AN 6996 Secure Card on File Overview

Type:
Bulletin announcement

Category:
Operations

Audience:
Acquirer
Digital activity customer
Issuer
Merchant
Processor
Network enablement partner

Region:
Global

Brand:
Mastercard®
Debit Mastercard®

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

Action Indicator:
Program or service requirement

System:
Authorization

Published:
24 January 2023

Effective:
24 January 2023

Executive overview

Mastercard previously announced Secure Card on File (SCOF), a product that enhances the electronic commerce (e-commerce) card-on-file (COF) tokenization proposition under an expanded scope of wallet identifier (WID), value 327. The scope of this bulletin announcement clarifies the standard set of foundational technical requirements for merchants, commerce platforms, payment service providers (PSPs), payment gateways, issuers, and acquirers. Mastercard has not changed the existing requirements for issuers to participate in WID value 327.

Effective date details

Date	Details
24 January 2023	The SCOF program is available for all new remote commerce tokenization implementations such as Mastercard Digital Enablement Service (MDES) for Merchants (M4M).

Customer benefit

The following list details benefits of the SCOF offering for token requestors, that is merchants, commerce platforms, PSPs, payment gateways, issuers, and acquirers:

- Connected e-commerce experience with other remote commerce use cases such as Click to Pay, benefiting from continuous enhancements on the Mastercard Secure Remote Commerce (SRC) platform
- Automated self-service onboarding through the Remote Commerce Onboarding and Registration Portal
- Commerce platform use cases with shareable tokens
- Transaction detail service (commerce platforms only)
- Token authentication framework

What Mastercard is doing

Mastercard is simplifying the remote commerce tokenization process with the SCOF offering, which leverages the SRC platform to provide value-added services for our customers and extend existing tokenization services that MDES powers such as M4M.

Date	Description of change
24 January 2023	Initial publication date

Token Requestor impact

Mastercard designed SCOF for the following use cases:

- Direct merchant: Eligible merchants integrate directly with SCOF application programming interfaces (APIs), enabling tokenization for primary account numbers (PANs) when used on a merchant website or mobile application.
- Commerce platforms: Eligible commerce platforms integrate directly with the SCOF APIs to facilitate e-commerce transactions through shareable tokens. These entities are primarily responsible for the following:
  – Managing commerce activities between consumers and merchants
  – Providing single sign-on services to the consumer at checkout
  – Storing and managing payment credentials on behalf of consumers
  – Sharing the token and pass payment credentials to integrated merchants, but are not directly involved in transaction processing
- On-behalf-of (OBO): PSPs provide tokenization services to merchants and commerce platforms and integrate with the SCOF APIs on their behalf.

Mastercard will provide existing customers using MDES for Merchants (M4M) with a migration path to transfer M4M credentials to SCOF.

Issuer impact

For issuers already supporting one or more remote commerce tokenization programs associated with WID value 327, Mastercard requires no new action or additional work.

Issuers should continue to use the standard set of foundational technical requirements as specified by the previously published bulletin announcements listed in the "Related information" section that follows:

- Issuers may continue to onboard for individual programs by following regional program requirements.
- Issuers may continue to process digitization requests and transactions for account ranges eligible for tokenization. Mastercard provides additional details in the *Remote Commerce Programs User Guide for Issuers* on the Technical Resource Center (TRC) on Mastercard Connect™.
- As the scope of WID, value 327, expands to support all remote commerce tokenization programs, the WID value does not uniquely identify a specific program as per AN 1021 Mastercard Digital Enablement Service for Merchants.
- Issuers can use token requestor ID (TRID) and consumer facing entity name (CFEN) to identify token requestors in remote commerce.

Existing announcements outlining issuer enrollment M4M across regions will also apply to SCOF. Refer to the following bulletin announcements for more details:

- AN 1551 Issuer Support to Mastercard Digital Enablement Service for Merchants in Latin America and the Caribbean Region
- AN 1557 Revised Mastercard Digital Enablement Service (MDES) Program Requirement for Issuers in the Canada and U.S. Regions
- AN 1735 Revised Mastercard Digital Enablement Service Program Requirement for Issuers in the Canada and U.S. Regions

- AN 2048 Issuer Enrollment in Mastercard Digital Enablement Service for Merchants in the Europe Region
- AN 2759 Issuer Enrollment in the Mastercard Digital Enablement Service for Merchants in the Middle East/ Africa Region

Related information

- AN 1001 Electronic Security Level Indicator Validation and Usage
- AN 1021 Mastercard Digital Enablement Service for Merchants
- AN 1121 Revised Standards Credential-on-File and Recurring Payments Transactions
- AN 1551 Issuer Support to Mastercard Digital Enablement Service for Merchants in Latin America and the Caribbean Region
- AN 1557 Revised Mastercard Digital Enablement Service (MDES) Program Requirement for Issuers in the Canada and U.S. Regions
- AN 1605 Mastercard Digital Enablement Service Enhancements to Support E-Commerce Transactions
- AN 1735 Revised Mastercard Digital Enablement Service Program Requirement for Issuers in the Canada and U.S. Regions
- AN 2031 Expanded Scope and Usage of Wallet Identifier, Value 327 Merchant Tokenization Program
- AN 2048 Issuer Enrollment in Mastercard Digital Enablement Service for Merchants in the Europe Region
- AN 2941 Digital Remote Commerce Enhancements
- AN 2058 Mastercard Secure Remote Commerce Program Requirement for Issuers in the U.S. Region
- AN 2687 Announcing Issuer Enrollment in MDES for Merchants in the Asia/Pacific Region
- AN 2759 Issuer Enrollment in the Mastercard Digital Enablement Service for Merchants in the Middle East/ Africa Region
- AN 3363 Mandatory Use of Digital Payment Data Field for Remote Commerce Transactions with Cryptograms
- AN 3942 MDES Issuer Guidance for Digital Remote Commerce Enhancements
- AN 3977 Mastercard Secure Remote Commerce Click to Pay Program Requirement for Issuers in the Canada Region
- AN 4037 Remote Commerce Acceptor Identifier Enhancements
- AN 4380 Secure Credential-on-File Tokenization for Commerce Platforms through Google Pay for the U.S. and Canada Regions
- AN 4564 Expanded scope and usage of wallet identifier for Commerce Platform Tokenization in the Europe region
- AN 4982 Revised Remote Commerce Acceptor Identifier Validation Service Results
- AN 5214 Transaction Detail Service Functionality Enabled for Secure Card-on-File Tokenization for Commerce Platforms for the U.S. and Canada Regions
- AN 5232 Mastercard Secure Card on File for Commerce Platforms Assigned Token Requestor ID Values
- AN 6566 Enhancing the Mastercard Digital Enablement Service Digital Payment Data Validation Service
- AN 6820 Mastercard Token Authentication Framework
- *Mastercard Secure Card on File*
- *Mastercard Secure Card on File Program Guide*
- *MDES Standard Token Implementation Plan for Remote Commerce Programs*
- *Remote Commerce Programs User Guide for Issuers*

Questions

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