AN 4152 EMV 3DS Identity Check Insights Request Initiated with MDES Tokens

Type:
Bulletin Announcement

Category:
Operations

Audience:
Acquirer
Issuer
Processor

Region:
Global

Brand:
Mastercard®
Debit Mastercard®
Maestro®

Product or Service:
Digital Secure Remote Payment
Mastercard Digital Enablement Service

Action Indicator:
Program or service requirement

System:
Authorization
Single Message System

Published:
9 March 2021

Effective:
16 June 2020
21 July 2021

Executive Overview

As previously announced, EMV 3-D Secure (3DS) Mastercard® Identity Check™ Insights requests previously known as "Data only," allow merchants to submit EMV 3DS data to Mastercard without requesting issuer authentication. These Identity Check (IDC) Insights requests can be submitted with Mastercard Digital Enablement Service (MDES) tokens, therefore Mastercard is updating the data issuers will receive in this scenario.

Effective Date Details

Date	Details
16 June 2020	Dual Message System (Authorization) and Single Message System for MDES based Insights transactions
21 July 2021	Announcing IDC Insights (non-MDES) transactions with kX AAV generation

Customer Benefit

Identity Check Insights requests allow merchants to submit EMV[1] 3DS data without requesting issuer authentication. Mastercard runs all EMV 3DS transactions through Smart Authentication, Mastercard's Risk Based Authentication (RBA) model. Mastercard generates an authentication risk assessment in the existing Digital Transaction Insights security fields in authorization data element (DE) 48 (Additional Data—Private Use), subelement 56 (Security Services Additional Data for Issuers), subfield 1 (Security Services Indicator) and subfield 2 (Security Services Data) that issuers receive and may consider during their authorization decision process.

What Mastercard is Doing

Mastercard reminds customers that currently an EMV 3DS Identity Check Insights request can also be submitted with an MDES token. In this case, issuers receive additional authentication risk assessment data, and token authentication service results that further help them with the decisioning process within Authorization Request/0100 and Financial Transaction Request/0200 messages.

---

[1] EMV is a registered trademark or trademark of EMVCo LLC in the United States and other countries.

Version History

Date	Description of Change
9 March 2021	• Updated the language throughout to reflect past effective dates as needed • Announcing IDC Insights (non-MDES) transactions with kX AAV generation starting 21 July 2021. Refer to AN 4882 Introduction of Accountholder Authentication Values for Identity Check Insights and Non-Payment Transactions • Revised DSRP and AAV information in the What Mastercard is Doing table
16 June 2020	Initial Publication Date

MDES Updates

Mastercard is clarifying the security level indicator (SLI) that is applicable for an EMV 3DS Identity Check Insights request when submitted with an MDES token.

The following table represents consumer-initiated transactions only, as Identity Check Insights requests are currently not applicable to subsequent transactions, such as partial shipments or recurring payments.

WHEN the Authorization Platform receives a message containing...					THEN the Authorization Platform forwards...	
Program(s)	Primary Account Number (DE 2)	Cryptogram in UCAF field (DE 48, subelement 43) Or Digital Payment Data (DE 104, subelement 001)	Security Level Indicator (DE 48, subelement 42)	Digital Transaction Insight (DE 48, subelement 56, SF 1-2)*	Security Level Indicator (DE 48, subelement 42)	Liability Shift?
MDES and Identity Check Insights	MDES token	• Digital Secure Remote Payment (DSRP) cryptogram present in DE 104, subelement 001 • No AAV	214	Present	242 (When initiated via a device wallet)	Yes
					246 (When initiated via an e-commerce tokenization program associated with Wallet ID value 327)	No

		WHEN the Authorization Platform receives a message containing...				**THEN the Authorization Platform forwards...**	
Program(s)	**Primary Account Number (DE 2)**	**Cryptogram in UCAF field (DE 48, subelement 43) Or Digital Payment Data (DE 104, subelement 001)**	**Security Level Indicator (DE 48, subelement 42)**	**Digital Transaction Insight (DE 48, subelement 56, SF 1-2)***	**Security Level Indicator (DE 48, subelement 42)**	**Liability Shift?**	
MDES and Identity Check Insights	MDES token	• DSRP cryptogram present in DE 104, subelement 001 • AAV present with "kX" leading indicator in DE 48, subelement 43	214	Present	242 (When initiated via a Device Wallet)	Yes	
					246 (When initiated via an e-commerce tokenization program associated with Wallet ID value 327)	No	
MDES and ID Check Insights	MDES token	• No DSRP cryptogram present in DE 104, subelement 001 • AAV present with "kX" leading indicator in DE 48, subelement 43	214	Present	210 - Decline	No	

Program(s)	Primary Account Number (DE 2)	Cryptogram in UCAF field (DE 48, subelement 43) Or Digital Payment Data (DE 104, subelement 001)	Security Level Indicator (DE 48, subelement 42)	Digital Transaction Insight (DE 48, subelement 56, SF 1-2)*	Security Level Indicator (DE 48, subelement 42)	Liability Shift?
WHEN the Authorization Platform receives a message containing...				THEN the Authorization Platform forwards...		
MDES and ID Check Insights MDES token		• No DSRP cryptogram present in DE 104, subelement 001 • No AAV present with "kX" leading indicator in DE 48, subelement 43	214	Present	210 - Decline	No
Identity Check Insights Only	Primary Account Number (PAN not tokenized)	AAV present with "kX" leading indicator in DE 48, subelement 43	214	Present	214	No
Identity Check Insights Only	Primary Account Number (PAN not tokenized)	None	214	Present	214	No

Testing Recommended

Mastercard recommends testing for acquirers and issuers to support this bulletin.

Related Documentation

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

Announcements

Refer to these previously published announcements for more information:

- "AN 2479—Electronic Commerce Security Level Indicators for the Mastercard Identity Check Program"
- As communicated with Release 20.Q2 "AN 3363—Mandatory Use of Digital Payment Data Field for Remote Commerce Transactions with Cryptograms" Mastercard now requires acquirers to submit the DSRP cryptogram in DE 104 (Digital Payment Data), subelement 001 (Digital Payment Cryptogram)
- "AN 2122—Introduction of Mastercard Digital Transaction Insights Service" for more information about Digital Transaction Insights values
- Mastercard has introduced a non compliance Data Integrity Monitoring Program. Refer to "AN 4670 New Data Integrity Monitoring Program Edits for Digital Secure Remote Payment Cryptogram"
- "AN 4882 Introduction of Accountholder Authentication Values for Identity Check Insights and Non-Payment Transactions"

Questions

Customers with questions about the information in this announcement should contact Global Customer Service using the contact information on the Technical Resource Center.