Block Protection Key]) contains the attributes provided in a Network Management Request/0800 message.

	Attribute	Value
Subelement ID	n–2	09
Subelement Length	n–3	080
Data Representation	an–80	

Usage

Following is the usage of subelement 09 (whether it is mandatory, conditional, optional, or system provided) in applicable messages.

Message	Org	Sys	Dst
Network Management Request/0800 —PEK Exchange	•	M	M

©2018 MasterCard. Proprietary. All rights reserved.

Usage			
Network Management Request Response/0810—PEK Exchange	O	C	•
Network Management Request Advice/0820—PEK Exchange	•	•	•

Subelement 9—ANSI X9 TR-31 Key Block Key (192-bit Key Block Protection Key)

DE 110, subelement 9 (ANSI X9 TR-31 Key Block Key [192-bit Key Block Protection Key]) contains the attributes provided in a Network Management Request/0800 message.

	Attribute	Value
Subelement ID	n–2	09
Subelement Length	n–3	096
Data Representation	an–96	

Usage			
Following is the usage of subelement 09 (whether it is mandatory, conditional, optional, or system provided) in applicable messages.			
Message	**Org**	**Sys**	**Dst**
Network Management Request/0800—PEK Exchange	•	M	M
Network Management Request Response/0810—PEK Exchange	O	C	•
Network Management Request Advice/0820—PEK Exchange	•	•	•

Subelement 10—Key Check Value

DE 110, subelement 10 (Key Check Value) contains the attributes in a Network Management Request/0800 message.

	Attribute	Value
Subelement ID	n–2	10
Subelement Length	n–3	006
Data Representation	an–6	

Usage			
Following is the usage of subelement 10 (whether it is mandatory, conditional, optional, or system provided) in applicable messages.			
Message	**Org**	**Sys**	**Dst**
Network Management Request/0800 —PEK Exchange	•	M	M
Network Management Request Response/0810—PEK Exchange	O	C	•

©2018 MasterCard. Proprietary. All rights reserved.

Usage			
Network Management Request Advice/0820—PEK Exchange	•	M	M

Single Message System

Mastercard will update the Single Message System as follows.

Single Message System Data Element Definitions

Mastercard will update the following data elements to support this announcement.

DE 70—Network Management Information Code

The Single Message System uses DE 70 (Network Management Information Code) to identify network status. The Customer Processing System (CPS) may use Additional Data (DE 48) in conjunction with DE 70 to provide network status or control information.

Usage

This data element indicates the specific classification and purpose of network management (08xx) messages. It must be present in all network management (08xx) messages.

Following is the usage of DE 70 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages.

Message	Org	Sys	Dst
Network Management Request/0800—PEK Exchange and Network Management Request	M	X	•
Network Management Request Response/0810—PEK Exchange and Network Management Response	M	X	•
Network Management Advice/0820—PEK Exchange	•	X	C

Values

This table lists all Network Management Information Codes valid on the Single Message System.

Network Management Information Codes

Code	Description
163	Solicitation for Encryption Key Exchange - TR-31 Keyblock
164	Encryption Key Exchange Confirmation of Success
165	Encryption Key Exchange Advice of Failure

DE 110—Additional Data–2

DE 110 (Additional Data-2) is reserved for use based on product type.

©2018 MasterCard. Proprietary. All rights reserved.

Attributes

Data Representation:	ISO Standard: ans...999; LLLVAR Mastercard Standard: ans...999; LLLVAR
Length Field:	3 positions, value =...999
Data Field:	Contents of subelements 1-10
Subelements:	10
Justification:	See "Subelements"

Usage

Following is the usage of DE 110 (whether it is mandatory, conditional, optional, system provided, or not required) in applicable messages.

Message	Org	Sys	Dst
Network Management Request/0800—PEK Exchange and Network Management Request	C	•	M
Network Management Request Response/0810—PEK Exchange and Network Management Response	C	M	M
Network Management Advice/0820—PEK Exchange	C	•	M

Application Notes

DE 110 provides supplemental data in a message when a specific ISO-designated data element is not available. It is a free-format, variable-length alphanumeric data element that may be used for multiple purposes. This data element's content may vary by program and service.

The following tables provide formats and descriptions for the subelements in DE 110. There are ten subelements but as subelements are added, the subelement sequence will not have to be in the order of ID value.

Subelement 9—ANSI X9 TR-31 Key Block Key (128-bit Key Block Protection Key)

DE 110, subelement 9 (ANSI X9 TR-31 Key Block Key [128-bit Key Block Protection Key]) contains the attributes provided in a Network Management Request/0800 message.

	Attribute	Value
Subelement ID	n–2	09
Subelement Length	n–3	080
Data Representation	an–80	

Usage

Following is the usage of subelement 09 (whether it is mandatory, conditional, optional, or system provided) in applicable messages.

Message	Org	Sys	Dst
Network Management Request/0800 —PEK Exchange	•	M	M

©2018 MasterCard. Proprietary. All rights reserved.

Usage			
Network Management Request Response/0810—PEK Exchange	O	C	•
Network Management Request Advice/0820—PEK Exchange	•	•	•

Note:

For additional information customers should refer to the X9 TR-31 Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms specifications.

Subelement 9—ANSI X9 TR-31 Key Block Key (192-bit Key Block Protection Key)

DE 110, subelement 9 (ANSI X9 TR-31 Key Block Key [192-bit Key Block Protection Key]) contains the attributes provided in a Network Management Request/0800 message.

	Attribute	Value
Subelement ID	n–2	09
Subelement Length	n–3	096
Data Representation	an–96	

Usage			
Following is the usage of subelement 09 (whether it is mandatory, conditional, optional, or system provided) in applicable messages.			
Message	**Org**	**Sys**	**Dst**
Network Management Request/0800 —PEK Exchange	•	M	M
Network Management Request Response/0810—PEK Exchange	O	C	•
Network Management Request Advice/0820—PEK Exchange	•	•	•

Subelement 10—Key Check Value

DE 110, subelement 10 (Key Check Value) contains the attributes in a Network Management Request/0800 message.

	Attribute	Value
Subelement ID	n–2	10
Subelement Length	n–3	006
Data Representation	an–6	

©2018 MasterCard. Proprietary. All rights reserved.

Usage

Following is the usage of subelement 10 (whether it is mandatory, conditional, optional, or system provided) in applicable messages.

Message	Org	Sys	Dst
Network Management Request/0800 —PEK Exchange	•	M	M
Network Management Request Response/0810—PEK Exchange	O	C	•
Network Management Request Advice/0820—PEK Exchange	•	M	M

©2018 MasterCard. Proprietary. All rights reserved.