



# Mastercard Digital Enablement Service

Issuer Implementation Guide

13 June 2019

# Summary of Changes, 13 June 2019

The Summary of Changes contains a list of updates made to this document since its previous release.

Description of Change	
Added the following changes to the card art image assets topic:	<a href="#">Card Art Image Assets</a>
<ul style="list-style-type: none"><li>Added a new section about <b>Vertical Cards</b></li><li>Added a note about replacing PDF file formats for <b>Card Art Image Assets</b> with SVG file formats</li><li>Added a note about the inclusion of <b>Program Identifiers</b></li></ul>	
The following <b>POS Entry Mode 10</b> changes were made: <ul style="list-style-type: none"><li>Added a note about legacy <i>POS Entry Mode 82</i></li><li>Replaced <i>POS Entry Mode 82</i> with <i>POS Entry Mode 10</i> in the note:</li><li>Added <i>POS Entry Mode 10</i> to the POS Entry Mode list</li></ul>	<ul style="list-style-type: none"><li><a href="#">Single Message and Dual Message Support</a></li><li><a href="#">Partial Shipments Recurring Payment Transactions</a></li><li><a href="#">Decision Matrix Structure</a></li></ul>
Removed all references to <b>Elliptic Curve Digital Signature Algorithm (ECDSA)</b>	<ul style="list-style-type: none"><li><a href="#">Issuer Initiated Digitization</a></li><li><a href="#">Appendix C Mastercard Key Certification Process</a></li></ul>
Added the correct timestamp format for <b>Tokenization Authentication Value (TAV)</b> generation	<a href="#">TAV Encoding and Examples</a>
Amended content in order to highlight best practice for handling <b>CVC 2 Verification</b>	<a href="#">CVC2 Verification</a>
Added a note about <b>MDES Transaction Data Service (TDS)</b> delivery time	<a href="#">Transaction Detail Service</a>
Added the following bulletin to <i>Related Publications</i> : <i>AN 2638—Digital Secure Remote Payment Liability Rules</i>	<a href="#">AN 2638—Digital Secure Remote Payment Liability Rules</a>

---

# Contents

<b>Summary of Changes, 13 June 2019.....</b>	<b>2</b>
<b>Chapter 1: Using this Guide.....</b>	<b>9</b>
Purpose, Scope, and Audience.....	10
Abbreviations and Acronyms.....	11
Related Publications.....	13
<b>Chapter 2: Introduction.....</b>	<b>19</b>
What is MDES?.....	20
MDES Participants and Interactions.....	21
Interactions and Activities for Device-Based Deployments.....	24
Interactions and Activities for Server-Based Deployments.....	26
MDES Features and Benefits.....	27
Supported Card Products.....	30
Mastercard APIs.....	30
<b>Chapter 3: Implementation.....</b>	<b>31</b>
Getting Ready for Digitization.....	32
Project Initiation.....	32
Issuer Enablement.....	32
Working with Processors.....	34
Issuer Enablement and Maintenance Processes.....	35
Access to the MDES Application.....	35
Testing with Mastercard.....	36
Mastercard Dual and Single Message System Release Enhancements.....	37
Wallet Provider Certification.....	38
Go-Live.....	38
Issuer Maintenance.....	39
Issuer Responsibilities.....	39
Token Implementation Plans.....	40
External Token Service Providers.....	40
Alternative Network Processing.....	41
Define and Implement Risk Management Policy.....	42
Merchant Tokenization.....	42
Maximum Number of Transaction Credentials.....	46
How Token Languages are Decided and Personalized.....	47

---

<b>Chapter 4: Pre-digitization.....</b>	<b>48</b>
What is Pre-digitization?.....	50
Example Cardholder Pre-digitization Experience.....	51
Pre-digitization Messages.....	52
Card Availability.....	59
Overview.....	59
Account Status Inquiry (ASI) Message.....	61
Tokenization Eligibility Request (TER) Message.....	61
Card Eligibility.....	66
Overview.....	66
Issuer-Initiated Digitization.....	71
TAV Creation.....	87
TAV Digital Signature Algorithm.....	88
TAV Digital Signature Generation.....	89
TAV Encoding and Examples.....	93
Card Eligibility Pre-digitization Message.....	96
Account Status Inquiry (ASI) Message.....	97
Tokenization Authorization Request (TAR) or Authorize Service Message.....	97
Providing an Alternate Account Identifier for a Token.....	104
Providing External Token Data.....	105
MDES Issuer Personalization Data.....	105
Checking the CVC 2, Expiration Date and Address.....	108
Eligibility Rules.....	109
About Rules and Rule Sets.....	110
Wallet Provider Account Data Elements and Scores.....	112
Pre-digitization Message Response Data Elements.....	115
Default Eligibility Decision.....	116
Cardholder Authentication and Token Activation.....	116
Overview.....	117
About Activation Methods.....	118
Issuer App Token Activation.....	121
Issuer App Token Activation via TAV.....	121
Issuer App Token Activation via Customer Service API.....	123
Activation by Activation Code.....	126
MDES Controls Activation Codes.....	127
Issuer Controls Activation Codes.....	129
Activation Code Notification (ACN) Message.....	130
Deliver Activation Code API Message.....	131
Validate Activation Code API Message.....	131
Activation by Call Center.....	132
Tokenization Completion.....	133

Overview.....	133
Tokenization Complete Notification (TCN) Message.....	134
Notify Service Activated API Message.....	137
Issuer-Initiated Digitization with MDES Token Connect.....	137
Consumer Experience.....	137
Benefits of Token Connect.....	139
Security Guidelines.....	139
Security Risks associated with MDES Token Connect.....	139
Consumer Login in Issuer's Interface.....	140
Device Binding.....	140
Issuer Callback URL.....	141
Card Eligibility Decision.....	142
Lifecycle Events.....	143
Tokenization Event Notification (TVN) Message.....	144
Notify Token Updated API Message.....	146
Cardholder-Initiated Token Deactivation for Apple Pay.....	146
Halting Digitization.....	146
Card Art Support and Associated Data.....	147
<b>Chapter 5: Token Management.....</b>	<b>149</b>
What is a Token?.....	150
Token Designation Service.....	151
<b>Chapter 6: Payment Account Reference (PAR).....</b>	<b>160</b>
What is PAR?.....	161
When Mastercard is the BIN Controller.....	161
When Mastercard is Not the BIN Controller.....	164
<b>Chapter 7: Provisioning.....</b>	<b>165</b>
What is the Provisioning Service?.....	166
Mastercard Provisioning Service Security for Secure Elements.....	167
<b>Chapter 8: Wallet Providers and Token Requestors.....</b>	<b>168</b>
What is a Token Requestor?.....	169
Token Requestor Functions.....	169
Token Requestor ID and Wallet ID.....	171
Token Requestor Models.....	172
<b>Chapter 9: Mastercard Cloud-Based Payments (MCBP).....</b>	<b>177</b>
User Experiences Supported by MCBP.....	178

Wallet Configurations Supported by MDES.....	185
Warning about MDES Security Controls for MCBP 2.0.....	187
<b>Chapter 10: Shared Cardholder Verification Method on a Cardholder-Owned Device.....</b>	<b>189</b>
What is Shared CVM?.....	190
Cardholder Verification Methods.....	190
How Shared CVM Works.....	193
Cardholder Experience at the Point of Sale.....	194
Security Considerations.....	194
Issuer Considerations.....	195
<b>Chapter 11: Digital Secure Remote Payment (DSRP).....</b>	<b>196</b>
Benefits for Issuers.....	198
DSRP Support.....	199
Partial Shipments, Recurring Payment Transactions and Incremental Authorizations.....	201
Implementation.....	202
<b>Chapter 12: Transaction Processing.....</b>	<b>203</b>
Benefits of Transaction Processing.....	204
Single Message and Dual Message Support.....	205
Transaction Detail Service.....	208
Alternative Routing Solution.....	210
<b>Chapter 13: Transaction Analysis.....</b>	<b>213</b>
What is Transaction Analysis?.....	214
Wallet Provider Options for Transaction Analysis.....	216
Issuer Options for Transaction Analysis.....	217
List of Real-Time Validations.....	218
Impact on the Issuer Decision Process.....	221
<b>Chapter 14: Affiliate Range Information.....</b>	<b>227</b>
Affiliate Range Identification and Maintenance Obligation.....	228
Affiliate Range Process.....	228
<b>Chapter 15: Fraud Information.....</b>	<b>233</b>
Chargeback Rights Associated with Tokenized and DSRP Transactions.....	234
Mobile Contactless Transactions.....	234
DSRP Transactions.....	236

Partial Shipments and Recurring Payment Transactions.....	236
<b>Chapter 16: Operational Management.....</b>	<b>238</b>
Customer Service Overview.....	239
Customer Support Model.....	240
Customer Service Tools.....	240
Customer Service Tools Functions.....	241
Issuer File Updates.....	242
Reporting.....	243
Changing Your Product Code.....	243
<b>Chapter 17: Testing Strategy.....</b>	<b>244</b>
Overview.....	245
Mastercard Test Facility Functions.....	246
Test Scripts—Dual and Single Message.....	246
Customer Service Tools Testing.....	246
Issuer Certification and Account PAN Whitelisting.....	247
<b>Chapter 18: Licensing.....</b>	<b>248</b>
Licenses and Agreements.....	249
<b>Appendix A: Token Transaction Flows.....</b>	<b>250</b>
<b>Appendix B: Transaction Analysis Technical Details.....</b>	<b>254</b>
Overview.....	255
Decision Matrix Structure.....	256
Fixed Values Defined by Mastercard.....	259
Default Decision Matrix.....	259
Test Result Codes.....	259
Values Depending on the Wallet User Experience.....	262
Decision Matrix.....	262
Test Result Codes.....	262
Default Values Configurable by the Issuer.....	264
Issuer Override for Cardholder Verification.....	264
Issuer Override for Fraud Control.....	265
Issuer Strengthened Control on Token Authentication to Terminal.....	266
Issuer Strengthened Control on Wallet Overrule.....	267
Test Result Codes for Cardholder Verification.....	267
Test Result Codes for Fraud Control.....	272
Test Result Codes for Token Authentication to Terminal.....	276

Test Result Codes for Wallet Overrule.....	276
<b>Appendix C: Mastercard Key Certification Process.....</b>	<b>278</b>
<b>Appendix D: Card Art and Associated Data for MDES.....</b>	<b>281</b>
Card Art Image Assets.....	282
Visual Appearance Assets.....	285
Display Text Assets.....	286
Issuer Mobile Banking App Assets.....	289
Transaction Detail Service Direct (TDS Direct) Assets.....	290
Wireframe for Card Background (Non-Combined Only).....	290
Mastercard Card Image Standards.....	291
Card or Account Reference Icon Standards.....	293
<b>Appendix E: Commercial Cards.....</b>	<b>294</b>
MDES and Commercial Enhanced Data.....	295
Processors.....	295
BIN Enablement.....	295
<b>Appendix F: MDES Register for Issuer Pre-digitization Network Message Values.....</b>	<b>296</b>
<b>Appendix G: Wallet Provider Tokenization Recommendations, Reasons, and Interpretation.....</b>	<b>304</b>
<b>Appendix H: Terminology.....</b>	<b>307</b>
<b>Notices.....</b>	<b>310</b>

## Chapter 1 Using this Guide

*This section describes the purpose of this guide, abbreviations, acronyms, and references to related publications.*

---

Purpose, Scope, and Audience.....	10
Abbreviations and Acronyms.....	11
Related Publications.....	13

## Purpose, Scope, and Audience

This guide helps Mastercard issuers understand and use the Mastercard Digital Enablement Service (MDES).

### Scope

This guide includes the following:

- MDES overview, key benefits, and features
- Issuer implementation activities, prerequisites, and responsibilities
- Dual Message System and Single Message System interface updates
- Pre-digitization stages and interactions, which determine whether a card can be digitized
- Provisioning process, where a device is provisioned with the tokenized payment credentials
- Token management and the Token Designation Service
- Payment Account Reference (PAR) support
- Mastercard Cloud-Based Payments (MCBP) user experiences and supported wallet configurations
- Cardholder Verification Methods (CVMs)
- Digital Secure Remote Payment (DSRP)
- Transaction processing, Transaction Analysis, and chargeback rules
- Customer Service Tools and available reports
- Issuer testing and certification processes
- Requirements for card art and associated Product Configuration data

**NOTE: The term ‘Wallet Provider’ is used throughout this guide and is generally equivalent to ‘Token Requestor.’**

### Audience

The following audiences should review this guide:

- Issuer and issuer processor business staff
- Issuer and issuer processor operations staff who need to understand the impact of MDES on their operational activities
- Issuer staff responsible for implementing system and process changes to support MDES

### How to Use this Guide

This guide supports issuer implementation and onboarding to an existing Wallet Program or service participating in MDES.

**NOTE: Issuers interested in building a Masterpass wallet, using the Masterpass Software Development Kits (SDKs) and functionality, should refer to the *Masterpass by Mastercard Wallet-Onboarding Guide*. Issuers interested in integrating their own wallet programs with MDES should refer to *MDES—Wallet Provider Implementation Guide*. Both guides are on the MDES Information Center on Publications in Mastercard Connect™ ([www.mastercardconnect.com](http://www.mastercardconnect.com)).**

Some of the diagrams in this guide show alternative paths depending on the digitization eligibility decision (whether digitization can proceed). These paths are color-coded as follows:

-  Approve
-  Approve, but require authentication
-  Decline

Mastercard provides updated versions of this guide when necessary. Readers should always ensure they are using the latest version, available on the MDES Information Center.

## Mastercard Contacts

For further information on MDES, contact your Mastercard representative.

## Abbreviations and Acronyms

---

The following abbreviations and acronyms are used in this guide.

Abbreviation	Description
AC	Application Cryptogram
ACN	Activation Code Notification
AID	Application Identifier
AIP	Application Interchange Profile
API	Application Programming Interface
ARPC	Authorization Response Cryptogram
ARQC	Authorization Request Cryptogram
ASI	Account Status Inquiry
ATC	Application Transaction Counter
AVS	Address Verification Service
CDCVM	Consumer Device Cardholder Verification Method
CIS	Customer Implementation Services
CMS	Credentials Management System
CVC	Card Validation Code

---

<b>Abbreviation</b>	<b>Description</b>
CVM	Cardholder Verification Method
CVR	Card Verification Results
DE	Data Element
DSRP	Digital Secure Remote Payment (formerly Chip Secured Remote Payment [CSRP])
EMV®	Europay, Mastercard, and Visa
HCE	Host Card Emulation
HVT	High-value transaction
IBAN	International Bank Account Number
IP	Internet Protocol
ISO	International Standards Organization
KDI	Key Derivation Index
LVT	Low-value transaction
MCBP	Mastercard Cloud-Based Payments
MCM	M/Chip Mobile (previously known as Mobile Mastercard PayPass)
MD	Mobile Device
MDES	Mastercard Digital Enablement Service
MMPP	see MCM (M/Chip Mobile)
MNO	Mobile Network Operator
MPA	Mobile Payment Application, which is also known as the wallet application
mPIN	Mobile Personal Identification Number
NFC	Near Field Communication
NIV	Network Interface Validation
ODA	Offline Data Authentication
OEM	Original Equipment Manufacturer
PAN	Primary Account Number (Account PAN)
PAR	Payment Account Reference
PDA	Personal Digital Assistant
POS	Point of Sale
QR	Quick Response Code
SE	Secure Element
SIM	Subscriber Identity Module

Abbreviation	Description
SP	Service Provider
SUK	Single Use Key
TAR	Tokenization Authorization Request
TAV	Tokenization Authentication Value
TCN	Tokenization Complete Notification
TEE	Trusted Execution Environment
TER	Tokenization Eligibility Request
TIP	Token Implementation Plan
TRID	Token Requestor ID
TSM	Trusted Service Manager
TSP	Token Service Provider
TVN	Tokenization Event Notification
TVR	Terminal Verification Results
UCAF	Universal Cardholder Authentication Field
UIICC	Universal Integrated Circuit Card
UMD	User and Mobile Device
WID	Wallet ID

---

## Related Publications

The following documents and resources provide information directly related to the subjects discussed in this guide.

**NOTE: Mastercard reserves the right to release new versions of documents referenced by this guide. Issuers should check for the latest documentation versions and the impacts of any amendments they contain when developing or updating their solutions.**

Unless specified differently, documentation referenced in this guide can be found on the MDES Information Center on Publications in Mastercard Connect™ ([www.mastercardconnect.com](http://www.mastercardconnect.com)).

### Reference Guides

The following resources provide information about different MDES implementation aspects.

Aspect	Title
Summary of feature updates and enhancements	<i>MDES—Platform Update</i> (for each release)
Overviews	<i>MDES Demo Video</i> <i>MDES Process Flow</i> <i>MDES—Implementation Quick Reference Guide</i> <i>MDES—Implementation Quick Reference eLearning</i>
Implementation	<i>MDES—Issuer Enablement</i> <i>MDES—Issuer Maintenance</i> <i>MDES—Baseline Configuration and Fraud Best Practices Guide</i> Various Token Implementation Plans
Pre-digitization API messages	<i>MDES Pre-Digitization API</i> <i>MDES Pre-Digitization API Pre-Warning Notice</i> (for each release)
Pre-digitization and transaction network messages	<i>MDES—Technical Specifications for Dual and Single Message Systems</i> <i>Customer Interface Specification</i> ** <i>Single Message System Specifications</i> **
Customer Service Tools	<i>MDES—Customer Service Application User Guide</i> <i>MDES—Customer Service Application Video Tutorials</i> <i>MDES Customer Service API</i> * <i>MDES Customer Service API Pre-Warning Notice</i> (for each release)
Reporting	<i>MDES—Issuer PortfolioAnalytics Reports</i>

\* The MDES Pre-Digitization API and MDES Customer Service API documentation is on the Mastercard Developers site (<https://developer.mastercard.com>).

\*\* These specifications are on Publications in Mastercard Connect™.

The following resources may also be of use:

- *DSRP—Acquirer Implementation Guide*
- *Mastercard Rules*
- *Transaction Processing Rules*

## MDES Apple Pay Reference Documents

There are resources available to issuers supporting Apple Pay.

The MDES Apple Pay reference documents are in the 'MDES – Apple' application in **My Apps** on Mastercard Connect™ ([www.mastercardconnect.com](http://www.mastercardconnect.com)). If the application is not there, it can be requested via **Store** if your Mastercard Connect Security Administrator has made it available to you. Access to the 'MDES – Apple' application will only be approved if your company has completed the MDES and Apple mandatory agreements.

### Announcements (Release Articles and Bulletins)

Mastercard previously notified customers of future MDES changes using release articles and bulletins. To enhance the way customers access this separate (but related) information, Mastercard is consolidating these release articles and bulletins into one communication type, known as 'announcements,' which are being added to the new Technical Resource Center; see Access to the Technical Resource Center.

The following announcements and release articles relate to MDES and are available in both the Technical Resource Center and the MDES Information Center (select **Release Articles**).

Release	Title
19.Q2	AN 2638—Digital Secure Remote Payment Liability Rules Change
18.Q4	AN 2031—Expanded Scope and Usage of Wallet Identifier, Value 327 Merchant Tokenization Program - 28 September 2018
18.Q3	<ul style="list-style-type: none"><li>• AN 1605—Mastercard Digital Enablement Service Enhancements to Support E-Commerce Transactions</li><li>• AN 1557—Revised Mastercard Digital Enablement Service (MDES) Program Requirement for Issuers in the Canada and U.S. Regions</li><li>• AN 2048—Issuer Enrollment in Mastercard Digital Enablement Service for Merchants in the Europe Region</li><li>• AN 1748—Revised Standards—Tokenization and DSRP for the Asia/Pacific Region</li><li>• AN 1551—Issuer Support to Mastercard Digital Enablement Service for Merchants in Latin America and the Caribbean Region</li><li>• "AN 1121—Revised Standards—Credential-on-File and Recurring Payments Transactions," March 2018</li></ul>
18.Q2	<ul style="list-style-type: none"><li>• AN 1103—Credential on File Indicator for Mastercard-Branded Transactions</li><li>• AN 1087—Support of Payment Transactions Using Tokens With or Without Cryptographic Data</li><li>• AN 1089—Mastercard Digital Enablement Service Enhancement for Decline Advices</li><li>• AN 1410—Additional Controls in Transaction Analysis</li></ul>

<b>Release</b>	<b>Title</b>
17.Q4	<ul style="list-style-type: none"> <li>• AN 1001—Electronic Commerce Security Level Indicator Validation and Usage</li> <li>• AN 1002—Miscellaneous Core Systems Updates</li> <li>• AN 1021—Mastercard Digital Enablement Service for Merchants</li> <li>• AN 1023—Enhancements to Payment Account Reference</li> <li>• AN 1039—MDES Enhancement to Support Masterpass Electronic Commerce Transactions</li> <li>• AN 1055—Mastercard Digital Enablement Service Alternate Account Identifier in Pre-Digitization Messages</li> </ul>
17.Q3	Global Security Bulletin No. 8, 15 August 2017
17.Q2	<ul style="list-style-type: none"> <li>• Global 534—Card Sequence Number in Mastercard Digital Enablement Service Transactions</li> <li>• Global 542—Mastercard Digital Enablement Service Enhancements Supporting New Transaction Analysis Capabilities and CVM Models for MCBP-Based Tokens</li> <li>• Global 594—Mastercard Support of Payment Account Reference</li> </ul>
16.Q4	<ul style="list-style-type: none"> <li>• Global 122—Integration of Automatic Billing Updater and Mastercard Digital Enablement Service</li> <li>• Global 517—Mastercard Support of Payment Account Reference in Messages</li> <li>• Global 535—Mastercard Digital Enablement Service New Action Required Indicator Values for PAN Mapping File Issuer File Update Requests—Reminder</li> <li>• Global 536—Mastercard Digital Enablement Service Issuer Token Personalization Data in Pre-Digitization Messages</li> <li>• Global 537—Mastercard Digital Enablement Service Declined Advice Enhancement for Suspended and Deactivated Device Tokens</li> <li>• Global 538—Point of Sale Card Data Terminal Input Capability Indicators for Digital Secure Remote Payment Transactions</li> </ul>
16.Q3	Global 528—Mastercard Digital Enablement Service New Action Required Indicator Values for PAN Mapping File Issuer File Update Requests
16.Q2	<ul style="list-style-type: none"> <li>• Global 581—Mastercard Digital Enablement Service Card on File Service Security Enhancements</li> <li>• Global 582—Mastercard Digital Enablement Service Data Enhancements</li> <li>• Global 585—Mastercard Digital Enablement Service: Single Token Account Range Assignment for Device and Card on File Tokens</li> <li>• Global 586—Mastercard Digital Enablement Service Point of Sale Entry Mode and Card Data: Input Mode</li> <li>• Global 587—Digital Secure Remote Payment Enhancement</li> <li>• Global 588—Mastercard Digital Enablement Service Pre-and Post-Digitization Messages Clarifications</li> <li>• U.S. 410—Maestro Switching of Visa Tokenized Transactions</li> </ul>
16.Q1	<ul style="list-style-type: none"> <li>• Global 579—Mastercard Digital Enhancement Service Support of Purchasing Cards</li> <li>• Global 580—Mastercard Digital Enablement Service—Dynamic Magnetic Stripe Data</li> </ul>

<b>Release</b>	<b>Title</b>
15.Q4	<ul style="list-style-type: none"> <li>• Global 450—Mastercard Digital Enablement Service Pre- and Post-Digitization Messages Enhancements for Maestro</li> <li>• Global 590—Mastercard Digital Enablement Service Transaction Details Service Enhancement</li> <li>• Global 591—Digital Secure Remote Payment Enhancements—Reminder</li> <li>• Global 592—Mastercard Digital Enablement Service Token Requestor ID</li> <li>• Global 593—Mastercard Card on File Tokenization Service Enhancement</li> <li>• U.S. 455—Maestro Switching of Visa Tokenized Transactions</li> </ul>
15.Q3	<ul style="list-style-type: none"> <li>• Global 130—Mastercard Digital Enablement Service Report Enhancements</li> <li>• Global 595—Mastercard Digital Enablement Service Support for Maestro and Consumer Prepaid Cards</li> <li>• Global 596—Mastercard Digital Enablement Service Renaming of Activation Code Distribution Method Fields and Positions</li> </ul>
15.Q2	<ul style="list-style-type: none"> <li>• Global 530—Mastercard Digital Enablement Service Enhancements</li> <li>• Global 570—Digital Secure Remote Payment Enhancements</li> <li>• Global 572—Mastercard Digital Enablement Service Cloud-Based Payments—Reminder</li> <li>• Global 573—Mastercard Digital Enablement Service Pre- and Post-Digitization Messages Enhancements</li> </ul>
15.Q1	<ul style="list-style-type: none"> <li>• Global 350—Mastercard Digital Enablement Service Clearing Processing for Suspended/Deactivated Tokens</li> <li>• Global 516—Mastercard Digital Enablement Service Implementation of Request/Response and Advice Messages—Reminder</li> <li>• Global 571—Mastercard Digital Enablement Service Cloud-Based Payments</li> </ul>
14.Q4	<ul style="list-style-type: none"> <li>• Global 597—Enhancements to Mastercard Digital Enablement Service</li> <li>• Global 598—Addition of ATC Validation for the Mastercard Digital Enablement Service and M/Chip Cryptogram Validation Services</li> </ul>
14.Q3	Global 550—Enhancements to Mastercard Digital Enablement Service
14.Q2	Global 510—Enhancement to Mastercard Digital Enablement Service
14.Q1	Global 501—Enhancement to Mastercard Digital Enablement Service
13.Q4	Global 561—New Digital Enablement Service

**NOTE: The content in this implementation guide is intended to support functionality defined through Release 18.Q1. Subsequent functionality, changes, and enhancements to future releases are incorporated into this guide during bi-annual updates of the core Dual Message System and Single Message System manuals aligned with release implementations.**

Announcements are currently available in the Technical Resource Center ([new](#)).

**NOTE: To access the Technical Resource Center:**

- Log into Mastercard Connect.
- Click Support.
- Select Technical Resource Center.
- Enter your search text (preferably the full title of the document) in the Title Search pane and press Enter.
- If you have entered the details correctly and if your document exists in the portal, it will be displayed on the screen, along with a list of related documents, in some cases. Select the document you want to view by clicking the appropriate document link from the list. It will open in a new window.

---

## Chapter 2 Introduction

*This section introduces MDES.*

---

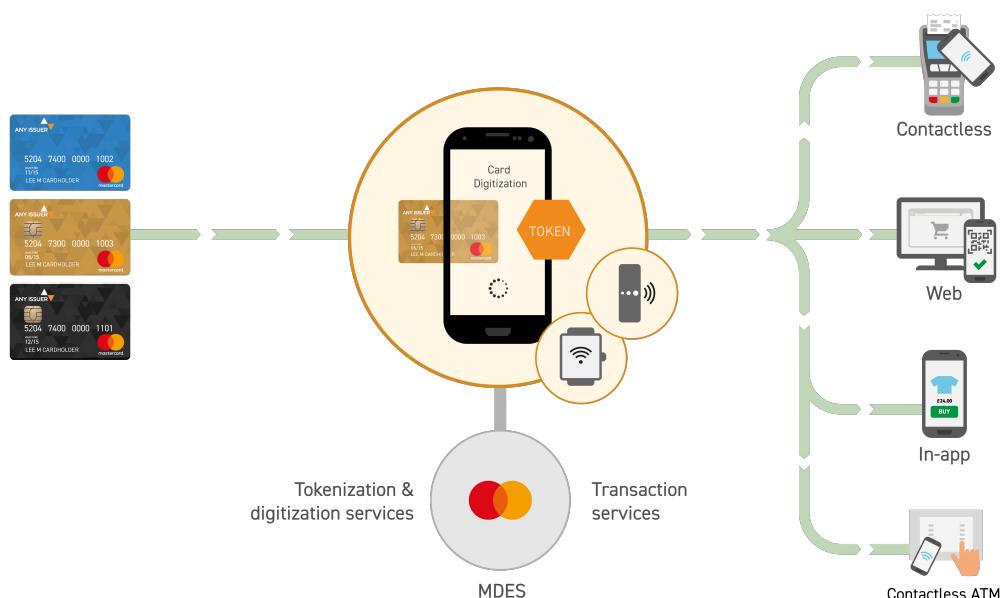
What is MDES?.....	20
MDES Participants and Interactions.....	21
Interactions and Activities for Device-Based Deployments.....	24
Interactions and Activities for Server-Based Deployments.....	26
MDES Features and Benefits.....	27
Supported Card Products.....	30
Mastercard APIs.....	30

## What is MDES?

The Mastercard Digital Enablement Service (MDES) is a secure, globally-scalable digitization service for generating and provisioning digital payment credentials into mobile devices, smart wearables, PCs, and other form factors.

MDES enables a simpler, more secure digital payment experience by tokenizing cardholders' PANs. Tokenization replaces a PAN with a unique payment token (an alternative number) that is specific to the platform or entity that will use the token, such as a particular wallet application on a particular device. Digitization provisions the token to the target platform or device so it can be used instead of the PAN to perform financial transactions, including contactless payments (using an NFC-enabled device), web and in-app purchases.

**Figure 1: MDES—Digitization for Different Payment Methods and Devices**



The cardholder's PAN is not used in token transactions, reducing the possibility and impact of account data compromise. If a device is lost or stolen, only the tokens created for that device need to be replaced; the physical card can still be used. If a token is somehow intercepted, it cannot be used for payments because a token can only be used by the device to which it was provisioned.

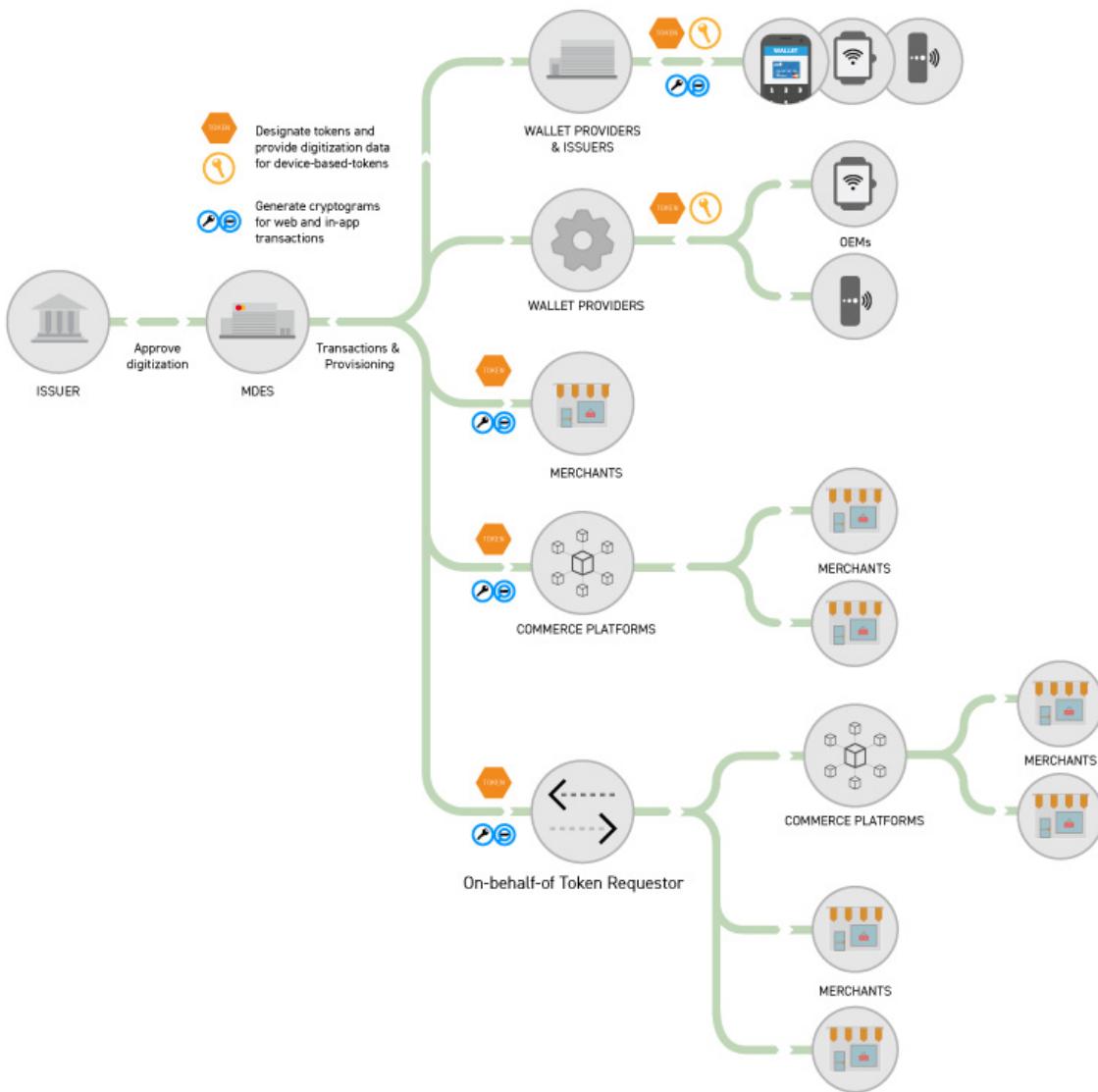
MDES is a single integrated platform for issuers, Wallet Providers, merchants, and other Token Requestors, and enables the digitization of supported Mastercard card types for many digital payment methods. The MDES end-to-end services are supported by the reliability and global reach of the Mastercard Network.

## MDES Participants and Interactions

MDES connects Wallet Providers, Token Requestors and Mastercard issuers (who can also be Wallet Providers).

Token Requestors integrate with MDES to request tokens for Mastercard payment cards, which can be used for digital payments (token transactions). Example Token Requestors:

- **Issuers** and **Wallet Providers**, who provide wallet applications for cardholders to digitize their cards and make digital payments via existing contactless technology and other point-of-sale (POS) systems, and via new remote payment methods such as app-to-app payments. Wallet Providers can provide wallets for their own devices (such as smart phones, smart watches and fitness bands) or partner with device manufacturers (OEMs).
- **MERCHANTS**, who digitize the consumer Account PANs stored on their servers, so they can use tokens and cryptograms for browser-based e-commerce and in-app transactions.
- **Commerce Platforms**, which offer users goods and services from third-party merchants, and digitize users' Account PANs so that tokens and cryptograms are used for transactions.
- **On-Behalf-of Token Requestors (OBOTRs)**, who initiate and request tokenization of consumers' Account PANs on-behalf of merchants and/or commerce platforms, so that tokens and cryptograms are used for transactions.



Issuers can benefit from connectivity to participating Wallet Providers and Token Requestors, so their Mastercard cards can be digitized for existing and emerging digital payment methods. Mastercard is the trusted partner, managing the integration between the parties.

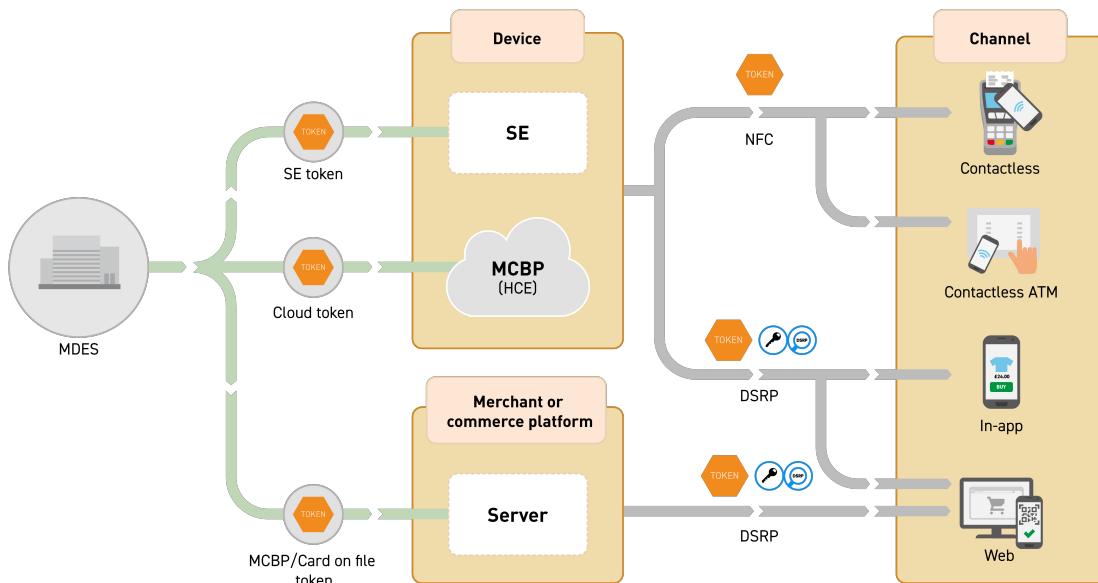
During issuer enablement (service setup), issuers choose the wallet programs they want to support and control how their Mastercard cards are digitized by providing Product Configurations and settings specific to each program. Mastercard works with issuers and Wallet Providers to help ensure that implementations work as expected.

**NOTE: Issuers who support the MDES for merchants program are automatically integrated with all merchants using that program. Effective 1 September 2018, Mastercard require all North America issuers using MDES to process digitization requests and transactions for MDES for merchants across all portfolios eligible for tokenization.**

## Provisioning Models

MDES tokens can be provisioned to a range of devices and platforms. As the following diagram shows, different types of tokens can be digitized to several targets, such as a device's Secure Element (SE), a Mastercard Cloud-Based Payments (MCBP) application, and a server. Depending on the deployment, the provisioned tokens can be used for contactless transactions (using NFC) or Digital Secure Remote Payment (DSRP) transactions.

**Figure 2: Provisioning Models**



**NOTE: Samsung Pay also supports Dynamic Magnetic Stripe Data (DMSD), which allows payments at terminals that only have a magnetic stripe reader.**

MDES token transactions use the existing payments infrastructure. The transaction message sent to the acquirer includes the token and a cryptogram (for DSRP), instead of the Account PAN. Mastercard token transactions are routed through the Mastercard Network, where MDES validates them and maps the tokens back to the Account PANs for authorization by the issuer.

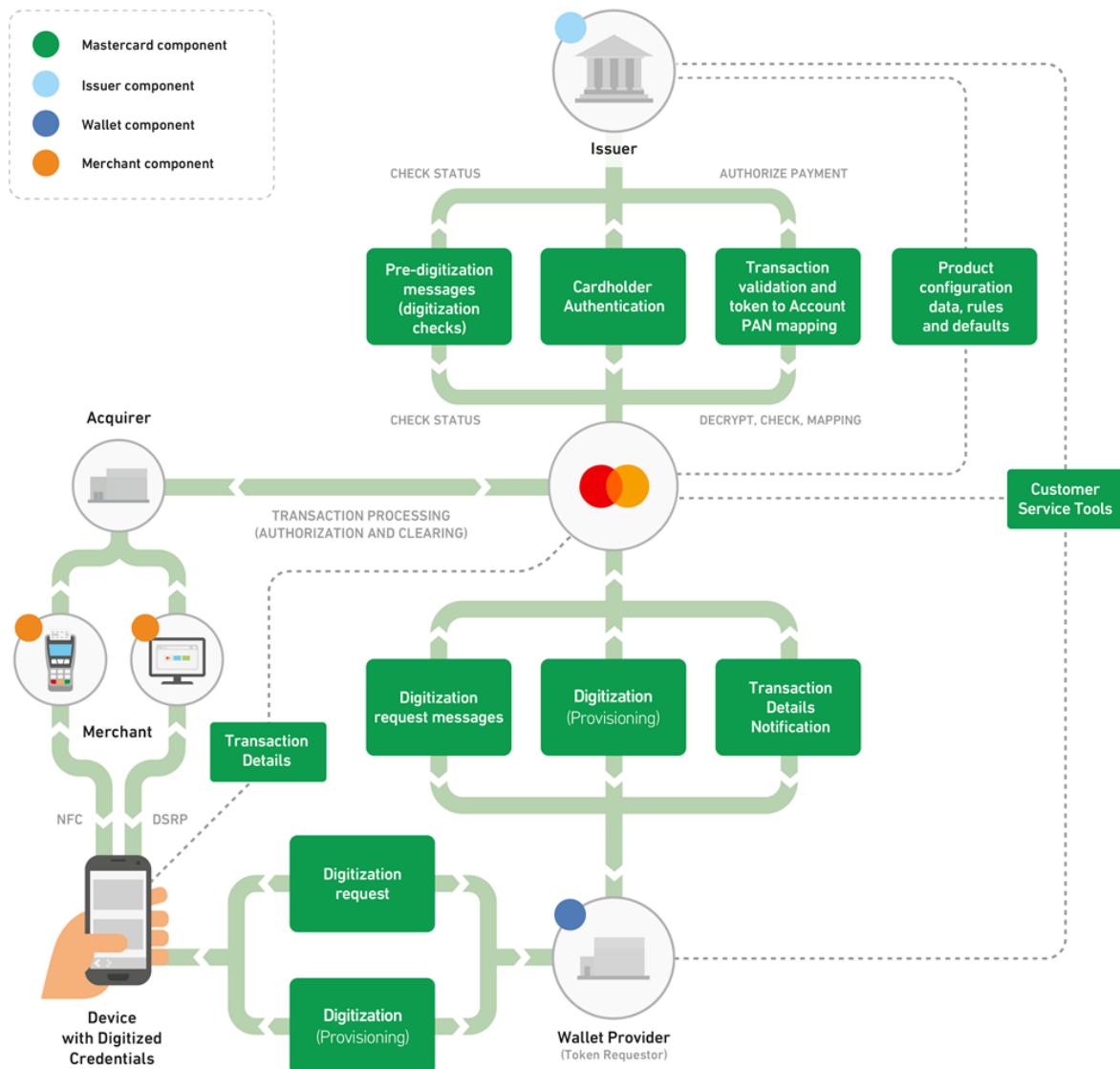
**NOTE: For more information, refer to the Token Management chapter.**

**NOTE: For information on MCBP and DSRP, refer to those chapters.**

## Interactions and Activities for Device-Based Deployments

For device-based wallets, the cardholder typically initiates the digitization of their payment card, and the token and payment credentials are provisioned to the device.

The following diagram shows the relationship between the main MDES participants.



### Issuer/Issuer Processor:

- Specifies the account ranges within Bank Identification Numbers (BINs) that are available for digitization, and provides related Product Configuration data (such as card art and cardholder Terms and Conditions)
- Configures rules and interacts with MDES during each digitization request, via pre-digitization messages, to determine whether the digitization can occur; issuers may decide that additional cardholder authentication is required before a token is activated

- Authorizes or declines the token transactions that have been validated by MDES
- Uses the MDES Customer Service Tools to address cardholder queries and manage the lifecycle of their cardholders' tokens, such as suspending and deactivating them

**Wallet Provider (Token Requestor):**

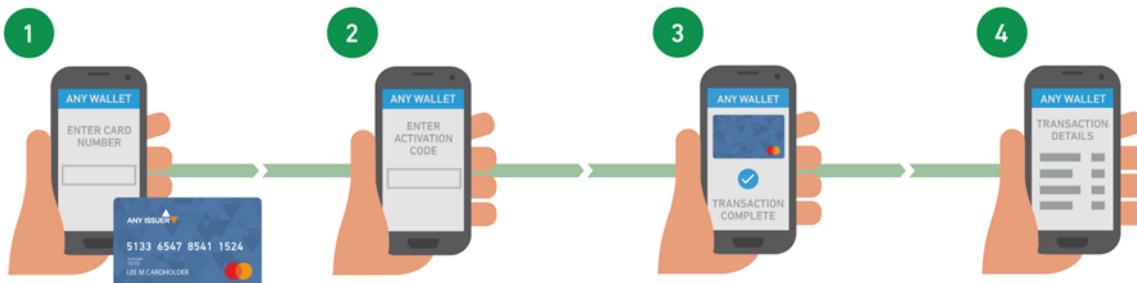
- Provides a wallet application that enables cardholders to request card digitization, validate their identity (if required by the issuer), and use their digitized cards for payments
- Sends cardholder digitization requests to MDES
- (Depending on the implementation) Provisions the token and payment credentials to either:
  - The device's SE, via the Secure Element Issuer Trusted Service Manager (SEI TSM)
  - A Credentials Management System (CMS) that provides keys to a Mastercard Cloud-Based Payments (MCBP) application in a device or on a server

**MDES:**

- Stores the issuer's Product Configurations and makes its card art and related textual data available to Wallet Providers, via the Mastercard Card Image Repository
- Facilitates the digitization requests, passing the required data between the Wallet Provider and the issuer
- Allocates a unique token to replace a cardholder Account PAN
- Prepares the provisioning package for sending the token (and associated credentials and data) to the target device
- Validates each Mastercard token transaction and cryptogram (if used), applies token controls, and maps the token back to the Account PAN before forwarding the transaction to the issuer for authorization
- Notifies the Wallet Provider that cardholder transaction details are available, and delivers them directly to the device or solution

**Cardholder**—Activities depend on the type of device and the deployment, for example:

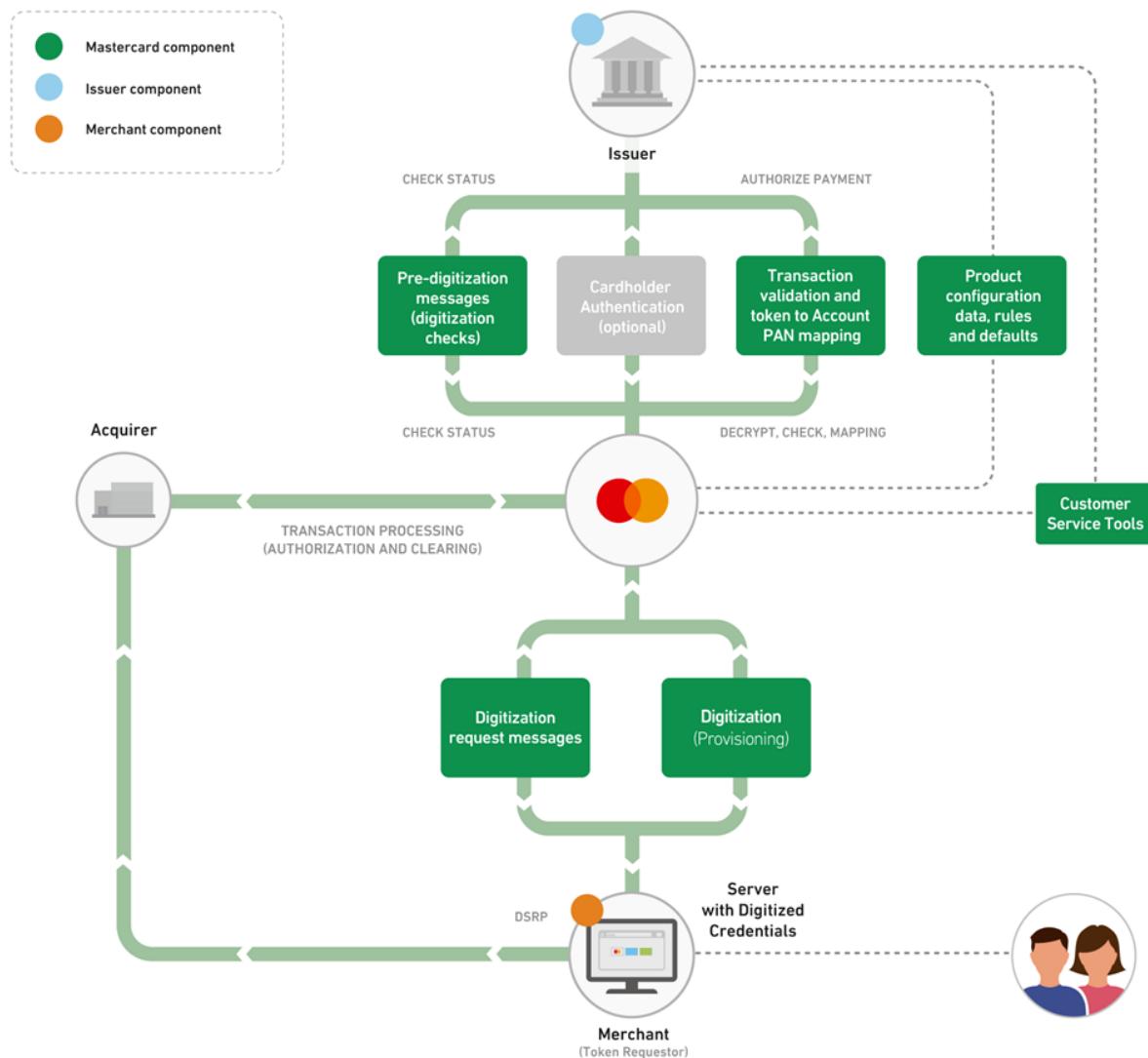
1. Requests digitization of their payment card, agreeing to the issuer's Terms and Conditions.
2. (If required by the issuer) Enters the Activation Code sent to them, to validate their identity. This is just one of the Activation Methods that the issuer may choose to provide.
3. Makes payments, selecting the required digitized card.
4. Views details of their MDES token transactions (such as the merchant name and transaction amount).



## Interactions and Activities for Server-Based Deployments

For server-based implementations, the token and payment credentials are provisioned to a server. An example is the MDES for merchants program, where merchants use MDES to tokenize the consumer Account PANs stored on their servers. The merchants initiate the digitization; the cardholders might not be present or aware of it happening.

The following diagram shows the relationship between the main MDES participants.



**Issuer/Issuer Processor**—Activities are similar to those for a device-based wallet implementation, except that cardholder authentication is optional because the cardholder might not be present during digitization. The provisioned token is activated automatically.

### Merchant (Token Requestor):

- Requests digitization of its consumers' Account PANs and stores the tokens securely
- Requests and securely stores cryptograms from MDES

- (Optional) Uses the issuer's card art (supplied by MDES during digitization) to show a representation of the digitized card to the cardholder
- When a cardholder initiates a transaction, uses the cardholder's token (instead of their Account PAN) and cryptogram and uses them to send a token DSRP transaction to the acquirer or payment processor for authorization

**MDES**—Activities are similar to those for a device-based wallet implementation, except that cardholder transaction details are not delivered to the merchant.

**Cardholder**—Activities depend on the merchant application and the type of device used to access it, for example:

1. Logs into the merchant application, validating their identity.
2. Selects goods or services and makes payment using the card digitized by the merchant.
3. Is notified of the transaction outcome.



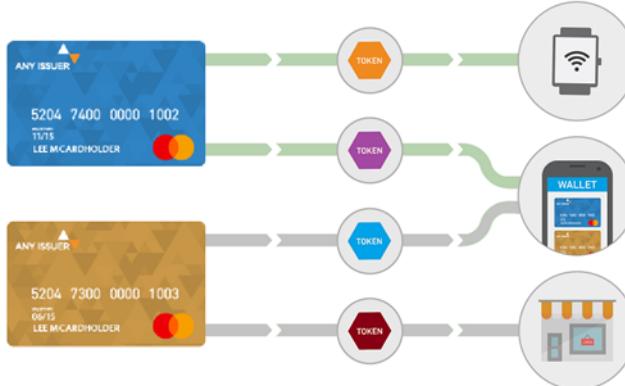
## MDES Features and Benefits

Mastercard issuers can use MDES to digitize their cardholder credentials without needing to build their own tokenization and digitization platforms. The MDES platform provides all the required digitization and transaction services, and connectivity to all participating Wallet Providers and Token Requestors.

### Features for Issuers

MDES features include the following.

Feature	Description
Flexible Product Configurations	Issuers can define different digitization parameters and defaults for each wallet program they support, including: <ul style="list-style-type: none"><li>• The account ranges that are available for digitization</li><li>• The card art and cardholder Terms and Conditions to be used</li><li>• Eligibility rules and default digitization decisions</li><li>• Default Activation Methods, if cardholder authentication is required prior to digitization</li></ul>

Feature	Description
Pre-digitization Messages	<p>Issuers can choose to receive enhanced network messages and/or web service (API) messages from MDES for each digitization request. These messages provide data that an issuer can use to determine whether it wants to permit the digitization.</p>  <p>For device-based wallets, issuers may decide that additional cardholder authentication is required before a token is activated, and they can supply different Activation Methods to MDES.</p>
Tokenization	<p>MDES allocates a unique token and generates a cryptographic key for each tokenization request. The token and key are specific to the platform or instance, such as a particular wallet application on a particular device. When Account PANs are tokenized for different applications, devices or programs, MDES issues different tokens and keys for each target.</p> 
	<p>The Mastercard Token Designation Service manages the availability and lifecycle of each token.</p>
Digitization	<p>MDES prepares the provisioning package, generating the cryptographic keys, personalization scripts and data for provisioning the token to the target, such as a device's SE, an MCSP application, or a secure server.</p>
Card Image Repository	<p>Mastercard manages the repository of issuer card art and related textual data, which are to be used by Wallet Providers within their user interfaces (according to the issuer's Product Configurations).</p>

Feature	Description
Transaction Processing Service	<p>This Mastercard service validates each token transaction, applies token controls, and maps the token to the Account PAN before forwarding the transaction to the issuer for authorization. The PAN is mapped back to the token when the authorization response is sent to the acquirer.</p>  <p>MDES uses cryptographic keys for EMV® and Card Validation Code 3 (CVC 3) verification. Mastercard generates and stores these keys for the token account ranges.</p>
Customer Service Tools	<p>The Mastercard Customer Service Application and Customer Service API are available for issuers to help their representatives or agents address cardholder queries and tokenization issues. Issuers can use the Mastercard application or integrate their own application with the API. For more information, see the Customer Service Tools section.</p> <p>The Customer Service Application is also available to Wallet Providers, with limited functionality, to assist visibility and investigations.</p>
Reporting Tools	Several MDES reports are available for issuers, which provide data about different aspects of the issuer's MDES implementation, such as the Wallet Providers servicing their account ranges, tokenization counts, and transaction activity.

## Benefits to Issuers

MDES offers many benefits to issuers, including the following:

- A range of business services for the complete end-to-end implementation of an issuer's tokenization and digitization requirements
- Tokenization and digitization performed as services, so issuers are not burdened with significant upfront and ongoing investment (in costs and time)
- A quick way to make an issuer's card account ranges available for digital payments through multiple Wallet Providers
- A single point of management where Mastercard handles integration and communication with the Wallet Providers and provisioning components
- A reduced time-to-market for issuers to roll out new digital device-based payment solutions to their cardholders
- Support of EMV/Chip requirements, delivering security and reduced fraud of chip-based payment processing for digitized cards

## Supported Card Products

MDES supports the digitization of existing card accounts and can tokenize Mastercard and Maestro-branded Account PANs.

Supported card products:

- Consumer debit, credit and prepaid
- Small Business cards
- Commercial cards

*Support for Mastercard Multicard, Mastercard Commercial Fleet (MCF) and Mastercard Government Fleet (MGF) product types:* Tokens will not support merchant POS systems prompting for additional data required by Fleet cards. Therefore, issuers must inform cardholders they will still need to present their cards at merchant POS terminals that require prompting.

Issuers and Digital Activity Customers (DACS) wishing to use MDES and MCBP for non-Mastercard branded transactions (co-brand/Private Label) are required to sign a separate commercial agreement with Mastercard.

MDES can only allocate the Card on File token type (used for server-based tokens) for Mastercard consumer product and acceptance brands, and Debit Mastercard. Contact your Mastercard representative for more information.

## Mastercard APIs

---

Several Mastercard APIs are useful to MDES issuers.

API	Purpose
MDES Pre-Digitization API	Interact with MDES during digitization and tokenization requests
MDES Customer Service API	Perform Customer Service activities
Payment Account Management API	Perform account-related operations across Mastercard services

These APIs are accessed through the Mastercard Developers site (<https://developer.mastercard.com>).

For APIs relevant to issuer wallet interactions with MDES, refer to the *MDES—API Specification* on the MDES Information Center on Publications in Mastercard Connect™ ([www.mastercardconnect.com](http://www.mastercardconnect.com)).

## Chapter 3 Implementation

*To participate in MDES, issuers must meet prerequisites and complete implementation activities.*

---

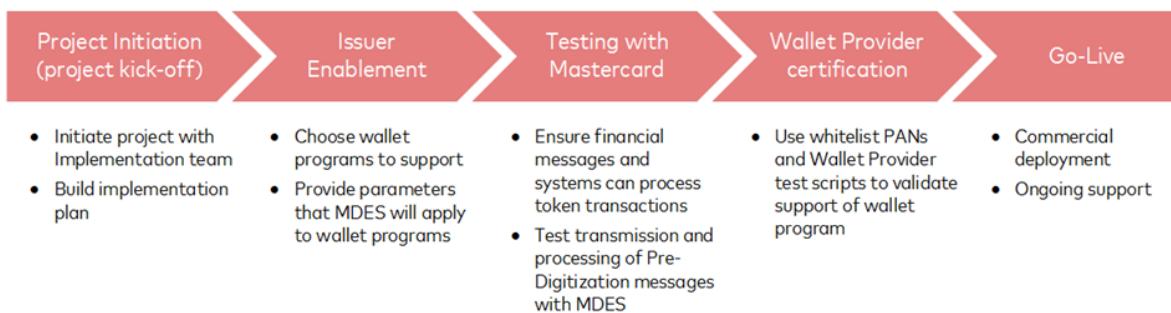
Getting Ready for Digitization.....	32
Project Initiation.....	32
Issuer Enablement.....	32
Working with Processors.....	34
Issuer Enablement and Maintenance Processes.....	35
Access to the MDES Application.....	35
Testing with Mastercard.....	36
Mastercard Dual and Single Message System Release Enhancements.....	37
Wallet Provider Certification.....	38
Go-Live.....	38
Issuer Maintenance.....	39
Issuer Responsibilities.....	39
Token Implementation Plans.....	40
External Token Service Providers.....	40
Alternative Network Processing.....	41
Define and Implement Risk Management Policy.....	42
Merchant Tokenization.....	42
Maximum Number of Transaction Credentials.....	46
How Token Languages are Decided and Personalized.....	47

## Getting Ready for Digitization

The issuer implementation activities for MDES are the same regardless of whether issuers use a service provider to perform their card processing or keep it in-house.

Mastercard works with issuers during MDES implementation and engages as needed when there are updates to MDES. Mastercard is committed to providing MDES marketing materials and standard release documentation.

MDES implementation typically has five main stages:



**NOTE: The actual stages and tasks may vary, depending on the implementation plan.**

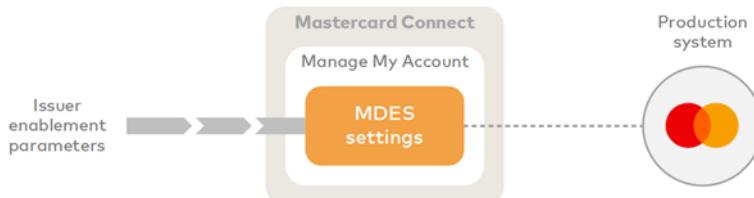
### Project Initiation

During this stage, the issuer gets in touch with the Mastercard regional office to initiate an MDES project with the Mastercard Customer Implementation Services (CIS) team. The CIS team explains the implementation process and builds a mutually-agreed implementation plan.

### Issuer Enablement

During this stage, the issuer registers for MDES, chooses the Wallet Providers and programs it wants to support, and provides the settings MDES uses for each program during digitization and when processing MDES-enabled digital payments.

The issuer's enablement parameters are configured and maintained using the 'Mastercard Digital Enablement Service' application (service), which is accessed from Mastercard Connect™; refer to Access to the MDES Application.



**NOTE: Changes made to the application are reflected in the production system. Before configuring MDES, issuers should review the data required and its impact on MDES.**

Issuer enablement activities include, but are not limited to, the following.

<b>Aspect</b>	<b>Activities</b>
General parameters	<p>Provide:</p> <ul style="list-style-type: none"> <li>• The country where the issuer wants to enable MDES</li> <li>• Issuer call center contact numbers</li> <li>• Billing Interbank Card Association (ICA) number</li> <li>• Billing currency</li> <li>• Card Program Identifier (debit or credit)</li> <li>• The transaction types to be supported, such as International cashback and Domestic cashback (both only available for Debit Mastercard products)</li> </ul>
Wallet programs	Select the wallet programs (Wallet Providers) and MDES programs to support, and review and agree to the associated Terms and Conditions.
Profiles	<p>Configure card profiles and wallet configuration profiles, which includes:</p> <ul style="list-style-type: none"> <li>• The supported Activation Methods that are provided to the Wallet Provider when cardholder authentication is required during pre-digitization; refer to the About Activation Methods section</li> <li>• The allowed Cardholder Verification Methods (CVMs) when the provisioned tokens are used for contactless transactions; refer to the Mastercard Cloud-Based Payments (MCBP) chapter</li> </ul>
Account ranges	<p>Identify the account ranges that are available for digitization to a specific wallet application or MDES program; refer to the Card Availability section.</p> <p>An account range is a specific series of available PANs within a Bank Identification Number (BIN). Issuers can specify multiple account ranges with gaps, if they want to exclude some ranges. Each range must be specified as 6–11 digits, for example (where XXXX would be four digits):</p> <ul style="list-style-type: none"> <li>• 54XXXX—A 6-digit range, where 54XXXX0000000000 is the lowest PAN in range and 54XXXX9999999999 is the highest PAN in range</li> <li>• 54XXXX99999—An 11-digit range, where 54XXXX9999900000 is the lowest PAN in range and 54XXXX9999999999 is the highest PAN in range</li> </ul> <p>Once enabled by the issuer, all cards with PANs within the specified ranges can be digitized by the relevant programs. Cards outside those ranges cannot be digitized by those programs.</p> <p><b>NOTE: MDES can only be configured for account ranges with a live status in production (account ranges in 'Assigned' status are excluded).</b></p> <p>The issuer may need to work with their processors and regional networks to ensure they understand and are prepared for the implications of enabling the specific account ranges.</p> <p>For information about how product codes relate to account ranges, see Changing Your Product Code.</p>

Aspect	Activities
Product Configuration	<p>Provide:</p> <ul style="list-style-type: none"> <li>Digital card images and assets based on the use of Mastercard brands in digital wallets</li> <li>Cardholder Terms and Conditions, which cardholders accept during digitization for wallet programs</li> </ul> <p><b>NOTE: Mastercard strongly recommends that an issuer provides its own Terms and Conditions that apply to cardholders' use of the issuer's cards in the digital wallet. If an issuer does not provide any cardholder Terms and Conditions to Mastercard, the issuer acknowledges that Mastercard may use the following default statement for this purpose:</b></p> <p><b><i>The storage and usage of your payment card number (and credentials corresponding to your payment card number) in this digital wallet are subject to the terms and conditions of the applicable cardholder agreement with your payment card issuer, as in effect from time to time. Please contact your payment card issuer for more information.</i></b></p> <p>The display of these assets to cardholders depends on the type of program. For more information about these assets, see the Card Art and Associated Data for MDES appendix.</p>
Pre-digitization and lifecycle messages	Choose the network messages and/or web service (API) messages the issuer wants to receive from MDES, to get relevant information and make decisions during the pre-digitization processes; refer to the Pre-digitization chapter. The messages choices are set at an account range level.
Rules and default decisions	Specify the Card Eligibility rules and default decisions that MDES uses to determine whether digitization can proceed; refer to the Eligibility Rules section.
Authorization parameters	Configure parameters such as the decision matrix values that are used when approving or declining token transactions; refer to the Transaction Analysis chapter.
Transaction Detail Service (TDS)	Specify whether MDES uses the Mastercard TDS or the issuer's TDS to supply token transaction details to the cardholder; refer to the Transaction Detail Service section.

## Working with Processors

If the issuer wants a processor to manage their account range or their digital portfolio, they need to make sure that their MDES configurations are compatible.

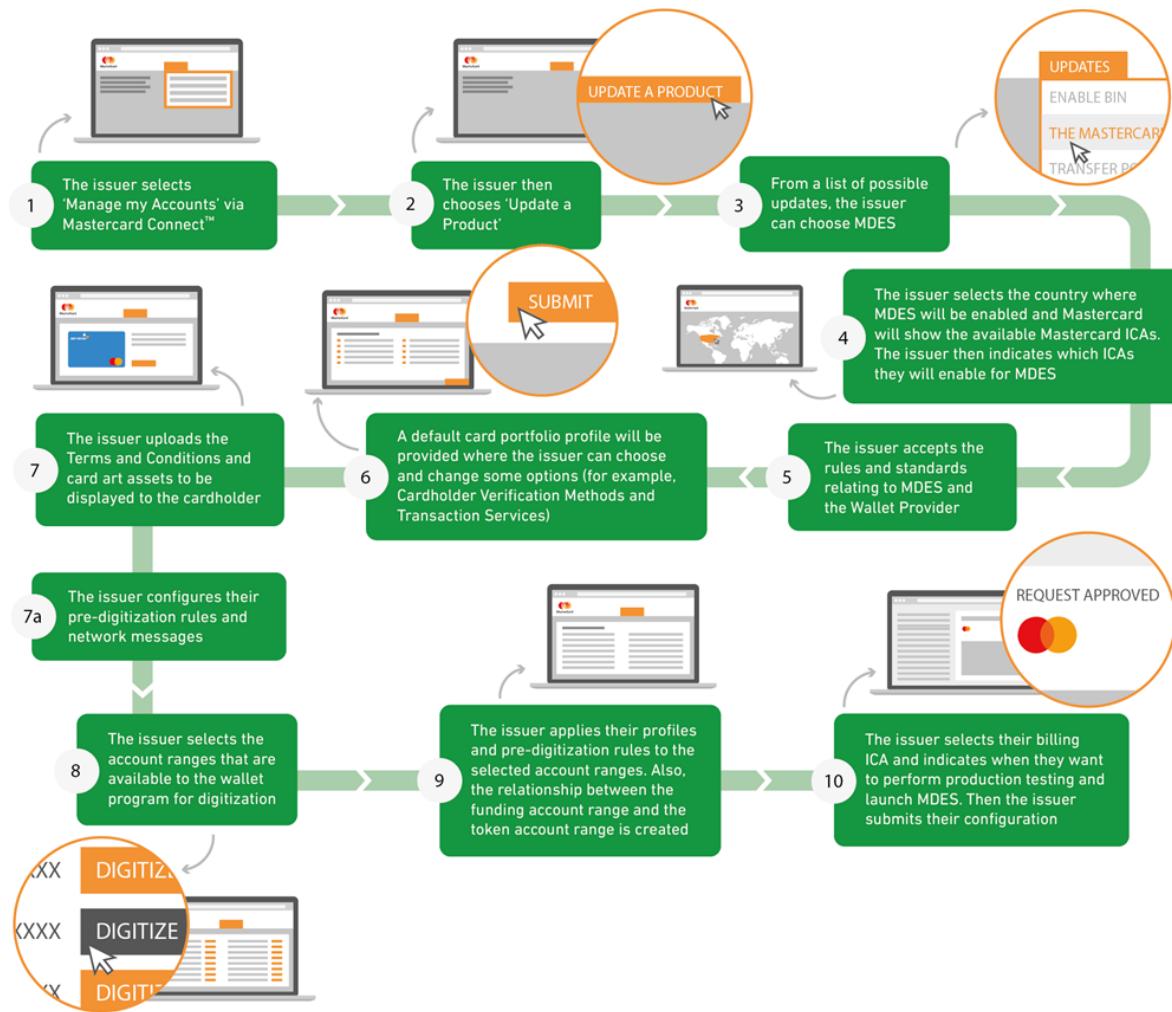
The issuer also needs to confirm the following with the processor:

- who would provide the product configuration id values
- what pre-digitization lifecycle they will need to use

## Issuer Enablement and Maintenance Processes

The issuer's enablement parameters are configured and maintained using the 'Mastercard Digital Enablement Service' application (service). For information on configuring the application, refer to the *MDES—Issuer Enablement* and *MDES—Issuer Maintenance* guides on the MDES Information Center on Publications in Mastercard Connect™.

The following diagram shows an example of the issuer enablement process.

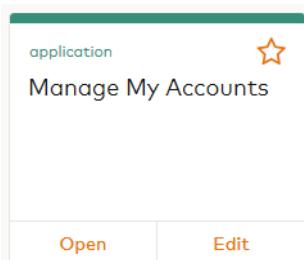


**NOTE:** This is a high-level summary of some of the steps. For the detailed screens and information, refer to the *MDES—Issuer Enablement* guide.

## Access to the MDES Application

The 'Mastercard Digital Enablement Service' application (service) is accessed from Mastercard Connect™.

To open the application, log into Mastercard Connect™ ([www.mastercardconnect.com](http://www.mastercardconnect.com)), open the 'Manage My Accounts' application (shown below) in **My Apps**, and then select **Update a Product > Mastercard Digital Enablement Service**.

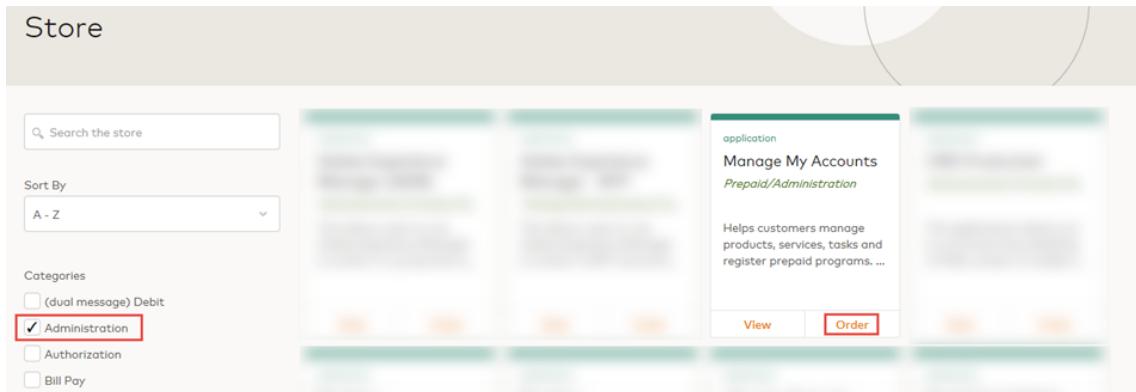


If the 'Manage My Accounts' application is not available in **My Apps**:

1. Click **Store**.



2. Locate the 'Manage My Accounts' application and click its **Order** button. The application is in the Administration category.



3. Click **Place Order**.

The request is routed to the Security Administrator for approval. Once approved, the 'Manage My Accounts' application appears in **My Apps**.

For information on adding the 'Mastercard Digital Enablement Service' application (service), refer to the *MDES—Issuer Enablement* guide.

## Testing with Mastercard

During this stage, the issuer ensures that their systems can interact with MDES and process the pre-digitization and financial transaction messages.

**NOTE: Mastercard strongly recommends that issuers perform functional testing and network interface validation (NIV) testing to support MDES. These tests cover the new fields and data elements (DE) for pre-digitization message support (if the issuer decides to support these messages) and transaction processing.**

**NOTE:** The issuer testing should include checking:

- The issuer systems can receive, process and respond to the chosen MDES pre-digitization and lifecycle network messages and/or API messages (as selected during issuer enablement)
- The authorization and clearing systems can process token transaction authorization network messages (Authorization Request/0100 or Financial Transaction Request/0200, depending on whether the issuer is connected to the Dual Message System or Single Message System)
- The issuer Customer Services teams or systems can interact with the MDES Customer Service Tools (Application or API)

**NOTE:** Mastercard provides test environments and manages the testing process. When testing is complete, Mastercard provides a testing acknowledgment letter.

**NOTE:** For more information on testing, refer to the Testing Strategy chapter.

**NOTE:** MDES readiness and enablement (for digital mobile and DSRP transactions) is a separate activity and is not dependent on Issuer EMV migration for physical contact/contactless cards which the issuer may also want to do.

### **Mastercard Dual and Single Message System Release Enhancements**

Through its quarterly Release cycle publications, Mastercard has introduced several enhancements to Single and Dual Message format specifications to support MDES.

Depending on the issuer's business needs, some or all of these enhancements may need to be implemented. These updates are applied to the issuer/issuer processor's Dual Message System and Single Message System interfaces.

The release articles specific to MDES are listed in Related Publications.

**NOTE:** To ensure the current MDES updates are applied to the issuer interfaces, refer to the most recent Mastercard Release Articles, available on Publications in Mastercard Connect™ ([www.mastercardconnect.com](http://www.mastercardconnect.com)).

In addition, all format specification details are added to the current versions of the following manuals, also available on Publications:

- *Authorization Manual*
- *Customer Interface Specification* (for Dual Message System Authorization)
- *IPM Clearing Formats* (for Dual Message System Clearing)
- *Single Message System Specifications* (for Single Message System)
- *Account Management System User Manual* (for Dual Message System and Single Message System)
- *MDES—Technical Specifications for Dual and Single Message Systems*

## Wallet Provider Certification

During this stage, the issuer uses Wallet Provider test scripts (if provided) to validate its implementation and support of the wallet program.

**NOTE: Wallet Provider Certification is also known as 'Issuer Certification.'**

The testing involves the issuer performing a set of tests in the production environment using real devices and a limited set of Account PANs (referred to as Whitelist Account PANs), which are specified during issuer enablement.

The certification testing typically includes checking:

- Card digitization and the appearance of the issuer Terms and Conditions
- The appearance of the issuer card art in the wallet application
- Different payment scenarios using the digitized cards on the device
- Token lifecycle management, such as suspending and deleting tokens

The issuer should complete all of the testing scenarios and return details of the test results to Mastercard and the Wallet Provider. When all tests are successfully validated, the certification process is complete.

For more information on certification, refer to the Issuer Certification and Account PAN Whitelisting section (in the Testing Strategy chapter).

## Go-Live

When the issuer has completed all testing and certification, it is ready for commercial launch (go-live) for the wallet program. The issuer provides Mastercard with a preferred go-live date, which must be agreed with the Wallet Provider.

The issuer's preparation for the go-live date should include:

- Preparing launch marketing campaigns to educate the relevant cardholders on the availability, benefits and use of card digitization
- Training their operational support teams on MDES, including customer service, chargeback, fraud reporting, and billing
- Ensuring its customer service activities are ready

On the agreed go-live date, Mastercard completes the setup in the production environment and notifies the issuer that all requested account ranges are ready for digitization.

**NOTE: For information about sales and press materials, and MDES training, contact your Mastercard representative.**

## Issuer Maintenance

---

Provides guidance for issuers to perform maintenance tasks so they can implement self-service tasks without risking their enablements

### Issuer Maintenance Tasks

Following an enablement, the issuer needs to be able to maintain their own MDES configurations and handle operations such as changing their card art or updating their profile settings.

**NOTE: It is recommended that they test these changes in MTF before moving them to Production.**

**NOTE: For information on issuer maintenance tasks, see [MDES—Issuer Maintenance](#).**

## Issuer Responsibilities

---

Issuers participating in MDES have the following responsibilities.

- Indicating Affiliate Range information, if they are Principal Customers with Affiliates (see Affiliate Range Information).
- Following the Token Implementation Plan (TIP) for the wallet program (see Token Implementation Plans).
- Supporting the real-time pre-digitization messages and fields where applicable.
- Delivering Activation Codes to their cardholders where required (see Activation by Activation Code).
- Defining the eligibility rules, during issuer enablement, which will help determine whether a digitization request can proceed (see Eligibility Rules).
- Checking the card Account PAN and expiration date values as part of the real-time pre-digitization messages.

**NOTE: Mastercard does not check the Account PAN expiry date during pre-digitization.**

- Checking the CVC 2 value (when available) as part of the real-time pre-digitization messages. The issuer is responsible for keeping count of the number of invalid CVC 2 attempts performed by the cardholder, and making a risk-based decision as to whether to approve a digitization request with an invalid CVC 2 value. Mastercard does not track invalid CVC 2 retries or validate the cardholder's CVC 2 on behalf of the issuer.
- Checking the billing address (when available) as part of the real-time pre-digitization messages.
- Checking the latest status of the card and only approving digitization if the card is 'in good standing.'

- Checking the expiration date of the Account PAN when a transaction is performed with a token.

**NOTE: Mastercard does not check the Account PAN expiry date for transactions performed with a token.**

- Receiving and authorizing transactions performed with a cardholder's token.

If an issuer is using MDES to provision tokens that have been generated by a third-party Token Service Provider (TSP), the issuer must provide the Token Requestor ID (TRID) and external token data to MDES; see External Token Service Providers.

## Token Implementation Plans

---

Each MDES wallet program has a Token Implementation Plan (TIP), which assists issuers integrating with that wallet program.

The TIP provides specific details of the program, such as:

- Issuer Terms and Conditions requirements
- Decisioning data supplied for digitization requests, and the supported additional cardholder authentication methods
- Supported additional Cardholder Verification Methods (CVMs) for transactions
- Supported token transaction types
- Transaction Detail Service (TDS) applicability and requirements
- Wallet Provider branding guidelines

The TIPs are available on the MDES Information Center on Publications in Mastercard Connect™ ([www.mastercardconnect.com](http://www.mastercardconnect.com)).

## External Token Service Providers

---

MDES includes support for issuers who want to provision tokens that are generated by a third-party Token Service Provider (TSP) instead of MDES. This support is exclusive to the MDES Pre-Digitization API; the pre-digitization network messages do not currently provide this functionality.

When an external TSP is used, the issuer must provide the following in its Authorize Service API response messages to MDES:

- The external token; see Providing External Token Data
- The Token Requestor ID (TRID)

The TSP is responsible for assigning the TRID. The 11-digit TRID identifies the Token Requestor and Token Domain, and it is unique per TSP (the first 3 digits identify the TSP). For more information about TRIDs, see Token Requestor ID and Wallet ID.

The supplied TRID value will be stored and used by MDES, where appropriate. For example, in the case of the MDES Pre-Digitization API, the TRID will be used when sending notifications to the issuer via Notify Service Activated request messages.

The following table summarizes which MDES Pre-Digitization API request messages will include the TRID value (depending on the TSP used).

API Request Message	MDES Used as TSP	External TSP
Authorize Service	Yes	No
Request Activation Methods	Yes	No
Notify Service Activated	Yes	Yes

## Alternative Network Processing

Mastercard has developed specifications for regional debit networks to facilitate the processing of transactions that originate with Mastercard tokens but are not processed on the Mastercard Network.

An alternative network that has been identified by an issuer as a Debit Payment Network to process such transactions may receive the relevant specifications from Mastercard and develop the connections in accordance with, and subject to the terms of, the specifications. When a merchant elects to route a Mastercard debit token to a regional debit network that has agreed to participate in the alternative routing solution, MDES is able to perform token to Account PAN mapping, cryptography validation, and the application of token domain controls.

Refer to the Transaction Processing chapter for details on alternative network routing.

Issuers need to consider the following prerequisites for alternative network routing when implementing MDES. Mastercard partners with issuers to support them through this process:

- Notify alternative network(s) that the issuer is using the MDES alternative routing solution
- Prepare host/issuer processor to accept token transactions from alternative networks
- Notify Mastercard of their alternative networks for debit routing
- Execute an agreement with the alternative network relating to the processing of the issuer's Mastercard tokens
- Ensure the alternative network has executed any other agreement deemed necessary by Mastercard
- Ensure the alternative network agrees to comply with the specifications and performs functional and connectivity testing as required to support the service requests to MDES
- Provide token account ranges to the alternative network

## Define and Implement Risk Management Policy

Issuers should develop a risk management policy based on their respective service propositions. The issuer risk management policy should consider all aspects of how MDES operates.

Examples of items that need to be considered include the following:

- Operation in a domestic versus a global environment
- Analysis of new data elements provided in the token transactions
- Analysis of risk management associated with EMV-based digital transactions
- Analysis of additional data elements provided in the pre-digitization process (such as details on the cardholder's mobile device)

This risk management policy needs to be considered in the development of the marketing and cardholder communication plans. Any impacts for issuer systems due to the risk management policy need to be identified and incorporated into the implementation plans.

## Merchant Tokenization

This section summarizes implementation considerations for the MDES for merchants program.

The MDES for merchants program enables merchants and their Payment Service Providers to digitize the consumer Account PANs stored on their servers, replacing them with MCBP tokens that can be used for Digital Secure Remote Payment (DSRP) transactions. The merchant uses its proprietary user authentication mechanism to authenticate consumers before allowing them to make token transactions.

Issuers who opt to support the MDES for merchants program (for applicable account ranges) are automatically committed to supporting *all* merchants using the program. Issuers are not able to opt in or out of particular merchants. Mastercard certifies the merchants joining the program.

Each merchant using the program has a unique Token Requestor ID (TRID), enabling the issuer to identify the merchant. Token requests and transactions are marked with a fixed Wallet ID (WID) value of **327**, which enables issuer systems to track digitization requests and transactions relating to merchant tokenization.

**NOTE: For more information, see the Token Requestor ID and Wallet ID section.**

During pre-digitization, the issuer may decide whether to approve or decline each digitization request by examining the data in the request to assess specific risks associated with the given account.

### MDES for Merchants Regional Program Mandates

#### North America:

**NOTE: Effective 1 September 2018:**

Mastercard will require all North America issuers using MDES to process digitization requests and transactions for MDES for Merchants across all portfolios eligible for tokenization.

**Latin America & Caribbean:**

**NOTE: Effective 1 November, 2018:**

- Issuers that are either live on MDES or have an ongoing project that started before 1 July 2018 are required to support MDES for Merchants
- New MDES issuers (those that start a MDES implementation project after 1 July 2018) must comply with the MDES for Merchants program requirements to receive the certification letter from Mastercard

**NOTE: Effective 1 June 2019:**

All issuers participating in MDES must have all BINs enabled for the MDES for Merchants program.

**Europe:**

**NOTE: Effective 1 November, 2018:**

Issuers that start a new MDES project (whether onboarding to MDES for the first time or onboarding to an additional device/use case) are required to implement changes in authorization and clearing messages. The required changes are to implement support for the MDES for Merchants indicators in tokenized transactions to receive a certification letter from Mastercard.

**NOTE: Effective 31 December 2019:**

- All issuers participating in MDES must have all eligible BIN portfolios enabled for MDES for Merchants, in accordance with the requirements communicated in AN 2048 (published on Aug 31, 2018).
- All issuers not participating in MDES or an equivalent Mastercard certified tokenization service, will be enrolled by Mastercard to an OB service with associated commercial terms.

**Asia-Pacific:**

**NOTE: Effective 1 Jan 2019:**

Issuers that start a new MDES project (whether onboarding to MDES for the first time or onboarding to an additional device/use case) are required to implement and test MDES for Merchants related changes in digitization, authorization and clearing messages.

**Notable Differences from Wallet Programs**

Some of the differences include the following:

- The merchant initiates the digitization requests, typically without cardholder interaction or knowledge.
- The merchant does not provide the issuer's Terms and Conditions to its cardholders because they are unlikely to be present during digitization.
- There is no mobile device compatibility check.
- MDES will not send a Tokenization Eligibility Request (TER) message.
- For Card Eligibility pre-digitization messages (ASI, TAR or Authorize Service):
  - If the issuer does not respond to the first message, MDES will not send a second (retry) message.
  - The issuer must be able to process the message without requiring the cardholder name, CVC 2, and address data.
  - Issuers should validate the CVC 2 if present but be able to process the message if the CVC 2 is not present. Issuers should decline the message if the value provided does not match the valid value for the card.
- Additional cardholder authentication by the merchant is **optional** and does not activate the token.

If the issuer's eligibility decision is 'Approve, but require authentication,' the token has a Token Assurance Level (TAL) value of 00 (Not Authenticated). Merchants may perform additional cardholder authentication at any time during the life of the token. The benefit of doing so is to change the token's TAL value, which might provide a higher expected transaction approval rate.

Because the additional cardholder authentication can occur at any time, the issuer will receive the Tokenization Complete Notification (TCN) or Notify Service Activated API message before a Request Activation Methods API message, an Activation Code Notification (ACN) message, or Deliver Activation Code API message.

## Processing Digitization Requests and Transactions

To support the MDES for merchants program, an issuer implementation should include the following considerations:

Aspect	Requirement
TRID	<p>Issuer systems must allow new TRID values to be accepted during (but not necessarily limited to) pre-digitization and transaction processing. This will avoid digitization requests and payments being declined only on the basis of a new TRID.</p> <p>Issuers participating in the MDES for merchants program will see new TRIDs as merchants join the program. Mastercard will assign the TRIDs without prior notice.</p>

Aspect	Requirement
TAL	<p>Issuers must support the use of the TAL value in Authorization messages to distinguish between tokens that are Authenticated and Not Authenticated.</p> <p><b>NOTE: Optional Cardholder Authentication as a feature for adjusting the TAL value may be made available at a future date as determined by Mastercard. However, issuers must support the value in messages for the current phase of issuer implementation.</b></p> <p>A transaction using a token that is Not Authenticated must not be automatically declined. Merchants are expected to replace all Account PAN data with tokens, and some or all of those tokens may be Not Authenticated. They may remain Not Authenticated for the life of the token (for example, for merchants not supporting any additional cardholder authentication). The assurance of a transaction with a token that is Not Authenticated should be considered greater than or equal to the assurance of a transaction performed using the Account PAN.</p>
DSRP transactions	<p>Issuers and their processing partners must be able to process DSRP transactions containing an MCBP token and a UCAF cryptogram.</p> <p>Issuers must support the MDES for merchants tokenization-specific Security Level Indicators (Electronic Commerce Security Level Indicator and UCAF Collection Indicator) to allow proper identification of this transaction category (DSRP transaction containing card-on-file merchant tokens) for chargeback purposes.</p>
Token lifecycle	<p>Merchants must be able to transact with a token as long as the underlying account remains open and in good standing. If the Account PAN expires or the card is otherwise replaced, the issuer must update the MDES Mapping Service with the replacement Account PAN data, or otherwise maintain continuity of service for tokens.</p>

## Processing Credential on File Transactions

**NOTE: Processing of payment authorizations using MDES tokens should adhere to the requirements outlined in AN 1121 for Credential on File payments, which include the use of the new Point of Sale (POS) entry mode value of 10. Issuers should support POS entry mode value of 10 as well as POS entry mode value of 81 for MDES payment authorizations with MDES tokens within ecommerce.**

**NOTE: For more information, refer to the following documents:**

- **North America:** AN 1557—Revised Mastercard Digital Enablement Service (MDES) Program Requirement for Issuers in the Canada and U.S. Regions
- **Europe:** AN 2048—Issuer Enrollment in Mastercard Digital Enablement Service for Merchants in the Europe Region
- **Asia-Pacific:** AN 1748—Revised Standards—Tokenization and DSRP for the Asia/Pacific Region

- **Latin America and Caribbean:** AN 1551—Issuer Support to Mastercard Digital Enablement Service for Merchants in Latin America and the Caribbean Region
- "AN 1121—Revised Standards—Credential-on-File and Recurring Payments Transactions," March 2018
- "AN 1001—Electronic Commerce Security Level Indicator Validation and Usage," Release 17.Q4 article
- "AN 1021—Mastercard Digital Enablement Service for Merchants," Release 17.Q4 article
- "Mastercard Digital Enablement Service—Customer Impact of MDES for Merchants Program—Update" *Bulletin No. 1*, 4 May 2017
- "AN 2031—Expanded Scope and Usage of Wallet Identifier, Value 327 Merchant Tokenization Program," 28 September 2018

**NOTE: There are updated fraud prevention rules for handling MDES for Merchants transactions**

## Maximum Number of Transaction Credentials

---

Each cloud-based payment transaction with a token uses one set of transaction credentials (also known as the payment keys used to generate cryptograms). The Credentials Management System Dedicated (CMS-D) sends several sets of transaction credentials to the wallet application during the replenishment process.

When an issuer enables a cloud-based wallet program (during issuer enablement), the issuer must set the maximum number of transaction credentials that can be stored simultaneously on a cardholder's device per digitized card. The selected value depends on the issuer's view on security and usability. It can be a value in the range 6–24.

### Transit Aggregated Fare Use

Issuers supporting transit transactions should bear in mind that cardholders might have no data connectivity while traveling on transit systems (such as underground rail networks) and so their wallet applications might be unable to replenish payment keys during those journeys.

Such transit systems may require cardholders to tap both in and out, and journeys that involve multiple railway lines may result in multiple taps per journey. Each tap will use a set of keys, and some systems might not allow cardholders to exit unless the wallet application has at least one set of keys (for performing a valid, zero-value transaction).

The maximum key level for the wallet application should allow for typical or (ideally) worst-case journeys with regard to the number of possible taps. 10 keysets could be required, in addition to ordinary purchases and DSRP transactions.

## How Token Languages are Decided and Personalized

---

Tokens can be provisioned with a terminal language preference list, which determines the language used by a contactless terminal when a token is used for a contactless payment.

The issuer provides the language preferences for an account range during issuer enablement, for example 1 = EN, 2 = FR, 3 = ES.

On supported wallets, the consumer can influence the preferred terminal language at digitization time. If the Wallet Provider supplies a language in the digitization request and that language is included in the issuer's language preferences (for the associated account range), the Wallet Provider-supplied language will be moved to the top of the list. For example, if the Wallet Provider supplied language FR, the token's terminal language preference list would be 1 = FR, 2 = EN, 3 = ES.

If the Wallet Provider supplies a language that is not in the issuer's language preferences, it has no effect (it is not added to the token's list).

**NOTE: When a token has been provisioned, its language preferences cannot be changed.**

# Chapter 4 Pre-digitization

*This section describes the pre-digitization process for cardholders digitizing their cards using MDES.*

---

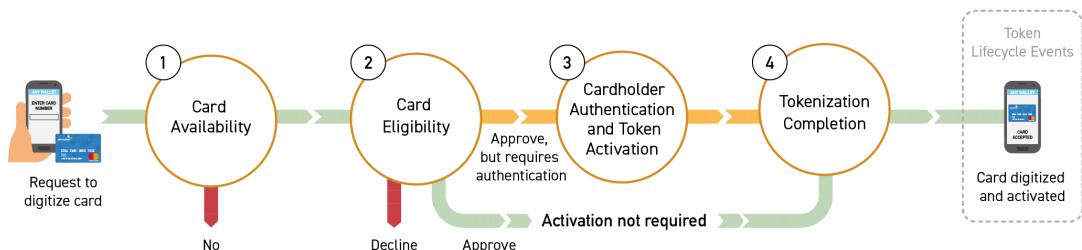
What is Pre-digitization?.....	50
Example Cardholder Pre-digitization Experience.....	51
Pre-digitization Messages.....	52
Card Availability.....	59
Overview.....	59
Account Status Inquiry (ASI) Message.....	61
Tokenization Eligibility Request (TER) Message.....	61
Card Eligibility.....	66
Overview.....	66
Issuer-Initiated Digitization.....	71
TAV Creation.....	87
TAV Digital Signature Algorithm.....	88
TAV Digital Signature Generation.....	89
TAV Encoding and Examples.....	93
Card Eligibility Pre-digitization Message.....	96
Account Status Inquiry (ASI) Message.....	97
Tokenization Authorization Request (TAR) or Authorize Service Message.....	97
Providing an Alternate Account Identifier for a Token.....	104
Providing External Token Data.....	105
MDES Issuer Personalization Data.....	105
Checking the CVC 2, Expiration Date and Address.....	108
Eligibility Rules.....	109
About Rules and Rule Sets.....	110
Wallet Provider Account Data Elements and Scores.....	112
Pre-digitization Message Response Data Elements.....	115
Default Eligibility Decision.....	116
Cardholder Authentication and Token Activation.....	116
Overview.....	117
About Activation Methods.....	118
Issuer App Token Activation.....	121
Issuer App Token Activation via TAV.....	121
Issuer App Token Activation via Customer Service API.....	123
Activation by Activation Code.....	126
MDES Controls Activation Codes.....	127

---

Issuer Controls Activation Codes.....	129
Activation Code Notification (ACN) Message.....	130
Deliver Activation Code API Message.....	131
Validate Activation Code API Message.....	131
Activation by Call Center.....	132
Tokenization Completion.....	133
Overview.....	133
Tokenization Complete Notification (TCN) Message.....	134
Notify Service Activated API Message.....	137
Issuer-Initiated Digitization with MDES Token Connect.....	137
Consumer Experience.....	137
Benefits of Token Connect.....	139
Security Guidelines.....	139
Security Risks associated with MDES Token Connect.....	139
Consumer Login in Issuer's Interface.....	140
Device Binding.....	140
Issuer Callback URL.....	141
Card Eligibility Decision.....	142
Lifecycle Events.....	143
Tokenization Event Notification (TVN) Message.....	144
Notify Token Updated API Message.....	146
Cardholder-Initiated Token Deactivation for Apple Pay.....	146
Halting Digitization.....	146
Card Art Support and Associated Data.....	147

## What is Pre-digitization?

Pre-digitization is the set of processes that must happen before a token is ready for use.



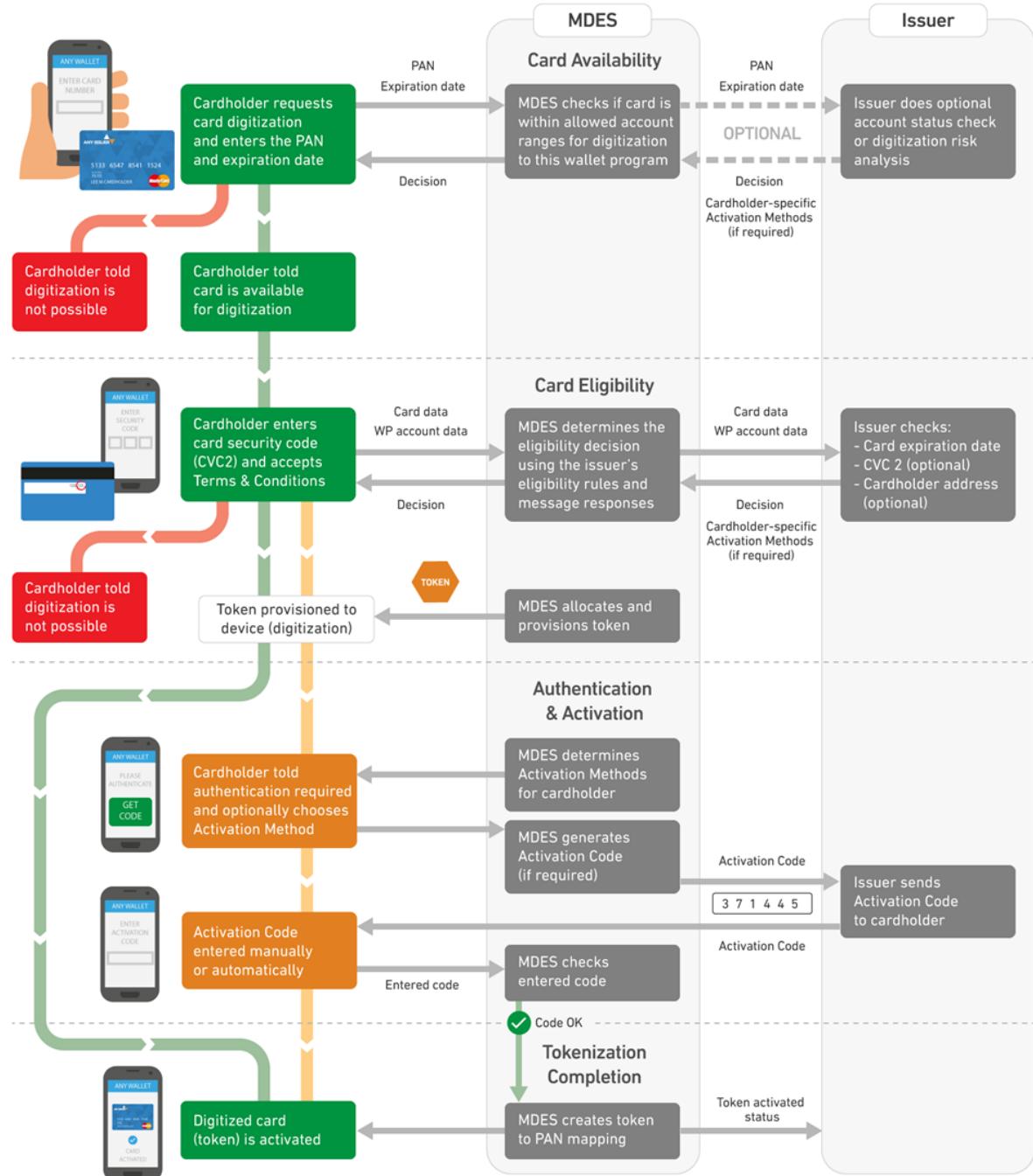
Stage	Description
1 Card Availability	The Wallet Provider or Token Requestor checks whether a card is available (within an allowed account range) for digitization to a specific wallet application or MDES program.
2 Card Eligibility	Determines whether the card can be digitized to a specific device or server (depending on the MDES program or implementation). The eligibility decision is one of the following: <ul style="list-style-type: none"> <li>Approve</li> <li>Approve, but require authentication</li> <li>Decline</li> </ul>
3 Cardholder Authentication and Token Activation	For wallet programs, if the eligibility decision is 'Approve, but require authentication,' the cardholder must verify their identity before their token is activated (for example, by entering an issuer-provided Activation Code into the wallet application on their device). MDES supports several methods of authentication and token activation.
<b>NOTE: This stage is optional for merchant and commerce platform programs, where tokens are activated automatically (unless digitization is declined).</b>	
4 Tokenization Completion	MDES notifies the issuer that the token is active and can be used to make payments.

For issuer wallet programs, all these stages apply regardless of whether the issuer already knows that a card is available and eligible for digitization. The Card Availability and Card Eligibility stages provide the IDs for the relevant assets (such as the card art and Terms and Conditions) so the issuer wallet can retrieve and show those assets to the cardholder.

The token can go through different lifecycle events, such as activation and suspension. For more information, refer to the Lifecycle Events section and Token Management chapter.

## Example Cardholder Pre-digitization Experience

This example shows a cardholder digitizing a card to a device wallet application. It highlights some of the activities and some of the data passed during each pre-digitization stage.



**NOTE: This is an example user experience for a wallet program. Wallet Providers and issuers may support different user experiences and processes. This example implementation shows MDES generating and validating Activation Codes. Issuers can choose to generate and validate their own codes, see Activation by Activation Code.**

The diagram shows how the cardholder and wallet activities relate to each pre-digitization stage and the issuer.

The diagram does not show all the possible activities, interactions and data elements that can be passed. For example, the Wallet Provider checks MDES to see if the device is compatible with digitization (for device-based wallet programs) and retrieves the issuer assets it needs to show the user, such as the Terms and Conditions and card art. These interactions do not involve the issuer.

Information about the interactions and data relevant to the issuer is provided in the sections that follow.

The MDES pre-digitization stages and functionality allow for different implementations, for example:

- An issuer banking application on the device could interact directly with the wallet application, enabling the cardholder to initiate card digitization from the issuer application (where their identity has already been validated and their card details are already entered).

**NOTE: See the following:**

- [Issuer-Initiated Digitization](#)
- [Issuer-initiated digitization with Token Connect](#)

- If additional cardholder authentication is required, the cardholder could log into an issuer application to confirm the digitization; see Issuer App Token Activation.
- Issuers can choose to generate and validate their own Activation Codes; see Activation by Activation Code.
- For merchant and commerce platform programs (if supported by the issuer), the Cardholder Authentication and Token Activation stage is not required.

**NOTE: See [Merchant Tokenization](#).**

## Pre-digitization Messages

During issuer enablement, issuers can select which pre-digitization and lifecycle messages they want to receive from MDES, to get relevant information and make decisions during the pre-digitization stages.

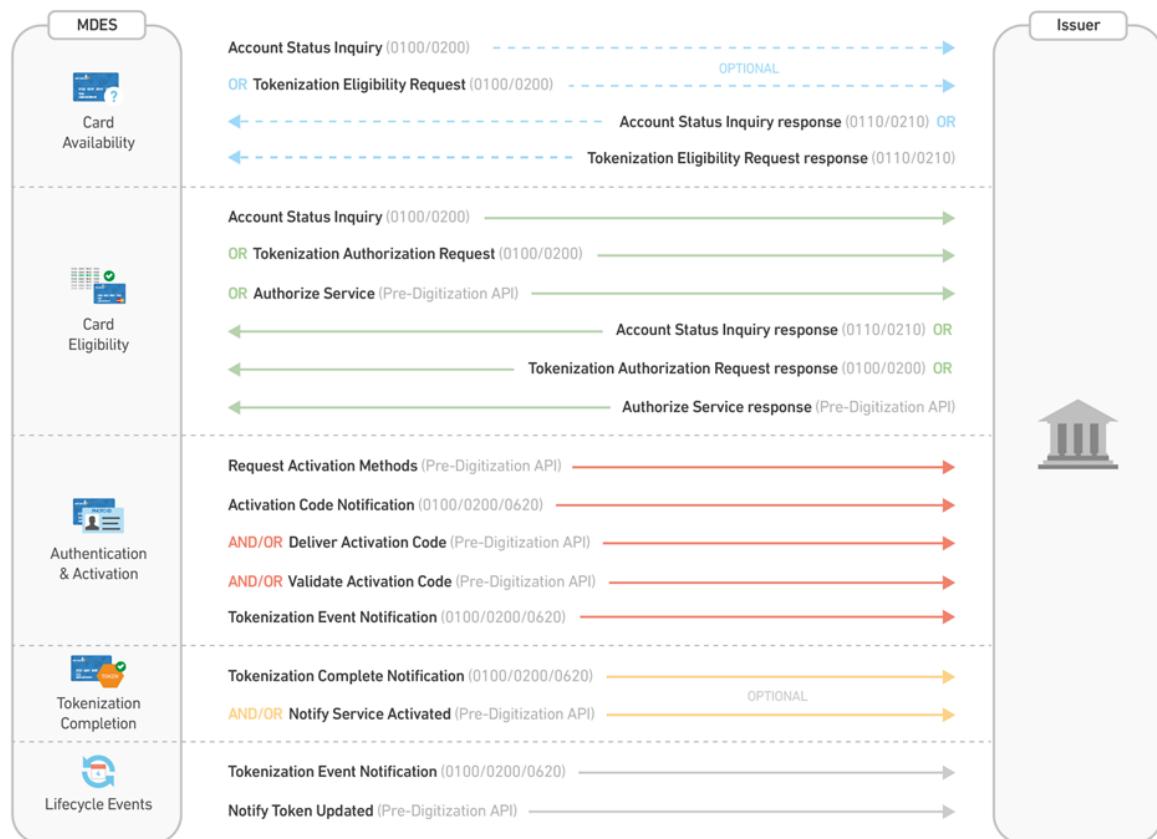
The following diagram shows the ISO 8583 network messages and web service API messages that can be used for each pre-digitization stage. The types of messages chosen depend on the issuer's system architecture and the digitization processes it wants to support.

**NOTE: MDES allows pre-digitization messages to be configured at the account range level and, if necessary, at the Wallet level. This allows some wallets/programs to be configured with alternative or simpler message flows, for example, only having TAR eligibility for MDES for Merchants.**

**NOTE: If the issuer wants to make a specific configuration at the Wallet level, they should contact their local CIS representative.**

This chapter describes how the messages can be used.

**Figure 3: Message Flows for Pre-digitization**



**NOTE: Issuers must support the Account Status Inquiry (ASI), Tokenization Authorization Request (TAR), or Authorize Service message for Card Eligibility checks.**

The following table shows how the network messages correspond to the web service API messages.

Network Message	API Message
Tokenization Eligibility Request (TER)	—

---

<b>Network Message</b>	<b>API Message</b>
Tokenization Authorization Request (TAR)	Authorize Service
—	Request Activation Methods
Activation Code Notification (ACN)	Deliver Activation Code
—	Validate Activation Code
Tokenization Complete Notification (TCN)	Notify Service Activated
Tokenization Event Notification (TVN)	Notify Token Updated

---

The pre-digitization message choices are configured per account range, not at the wallet level or issuer level. With the exception of Card Availability and Card Eligibility messages, issuers can choose to receive both network messages and API messages. This enables issuers to choose messages that best suit their implementations.

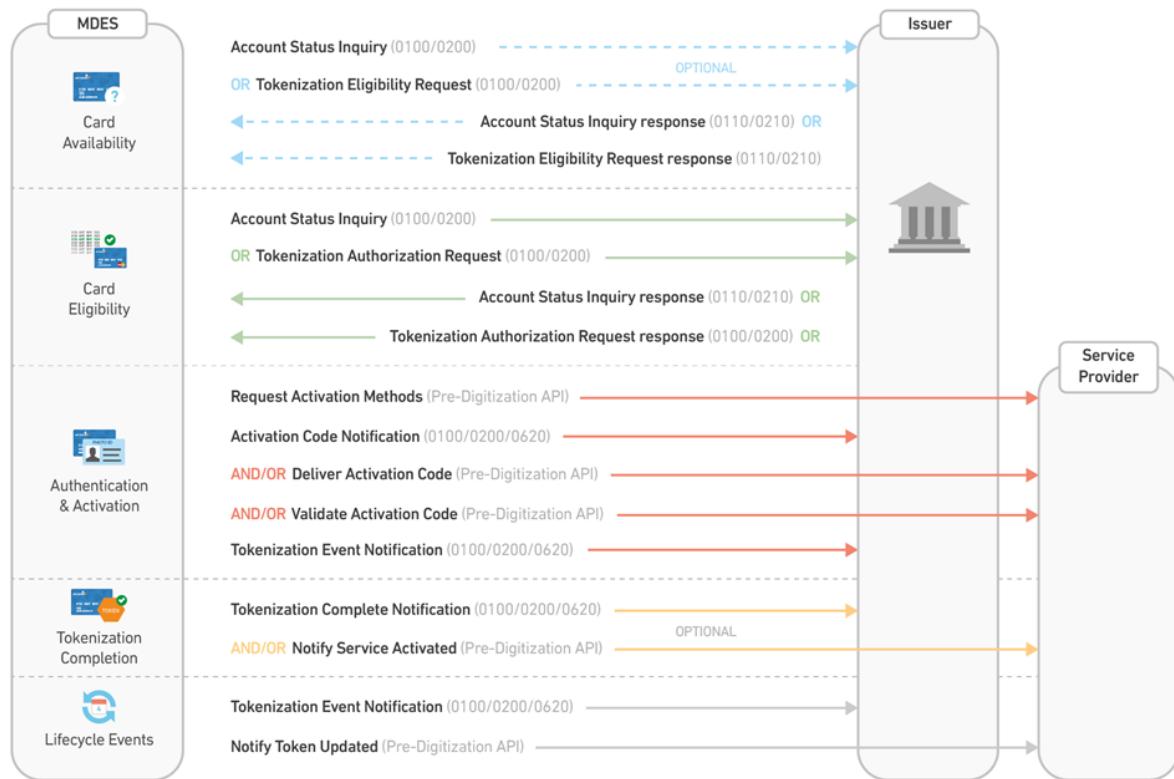
Imagine a situation where the same account range needs to be enabled for an issuer wallet (managed by the issuer via network messages) and other Token Requestors (managed by a service provider via the MDES pre-digitization APIs). In this case, pre-digitization messages are required by both parties.

To satisfy this requirement (as shown in the following diagram):

- The issuer processes the Card Availability and Card Eligibility network messages, checking the eligibility requests for all wallets.
- Authentication & Activation, Tokenization Completion and Token Lifecycle messages can be sent to both parties:
  - Network messages to the issuer
  - API messages to the service provider

The issuer and service provider receive messages for all wallets but they only process the messages with the Wallet ID (WID) that they support; see Token Requestor ID and Wallet ID.

**Figure 4: Example Message Flows for Mixed Message Requirement**



## Network Messages

Details on pre-digitization network message support are provided in *MDES—Technical Specifications for Dual and Single Message Systems*, available on the MDES Information Center on Publications in Mastercard Connect™ ([www.mastercardconnect.com](http://www.mastercardconnect.com)).

**NOTE: For technical details, such as detailed message layouts and data element definitions, refer to the *Customer Interface Specification* or *Single Message System Specifications*.**

All network messages are supported for both the Dual Message System and Single Message System interfaces. Issuers receive either Authorization Request/0100 or Financial Transaction Request/0200 message types depending on the system through which they receive the Activation Code Notification (ACN), Tokenization Complete Notification (TCN) and Tokenization Event Notification (TVN) messages. Issuers can alternatively choose to receive Administrative Advice/0620.

The pre-digitization network messages contain data provided by the Wallet Provider. If any of that data was not ISO 8859-1 compliant, MDES will have replaced it with either one period character (U+002E) or two period characters (U+FFFF), such as for emoji (to maintain constant UTF-16 spacing).

**NOTE: The ASI messages and pre-digitization network messages sent by MDES contain the indication that they originate from the United States. For Local Use Only account ranges, MDES adjusts the country indicators (country code and currency code) to make the corresponding ASI or pre-digitization network messages look like they originate from the domestic network. This way, the ASI and pre-digitization messages will not be systematically declined for account ranges marked as Local Use Only (see Local Use Only Account Ranges).**

## API Messages

The MDES Pre-Digitization API provides a set of web services that make the pre-digitization process accessible to issuers over Open API. These services support rapid deployment of MDES functionality as an alternative to network messages, with delivery to server endpoints.

This chapter briefly describes the API messages. For full information on the messages and their parameters, refer to the MDES Pre-Digitization API documentation on the Mastercard Developers site (<https://developer.mastercard.com>).

## Timeouts and Retries

When MDES does not receive a response to a pre-digitization message (except ASI [Card Eligibility], TAR or Authorize Service), MDES waits a limited period of time before resending the original message. The timeout period varies by region; for more information, see the *Customer Interface Specification*. For example, the timeout period is 5 seconds in the United States. There is a maximum of three retry attempts.

If issuers choose not to receive pre-digitization messages (except for ASI [Card Eligibility]), they can check pre-digitization status changes and failures using the Customer Service Tools.

## Card Eligibility Message Timeout and Retry Logic for Wallet Programs

For wallet programs, when MDES does not receive an **immediate** response to a Card Eligibility pre-digitization message (ASI, TAR or Authorize Service), the following retry logic applies:

1. MDES informs the Wallet Provider that no digitization decision has yet been determined.
2. A second Card Eligibility pre-digitization message is sent to the issuer and MDES awaits the issuer's response to this second message. Issuers should therefore expect to receive, process and respond to a second message. MDES waits for 15 seconds for a response to this second message
3. Following an advice of no decision by an issuer, a Wallet Provider may, within a few seconds (this period depends on the Wallet Provider and their expectations regarding an acceptable user experience), contact MDES to request whether the issuer's response has been received and whether a decision has been determined. MDES uses **only** the response to the second Card Eligibility pre-digitization message. If the message response is still not received, the Wallet Provider is again informed the digitization decision is yet to be determined.
4. When MDES does not receive the response to the second Card Eligibility pre-digitization message after a time-out period of 15 seconds, a decision is determined pursuant to the

- applicable eligibility rules or the default eligibility decision, and the Wallet Provider is informed of that decision when they next inquire.
5. A Wallet Provider may choose to not further inquire for the decision, in which case digitization does not proceed regardless of the response to the second Card Eligibility pre-digitization message.

**NOTE: The above retry logic does not apply to merchant and commerce platform tokenization. For those programs, if the issuer does not respond to a Card Eligibility pre-digitization message, MDES will not send a second message.**

Issuers are strongly advised to design their pre-digitization message processing to provide an immediate response to the first message received to ensure their intended and timely digitization decision. Issuers should design their solution to respond to MDES within 1,200ms to ensure the retry processing is not invoked.

Issuers may wish to repeat the response to the first Card Eligibility pre-digitization message (if available) when the second pre-digitization message is received to ensure a timely response, or process the second message independently of the first.

## Identifiers in Messages

Where relevant, the following identifier values are provided in the pre-digitization request messages that MDES sends to issuers.

Identifier	Identifies	Assigned by
Token Requestor ID (TRID)	A Token Requestor (and Token Domain) that is directly integrated with MDES and using it for tokenization, such as a Wallet Provider, merchant, or issuer; see Token Requestor ID and Wallet ID.	Mastercard or the Token Service Provider (TSP) to the Token Requestor
Wallet ID (WID)	The wallet application, program or service associated with the Token Requestor or Wallet Provider; see Token Requestor ID and Wallet ID.	Mastercard Franchise Development
Payment Application Instance ID	An instance of the payment application (wallet application) on a device; unique across a WID. For example, if the same wallet application is installed twice on a device for two user profiles, there will be two instances of it. This ID is not present for particular implementations.	Token Requestor
Correlation ID	A card digitization attempt; the same unique value is used in all pre-digitization messages relating to a digitization, enabling issuers to link the messages. For example, if a cardholder enters an invalid CVC 2 during digitization, the multiple Card Eligibility request messages will have the same Correlation ID.	MDES

The TRID and WID enable the issuer to identify the Wallet Provider and wallet application/program, see Token Requestor Models.

## Declined Digitizations

Issuers are not informed when MDES declines digitizations due to eligibility rules. Issuers can use the MDES Provisioning Rules Report to see details about cardholder eligibility decision processing and the rules that have been triggered; refer to the *MDES—Issuer Portfolio Analytics Reports* guide.

## Local Use Only Account Ranges

For pre-digitization network messages, Mastercard acts as the acquirer (ICA 15611) with a U.S. originating source. In situations where the issuer account range is defined as Local Use Only (domestic traffic), there might be an inconsistency between issuer non-U.S. countries (for example, France) and the MDES U.S. source. This can result in Mastercard declining the digitization requests, because the messages conflict with Local Use Only-related edits at account range level.

The services for sending Authorization Request/0100 MDES pre-digitization network messages and ASI messages have been modified to allow MDES to conditionally provide the local values within the following data elements for Local Use Only account ranges (see the note):

- DE 43 (Card Acceptor Name/Location for All Transactions), subfield 5 (Card Acceptor State or Country Code) = 3-character alpha state or country code (if not the United States) of the merchant
- DE 49 (Currency Code, Transaction) = 3-digit numeric local currency code
- DE 61 (POS Data), subfield 13 (POS Country Code) = 3-digit numeric country code of the point-of-sale (POS) location

These data elements apply to all pre-digitization network message types: ASI, TER, TAR, ACN, TCN, TVN. This means that when an issuer has opted to receive such messages as Authorization Request/0100 for a Local Use Only account range (see the note), those messages are initiated from an ICA associated with the country of the issuer (instead of being associated with the United States, which has the code 840) so that the messages are accepted inside the country.

**NOTE: This functionality has been applied at CID level with the 18.Q1 release and will be enabled at account range level with the 18.Q2 release.**

## Card Availability

Card Availability is the Wallet Provider or Token Requestor checking whether a card is available (within an allowed account range) for digitization to a specific wallet application or MDES program.

### Overview

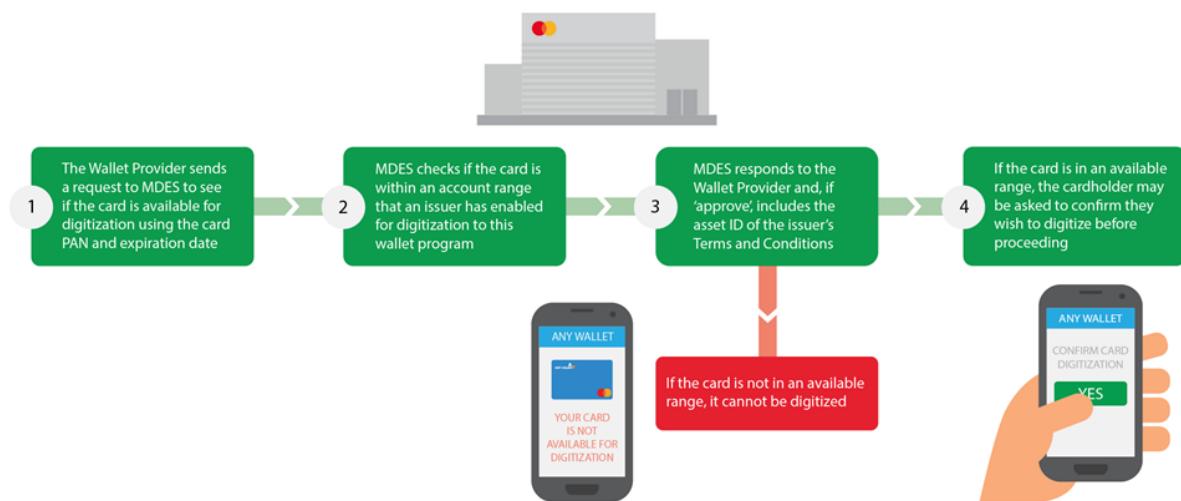
During issuer enablement, issuers specify which account ranges are available for digitization.

Each digitization request is checked against the allowed account ranges for the wallet program or MDES program. If the Account PAN is within an allowed range, the Wallet Provider is provided with issuer-specified information, such as the asset ID for the Terms and Conditions for that card range. The Wallet Provider then retrieves and displays the Terms and Conditions to the cardholder for acceptance before the pre-digitization process continues.

**NOTE: Cardholders might not be present during merchant or commerce platform tokenization, so those MDES program participants do not provide issuer Terms and Conditions to their cardholders during digitization.**

The Terms and Conditions, card art and other assets to be displayed by Wallet Providers within their wallet application or user interface are configured during issuer enablement. The complete set of graphical and textual assets is termed a Product Configuration. Individual assets may be cached by the Wallet Provider or device.

**Figure 5: Checking a Card is in an Available Account Range (Illustrative)**



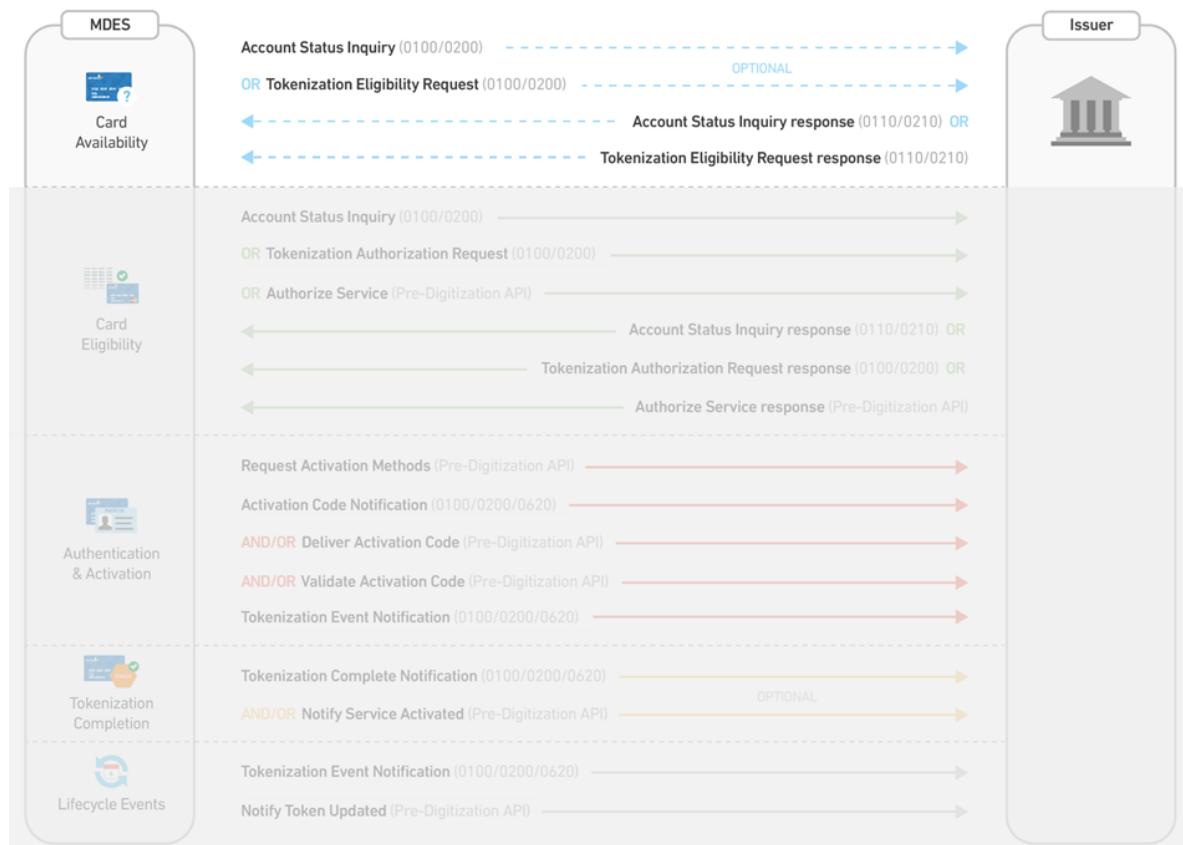
An issuer may optionally be notified about the Card Availability check, by choosing to receive an Account Status Inquiry (ASI) or Tokenization Eligibility Request (TER) network message.

**NOTE: There are no pre-digitization API messages available to an issuer during Card Availability. MDES does not send a TER message for merchant and commerce platform tokenization.**

The Card Availability message gives the issuer an opportunity to provide a response to MDES that approves the continuation of pre-digitization or indicates that the card is ineligible for digitization (for example, when a card account does not exist or is closed). If the issuer sends a response message, it is processed by MDES during the next phase (Card Eligibility); the Card Availability response back to the Wallet Provider is not delayed.

The following diagram shows the pre-digitization messages that can be sent during Card Availability.

**Figure 6: Message Flows for Card Availability**



## Account Status Inquiry (ASI) Message

Issuers can choose to receive this network message, during Card Availability, so that they can perform an account status check prior to receiving the formal digitization request (during Card Eligibility).

ASI messages are sent as Authorization Request/0100 or Financial Transaction Request/0200 message types, depending on whether the issuer is connected to the Dual Message System or Single Message System, respectively.

### Message Request Details

The ASI message that an issuer receives during Card Availability contains the following:

- Card Account PAN
- Card Account PAN Expiration Date

This is a subset of the information provided by an ASI message received during Card Eligibility.

### Issuer Processing and Message Response Details

An issuer should perform an account status check and a digitization risk analysis based on the information provided, and respond indicating Approve (DE 39 = 00 or 85) or Decline (DE 39 = 05 or any other value) digitization.

**NOTE: The message response codes of 00—‘Approve’ and 85—‘Not Declined’ are treated as equivalent within MDES. The expectation is that the issuer provides code 85—‘Not Declined’ when responding to an ASI message.**

## Tokenization Eligibility Request (TER) Message

Issuers can choose to receive this network message, during Card Availability, so that they can perform an account status check or digitization risk analysis prior to receiving the formal digitization request (during Card Eligibility).

**NOTE: MDES does not send a TER message for merchant and commerce platform tokenization.**

TER messages are sent as Authorization Request/0100 or Financial Transaction Request/0200 message types, depending on whether the issuer is connected to the Dual Message System or Single Message System, respectively.

### Message Request and Issuer Processing Details

In addition to including the information contained in an Account Status Inquiry (ASI), the TER message can contain other information about the digitization that may be used by an issuer to assess specific risks and also assist with the identification of the cardholder.

Data	Description
Device Type	The type or form factor of the device initiating the digitization request (for example, a phone, tablet, or PC). New values indicate only the form factor, rather than the exact type of device and storage technology deployed by the device.
Wallet ID (WID)	Typically the ID of the program or service associated with the Wallet Provider, see Token Requestor ID and Wallet ID.
Token Requestor ID (TRID)	The ID assigned by Mastercard or the Token Service Provider (TSP) to the Token Requestor.
Storage Technology	A value indicating the storage technology of the requested token.

The following additional data may be supplied.

Data	Description
Correlation ID	A unique value assigned to a card digitization, enabling issuers to link the pre-digitization messages relating to that digitization. For example, if a cardholder enters an invalid CVC 2 during digitization, the multiple Card Eligibility request messages will have the same Correlation ID.
Account PAN Source	The Wallet Provider may indicate the method of Account PAN capture (for example, manually entered by the cardholder or 'card on file' from the Wallet Provider). Values: <ul style="list-style-type: none"> <li>• 1 = Card on File</li> <li>• 2 = Card added manually</li> <li>• 3 = Card added via application</li> </ul>
Payment Application Instance ID	The identifier associated with the payment application instance on a device. The Wallet Provider's TIP describes what this field provides. In the case of Apple Pay, this field provides the Secure Element ID (SE ID) for the token. The issuer may perform checks against lists of payment application instances or Secure Elements that are associated with devices that have been reported as lost or stolen by their cardholders so that they may decline digitization to such devices.
<b>NOTE: Mastercard does not maintain a list of devices and does not expect Wallet Providers to maintain such a list.</b>	
Number of Active Tokens for the Account PAN	The number of active or suspended tokens for the Account PAN digitized to devices.  An issuer can limit the number of active digital devices per card and decline any further digitization requests. MDES allows an unlimited number of active tokens (SE or cloud-based) per Account PAN, refer to Token Designation Service.

Data	Description
Wallet Provider Account ID Hash	<p>When provided by the Wallet Provider, the issuer may use this hash value to match against known identifiers for the cardholder; for example, their email addresses on file. If the hash values match, this may aid an issuer's digitization decision by providing additional factors to help verify that the Wallet Provider account holder is indeed their cardholder, or to differentiate between primary and secondary cardholders.</p> <p>The Wallet Provider computes the hash over an email address; MDES receives this and includes it in the data sent to the issuer. The issuer computes the hash of the email address on file for the cardholder; if it matches the hash of the one received from the Wallet Provider, the comparison with the hash value received from the Wallet Provider may be used by the issuer to assist determining the digitization decision. Hashing is used to help the issuer verify the cardholder email (or other relevant identifiers that the issuer may have for the cardholder) without the Wallet Provider providing the full email for privacy and security reasons.</p> <p>When the Wallet Provider is Apple Pay, the hash is generated using the PBKDF2 algorithm (PKCS #5). PBKDF2 is performed using 10 iterations, a salt, and the lowercase account ID as the password. The salt is calculated by taking the lower case UTF-8 bytes from the account ID and performing a SHA-256. Hash calculation example:</p> <ul style="list-style-type: none"> <li>• Input (Password): csharp@walletprovider.com</li> <li>• Salt: 41404d1bca85ddb59ab21466e277ac1ac5f61470be120c82a21b1e45b52 48123</li> <li>• Count: 10</li> <li>• Output: 7098014b646d44c6f3b454c5d54f7a32b3b46e2b0c8e2367f3e5307e303 6dfe6</li> </ul> <p><b>Java Example</b></p> <pre> public static void main(String[] args) throws UnsupportedEncodingException, DecoderException, NoSuchAlgorithmException, InvalidKeySpecException {     pbkdf2Hash("email address:cardholdername@walletprovider.com"); }  private static void pbkdf2Hash(String in) throws NoSuchAlgorithmException, InvalidKeySpecException {     int iterations = 10;     int keyLength = 32 * 8;     MessageDigest digest = MessageDigest.getInstance ("SHA-256");     [] salt =     digest.digest(in.toLowerCase().getBytes(StandardCharsets.UTF_8));      char[] passwordChars = in.toLowerCase().toCharArray();     SecretKeyFactory skf =     SecretKeyFactory.getInstance( "PBKDF2WithHmacSHA256" );     PBEKeySpec spec = new PBEKeySpec( passwordChars, salt,     iterations, keyLength );     SecretKey key = skf.generateSecret( spec ); } </pre>

Data	Description
	<pre>String hashedStrings = Hex.encodeHexString(key.getEncoded()); System.out.println(hashedStrings); }</pre>
C# Example	<pre>public static byte[] pbkdf2Hash(String password) {     int iterations = 10;     int length = 32;     byte[] bytes = Encoding.UTF8.GetBytes(password.ToLower());     SHA256Managed hashstring = new SHA256Managed();     byte[] salt = hashstring.ComputeHash(bytes);     var pbkdf2 = new Rfc2898DeriveBytes(password, salt, iterations,     HashAlgorithmName.SHA256);     return pbkdf2.GetBytes(32); }</pre>
	<p>For all other Wallet Providers, the field contains the hash resulting from the following ‘accountIdHash’ algorithm, right-padded with spaces. ‘accountId’ is the lower case UTF-8 bytes of the account ID:</p> <pre>public String accountIdHash (String accountId) {     String random8Bytes = 123CCB2F30BA420B     return random8Bytes + lessSignificant24bytes(strongerHash(accountId + random8Bytes)) } public String strongerHash(String dataToHash) {     String currentHash = dataToHash;     for (int i = 0; i &lt; 5000; i++) {         currentHash = sha256(currentHash);     }     return sha256(sha256(dataToHash) + currentHash); }</pre>

**NOTE: “String random8Bytes = 123CCB2F30BA420B” is a fixed value for all Wallet Providers.**

Hash calculation example:

- email address: cardholdername@walletprovider.com
- accountId: 63617264686F6C6465726E616D654077616C6C657470726F76696465722E636F6D
- random8Bytes: 123CCB2F30BA420B
- output:  
123CCB2F30BA420B2476A8250E0E146164385A34D34CC9E3A5680D7C5252C481

Cardholder Name	When the cardholder name is provided by the Wallet Provider, the issuer may be able to match it against the cardholder name on file. The issuer may also be able to differentiate between primary and secondary cardholders.
-----------------	--

---

Data	Description
Token Type	The value indicating the type of token: <ul style="list-style-type: none"> <li>• C = Mastercard Cloud-Based Payments (MCBP)</li> <li>• S = Embedded Secure Element</li> <li>• F = Card on File</li> </ul>

---

### Tokenization Eligibility Request (TER) Response Details

The response to the TER should indicate 'Approve' (DE 39 = 00), 'Approve, but require authentication' (DE 39 = 85) or 'Decline' (DE 39 = 05 or any other value) digitization.

The issuer may also include the following additional data within the TER response.

---

Data	Description
Issuer Product Configuration ID	Provided when an issuer wants to display different card art and card text from the defaults for the card's account range; refer to the Card Art and Associated Data for MDES appendix. The Issuer Product Configuration ID can be right-padded and left-padded with spaces.
PAN Sequence Number	Provided when an issuer has identified a specific card or cardholder from the data provided in the TER message. For more information, see the Account PAN Sequence Number section.
Activation Methods	Provided when the card eligibility decision is 'Approve, but require authentication', and the issuer wants to provide cardholder-specific communication channels for the distribution of an Activation Code to the cardholder.  Multiple Activation Methods may be provided. The number of methods depends on the available space within DE 124, which has 199 characters available.

**NOTE: The Activation Methods are detailed in the About Activation Methods section.**

---

### Account PAN Sequence Number

The Account PAN Sequence Number may be used by an issuer to identify a specific card or cardholder. Examples of how this might be used include:

- An Account PAN may have two cards associated with it: one for the primary cardholder and one for their partner. Each person is given a different Account PAN Sequence Number to distinguish between them.

- An Account PAN may have expired. When the issuer updates the card, the issuer re-uses the same Account PAN, updates the expiry date, and increments the Account PAN Sequence Number to denote the new generation of card.
- A card with multiple products can use the Account PAN Sequence Number to distinguish between products, for example, one number for credit and another for debit.

If the issuer knows, or can uniquely identify, the specific card or cardholder from the data provided in the TER or TAR messages, the issuer can include an Account PAN Sequence Number in the TER or TAR responses, so that it is then known to, and retained by, MDES. Mastercard can then include the Account PAN Sequence Number in the relevant transaction messages to the issuer, enabling the issuer to relate them to the specific card or cardholder. For more information, refer to “Global 534—Card Sequence Number in Mastercard Digital Enablement Service Transactions,” Release 17.Q2 article.

**NOTE: If the Account PAN Sequence Number is not known, or is not uniquely identifiable, at the time of the TER or TAR messages and responses, it is still possible for the issuer to provide the Account PAN Sequence Number later in the process, via an Issuer File Update Request/0302, a bulk file, or the MDES Customer Service Tools (Application or API).**

**The Account PAN Sequence Number must be a value in the range 000–099. If the issuer sends an invalid number (via a TER or TAR message, the Pre-Digitization API, an Issuer File Update Request/0302, or a bulk file), it will be ignored. If the issuer tries to update the token with an invalid number via the Customer Service Tools, the update request will be rejected.**

## Related Concepts

[Card Art and Associated Data for MDES](#)

# Card Eligibility

---

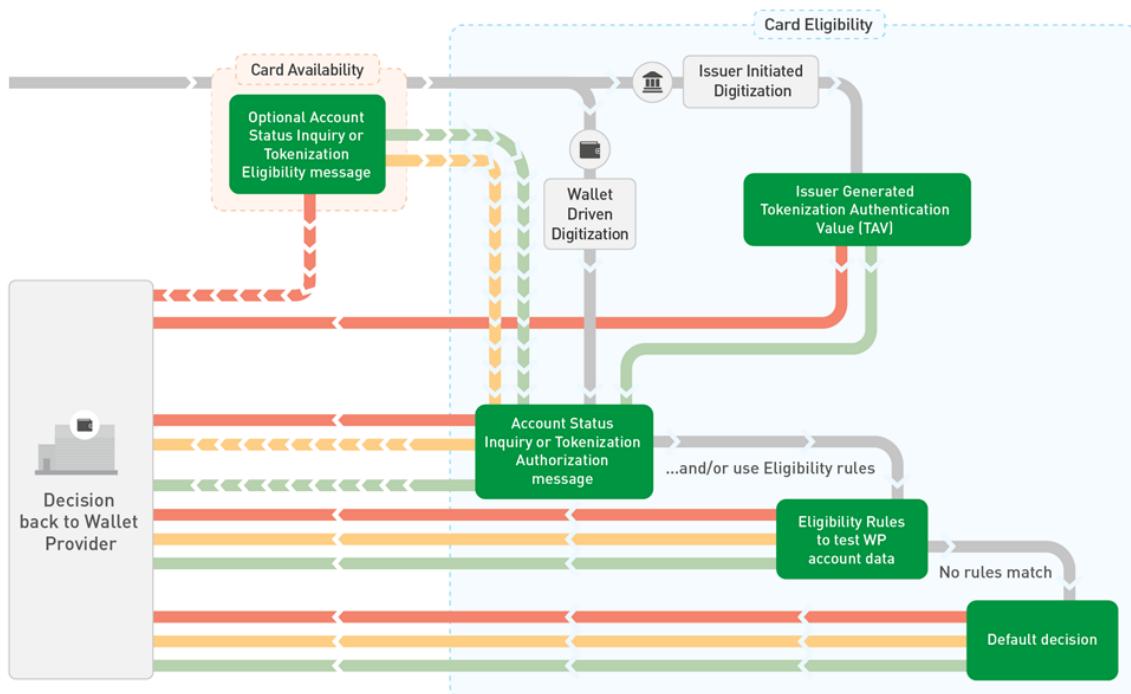
Card Eligibility determines whether a card can be digitized to a specific device or server (depending on the MDES program or implementation) when the cardholder, Wallet Provider or Token Requestor requests digitization.

## Overview

MDES provides the issuer with a number of options and tools to determine whether a card is eligible for digitization.

The following diagram shows the high-level Card Eligibility process.

**Figure 7: High-Level Eligibility Decision Process**



These eligibility options are configured during issuer enablement (refer to the Issuer Enablement section). The eligibility outcome is one of the following decisions.

Decision	Outcome
Approve	<p>Approve the digitization request without further cardholder interaction.</p> <p>The Wallet Provider is informed. The Account PAN is tokenized and the token is provisioned to the target device, server or solution. Refer to Tokenization Completion and Provisioning.</p> <p>The token is active and can be used for transactions.</p>
Approve, but require authentication	<p>Approve the digitization request but seek additional cardholder authentication.</p> <p>The Wallet Provider is informed. The Account PAN is tokenized and the token is provisioned to the target device, server or solution. However:</p> <ul style="list-style-type: none"> <li>For wallet programs, the token is in an <b>inactive</b> state. Additional cardholder authentication is required before the token is activated and can be used for transactions. Refer to Cardholder Authentication and Token Activation.</li> <li>For merchant and commerce platform tokenization, the token is <b>active</b> and can be used for transactions. The token has a Token Assurance Level (TAL) value of 00 (Not Authenticated). Additional cardholder authentication is not required, but doing it can change the token's TAL value, which might provide a higher expected transaction approval rate.</li> </ul>

---

Decision	Outcome
Decline	<p>Reject the digitization request.</p> <p>The Wallet Provider is informed, and no further activities are performed for this specific digitization.</p>

---

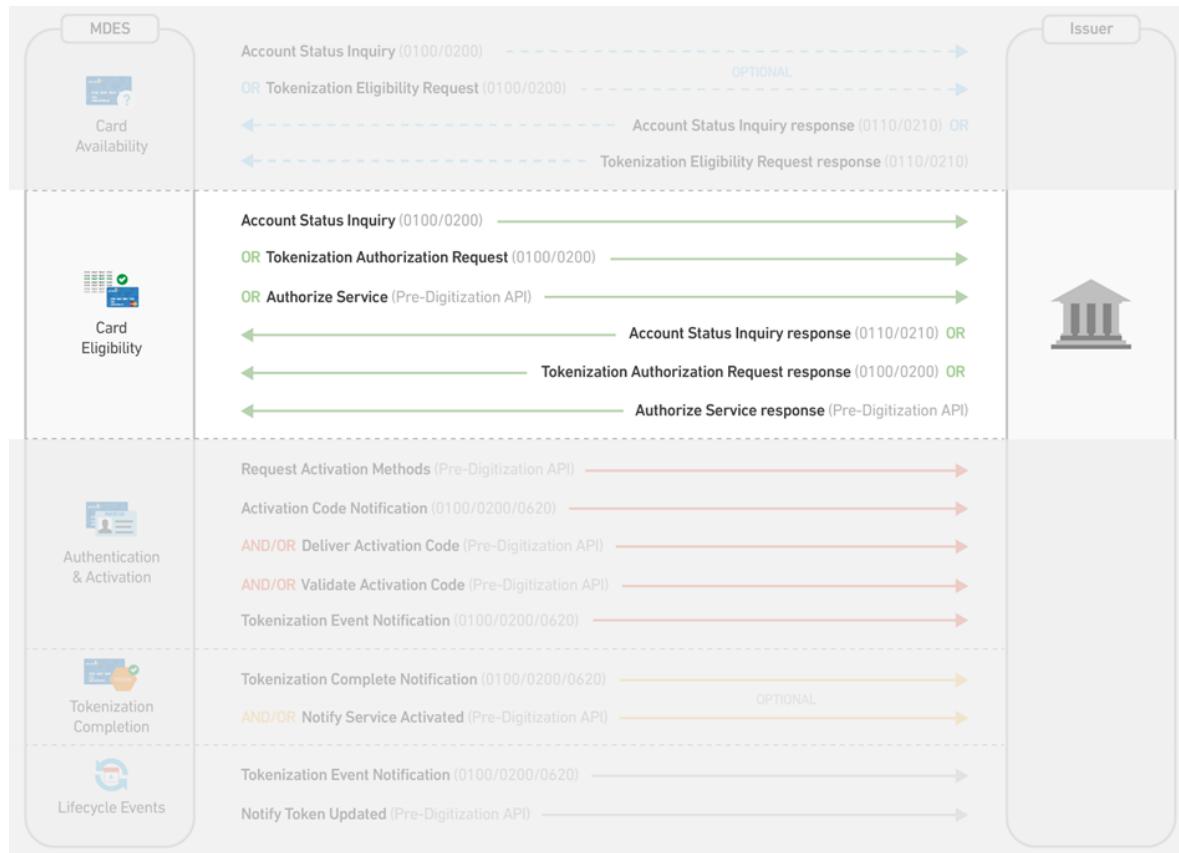
If the issuer has chosen to receive the optional Account Status Inquiry (ASI) or Tokenization Eligibility Request (TER) message during Card Availability and responds with a response of 'Decline', the eligibility decision is 'Decline' and digitization does not continue.

Eligibility can be determined through:

- **Issuer-initiated digitization**—The issuer can provide a digitization capability either directly or through their issuer mobile app.
- **Wallet-initiated digitization**—The Wallet Provider uses Card Eligibility when the cardholder has agreed to the issuer-provided Terms and Conditions and has confirmed their request to digitize their card within the wallet user interface.
- **Merchant or Commerce Platform-initiated digitization**—Participants performing merchant or commerce platform tokenization typically use Card Eligibility without any cardholder interaction.

The following diagram shows the pre-digitization messages that can be sent during Card Eligibility.

**Figure 8: Message Flows for Card Eligibility**



**NOTE: Issuers must choose whether to receive a pre-digitization network message or web service API message during Card Eligibility. They may not select both.**

The eligibility decision is determined by:

- **Card Eligibility pre-digitization messages (mandatory)**—The issuer receives messages for every digitization. The issuer may choose to receive one of the following message types:
  - An ASI network message, which includes CVC 2 and optional Address Validation Service (AVS)
  - A Tokenization Authorization Request (TAR) network message, which includes CVC 2, optional AVS, and information regarding the cardholder's Wallet Provider account and device
  - An Authorize Service API message, which includes all the information provided by a TAR message

**NOTE: When choosing the TAR or Authorize Service API message types, issuers can configure whether the eligibility rules will be used when the message response is not Decline, see Determining the Eligibility Decision.**

The issuer must delete immediately, and not store for any period of time, any data provided by the Wallet Provider (unless otherwise agreed-to between the issuer and the Wallet Provider).

- **Eligibility rules (optional)**—The issuer may define rules to determine eligibility based on the Wallet Provider-supplied account data elements or the issuer's message response values. Each rule determines whether digitization is 'Approve,' 'Approve, but require authentication,' or 'Decline.' However, if some of the data cannot be supplied by a Wallet Provider, the issuer can configure the rules to ignore this and continue to process only the data supplied.

Eligibility rules are executed in the following circumstances:

- When the ASI response is received from an issuer and the response code is not a 'Decline'
  - When the ASI response is not received from an issuer
  - When the TAR or Authorize Service response is not a Decline and the issuer chose the 'USE RULES' message option (for TAR) or 'FOR RULES' message option (for Authorize Service)
  - When the TAR or Authorize Service response is not received from an issuer
- **Default eligibility decision (mandatory)**—The issuer-configured default decision is used if the issuer's eligibility rules fail to determine a decision.

## Determining the Eligibility Decision

The pre-digitization message response is the first contributor to determining the eligibility decision. When an issuer responds to the pre-digitization message and the response indicates a Decline (DE 39 is not 00 or 85, or Decision value in the Authorize Service API response is DECLINED), the eligibility decision is Decline and digitization does not continue. This applies regardless of whether the issuer selects to receive an ASI, TAR, or Authorize Service message.

When the pre-digitization message response is not a Decline, the decision is determined by either the response or the eligibility rules and/or default decision for the account range, or a combination of both. The issuer configures these options in issuer enablement.

There are several configurations for processing pre-digitization network messages during Card Eligibility:

- **NONE**—The issuer does not receive a network message but must select and receive the Authorize Service API message.
- **ASI WITH CVC2 AND AVS**—The issuer receives an ASI message and when the response code is Approve, the decision is determined by the eligibility rules or the default decision.
- **TOKENIZATION AUTHORIZATION MESSAGE USE RESPONSE CODE**—The issuer receives a TAR and the response code indicates the 'Approve' or 'Approve, but require authentication' decision. **The eligibility rules and/or default decision are not used.**
- **TOKENIZATION AUTHORIZATION MESSAGE USE RULES**—The issuer receives a TAR and unless the response code indicates 'Decline,' the eligibility rules or default decision determine the decision.

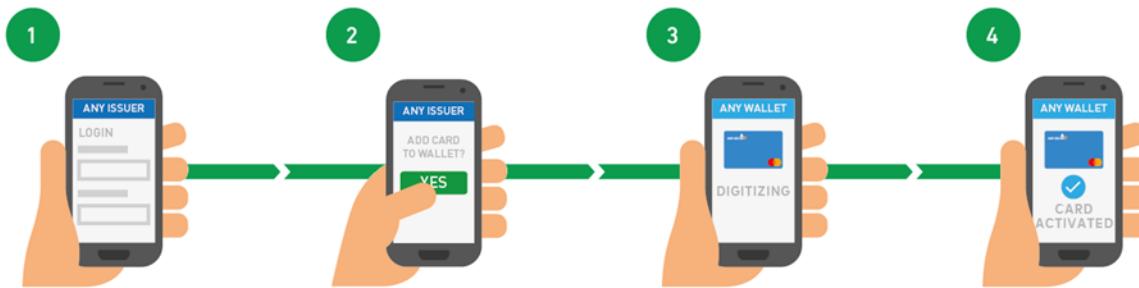
There are three configurations for processing web service API messages:

- NONE—The issuer does not receive an Authorize Service message but must select and receive a network message.
- AUTHORIZE SERVICE WEBSERVICE—The issuer receives an Authorize Service API message and the response indicates the ‘Approve’ or ‘Approve, but require authentication’ decision. **The eligibility rules and/or default decision are not used.**
- AUTHORIZE SERVICE WEBSERVICE FOR RULES—The issuer receives an Authorize Service response and unless the Decision value indicates ‘DECLINED,’ the eligibility rules or default decision determine the decision.

## Issuer-Initiated Digitization

Issuer-initiated digitization provides a digitization capability from an issuer, either directly or through an issuer’s mobile app, delivering an optimized consumer experience to digitize a card into a wallet application. It eliminates the need for a cardholder to enter card details in the wallet.

**Figure 9: High-Level User Experience for Issuer App-Initiated Digitization**



Wallet Providers define the proprietary APIs to be used by an Issuer App or an issuer’s server to push a digitization. MDES can process the following data:

- Encrypted card information (required)
- Tokenization Authentication Value (TAV) is highly recommended for all wallets except Apple Pay and Google where it is mandatory

For wallet programs other than Apple Pay, the issuer-initiated digitization data is intended to be passed through to MDES with the encrypted card information and TAV unchanged by the Wallet Provider.

**NOTE: The pass-through mechanism described in this guide does not apply to Apple Pay, where Apple re-encrypts the issuer-initiated digitization data; refer to the Apple Pay wallet API documentation.**

The Wallet Provider should also include the following data within their APIs:

- Network identifier—Enables the wallet to identify which brand is associated with the request (note that the encryption of the sensitive financial account information described in this document is only relevant to the Mastercard brand)
- Last four digits of the Account PAN—The wallet can display this with the token so that a cardholder can see the token is linked to their card

During the typical digitization workflow for wallet programs, the issuer's Terms and Conditions are returned by MDES to the Wallet Provider and then presented to the cardholder for acceptance before proceeding with digitization. Depending on the desired user experience, the Terms and Conditions may be presented by the wallet user interface, or alternatively the wallet application may pass the Terms and Conditions back to the Issuer App to be shown on the Issuer App user interface.

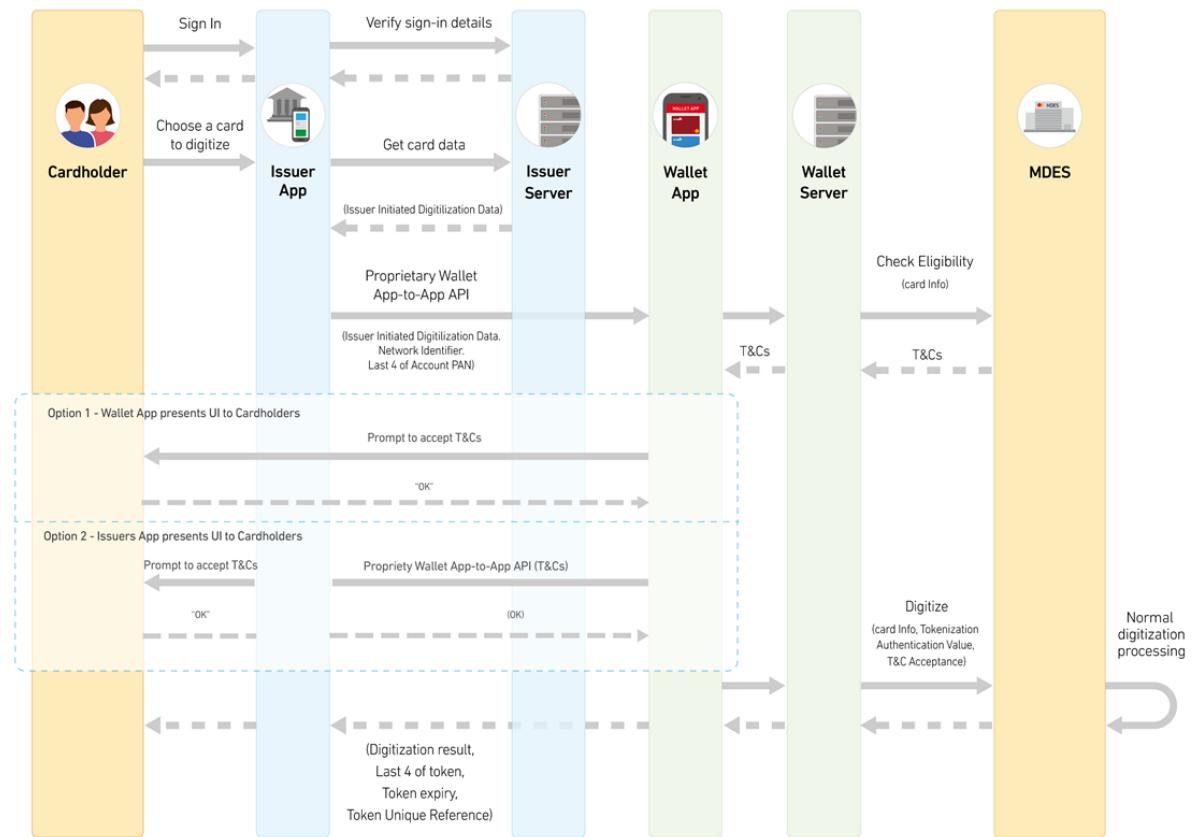
It is recommended that the complete issuer-initiated digitization data is passed to the Wallet Provider such that it can be considered a single blob of data that will not be affected by any specific API mechanism used by the app or server APIs. Additional data fields can be passed over the API using the format determined by the Wallet Provider.

A Wallet Provider should implement asynchronous APIs to initiate the digitization processes and should therefore provide a call-back mechanism so that the Issuer App may be informed of the result of the digitization processes.

Following digitization, a Wallet Provider may return some or all of the following data to the Issuer App or issuer server:

- Indication of success or failure—Reasons for failure are many and varied, so a Wallet Provider should consider which failures are appropriate to report to an issuer. Only situations that would allow the issuer to resolve a failure should be reported in detail, so that the issuer can take necessary corrective measures.
- Last four digits of the token—An issuer may want to display the last four digits of the token associated with a transaction, to provide a more complete statement facility.
- Token Expiration Date—An issuer may want to display the expiration date of the token, which will be different to that of the digitized card, within their Issuer App.
- Token Unique Reference—This value allows an issuer to perform lifecycle management activities using the MDES Customer Service API. Providing the value to the Issuer App may simplify consumer-driven lifecycle activities if deployed within the Issuer App and would, for example, permit the cardholder to delete a wallet token from within the Issuer App.
- Payment Application Instance ID—This value can assist the issuer in determining which device the card has been digitized to.

**Figure 10: Example of an Issuer App-Initiated Digitization Sequence**



### Issuer-Initiated Digitization Data Object Layouts

**NOTE: The field names stated here are examples of the field names that a proprietary App-to-App API could have.**

The **IssuerInitiatedDigitizationData** object is a base64-encoded JSON structure containing the following fields:

Suggested Object Name	Suggested Object Contents	Usage
<b>IssuerInitiatedDigitizationData</b>	cardInfo	Should only contain card data. Should not be provided if fundingAccountInfo present.
	fundingAccountInfo	Can contain card data or non-card based payments. Should not be provided if cardInfo present.
	tokenizationAuthenticationValue	(string, max length 2048), which is cryptographically-signed by the issuer to pre-authorize this digitization request.

The fundingAccountInfo field supersedes the cardInfo field for supplying encrypted card data. The introduction of the FundingAccountInfo object is to prepare Mastercard for future opportunities to support non-card-based payments. Customers will be informed of the details when such funding account use cases are implemented.

The issuer and wallet performing the issuer-initiated digitization must either both use cardInfo or both use fundingAccountInfo. The data structure must persist when the wallet is passing the information through to Mastercard. Issuers must follow the wallet's guidelines on support of the CardInfo object, the FundingAccountInfo object or both, and on any migration plan from the CardInfo object to the FundingAccountInfo object defined for the wallet.

**NOTE: The object used to provide a wallet with encrypted card information in an issuer-initiated digitization flow can differ from the object the issuer chooses to receive in pre-digitization messages. For example, an issuer can provide a wallet with the CardInfo object while being configured to receive the FundingAccountInfo object in Pre-Digitization API messages.**

The **FundingAccountInfo** object is a JSON structure containing the following fields.

Field and Description	Data Type	Max Length	Required?
<b>panUniqueReference</b>  For repeat digitizations (when the issuer supports it), the unique reference allocated to the financial account will be used to retrieve the financial account information. When supplied, the account information is omitted from FundingAccountData.  Only allowed if tokenUniqueReference is not present and encrypted data does not contain the account information.	String	64	Conditional

Field and Description	Data Type	Max Length	Required?
<b>tokenUniqueReference</b>  A unique reference assigned following the allocation of a token used to identify the token for the duration of its lifetime. For repeat digitizations (when the issuer supports it), the unique reference allocated to the token will be used to retrieve the financial account information. When supplied, the account information is omitted from FundingAccountData.	String	64	Conditional
<b>encryptedPayload</b>  Contains an encrypted FundingAccountData object.  Required if panUniqueReference and tokenUniqueReference are not present.	String. Hex-encoded data (case-insensitive).	N/A	Conditional

The **EncryptedPayload** object is a JSON structure containing the following fields.

Field and Description	Data Type	Max Length	Required?
<b>publicKeyFingerprint</b>  The fingerprint of the public key used to encrypt the ephemeral AES key.	String. Hex-encoded data (case-insensitive).	64	Yes
<b>encryptedKey</b>  One-time use AES key encrypted by the Mastercard public key (as identified by 'publicKeyFingerprint') using the OAEP or RSA Encryption Standard PKCS #1 v1.5 (depending on the value of 'oaepHashingAlgorithm').  Requirement is for a 128-bit key (with 256-bit key supported as an option).	String. Hex-encoded data (case-insensitive).	512	Yes
<b>oaepHashingAlgorithm</b>  Hashing algorithm used with the OAEP scheme. If omitted, then the RSA Encryption Standard PKCS #1 v1.5 will be used. Must be one of: <ul style="list-style-type: none"><li>• SHA256 = Use the SHA-256 algorithm</li><li>• SHA512 = Use the SHA-512 algorithm</li></ul>	String	6	No

Field and Description	Data Type	Max Length	Required?
<b>iv</b> The initialization vector used when encrypting data using the one-time use AES key. Must be exactly 16 bytes (32 character hex string) to match the block size. If not present, an IV of zero is assumed.	String. Hex-encoded data (case-insensitive).	32 (exact)	No
<b>encryptedData</b> Contains the encrypted FundingAccountData JSON object. Encrypted by the ephemeral AES key using CBC mode (IV as provided in 'iv', or zero if none provided) and PKCS#7 padding. The JSON object being encrypted will be defined in the context of the API call.	String. Hex-encoded data (case-insensitive).	256 K	Yes

The **FundingAccountData** object is a JSON structure containing the following fields.

Field and Description	Data Type	Max Length	Required?
<b>cardAccountData</b> The credit or debit card information for the account that is being tokenized. Required if financialAccountData is not present unless a valid panUniqueReference or tokenUniqueReference was given in FundingAccountInfo.	CardAccountData	N/A	Conditional
<b>financialAccountData</b> The financial account information for non-card based payment that is being tokenized. This could be a bank account or other type of financial account. Required if cardAccountData is not present unless a valid panUniqueReference or tokenUniqueReference was given in FundingAccountInfo.	FinancialAccountData	N/A	Conditional
<b>accountHolderData</b> Additional information that can be used to identify the account holder, such as name and address.	AccountHolderData	N/A	No

Field and Description	Data Type	Max Length	Required?
<b>source</b> The source of the account information. Must be one of: <ul style="list-style-type: none"> <li>• ACCOUNT_ON_FILE = Source was an existing account on file</li> <li>• ACCOUNT_ADDED_MANUALLY = Source was new account entered manually by the account holder</li> <li>• ACCOUNT_ADDED_VIA_APPLICATION = Source was new account added by another application (for example, Issuer banking app)</li> </ul>	String	32	Yes
<b>dataValidUntilTimestamp</b> The date/time after which this encrypted object is considered invalid. If present, all systems must reject this encrypted object after this time and treat it as invalid data.  Must be expressed in ISO 8601 extended format as one of the following, where [.sss] is optional and can be 1–3 digits: <ul style="list-style-type: none"> <li>• YYYY-MM-DDThh:mm:ss[.sss]Z</li> <li>• YYYY-MM-DDThh:mm:ss[.sss]±hh:mm</li> </ul> Must be a value no more than 30 days in the future. Mastercard recommends using a value of Current Time + 30 minutes.	String	29	No

The **CardAccountData** object is a JSON structure containing the following fields.

Field and Description	Data Type	Max Length	Required?
<b>accountNumber</b> The Account Primary Account Number of the card to be digitized.  Required unless a valid panUniqueReference or tokenUniqueReference was given in FundingAccountInfo.	String (numeric)	19 (min length 9)	Conditional
<b>expiryMonth</b> The month of the expiration date of the card to be digitized. Note that the expiry date may not be in the past. May be omitted if the card does not have an expiry date.  Required unless a valid panUniqueReference or tokenUniqueReference was given in FundingAccountInfo.	String (numeric)	2 (exact)	Conditional

Field and Description	Data Type	Max Length	Required?
<b>expiryYear</b> The year of the expiration date of the card to be digitized. Note that the expiry date may not be in the past. May be omitted if the card does not have an expiry date. Required unless a valid panUniqueReference or tokenUniqueReference was given in FundingAccountInfo.	String (numeric)	2 (exact)	Conditional

The **FinancialAccountData** object is a JSON structure containing the following fields.

Field and Description	Data Type	Max Length	Required?
<b>financialAccountId</b> The identifier of the financial account being tokenized. This could be a bank account number, or identifier or other types of financial accounts.	String (spaces not allowed)	64 (min length 9)	Yes
<b>interbankCardAssociationId</b> The ID assigned by Mastercard to the financial institution.	Number	11 (min length 3)	Yes
<b>countryCode</b> The country of the financial account. Expressed as a 3-letter (alpha-3) country code as defined in ISO 3166-1.	String	3 (exact)	Yes

The **AccountHolderData** object is a JSON structure containing the following fields.

Field and Description	Data Type	Max Length	Required?
<b>accountHolderName</b> The name of the account holder in the format LASTNAME/FIRSTNAME or FIRSTNAME LASTNAME.	String	27	Optional

The **CardInfo** object is a JSON structure containing the following fields.

Field and Description	Data Type	Max Length	Required?
<b>panUniqueReference</b>  For repeat digitizations (when the issuer supports it), the unique reference allocated to the Account PAN. When supplied, the tokenUniqueReferenceForPanInfo, accountNumber, expiryMonth and expiryYear are omitted from CardInfoData.  Only allowed if tokenUniqueReferenceForPanInfo is not present and encryptedData does not contain the account information.	String	64	Conditional
<b>tokenUniqueReferenceForPanInfo</b>  For repeat digitizations (when the issuer supports it), the unique reference allocated to the token will be provided to MDES and used to retrieve the account number and expiration date. When supplied, the panUniqueReference, accountNumber, expiryMonth and expiryYear are omitted from CardInfoData.  Only allowed if panUniqueReference is not present and encryptedData does not contain the account information.	String	64	Conditional
<b>publicKeyFingerprint</b>  The fingerprint of the public key used to encrypt the ephemeral AES key.	String. Hex-encoded data (case-insensitive).	64	Yes
<b>encryptedKey</b>  One-time use AES key encrypted by the Mastercard encryption public key (as identified by 'publicKeyFingerprint') using the OAEP or PKCS#1 v1.5 scheme (depending on the value of 'oaepHashingAlgorithm').  Requirement is for at least a 128-bit key (with 256-bit key supported as an option).	String. Hex-encoded data (case-insensitive).	512	Yes
<b>oaepHashingAlgorithm</b>  Hashing algorithm used with the OAEP scheme. Must be either: <ul style="list-style-type: none"><li>• SHA256</li><li>• SHA512</li></ul> If omitted, PKCS#1 v1.5 is used.	String	6	No

Field and Description	Data Type	Max Length	Required?
<b>iv</b>  The Initialization Vector (IV) used when encrypting data using the one-time use AES key. Must be exactly 16 bytes (32 character hex string) to match the block size.  If not present, an IV of zero is assumed.	String. Hex-encoded data (case-insensitive).	32 (exact)	No
<b>encryptedData</b>  Contains the encrypted CardInfoData object. Encrypted by the ephemeral AES key using CBC mode (IV as provided in 'iv', or zero if none provided) and PKCS#7 padding.	String. Hex-encoded data (case-insensitive).	256K	Yes

The **CardInfoData** object is a JSON structure containing the following fields.

Field and Description	Data Type	Max Length	Required?
<b>accountNumber</b>  The Account PAN of the card to be digitized.  Required unless panUniqueReference or tokenUniqueReferenceForPanInfo is provided in CardInfo.	String (numeric)	19 (min length 12)	Conditional
<b>expiryMonth</b>  The month of the expiration date of the card to be digitized. May be omitted if the card does not have a visible expiry date. The expiry date cannot be in the past.  Not required if panUniqueReference or tokenUniqueReferenceForPanInfo is provided in CardInfo or the card does not have an expiry date.	String (numeric)	2 (exact)	Conditional
<b>expiryYear</b>  The year of the expiration date of the card to be digitized. May be omitted if the card does not have a visible expiry date. The expiry date cannot be in the past.  Not required if panUniqueReference or tokenUniqueReferenceForPanInfo is provided in CardInfo or the card does not have an expiry date.	String (numeric)	2 (exact)	Conditional
<b>source</b>  The source of this card information. Must be: CARD_ADDED_VIA_APPLICATION	String	32	Yes

Field and Description	Data Type	Max Length	Required?
<b>cardholderName</b>  The name of the cardholder in the format LASTNAME/FIRSTNAME or FIRSTNAME LASTNAME.  Required unless panUniqueReference or tokenUniqueReferenceForPanInfo is provided in CardInfo.	String	27	Conditional
<b>billingAddress</b>  The billing address for the card to be digitized. Verified as part of reaching the digitization decision.	BillingAddress object	N/A	No
<b>dataValidUntilTimestamp</b>  The date/time after which this CardInfoData object is considered invalid. If present, all systems must reject this CardInfoData object after this time and treat it as invalid data.  Must be expressed in ISO 8601 extended format as one of the following, where [.sss] is optional and can be 1–3 digits: <ul style="list-style-type: none"><li>• YYYY-MM-DDThh:mm:ss[.sss]Z</li><li>• YYYY-MM-DDThh:mm:ss[.sss]±hh:mm</li></ul> Must be a value no more than 30 days in the future. Mastercard recommends using a value of Current Time + 30 minutes.	String	29	No

The **BillingAddress** object is a JSON structure containing the following fields.

Field and Description	Data Type	Max Length	Required?
<b>line1</b>  The first line of the billing address.	String	64	No
<b>line2</b>  The second line of the billing address.	String	64	No
<b>city</b>  The city of the billing address.	String	32	No
<b>countrySubdivision</b>  The country subdivision (for example, the state in the U.S.) of the billing address.	String	12	No

Field and Description	Data Type	Max Length	Required?
<b>postalCode</b> The postal code (for example, zipcode in the U.S.) of the billing address.	String	16	No
<b>country</b> The country of the billing address, expressed as a 3-letter (alpha-3) country code as defined in ISO 3166-1.	String	3 (exact)	No

## Encryption of Card Information

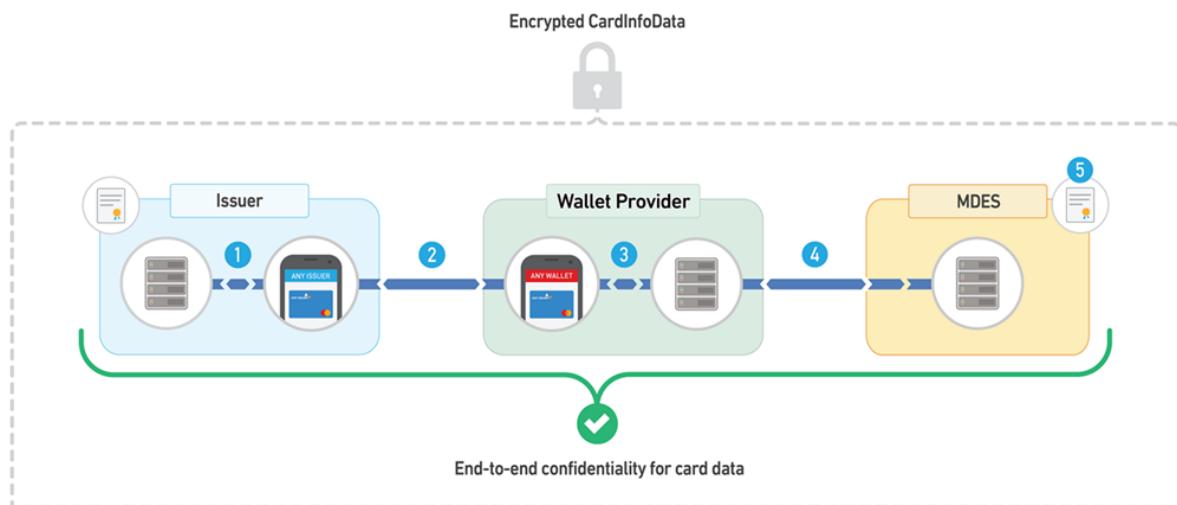
MDES receives card information in an encrypted format from an issuer via the Wallet Provider.

For wallet programs other than Apple Pay, the Wallet Provider provides a simple pass-through mechanism for the encrypted data package. This ensures the security of sensitive data for Wallet Providers who typically do not wish to deploy technology needed to protect the card information in conformance with PCI-DSS standards.

The pass-through mechanism described in this guide does not apply to Apple Pay; refer to the Apple Pay wallet API documentation.

The following diagram shows an example implementation where an Issuer App communicates with a Wallet Provider's wallet application to initiate the digitization of the card:

1. The Issuer App uses proprietary APIs that link it to the issuer's server, where the encryption of the card details is performed.
2. The Wallet Provider publishes an API for the issuer to use to pass the encrypted card data to the wallet application.
3. The wallet application uses proprietary APIs to pass the encrypted card data to the Wallet Provider server.
4. The Wallet Provider server calls the MDES API to initiate the digitization request.
5. MDES identifies the key that was used to encrypt the data from the issuer and decrypts the card details.



While this diagram shows an app-based approach, an issuer and Wallet Provider may also communicate using server-to-server connections. For example, this would enable an issuer to initiate digitization of a card from an online banking website into a server-based Wallet Provider, such as a large online merchant who wants to use tokens to initiate transactions (merchant tokenization) rather than capturing card details from cardholders.

### Requesting the Mastercard Encryption Public Key

For wallet programs other than Apple Pay, issuers must obtain the Mastercard RSA 2048-bit Public Key for encrypting their card details. Requesting the Public Key reuses existing Mastercard Key Management Services (KMS), but is mediated by the Mastercard Customer Implementation Services (CIS) team. Contact your CIS representative for more information on requesting the Mastercard encryption Public Key.

The issuer must insert the fingerprint of the Mastercard encryption Public Key into the publicKeyFingerprint field of the encryptedPayload field of the fundingAccountInfo object (or of the CardInfo object).

For Apple Pay, a different encryption key and process is used; refer to the Apple Pay wallet API documentation.

### Encrypting the Ephemeral AES Key

To create the encryptedKey field in the encryptedPayload field of the fundingAccountInfo object (or in the CardInfo object), the issuer:

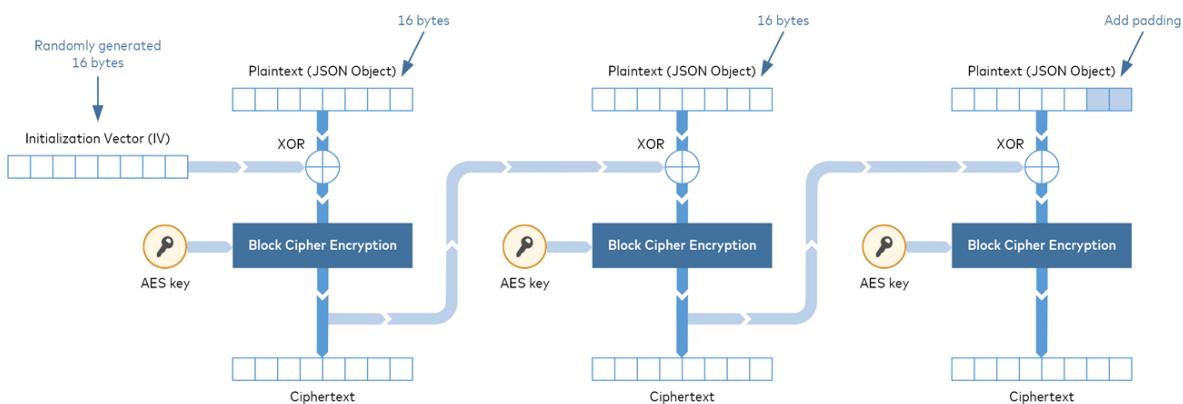
1. Generates a random 128-bit or 256-bit ephemeral AES key.
2. Determines the hashing algorithm to use with the OAEP scheme (SHA-256 or SHA-512) and indicates the choice in the oaepHashingAlgorithm field in the encryptedPayload field of the fundingAccountInfo object (or in the CardInfo object).
3. Encrypts the AES key with the Mastercard encryption public key using the OAEP or PKCS#1 v1.5 scheme, depending on the chosen hash algorithm.

### Encrypting Card Information

To create the encryptedData field in the encryptedPayload field of the fundingAccountInfo object (or in the CardInfo object), the issuer:

1. Optionally generates a random Initialization Vector (IV) of 16 bytes (32 character hex string) and indicates the choice in the iv field. If the issuer does not generate an IV value, zero shall be assumed.
2. Encrypts the fundingAccountData object (or the cardInfoData object) with the ephemeral AES key using CBC mode, the chosen IV, and PKCS#7 padding (conforming to FIPS PUB 140-2), as shown below.

**Figure 11: Cipher Block Chaining (CBC) Mode Encryption**



Sample content for fundingAccountInfo in JSON format is shown below:

```

"fundingAccountInfo": {
    "encryptedPayload": "475BEB65433044323232637393045D815FF9825E1DDE321469537FE461E824AA55BA31764DDC202
98BD77F6A45432433610DE9FBE37EE5AB3CBDA967B1D1461"
}

```

Sample content for encryptedPayload in fundingAccountInfo is shown below:

```

{
    "publicKeyFingerprint": "4c4ead5927f0df8117f178eea9308daa58e27c2b",
    "encryptedKey": "A1B2C3D4E5F611223345566",
    "oaepHashingAlgorithm": "SHA512",
    "encryptedData": "44323232637393045DDE321469537FE461E824AA55BA67BF645454330A32433610DE1D1461475BE
B6D815F31764DDC20298BD779FBE37EE5AB3CBDA9F9825E1"
}

```

Sample content for FundingAccountData (encryptedData in encryptedPayload) is shown below:

```

{
    "cardAccountData": {
        "accountNumber": "5123456789012345",
        "expiryMonth": "12",
        "expiryYear": "18"
    },
    "accountHolderData": "John_Doe_1357",
}

```

```
        "source": "ACCOUNT_ADDED_VIA_APPLICATION"  
    }
```

Sample content for cardInfo in JSON format is shown below:

```
"cardInfo": {  
    "encryptedData":  
    "45454330443232363739304532433610DE1D1461475BEB6D815F31764DDC20298BD779FBE37EE5  
    AB3CBDA9F9825E1DDE321469537FE461E824AA55BA67BF6A",  
    "publicKeyFingerprint": "4c4ead5927f0df8117f178eea9308daa58e27c2b",  
    "encryptedKey": "A1B2C3D4E5F6112233445566",  
    "oaepHashingAlgorithm": "SHA512"  
}
```

Sample content for CardInfoData (encryptedData in cardInfo) is shown below:

```
{  
    "accountNumber": "5123456789012345",  
    "expiryMonth": "12",  
    "expiryYear": "18",  
    "source": "CARD_ADDED_VIA_APPLICATION",  
    "cardholderName": "John Doe"  
}
```

### **Issuer Pre-Authorization of Digitization—Tokenization Authentication Value (TAV)**

Depending on the implementation and functionality supported by Wallet Providers, an issuer may generate a Tokenization Authentication Value (TAV) to push a digitization request. The TAV can be used to either:

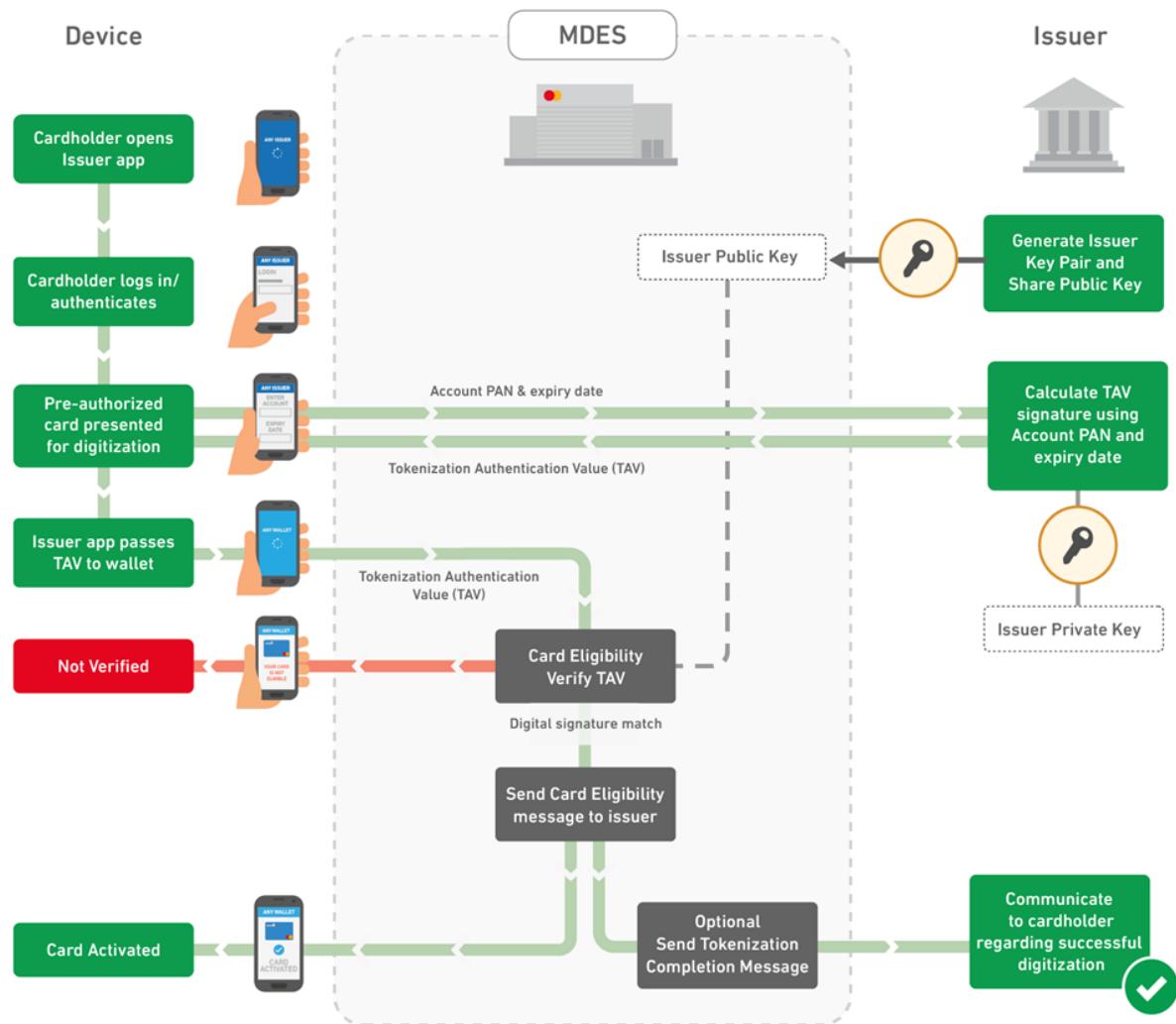
- Indicate an issuer's pre-authorization for a particular card to be digitized (prior to token allocation)
- Activate a token after it has been allocated; see Issuer App Token Activation via TAV

**NOTE: When a TAV is used to pre-authorize a card digitization, the issuer will still receive the Card Eligibility message for that card's digitization request (if the TAV signature is correctly verified). Mastercard strongly recommends that issuers authenticate the user as the cardholder of the card requested for digitization before creating the TAV and establish that the card is in good standing.**

The TAV contains a digital signature using an asymmetric key algorithm that approves the digitization of a token for an Account PAN (or any funding account).

**NOTE: Subsequent subsections provide details on the creation of a TAV, its data structure, the calculation method for the digital signature contained within the TAV, and the supporting Key Management processes.**

The following diagram shows an example of how issuer-initiated digitization using a TAV may be implemented.



MDES uses the predefined public key associated with the Account Range of the PAN to verify the signature contained in the TAV. If the signature is correct, MDES allocates the token (the issuer still receives the Card Eligibility message). If the signature is incorrect, MDES advises the Wallet Provider of a 'Decline' eligibility decision.

For issuer-initiated digitization, the Card Eligibility service does not implement a velocity count on the number of activation attempts using a TAV. If the attempt fails, it is not possible to activate a token using the MDES Customer Service tools and the digitization process has to restart from the beginning.

## TAV Creation

The Tokenization Authentication Value (TAV) is a base64-encoded JSON structure of data that has been defined in three formats.

### NOTE:

- **Issuers are advised to use TAV format 3 for any new developments.**
- **The Token Unique Reference is only relevant when requesting activation of a token that has already been allocated.**

The **TAV format 1** contains the following information:

- Version number
- Indicator of whether the optional Token Unique Reference is included in the signature calculation
- Digital signature algorithm identifier
- Digital signature calculated over:
  - Full PAN of the card being digitized
  - Expiration Date
  - Token Unique Reference Included indicator value
  - Optionally, Token Unique Reference value

The **TAV format 2** contains the following information:

- Version number
- Indicator of whether the optional Expiration Date is included in the signature calculation
- Indicator of whether the optional Token Unique Reference is included in the signature calculation
- Digital signature algorithm identifier
- Digital signature calculated over:
  - Full PAN of the card being digitized
  - Expiration Date Included indicator value
  - Optionally, Expiration Date
  - Token Unique Reference Included indicator value
  - Optionally, Token Unique Reference value

The **TAV format 3** contains the following information:

- Version number
- Digital signature algorithm identifier
- ISO 8601 format of the date and time (with Time Zone) the TAV expires
- Parameter includedFieldsInOrder which provides the field names for the values included in the digital signature calculation. The order of the field names must match the order that those field values are included in the digital signature. The field names should be concatenated into one string separated by | delimiter (UTF-8 hex 007C). List of applicable field names:

- dataValidUntilTimestamp—ISO 8601 format of the date and time (with Time Zone) the TAV expires and will no longer be honored. This time stamp field must be included, otherwise the TAV validation fails
- accountNumber—Funding Primary Account Number (FPAN) of the payment card being tokenized.

**NOTE: FPAN is required if the financialAccountInformation (FAI) is not provided**

- accountExpiry—Expiration date of the payment card being tokenized in MMYY format
- financialAccountInformation (FAI)—Identifier of the financial account being tokenized. This could be a bank account number or other types of financial accounts. The introduction of financialAccountInformation is to prepare Mastercard for future opportunities to support non-card-based payments. Customers will be informed of the details when such funding account use cases are implemented

**NOTE: FAI is required if the FPAN is not provided**

- tokenUniqueReference—Token Unique Reference associated with the token
- The accountNumber, financialAccountInformation or tokenUniqueReference must be included. Otherwise, the TAV validation fails.
- Digital signature calculated over a concatenated string of the included field values separated by a | delimiter, in the same order as specified in the includedFieldsInOrder field

### TAV Digital Signature Algorithm

The issuer includes a digital signature within the Tokenization Authentication Value (TAV).

This digital signature can be based on **RSA Algorithm**, in accordance with the PKCS#1 v2.1/RFC3447 standard.

**NOTE: For more information, refer to: <https://www.ietf.org/rfc/rfc3447.txt>**

When an RSA-based digital signature is used, the key should be of at least 2048-bits in length and less than or equal to 4096-bits in length (the Mastercard Certification Authority [CA] signing key is 4096-bits in length). The signature scheme must be RSASSA-PKCS1-v1\_5 (MDES does not support signature scheme RSASSA-PSS).

It is strongly advised that this digital signature creation process is implemented at a centralized facility and that the Private Key is retained within an appropriate secure environment. The Private Key used to create the digital signature shall not, under any circumstances, be passed to the issuer's mobile app, as the mobile app operating system environment is considered less secure and the Private Key may be more easily compromised within an accidentally or deliberately compromised device. This restriction does not, however, apply to the creation of the TAV containing the digital signature.

## Key Generation

The issuer shall create a Private/Public Key pair explicitly for the purpose of creating a Tokenization Authentication Value (TAV) digital signature.

The Public Key shall be identified using an issuer-defined Key Unique Reference and passed to the Mastercard Key Management Services (refer to the Mastercard Key Certification Process appendix) along with the issuer's CID (Customer Identifier) for certification. The Public Key is appropriate for RSA and the algorithm choice is included in the certification request.

The Public Key must be available to MDES for use in verifying a signature generated by the issuer and contained in the TAV.

The generated certificate shall be returned to the requestor. When a certificate is generated, Mastercard makes it available to MDES.

The issuer-defined Key Unique Reference shall be associated with the issuer within the issuer enablement process of MDES, accessed within the Mastercard Connect™ application. A Key Unique Reference must be associated to each issuer's funding account range. The same Key Unique Reference may be associated to multiple funding account ranges. When the same Key Unique Reference can be associated to account ranges from multiple CIDs, a certificate per CID must be requested from Mastercard Key Management Services.

Certificates have a limited lifetime (expected to be 4 years) and it is the issuer's responsibility to make sure another key is certified and configured within the MDES issuer enablement process in advance of certificate expiry.

**NOTE: The Key Unique Reference is not contained within the TAV JSON data structure.**

## TAV Digital Signature Generation

This section describes how the issuer generates the signature for the Tokenization Authentication Value (TAV).

To generate a TAV signature, the issuer should use the following process (which is shown in the diagrams below the steps):

1. The input data shall consist of a UTF-8 encoded character string consisting of the following (depending on the TAV format):
  - **TAV format 1**—A concatenated string of data:
    - Primary Account Number of the card to be tokenized (13–19 numeric digits)
    - Expiration Date of the card to be tokenized (4 numeric digits, in the format 'MMYY')
    - An indication of whether Token Unique Reference is included in the signature (either 'Y' or 'N')
    - Optional Token Unique Reference to which the TAV applies (a value of up to 48 characters)
  - **TAV format 2**—A concatenated string of data:
    - Primary Account Number of the card to be tokenized (13–19 numeric digits)
    - An indication of whether Expiration Date is included in the signature (either 'Y' or 'N')

- Optional Expiration Date of the card to be tokenized (4 numeric digits, in the format 'MMYY')
- An indication of whether Token Unique Reference is included in the signature (either 'Y' or 'N')
- Optional Token Unique Reference to which the TAV applies (a value of up to 48 characters)
- **TAV format 3**—A concatenated string of the included field values separated by a | delimiter (UTF-8 hex 007C), in the same order as specified in the includedFieldsInOrder field. Applicable field values:
  - ISO 8601 format of the date and time (with Time Zone) the TAV expires and will no longer be honored
  - Optional Primary Account Number of the card to be tokenized
  - Optional Expiration Date of the card to be tokenized
  - Optional identifier of the financial account being tokenized, such as a bank account number
  - Optional Token Unique Reference to which the TAV applies

**NOTE: The characters concatenated should be UTF-8 (also often referred to as ASCII or ISO-8559-1) encoded and not EBCDIC or any other encoding.**

2. The concatenated data shall be hashed using SHA-256 and signed using the issuer Private Key whose corresponding Public Key has been certified and associated with the issuer during the issuer enablement process.

**NOTE: This step must be performed within an appropriately secured server environment and should not be performed within an issuer's mobile app on a mobile device. It is advised that the keys used are held securely within an appropriate hardware security module (HSM).**

The algorithm used includes signing and hashing, and it shall be the RSA-based digital signature algorithm as specified by PKCS#1 v2.1/RFC3447 (specifically the method described in Section 8.2 RSASSA-PKCS1-v1\_5)."

3. The RSA signature value shall be base64 encoded and constitute the value of the digital signature within the TAV (the signature value should just be a base64-encoded representation of the raw signature bytes).

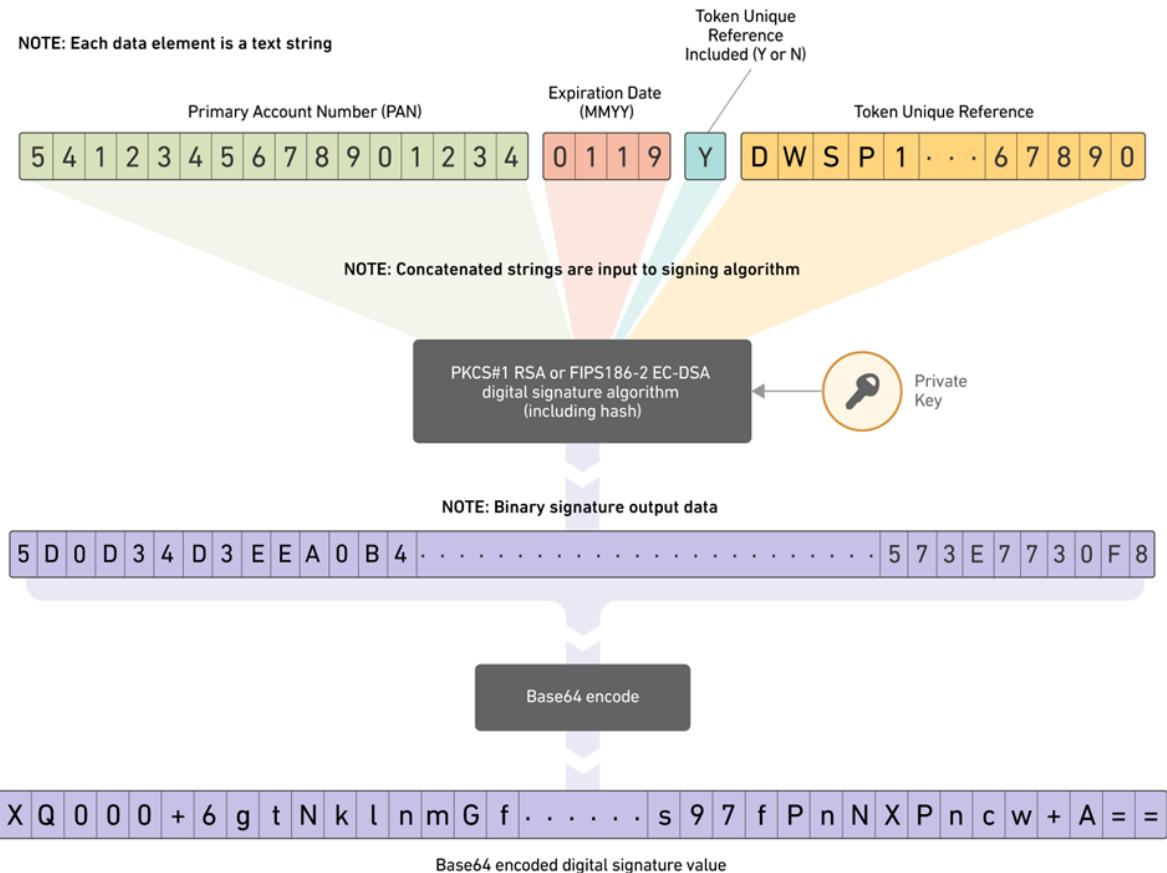
**NOTE: The input to the digital signature algorithm consists of the UTF-8 encoded strings concatenated together. There is no additional conversion required after the strings have been concatenated.**

**It is typical for developers to use an 'off the shelf' library to perform the digital signature. In such cases, it is advisable to confirm the exact digital signature algorithm implemented by the library. Using a library that does not conform to the correct specification will result in a signature that cannot be validated.**

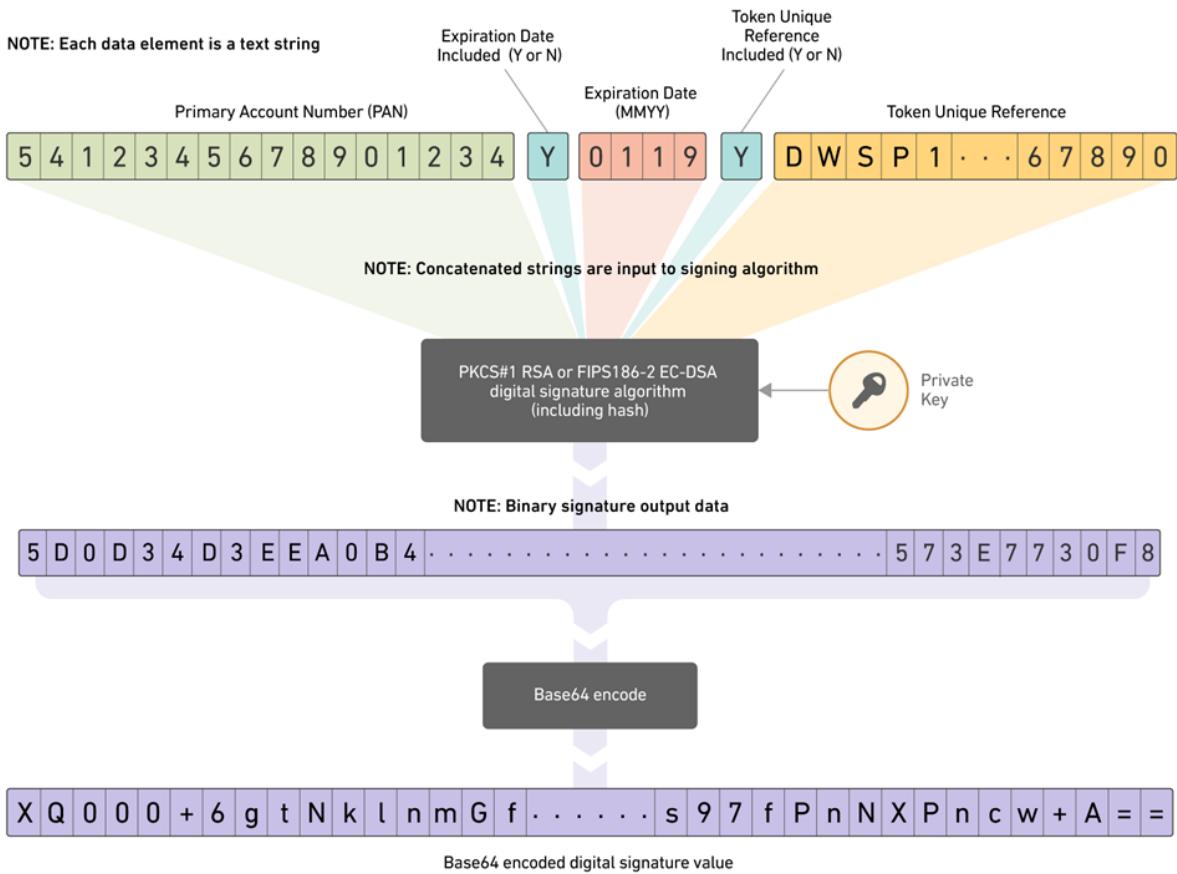
To complete the creation of the TAV, the other values of the TAV shall be inserted into the JSON structured data, and the whole TAV shall then be base64 encoded to form an

unstructured collection of data that is provided to the Wallet Provider. This activity is not shown in the diagrams below, but is covered in TAV Encoding and Examples.

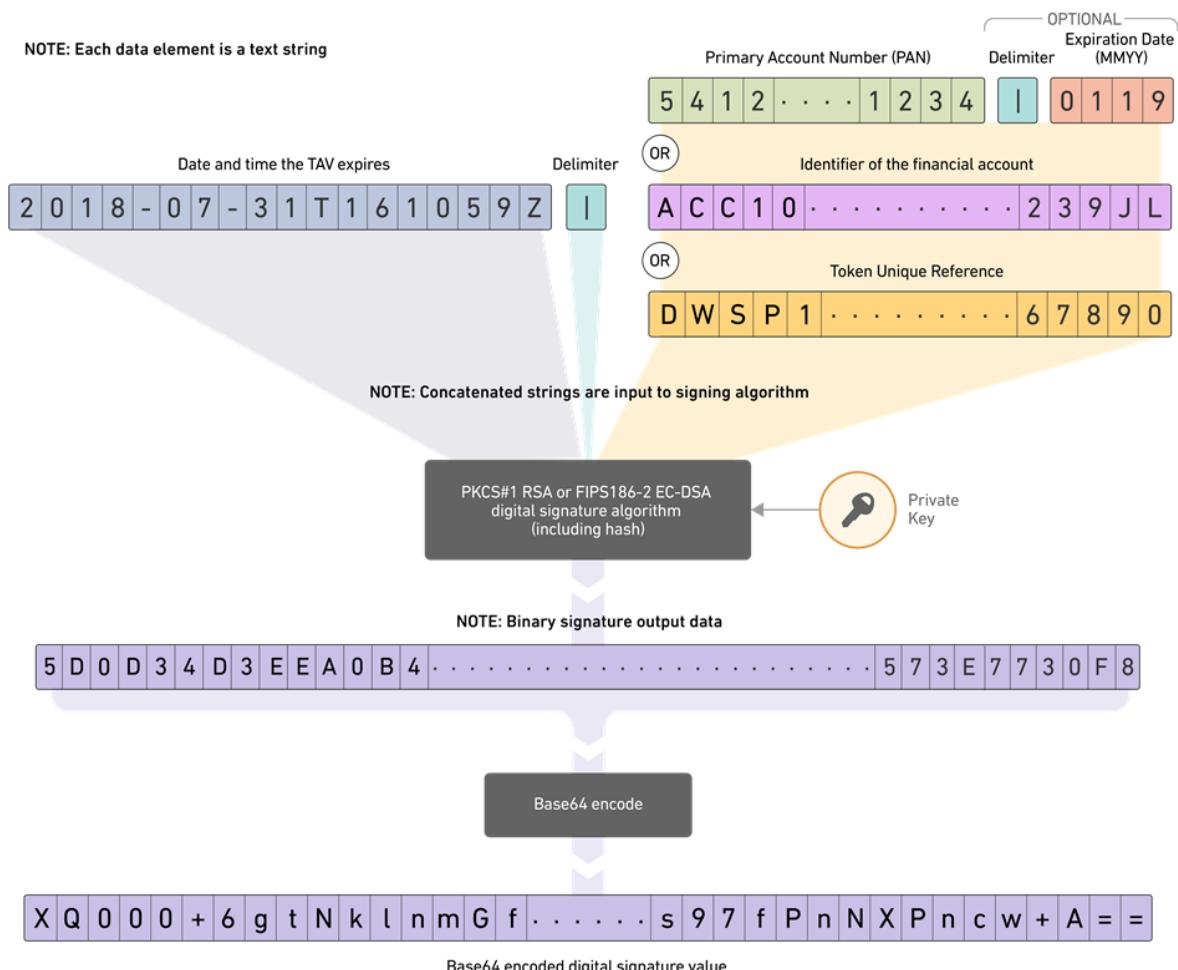
**Figure 12: TAV Format 1 Digital Signature Calculation Method**



**Figure 13: TAV Format 2 Digital Signature Calculation Method**



**Figure 14: TAV Format 3 Digital Signature Calculation Method**



### TAV Encoding and Examples

The Tokenization Authentication Value (TAV) is constructed as JSON (JavaScript Object Notation) and then base64 encoded.

This shall be in accordance with the following documents:

- RFC 7159: <http://tools.ietf.org/html/rfc7159>
- RFC 4648: <http://tools.ietf.org/html/rfc4648>

**NOTE: The JSON examples in the following subsections assume the RSA algorithm has been used to calculate the digital signature. The same example signature string has been used for all examples (the strings would differ in reality).**

### TAV Format 1

The elements of the TAV format 1 structure are defined as follows:

Field	Type	Value
version	String	'1'
tokenUniqueReferenceIncluded	String	'true' or 'false'
signatureAlgorithm	String	'RSA-SHA256'
signature	String	Base64 encoded

JSON example:

```
{
    "version": "1",
    "tokenUniqueReferenceIncluded": "true",
    "signatureAlgorithm": "RSA-SHA256",
    "signature": "XQ000+6gtNklnmGfcSJwAdqiI5g5GNJadSq73V70cboAN2nxbI0542E5cb9y8/QWN9rWcipkNYUB0g0R5Fv3POrB8HSjsuEKcnYGpWq6yfgdE917dbovPoYwpLzw1GUNRnXLjILkj12wAJ5LR0011WLdPrRjj14P7kPOZz6Vv3daxam0QpH5ijNp7GNH0wBWXPsU9TkeQfeQbfPUdDuXN10GAz3X7QPvHW+Hpi6861bRMip5eI9TGOCsAVBb0hxdjU4fJ/YPOCFn59gqSKERiiCaHq/D81KdqK1/0J9G49fwhP8rUlOFwN10PU0zy3M1P/+SZJEns97fPnPnPncw+A=="
}
```

This is base64 encoded to form the TAV data that is provided to the Wallet Provider:

```
ew0KICAgInZlcNp24iOiaiMSIsDQogICAidG9rZW5vbmlxdWVSZWlcmVuY2VJbmNs dWR1ZCI6ICJ0cnV1iwiNCiAgICJzaWduYXR1cmVBbGdvcml0aG0iOiaiU1NBLVNIQTi1NiIsDQogICAic21nbmF0dXJ1IjogI1hRMDAwKzZndE5rbG5tR2ZjU0p3QWRxaUk1ZzVHTkphZFNxNzNWNzBjYm9BTjJueGUJMDU0MkU1Y2I5eTgvUVdOOXJXY21wa05ZVUiwZzBSNUZ2M1BPcki4SFNqc3VFS2NuWUdwV3E2eWZnZEU5MTdkYm92UG9zd3BMencxR1VOUm5YTGpJTGtqMTJ3Quo1TFIwT2xsV0xkUHJSampsNFA3a1BPWhn02VnYzzGF4YW0wUXBINWlqTnA3R05IMHdCV1hQc1U5VGt1UWZlUWJmUFVkrHVYTwR0F6M1g3UVB2SFcrSHBJNjg2MWJSTWlwNWVJOVRHT0NzQVZCYjBoeGRqVTRmSi9ZUE9DRm41OWdxU0tFcmlpQ2Fics9EOGxLZHFLMS8wSj1HND1md2hQOHJVbE9Gd04xFBFVMHp5M00xUC8rU1pKRW5zOTdmUG50WFBUy3crQT09Ig0KfQ==
```

## TAV Format 2

The elements of the TAV format 2 structure are defined as follows:

Field	Type	Value
version	String	'2'
expirationDateIncluded	String	'true' or 'false'
tokenUniqueReferenceIncluded	String	'true' or 'false'
signatureAlgorithm	String	'RSA-SHA256'
signature	String	Base64 encoded

JSON example:

```
{
  "version": "2",
  "expirationDateIncluded": "true",
  "tokenUniqueReferenceIncluded": "true",
  "signatureAlgorithm": "RSA-SHA256",
  "signature": "XQ000+6gtNklnmGfcSJwAdqiI5g5GNJadSq73V70cboAN2nxbI0542E5cb9y8/QWN9rWcipkNYUB0g0R5Fv3POrB8HSjsuEKcnYGpWq6yfgdE917dbovPoYwpLzw1GUNRnXLjILkj12wAJ5LR0O11WLdPrRjj14P7kPOZZ6Vv3daxam0QpH5ijNp7GNH0wBWXPsU9TkeQfeQbfPUdDuXNl0GAz3X7QPvHW+Hpi6861bRMip5eI9TGOCsAVBb0hxdjU4fJ/YPOCFn59gqSKERiiCaHq/D81KdqK1/0J9G49fwhP8rUl0FWn10PU0zy3M1P/+SZJEns97fPnPXPncw+A=="
}
```

This is base64 encoded to form the TAV data that is provided to the Wallet Provider:

```
ew0KICAgInZ1cnNpb24iOiAiMiIsDQogICAiZXhwaXJhdGlvbkRhGVJbmNsdlWR1ZCI6ICJ0cnV1IiwNCiAgICJ0b2t1b1VuaxF1ZVJ1ZmVyZW5jZUluY2x1ZGVkIjogInRydWUiLA0KICAgInNpZ25hdHVyZUFsZ29yaXR0bSI6ICJSU0EtU0hBMjU2IiwNCiAgICJzaWduYXR1cmUiOiAiWFewMDArNmd0Tmtsbtm1HzmNTSndBZHfpSTVnNUdoSmFkU3E3M1Y3MGNib0FOMm54YkkwNTQyRTVjYj15OC9RV045c1djXBrT11VQjBnMFII1RnYzUE9yQjh1u2pzdUVL25ZR3BxCT5ZmdkRTkxN2rib3Zqb113cEx6dzFHvU5Sb1hMak1Ma2oxMndBSjVMUjBPbGxXTGRQc1Jqamw0UDdrUE9aejZWdjNkYXhhbTBRCeG1aWp0cDdHTkgwd0JXWFBzVT1Ua2VRZmVRYmZQVWREdVhObDBHQXozWDdRUHZIVytIcEk2ODYxY1JNaXA1ZUk5VEdPQ3NBVkJiMGh4ZGpVNGZKL11QT0NGbjU5Z3FTS0VyaW1DYUhxL0Q4bEtkcUsxLzBKOUc0OWZ3aFA4c1VsT0Z3TjEwUFUwenkzTTFQLytTWkpFbnM5N2Zqbk5YUG5jdytBPT0iDQp9
```

### TAV Format 3

The elements of the TAV format 3 structure are defined as follows:

Field	Type	Value
version	String	'3'
signatureAlgorithm	String	'RSA-SHA256'
dataValidUntilTimestamp	String	ISO 8601 Extended Format of the date and time (with Time Zone)
includedFieldsInOrder	String	Concatenation of Field Names separated by   delimiter (UTF-8 hex 007C). Applicable values: <ul style="list-style-type: none"> <li>• dataValidUntilTimestamp (mandatory)</li> <li>• accountNumber (optional)</li> <li>• accountExpiry (optional)</li> <li>• financialAccountInformation (optional)</li> <li>• tokenUniqueReference (optional)</li> </ul> accountNumber, financialAccountInformation, or tokenUniqueReference must be present.
signature	String	Base64 encoded

JSON example:

```
{  
    "version": "3",  
    "signatureAlgorithm": "RSA-SHA256",  
    "dataValidUntilTimestamp": "2018-07-3T16:10:59Z",  
    "includedFieldsInOrder": "dataValidUntilTimestamp|accountNumber|  
accountExpiry",  
    "signature": "XQ000+6gtNk1nmGfcSJwAdqiI5g5GNJadSq73V70cboAN2nxBI0542E5cb9y8/  
QWN9rWcipkNYUB0g0R5Fv3POrB8HSjsuEKcnYGpWq6yfgdE917dbovPoYwpLzw1GUNRnXLjILkj12wAJ5  
LR0O11WLdPrRjj14P7kPOZZ6Vv3daxam0QpH5ijNp7GNH0wBWXPsU9TkeQfeQbfPUdDuXNl0GAz3X7QPv  
HW+HpI6861bRMip5eI9TGOCsAVBb0hxdjU4fJ/YPOCFn59gqSKErliCaHq/  
D81KdqK1/0J9G49fwhP8rUlOFwN10PU0zy3M1P/+SZJEns97fPnPnPncw+A=="  
}
```

This is base64 encoded to form the TAV data that is provided to the Wallet Provider:

```
ew0KICAgInZ1cnNpb24iOiAiMyIsDQogICAic21nbmF0dXJ1QWxnb3JpdGhtIjogIlJTQS1TSEEyNTYiL  
A0KICAgImRhdGFYWxpZFVudGlsVGltZXN0YW1wIjogIjIwMTgtMDctMzFUMTYxMDU5WiIsDQogICAiaW  
5jbHVkZWRGaWVsZHNJbk9yZGVyIjogImRhdGFYWxpZFVudGlsVGltZXN0YW1wfGFjY291bnROdW1izXJ  
8YWNjb3VudEV4cG1yeSIsDQogICAic21nbmF0dXJ1IjogIlhRMDAwKzZndE5rbG5tR2ZjU0p3QWRxaUk1  
ZzVHTkphZFNxNzNWNzBjYm9BTjJueGJJMDU0MkU1Y2I5eTgvUVdOOXJXY21wa05ZVUIwZzBSNUZ2M1Bpc  
kI4SFNqc3VFS2NuWUdwV3E2eWzNZEU5MTdkYm92UG9Zd3BMencxR1VOUm5YTGpJTGtqMTJ3QUo1TFIwT2  
xsV0xkUHJSampsNFA3a1BPWno2VnYzZGF4YW0wUXBINWlqTnA3R05IMHdCV1hQc1U5VGt1UWZ1UWJmUFV  
kRHVYTmwR0F6M1g3UVB2SFcrSHBJNjg2MWJSTW1wNWVJOVRHT0NzQVZCYjBoeGRqVTNmSi9ZUE9DRm41  
OWdxU0tFcmlpQ2F1cS9EOGxLZHFLMs8wSj1HND1md2hQOHJVbE9Gd04xMFBVMH5M00xUC8rU1pKRW5zO  
TdmUG50WFBuY3crQT09Ig0KfQ==
```

## Card Eligibility Pre-digitization Message

For each digitization request, MDES sends the issuer a Card Eligibility pre-digitization message: an Account Status Inquiry (ASI), Tokenization Authorization Request (TAR), or Authorize Service message.

### Pre-digitization Recommendations

It is mandatory that an issuer supports the ASI, TAR, or Authorize Service message for digitization authorization. It is highly recommended that Card Validation Code 2 (CVC 2) verification should be performed (where available) for a digitization request. This is to mitigate the risk of digitizing card credentials based solely on the Account PAN and Expiration Date.

### Message Response Timeout

If MDES does not receive an **immediate** response to a Card Eligibility pre-digitization message (ASI, TAR or Authorize Service), it informs the Wallet Provider that no digitization decision has yet been determined. For wallet programs, MDES then sends a second pre-digitization message to the issuer.

**NOTE: For merchant and commerce platform tokenization, MDES will not send a second message.**

Issuers are strongly advised to design their pre-digitization message processing to provide an immediate response to the first message received to ensure their intended and timely

digitization decision. For more information, refer to Card Eligibility Message Timeout and Retry Logic for Wallet Programs, in the Pre-digitization Messages section.

### **Account Status Inquiry (ASI) Message**

Issuers can choose to receive this network message, during Card Eligibility, as the formal digitization request.

ASI messages are sent as Authorization Request/0100 or Financial Transaction Request/0200 message types, depending on whether the issuer is connected to the Dual Message System or Single Message System, respectively.

#### **Message Request Details**

The ASI message received by an issuer during Card Eligibility contains the following:

- Card Account PAN
- Card Account PAN Expiration Date
- CVC 2
- Address Verification Service Request Indicator
- Address Verification Service data

This is more than the information provided by an ASI message received during Card Availability.

#### **Issuer Processing Details**

An issuer should perform an account status check, CVC 2 match check (when available) and AVS address matching (if AVS data present and issuer supported), and respond in the Authorization Request Response/0110 or Financial Transaction Request Response/0210 message, indicating Approve (DE 39 = 00 or 85) or Decline (DE 39 = 05 or any other value) digitization. The issuer should also include the Address Verification Service Response (DE 48, subelement 83) and Card Validation Code Result for CVC 2 in DE 48, subelement 87.

#### **Message Response Details**

The response code (DE 39) is interpreted by MDES as follows:

- Continue (DE 39 = 00 or 85)
- Decline (DE 39 = 05 or any other value)

The 'Continue' response causes the card eligibility process to determine an eligibility decision using the eligibility rules and/or default eligibility decision.

### **Tokenization Authorization Request (TAR) or Authorize Service Message**

Issuers can choose to receive this network or API message, during Card Eligibility, as the formal digitization request.

TAR messages are sent as Authorization Request/0100 or Financial Transaction Request/0200 message types, depending on whether the issuer is connected to the Dual Message System or

Single Message System, respectively. Authorize Service messages are sent as web service API messages.

### Message Request and Issuer Processing Details

In addition to the information contained in an Account Status Inquiry (ASI), the TAR or Authorize Service message contains other information about the digitization that may be used by an issuer to assess specific risks associated with the Wallet Provider account and the device. The Authorize Service API contains the same information, but formats and names may differ from the list below. For full details, refer to the API documentation on the Mastercard Developers site.

Data	Description
Device Type	The type or form factor of the device initiating the digitization request (for example, a phone, tablet, or PC). New values indicate only the form factor, rather than the exact type of device and storage technology deployed by the device.
Wallet ID (WID)	Typically the ID of the program or service associated with the Wallet Provider, see Token Requestor ID and Wallet ID.
Token Requestor ID (TRID)	The ID assigned by Mastercard or the Token Service Provider (TSP) to the Token Requestor.
Storage Technology	A value indicating the storage technology of the requested token.

The following additional data may be supplied.

Data	Description
Correlation ID	A unique value assigned to a card digitization, enabling issuers to link the pre-digitization messages relating to that digitization. For example, if a cardholder enters an invalid CVC 2 during digitization, the multiple Card Eligibility request messages will have the same Correlation ID.
Account PAN Source	The Wallet Provider may indicate the method of Account PAN capture (for example, manually entered by the cardholder or 'card on file' from the Wallet Provider). Values: <ul style="list-style-type: none"><li>• 1 = Card on File</li><li>• 2 = Card added manually</li><li>• 3 = Card added via application</li></ul>

Data	Description
Payment Application Instance ID	The identifier associated with the payment application instance on a device. The Wallet Provider's TIP describes what this field provides. In the case of Apple Pay, this field provides the Secure Element ID (SE ID) for the token. The issuer may perform checks against lists of payment application instances or Secure Elements that are associated with devices that have been reported as lost or stolen by their cardholders so that they may decline digitization to such devices.
<b>NOTE: Mastercard does not maintain a list of devices and does not expect Wallet Providers to maintain such a list.</b>	
Device Source IP address	The IP address of the device through which mobile device reaches the internet. This may be the following: <ul style="list-style-type: none"> <li>• A temporary or permanent IP address assigned to a home router.</li> <li>• The IP address of a gateway through which the device connects to a mobile network.</li> </ul>
Wallet Provider Account ID Hash	When the Wallet Provider has a consumer account identifier, a hash of this value will be provided. For details of how the Wallet Provider Account ID Hash is calculated, see the Tokenization Eligibility Request (TER) Message section (Message Request and Issuer Processing Details subsection).
Cardholder Name	The Cardholder Name can optionally be collected by wallet providers and submitted to MDES as part of Check Eligibility and Tokenize requests. If thus submitted, it will appear in the TER/TAR in either of the following formats: <ul style="list-style-type: none"> <li>• LASTNAME/FIRSTNAME</li> <li>• FIRSTNAME LASTNAME.</li> </ul>
Wallet Provider Tokenization Recommendation	<p>The recommended eligibility decision of the Wallet Provider, based on their account and device data:</p> <ul style="list-style-type: none"> <li>• 0 = Decline</li> <li>• 1 = Approve</li> <li>• 2 = Require additional authentication</li> </ul> <p>When the recommendation is 'Approve,' the Wallet Provider may specify the reasons in the Wallet Provider Tokenization Recommendation Reasons value.</p> <p>When the recommendation is 'Require additional authentication' or 'Decline,' the Wallet Provider must include the reasons for the recommendation that apply in the Wallet Provider Tokenization Recommendation Reasons value. If none apply, the value may be excluded.</p>
Wallet Provider Tokenization Recommendation Standard Version	The version of the standards the Wallet Provider is using to determine the suggested tokenization recommendation.

Data	Description
Wallet Provider Device Score	<p>An integer value to indicate the status of the device. Valid values are 1 (indicating a poor status) through to 5 (indicating excellent status). A value of 3 indicates neutral status. The Wallet Provider may use any algorithm to determine the value. An unknown or new device should have neutral status.</p> <p>The Wallet Provider may consider the following when determining the device score:</p> <ul style="list-style-type: none"> <li>• Tenure of device ownership</li> <li>• Tenure of linkage to consumer account</li> <li>• How the device was activated, such as authorized via another trusted device</li> <li>• The device, operating system and software integrity, such as rooting, security status, trusted boot, bootloader</li> </ul>
Wallet Provider Account Score	<p>An integer value to indicate the status of the Wallet Provider's consumer account or relationship.</p> <p>Valid values are 1 (poor status) through to 5 (excellent status). A value of 3 indicates neutral status. The Wallet Provider may use any algorithm to determine the value. A new Wallet Provider account should have neutral status.</p> <p>A Wallet Provider may consider the following when determining the account score:</p> <ul style="list-style-type: none"> <li>• Tenure of the consumer relationship</li> <li>• Activity level of the consumer</li> <li>• Financial activity including timeliness of payment, levels of refund, disputes, missed payments, defaults only when applicable to the Wallet Provider's business activities with the consumer</li> <li>• Range of products used by the consumer</li> <li>• Consumer account compromise risk, including whether account credentials have been recently changed without confirmation via second factor authentication</li> </ul>
Number of Active Tokens for the Account PAN	<p>The number of active or suspended tokens for the Account PAN digitized to devices.</p> <p>An issuer can limit the number of active digital devices per card and decline any further digitization requests. MDES allows an unlimited number of active tokens (SE or cloud-based) per Account PAN, see Token Designation Service.</p>
Wallet Provider Tokenization Recommendation Reasons	The Wallet Provider reasons for the recommendation (see the Wallet Provider's Token Implementation Plan).

---

Data	Description
Device Location	<p>Latitude and longitude of the current device location, which is defined as:</p> <ul style="list-style-type: none"> <li>• Device Location Latitude—4 characters, containing hexadecimal encoded degrees where:           <ul style="list-style-type: none"> <li>– the first 2 characters represent the whole degrees</li> <li>– the second 2 characters represent 2 decimal places of precision.</li> </ul> </li> <li>• Device Location Longitude—4 characters, containing hexadecimal encoded degrees where:           <ul style="list-style-type: none"> <li>– the first 2 characters represent the whole degrees</li> <li>– the second 2 characters represent 2 decimal places of precision.</li> </ul> </li> </ul>

**NOTE: See the example Authorize Service API below for the following corresponding values:**

- **hexadecimal: 232F8B3E2**
- **decimal: 35.47/139.62**

	Hex	Decimal
Latitude whole number	23	35
Latitude decimal	2F	47
Longitude whole number	8B	139
Longitude decimal	3E	62
Direction	2	NE

- Device Location Lat/Long Sector—1 character, containing one of the following values:
  - 1 = Latitude = N, Longitude = W
  - 2 = Latitude = N, Longitude = E
  - 3 = Latitude = S, Longitude = W
  - 4 = Latitude = S, Longitude = E

This field contains spaces if the Wallet Provider has not provided this information.

**NOTE: While this service supports location precision to two decimal places, a Wallet Provider may provide less precise location information.**

**NOTE: A TAR network message provides hexadecimal encoded values whereas the MDES Pre-digitization API/Authorize Service value is not encoded.**

Data	Description
Mobile Number - Last Four Digits	The last four digits of the current voice or text telephone service number within the device. When the device is only capable of mobile data transfer using the cellular capabilities of the device, the number should not be provided. When a device depends on a linked device to provide mobile data capabilities and has voice or text telephone service, the voice or text service number of the linked device should be provided.
Token Type	<p>The value indicating the type of token:</p> <ul style="list-style-type: none"> <li>• C = Mastercard Cloud-Based Payments (MCBP)</li> <li>• S = Embedded Secure Element</li> <li>• F = Card on File</li> </ul>
Consumer Identifier	<p>An identifier for the cardholder, which can be provided by the Wallet Provider. If present, the issuer can use this identifier as part of its digitization approval process.</p> <p><b>NOTE: In an Authorize Service API request, the consumerIdentifier is conditionally included in the CardholderData structure (within the encrypted CardInfoData object). The Single Message System TAR message does not currently support the inclusion of the consumer identifier.</b></p> <p>This feature will be enabled on a market-by-market and wallet-by-wallet basis. Issuers and processors will not receive the new identifier unless they explicitly opt to receive it. The first implementation of this feature will be in support of the Korean market with Google Pay.</p>

The issuer should also perform a CVC 2 match check (when available) and AVS address matching (when available), and provide a response.

**NOTE: Wallet Provider-supplied account data may be used only for the purposes of determining the eligibility decision. The issuer must delete immediately, and not store for any period of time, any data provided by the Wallet Provider (unless otherwise agreed to between the issuer and the Wallet Provider).**

### Tokenization Authorization Request (TAR) Message Response Details

The manner in which the response code for TAR (DE 39) or Authorize Service (Decision) is interpreted by MDES depends on the message type option selected during issuer enablement:

- If the TAR 'USE RULES' option is chosen:
  - Continue (DE 39 = 00 or 85)
  - Decline (DE 39 = 05 or any other value)
- If the TAR 'USE RESPONSE CODE' option is chosen:
  - Approve (DE 39 = 00)
  - Approve, but require authentication (DE 39 = 85)

- Decline (DE 39 = 05 or any other value)
- If Authorize Service is used, the Decision is always used.

The ‘Continue’ response causes the card eligibility process to determine an eligibility decision using the eligibility rules and/or default eligibility decision.

The issuer may also include the following additional data within the TAR or Authorize Service response.

Data	Description
Issuer Product Configuration ID	Provided when an issuer wants to display different card art and card text from the defaults for the card’s account range; see the Card Art and Associated Data for MDES appendix. The Issuer Product Configuration ID can be right-padded and left-padded with spaces.
PAN Sequence Number	Provided when an issuer has identified a specific card or cardholder from the data provided in the TAR or Authorize Service message. For more information, see the Account PAN Sequence Number section, in the Tokenization Eligibility Request (TER) Message section.
Token Data and Activation Method(s)	<b>Activation Methods:</b> Provided when an issuer wants to provide cardholder-specific communication channels for the distribution of an Activation Code to the cardholder when the card eligibility decision is ‘Approve, but require authentication’. Multiple Activation Methods may be provided. For the TAR network message, the number of methods depends on the available space in DE 124, which has 199 characters available.

**NOTE: The Activation Methods are detailed in the About Activation Methods section.**

**Token Data:** Issuers can also provide:

- An Alternate Account Identifier in the TAR or Authorize Service response, see Providing an Alternate Account Identifier for a Token
- External token data in the Authorize Service response, see Providing External Token Data
- Additional token personalization data in the TAR response, see Providing Additional Personalization Data for a Token

## Related Concepts

[Card Art and Associated Data for MDES](#)

## Providing an Alternate Account Identifier for a Token

Issuers can provide an Alternate Account Identifier for a token in their TAR or Authorize Service response messages. When it is provided in an Authorize Service response, the identifier must be encrypted with the Mastercard public key for encryption.

An Alternate Account Identifier is a cardholder-friendly reference to a bank account, for example an IBAN (International Bank Account Number). It is typically useful for a Wallet Provider to display a suffix of this identifier to the cardholder to help them identify their tokenized card when they are not aware of their Account PAN.

### Effect of Providing an Alternate Account Identifier

Depending on the wallet implementation, MDES might provide a suffix of the issuer-supplied Alternate Account Identifier to the wallet attempting the digitization. The Wallet Provider's wallet documentation will identify whether and how the suffix is displayed to the cardholder.

### How to Use this Feature

Mastercard recommends that issuers provide the full Alternate Account Identifier to MDES so that it can be used for token search purposes when supporting cardholders.

Space characters in an Alternate Account Identifier are trimmed. The resulting value must be 9–64 characters.

To provide an Alternate Account Identifier value in a TAR response, include the value in the Token Data and Activation Method(s) data element. For information and examples of how to format that data element, refer to the *Customer Interface Specification* or *Single Message System Specifications*. If multiple Alternate Account Identifiers are provided in a TAR response, only the last one is validated and used (if valid).

For information on providing the Alternate Account Identifier value in an Authorize Service response message, refer to the API documentation on the Mastercard Developers site.

### Error Handling and Testing

Issuers must test the use of this feature thoroughly before using it in production. Issuers should work with their Mastercard representative to plan their testing, which should include testing with the Wallet Providers to validate the display of Alternate Account Identifier suffixes to cardholders.

If MDES encounters an error processing the Alternate Account Identifier value provided by the issuer, the digitization will proceed without any value. The issuer will not be informed that the data was invalid.

The issuer is also responsible for ensuring that the data provided through this feature meets applicable standards. Mastercard accepts no responsibility should an issuer provide invalid data that negatively impacts functionality or the cardholder experience.

## Providing External Token Data

If an issuer is using a third-party Token Service Provider (TSP), the issuer can provide an external token in the encrypted payload of its Authorize Service response message. MDES can then use the external token data when provisioning to the target device or server.

The encrypted token data includes the token issued for the digitization request, its expiration date (month and year) and optionally a sequence number. For full details, refer to the MDES Pre-Digitization API documentation on the Mastercard Developers site.

**NOTE: Refer to the *Mastercard Token Service Provider Standards* for information on providing token to PAN mapping data.**

## MDES Issuer Personalization Data

Issuers can take advantage of the ISO TAR Response message returned to MDES to provide issuer-proprietary information to be inserted in the token profile.

Issuers can provide additional cardholder-specific data (such as a loyalty ID) in their TAR response messages. The data is added to the token profile, enabling issuers and merchants to provide customized features and loyalty benefits to the cardholder at the point of service.

**NOTE: This feature does not apply to merchant and commerce platform tokenization, and it is not currently available when using the Authorize Service message.**

## How to Use this Feature

When the issuer receives a TAR message from MDES, or an earlier TER message if they opted to receive it, they identify the cardholder account being tokenized and determine whether additional personalization data is to be provided (for example, an associated loyalty ID).

Personalization data can also have tags that are used to meet regional requirements, for example, tag DF20 (AEPM Form Factor), which is used in France.

The steps for inserting multiple BER-TLV proprietary tags inside the FCI Issuer Discretionary Data template ('BF0C') that is available on the contactless interface, so that both non-US and domestic contactless readers will have access to these proprietary data elements and process them, are as follows:

- **Prepare the raw binary data block** to append inside the 'BF0C' tag (concatenation of all the BER-TLV data elements to insert). The data size should not be more than 200 bytes. The sample below depicts some custom tags and their values. 0xDF20 is a common tag personalized by issuers in France.

**Table 1: Custom Tags and their values**

Tag	Length	Description	Value
0xDF20	0x04	AEPM Form Factor	0x00 00 00 11

Tag	Length	Description	Value
0x5F54	0x08	Bank Identifier Code	0x42 41 4E 4B 46 52 39 39 ("BANKFR99")
0x5F55	0x02	Issuer Country Code (alpha2)	0x46 52 ("FR")
0xC0	0x10	Proprietary Loyalty Customer Identifier	(Cardholder-specific data) 16-digit number

The result is a cardholder-specific binary data block, for instance: DF 20 04 00 00 00 11 5F 54 08 42 41 4E 4B 46 52 39 39 5F 55 02 46 52 C0 10 11 22 33 44 55 66 77 88 99 11 22 33 44 55 66 77

**NOTE: This should be a raw binary value and not an ASCII or string representation of the data block.**

- **Add a 1-byte action ID to this data.** The Action ID provides instructions to MDES for processing the personalization data. A response message can include zero, one or several sets of personalization data (each with an Action ID). However, each Action ID may be used only once in the response message. For example, if the message contains three sets of personalization data and the Action IDs are 04, 05, 06, it is valid but if the Action IDs are 04, 05, 05, they become invalid as 05 is used twice in that message. MDES will use the Action IDs below to determine where the proprietary data needs to be personalized to the token profile:
  - 0x04: Append into BF0C (Contactless Payment Mode)
  - 0x05: Append into BF0C (Management Mode)
  - 0x06 : Append into BF0C (Contactless Payment AND Management Mode)

In this example, as a minimum, the data must be available for Contactless Payment Mode. The value chosen is 0x06.

**NOTE: It is always possible to have a value of 0x04.**

The result is a binary buffer - 0x06 + Binary Data Block:

06 **DF 20** 04 00 00 11 **5F 54** 08 42 41 4E 4B 46 52 39 39 **5F 55** 02 46 52 **C0** 10 11 22 33 44 55 66 77 88 99 11 22 33 44 55 66 77

**NOTE: This should be a raw binary value and not an ASCII or a string representation of the data block.**

- **Encode the result into a Base64 string**

The result is an 'ans' (alphanumeric special) string:

"Bt8gBAAAABFfVAhCQU5LRII5OV9VAkZSwBARljNEVWZ3ijkRljNEVWZ3"

- Place a '**t**' character before the string, to indicate to MDES that this data element corresponds to **token** personalization data. This enables the user to distinguish this subfield from authentication methods that are identified by a numeric character. Place a '**~**' character to indicate to MDES the end of the token personalization data.  
The result is an 'ans' string:

"**t**Bt8gBAAAABFfVAhCQU5LRII5OV9VAKZSwBARIjNEVWZ3iJkRljNEVWZ3~"

- Insert the result within the DE 124 field**, *Token Data and Activation Method(s)* subfield as if it was the last Activation Method:
  - There must be a '**|**' character to separate it from the (real) last Activation Method placed beforehand
  - There must be a '**||**' string placed afterwards to indicate to MDES this is the end of the Activation Methods field
  - Maximal length for the Activation Method(s) field is changed from 186 to **286** bytes and DE 124 max.length is changed from 199 to 299 bytes

The **result** is an 'ans' string for the *Token Data and Activation Method(s)* subfield, for instance:  
**1**(###) ### 4567**|** **2**a\*\*\*d@anymail.com**|**  
**t**Bt8gBAAAABFfVAhCQU5LRII5OV9VAKZSwBARIjNEVWZ3iJkRljNEVWZ3~ **||**

## Limitations

**Table 2:**

Property	Description
Host Tag	BF0C (FCI Issuer Discretionary Data)  The issuer-provided data is appended inside this tag. If the provided data includes tags that are already present, the data will overwrite the MDES generated value.
Maximum size of the provided data	200 Bytes
MDES control action	Blacklist—The issuer may include any data, except the MDES Control Tags for this action (see below). If the data contains an MDES Control Tag, it will not be personalized.
MDES Control Tags	9F4D (Log Entry) and 9F6E (Third Party Data)
TLV parsing check	Yes—The provided data must be TLV structured. If the data does not parse, it will not be personalized

Property	Description
Application compatibility	The action is compatible with the following payment applications: <ul style="list-style-type: none"><li>• Mobile Mastercard</li><li>• PayPass 1.0</li><li>• M/Chip Mobile 1.1</li></ul>

## Error Handling and Testing

Issuers must test this feature thoroughly before using it in production. They should work with their Mastercard representative to plan their testing.

If MDES encounters an error while processing the additional personalization data provided by the issuer, the digitization will proceed with the default MDES personalization and the additional data will not be included. The issuer will not be informed that the data was invalid.

The issuer is also responsible for ensuring that the data provided through this feature meets applicable standards. Mastercard accepts no responsibility should an issuer provide invalid data that negatively impacts the functionality or interoperability of the personalized token.

## Checking the CVC 2, Expiration Date and Address

This section describes how an issuer should handle the Card Validation Code 2 (CVC 2), card expiration date, and address data that are provided in the Card Eligibility pre-digitization message (Account Status Inquiry [ASI], Tokenization Authorization Request [TAR], or Authorize Service message).

**NOTE: To support merchant and commerce platform tokenization, the issuer must be able to process the Card Eligibility pre-digitization message without requiring the cardholder name, CVC 2, and address data. This is because the cardholder may not be present to provide such data for the digitization request.**

**The Authorize Service response message has been updated to allow issuers to provide CVC 2 validation results and Address Verification Service (AVS) results to MDES.**

## CVC 2 Verification

The Card Eligibility pre-digitization message may contain the CVC 2. The issuer should decline the message if the value provided does not match the valid value for the card. If the CVC 2 is **not** present in the message, the issuer should continue to process the provisioning request (specifically in merchant tokenization scenarios where the CVC 2 may not be passed).

However, if the CVC 2 fails verification, the issuer must provide the value N ('invalid CVC 2—non match') or INVALID, depending on the message type. The Wallet Provider is informed and may prompt the cardholder to re-enter the card's CVC 2 and then resubmit a digitization request to MDES (which sends another network message to the issuer).

## How an Unconfirmed CVC 2 Affects the Eligibility Decision

For wallet programs, an issuer is expected to verify the CVC 2 value is correct for the supplied card and indicate this within the message response. If the message response is **not** received (and CVC 2 is therefore not confirmed), the issuer should construct an eligibility rule to examine the 'ASI/TAR or Authorize Service Response' for a value of 'Not available' to ensure that the eligibility decision is 'Approve, but require authentication'. This is to ensure that digitization cannot occur without the minimum requirement for cardholder authentication being satisfied.

For merchant and commerce platform tokenization, an issuer must be able to process the Card Eligibility pre-digitization message without requiring the CVC 2. The issuer should decline the message if the value provided does not match the valid value for the card.

## CVC 2 Failure Velocity Checking

It is recommended that an issuer implements velocity checking in accordance with its own policy to mitigate the risk of a brute force attack on a card's CVC 2. When the velocity limit has been exceeded, an issuer may stop CVC 2 retry attempts by indicating that the CVC 2 verification was not processed (by providing the value P, 'CVC 2 not processed', or NOT\_PROCESSED, depending on the message type) and declining the message.

## Card Expiration Date Verification

The Card Eligibility pre-digitization message contains the card's expiration date. The issuer should decline the message if the value provided does not match the valid value for the card.

However, if the card's expiration date is incorrect, the issuer must provide the value N ('invalid CVC 2—non match') or INVALID, depending on the message type. This way the issuer does not indicate which element failed verification. The Wallet Provider is informed and may prompt the cardholder to re-enter the card's expiration date and then resubmit a digitization request to MDES (which sends another network message to the issuer).

## Address Verification Service (AVS)

Address Verification Service (AVS) support is optional. Address data is only present when supplied by the Wallet Provider. The issuer may use this information in accordance with its policy to 'Approve,' 'Decline,' or 'Approve, but require authentication' for the digitization request.

MDES makes the Address Verification Response (that may be provided by the issuer) available within the eligibility rules. If AVS is performed, the result should be provided. If the result is not provided, this status is also made available to the eligibility rules.

## Eligibility Rules

The issuer may optionally define rules to determine eligibility based on Wallet Provider-supplied account data or the issuer's pre-digitization message responses. Eligibility rules are defined during issuer enablement (refer to the *MDES—Issuer Enablement* guide).

The rules can be based on tokenization elements relating to:

- Data elements that are always provided by the Wallet Provider
- Data elements that might be provided by the Wallet Provider, depending on the implementation
- The issuer's message response values

**NOTE: Issuers' processor(s) may be interacting with MDES on their behalf. It is important to review the MDES configurations with their processor(s) and confirm their selections based on what their processor(s) support/s.**

### About Rules and Rule Sets

Eligibility rules consist of conditions and can be defined and ordered within Rule Sets.

Each rule determines whether the digitization decision is:

- **Approve**
- **Approve, but require authentication**—An issuer-supported method of cardholder authentication is required prior to activation (for wallet programs)
- **Decline**—The cardholder, their device, their Wallet Provider-supplied account data, or the pre-digitization message responses do not meet the issuer's eligibility requirements

Each rule consists of one or more conditions comparing the account data elements or message response values, and one or more corresponding values to be compared to each element. The condition operator (such as 'equal' or 'greater than') must also be specified; for the complete list of operators, see the Tokenization Element Type: Comparison Operators table.

If all conditions are true, the rule passes and the specified eligibility decision result is available.

The issuer can configure the rules to ignore data that cannot be supplied by a Wallet Provider and continue to process only the data supplied. When a specific account data element is not supplied (such as the device location), the situation can be ignored or the rule can fail. If none of the data elements specified in the rule are present, the rule fails.

Rules may be defined and ordered within a Rule Set. Each rule within the Rule Set is processed until one passes or all have failed. When all rules fail, the mandatory default eligibility decision is selected. Rules may only appear once within a Rule Set.

Before setting up the rules during issuer enablement, the issuer should consider the following:

- **Conditions within a rule operate under the 'AND' principle**—All the conditions on account data elements in the rule need to be true for the rule to pass. Example Rule Set:
  1. "Rule: Lower risk" = Approve if:

Data Element	Operator	Value
Account Score	>	4
Device Score	>	4

Both data element conditions need to be 'true' for the rule to pass.

2. "Rule: Higher risk" = Decline if:

Data Element	Operator	Value
Account Score	<	2

3. "Rule: Neutral risk" = Require Authentication if:

Data Element	Operator	Value
Account Score	<	5

- **Rules within a Rule Set operate under the 'OR' principle**—If the first rule within a Rule Set does not pass, the second rule is checked, and so on. Therefore, rules have a sequence or priority within the Rule Set. It is advised that rules that are more likely to pass be placed higher in the Rule Set sequence. Example Rule Set:
  1. "Rule: Higher risk"
  2. "Rule: Neutral risk"
  3. "Rule: Lower risk"

**Table 3: Tokenization Element Type: Comparison Operators**

Tokenization Element Type	Comparison Operator Description	Comparison Operator Symbol
String	Equals	=
	Not equals	!=
	In	In
	Not in	Not In
Reason codes	In	In
	Not in	Not In
Location	In	In
	Not in	Not In

Tokenization Element Type	Comparison Operator Description	Comparison Operator Symbol
Integer	Equals	=
	Not equals	!=
	Greater than	>
	Greater than or equals	>=
	Less than	<
	Less than or equals	<=
Decimal	Equals	=
	Not equals	!=
	Greater than	>
	Greater than or equals	>=
	Less than	<
	Less than or equals	<=
Masked IP range	In	In
	Not in	Not In

**Wallet Provider Account Data Elements and Scores**

The account data supplied by the Wallet Provider during pre-digitization can be used to determine the eligibility decision.

The account data elements may relate to:

- The cardholder
- The Wallet Provider's relationship with the cardholder
- The card account on file with the Wallet Provider
- The card's activity with the Wallet Provider
- The device

The specific account data available for a particular token implementation depends on the data made available by the Wallet Provider. Mastercard defines requirements for many of the elements, but a Wallet Provider may not be willing or able to provide all of them (some are optional).

**NOTE: For each wallet program, the list of data items provided to MDES is specified in the relevant Token Implementation Plan (TIP), see Token Implementation Plans.**

The following values or types of data may be provided:

- Length of time the cardholder has had an account with the Wallet Provider
- Length of time the card has been linked to the Wallet Provider account

- Whether the cardholder's billing and shipping addresses match
- Types of products the cardholder has purchased from or through the Wallet Provider (for example, digital downloads, mail order, in-store purchases)
- Current geolocation of the mobile device
- A score or rating of the account, device, or cardholder, based on the Wallet Provider's analysis of the data available to them. For example:
  - **Mobile device score**—Can indicate a Wallet Provider's view of the cardholder's mobile device use, if the Wallet Provider is a mobile phone operator
  - **Card account score**—Can indicate a Wallet Provider's view of the cardholder as a digital wallet customer, if the cardholder has been a longtime customer

The types of data and scores vary for different Wallet Providers. They can provide either the data used for the analysis, the scores, or both (depending on what has been previously agreed with Mastercard).

The issuer must delete immediately, and not store for any period of time, any data provided by the Wallet Provider (unless otherwise agreed to between the issuer and the Wallet Provider).

## Data Available to the Eligibility Rules

The following Wallet Provider-supplied elements are always available for use in the eligibility rules.

Tokenization Element	Description
Account PAN Source	Method of PAN capture (for example, manually entered by the cardholder or whether it is a 'card on file' from the Wallet Provider).
Storage Technology	A string indicating the storage technology of the requested token: <ul style="list-style-type: none"><li>• Device Memory</li><li>• Device Memory protected by Trusted Platform Module (TPM)</li><li>• Server</li><li>• Trusted Execution Environment (TEE)</li><li>• Secure Element (SE)</li><li>• Virtual Execution Environment (VEE)</li></ul>
Wallet ID (WID)	A string typically indicating the ID of the program or service associated with the Wallet Provider, see Token Requestor ID and Wallet ID. Examples: 103, 216, 217, 218, 327.
Token Requestor ID (TRID)	A string indicating the ID assigned by Mastercard or the Token Service Provider (TSP) to the Token Requestor.
Token Type	A string indicating the type of token being requested: <ul style="list-style-type: none"><li>• Secure Element (SE)</li><li>• Cloud</li><li>• Card on File</li></ul>

## Additional Data Available to the Eligibility Rules

Depending on the implementation, the following Wallet Provider-supplied elements may be available for use in the eligibility rules.

Tokenization Element	List of Values or a Single Value	Tokenization Element Type	Limited Values (If Any Limitation)
Device Type	A single value	Integer	An integer value indicating the type of device: <ul style="list-style-type: none"> <li>• 1 = Mobile phone</li> <li>• 2 = Tablet</li> <li>• 3 = Watch</li> </ul>
Language	A single value	String	The current language selection of the device. In accordance with ISO-639-1, a two-letter language code.
OS Name	A single value	String	The name of the device operating system.
OS Version Number	A single value	String	The version of the device operating system.
Device Source IP Address	A single value	Masked IP range	A subnet range indicated as an IPv4 network address (lower bound) with a backslash and a bit length mask. For example, when the indicated value for a mobile device IP address is 192.168.1.0/24, the rule passes when the mobile device IP address is within the network address.
Device Location	A single value	Location	A rectangle represented by the point at the North East (NE) and the point at the South West (SW). Format: NE latitude, NE longitude/SW latitude, SW longitude. The latitude and longitude are negative or positive integers encoded degrees with no decimal place. Values: <ul style="list-style-type: none"> <li>• Latitude: from -90 to 90</li> <li>• Longitude: from -180 to 180</li> </ul> Negative values indicate locations with southerly or westerly locations respectively.
Wallet Provider Account Score	Can be a list	Integer	From 1 to 5
Wallet Provider Device Score	Can be a list	Integer	From 1 to 5

Tokenization Element	List of Values or a Single Value	Tokenization Element Type	Limited Values (If Any Limitation)
Wallet Provider Tokenization Recommendation	A single value	String	Approve, Require additional authentication, Decline
Wallet Provider Tokenization Recommendation Reasons	A single value (for 'Approve' recommendation) or can be a list	Reason codes	Possible reasons are provided in the Wallet Provider Tokenization Recommendations, Reasons, and Interpretation appendix.
Wallet Provider Tokenization Recommendation Standard Version	A single value	String	01, 02

**Pre-digitization Message Response Data Elements**

Some issuer response elements are available for use in the eligibility rules.

Tokenization Element	List of Values or a Single Value	Tokenization Element Type	Limited Values (If Any Limitation)
ASI/TER Response	Can be a list	String	The issuer's response to Card Availability request: Continue, Require authentication, Not available
ASI/TAR or Authorize Service Response	Can be a list	String	The issuer's response to the Card Eligibility request: Approve, Require authentication, Not available
AVSAddressMatch	Can be a list	String	Whether the address matches: Y, N, NA
AVSPostalMatch	Can be a list	String	Whether the postal code matches: Y, N, NA

When a message has not been sent or a message response has not been received, the response value is 'Not available'. An issuer may enforce a policy to decline digitization or require cardholder authentication when the 'ASI/TAR or Authorize Service Response' is 'Not available'.

The following table shows the values that are provided for AVSAddressMatch and AVSPortalMatch when the Address Verification Service (AVS) Response is provided in the ASI, TAR or Authorize Service response. The AVS Response Code column in the table shows the values that can be provided in the ASI or TAR response. For the corresponding Authorize Service values, refer to the MDES Pre-Digitization API documentation on the Mastercard Developers site.

<b>AVS Response Code</b>	<b>Description</b>	<b>AVSAddressMatch Value</b>	<b>AVSPostalMatch Value</b>
A	Address matches, postal code does not	Y	N
N	Neither address nor postal code matches	N	N
R	Retry, system unable to process	NA	NA
S	AVS currently not supported	NA	NA
U	No data from issuer/Authorization Platform	NA	NA
W	For U.S. addresses, nine-digit postal code matches, address does not; for address outside the U.S., postal code matches, address does not	N	Y
X	For U.S. addresses, nine-digit postal code and address matches; for addresses outside the U.S., postal code and address match	Y	Y
Y	For U.S. addresses, five-digit postal code and address matches	Y	Y
Z	For U.S. addresses, five-digit postal code matches, address does not	N	Y

## Default Eligibility Decision

The eligibility decision is typically determined by the pre-digitization messages and/or eligibility rules. However, when the decision has **not** been determined by the messages or rules, the default eligibility decision is invoked.

During issuer enablement, an issuer may set the default eligibility decision to 'Approve,' 'Approve, but require authentication,' or 'Decline.' If the issuer selects 'Approve, but require authentication,' it must define a default Activation Method. If none is provided, its Customer Service phone number is used (for wallet programs). The Customer Service number is not added for merchant and commerce platform tokenization.

## Cardholder Authentication and Token Activation

For wallet programs, the Card Eligibility stage may determine that additional cardholder authentication is required before digitization can continue. When authenticated, the

cardholder's token can be activated using one of several methods, including an Activation Code, a Tokenization Authentication Value (TAV), or the Customer Service Tools.

## Overview

MDES supports a range of options for the completion of the authentication process by the issuer and cardholder. Each issuer designs its own policy and process for cardholder authentication using one or more of the options supported by MDES.

**NOTE: Additional cardholder authentication is optional for merchant and commerce platform programs, because cardholders might not be present during digitization. For those programs, the tokens are activated automatically (unless digitization is declined).**

MDES itself is unable to perform any explicit cardholder authentication processes. MDES supports only the implicit authentication of a cardholder by their card issuer.

The processes offered to a cardholder to complete authentication during pre-digitization may vary depending on the account range of the card being digitized, or the actual card being digitized (when card-specific Tokenization Eligibility Request [TER], Tokenization Authorization Request [TAR] or Authorize Service API messages are supported by an issuer).

MDES supports the following methods of cardholder authentication and subsequent activation:

- The distribution of an Activation Code to the cardholder using a trusted channel followed by automated or manual entry of the code into the mobile device's wallet application. The Wallet Provider may offer the cardholder a choice of channel in the wallet user interface when multiple card-specific channels are provided by an issuer.
- Activation via an Issuer App and direct interaction with the wallet application within the mobile device, resulting in MDES validating a cryptographically-signed message passed from the issuer via the Wallet Provider.
- Activation via an Issuer App whereby the cardholder authenticates to the Issuer App and the issuer systems activate the token using the Customer Service API.
- A cardholder-initiated call to an issuer-provided call center with activation subsequently requested by the issuer using the Customer Service Tools.
- An issuer-initiated automated voice phone call to a cardholder with activation subsequently requested by the issuer using the Customer Service Tools. The Wallet Provider may offer the cardholder a choice of card-specific phone numbers in the wallet user interface.

**NOTE: Other use case configurations may be constructed using the tools provided by MDES.**

The actual method of authenticating a cardholder using their credentials to gain access to either the Activation Code or activation capability is determined by the issuer and not part of MDES.

## About Activation Methods

MDES supports the communication of the available authentication methods and contact points via the Wallet Provider so that a cardholder may complete the appropriate authentication process determined by the issuer.

The communication channels that can be used for authentication and subsequent activation are known as 'Activation Methods.' Issuers can:

- Define *default* Activation Methods for an account range during issuer enablement (methods for the range and specific methods for each Wallet Provider)
- Provide *cardholder-specific* Activation Methods in the pre-digitization message responses (TER, TAR, Authorize Service, or Request Activation Methods), for example a cardholder's own mobile phone number or a specific call center number applicable to the type of account held

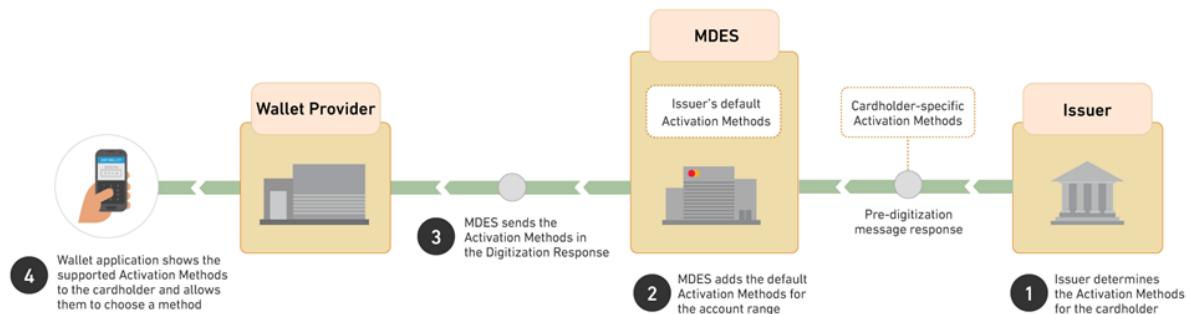
In addition, an issuer may select to receive the Request Activation Methods API message, when they have told MDES that a cardholder needs authenticating, so they can explicitly provide the Activation Methods in the response.

Each default Activation Method for a Wallet Provider can be set as 'Always to provide,' which means that MDES will always pass that method to the Wallet Provider. If the issuer provides Activation Methods in a pre-digitization message response:

- MDES ignores the default methods that are **not** set as 'Always to provide'
  - If a method in the response is the same *type* as an 'Always to provide' default method, MDES will use the value from the response
- For example, if the default Activation Method is for the cardholder to visit [www.anybank.com](http://www.anybank.com), and the response contains the same Activation Method type but the value is [www.anybank.co.uk](http://www.anybank.co.uk), MDES will use [www.anybank.co.uk](http://www.anybank.co.uk).

**NOTE: During issuer enablement, an issuer can define one Issuer App per device operating system for a Product Configuration; MDES will pass the appropriate Issuer App data to the Wallet Provider. MDES does not support the issuer providing different or additional Issuer Apps in its pre-digitization message responses.**

**Figure 15: Passing Activation Methods to the Wallet Provider**



The following types of Activation Methods are supported:

Type	Activation Method (Communication Channel)	Example Value (Cardholder-Specific Values May be Masked)	Default Set for an Account Range
1	Text message to cardholder's mobile phone number	(###) ### 1234	N/A
2	Email to cardholder's email address	j***s@ *****.com	N/A
3	Cardholder-initiated call to automated call center phone number	(555) 555 2345	No
4	Cardholder-initiated call to manned call center phone number	(555) 555 3456	Yes
5	Cardholder to visit a website	www.anybank.com	Yes
6	Cardholder to activate using an issuer's mobile app (Issuer App) on their device	(Any value provided is ignored)	Yes
7	Issuer-initiated voice call to cardholder's phone	(###) ### 4567	No

In the pre-digitization message response, Activation Method type 6 does not require a corresponding value; the appropriate Issuer App defined in the Product Configuration is used. When masking data, use EBCDIC or ASCII display character representation. For more information, see Data Representation Notations in the *Customer Interface Specification*.

Each account range may be configured with multiple communication channels, and multiple instances of the same communication channel may be provided. Similarly, multiple instances of the same communication channel type may be provided for a cardholder within the pre-digitization message responses.

If supported by the Wallet Provider, MDES provides the Activation Method choices so that the Wallet Provider may offer a choice to the cardholder within the user interface. MDES does not support changing the Activation Methods list once it has been determined.

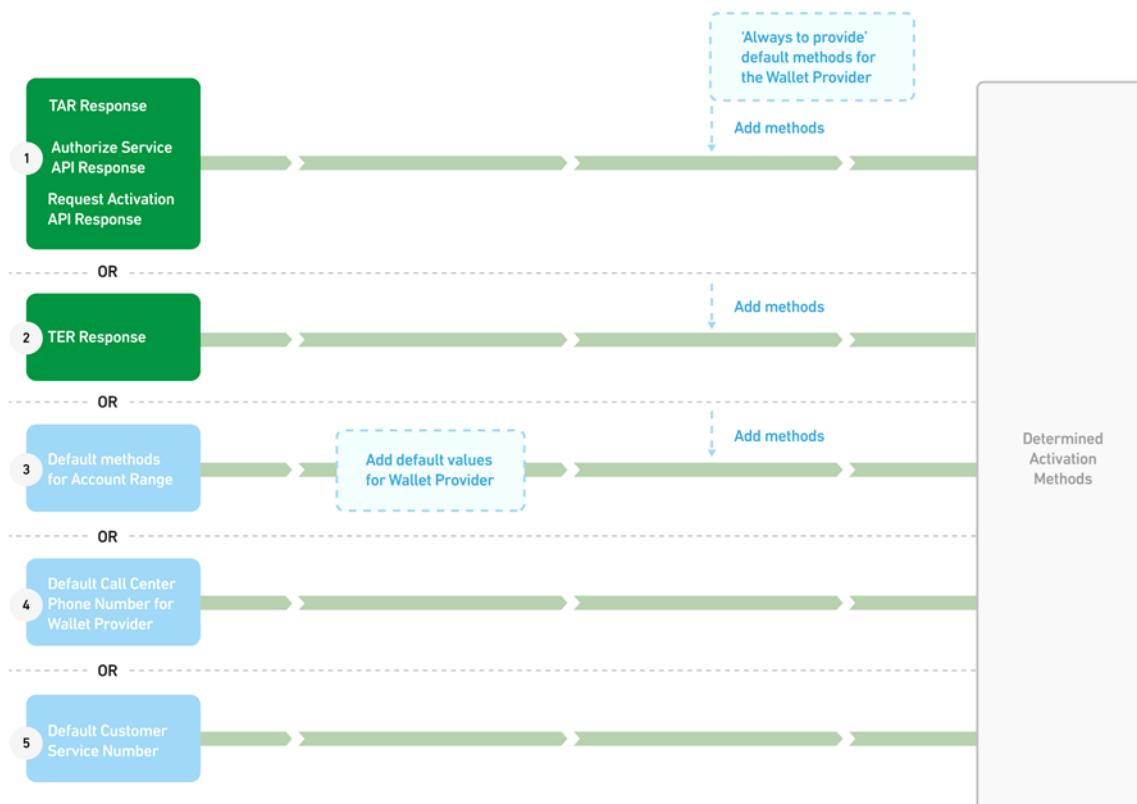
**NOTE: Additional cardholder authentication is optional for merchant and commerce platform programs, so an issuer should not assume those program participants will support its chosen authentication methods.**

## Determining the Activation Methods

As the following diagram shows, MDES determines the Activation Methods list for a cardholder during Pre-digitization as follows:

1. If there are Activation Methods in the TAR, Authorize Service and/or Request Activation Methods responses:

- a. Concatenate the methods from all those responses.
- b. Add the 'Always to provide' default methods for the Wallet Provider (for this account range), ignoring any methods that are already present in one of the responses (if any method types match, use the response values).
2. Otherwise, if there are Activation Methods in the TER response:
  - a. Use the methods from that response.
  - b. Add the 'Always to provide' default methods for the Wallet Provider (for this account range), ignoring any methods that are already present in the TER response (if any method types match, use the response values).
3. Otherwise, if there are default Activation Methods for the account range:
  - a. Use the default values set for the Wallet Provider (for this account range). Otherwise, use the default values for the account range.
  - b. Add the 'Always to provide' default methods for the Wallet Provider (for this account range).
4. Otherwise, if there is a default call center phone number for the Wallet Provider, use that.
5. Otherwise, use the default Customer Service phone number if it is a wallet program. (The Customer service number is not added for merchant and commerce platform tokenization.)



If MDES determines the Activation Method to be by Issuer App only, it adds the default call center phone number for the Wallet Provider, if one is set. Otherwise, it adds the default Customer Service phone number.

It is not guaranteed that the order of Activation Methods within the pre-digitization message responses will be preserved when displayed to the customer.

### **Request Activation Methods API Message**

Issuers can choose to receive this API message when they have told MDES that a cardholder needs authenticating. MDES will send the Request Activation Methods API message once, enabling the issuer to respond with the required Activation Methods.

For information on the Request Activation Methods API message and its parameters, refer to the MDES Pre-Digitization API documentation on the Mastercard Developers site.

### **Issuer App Token Activation**

Issuer app token activation is designed to support ‘in-app’ completion of the activation process.

The ‘app’ is typically the issuer’s own mobile app, which communicates directly with the wallet on the mobile device. Communication may be configured using:

- An ‘app-level’ API, when the wallet is simply another app within the mobile device
- An ‘OS-level’ API, when the wallet is built into the operating system of the mobile device

Configuration of this type of inter-app communication is outside of the scope of MDES.

### **Issuer App Token Activation via TAV**

When supported by the Wallet Provider, an issuer may generate a Tokenization Authentication Value (TAV) for a token awaiting activation within MDES. The TAV contains a digital signature created using an asymmetric key algorithm by the issuer, approving the activation of a token for a specific Account PAN and, optionally, an Expiration Date and Token Unique Reference.

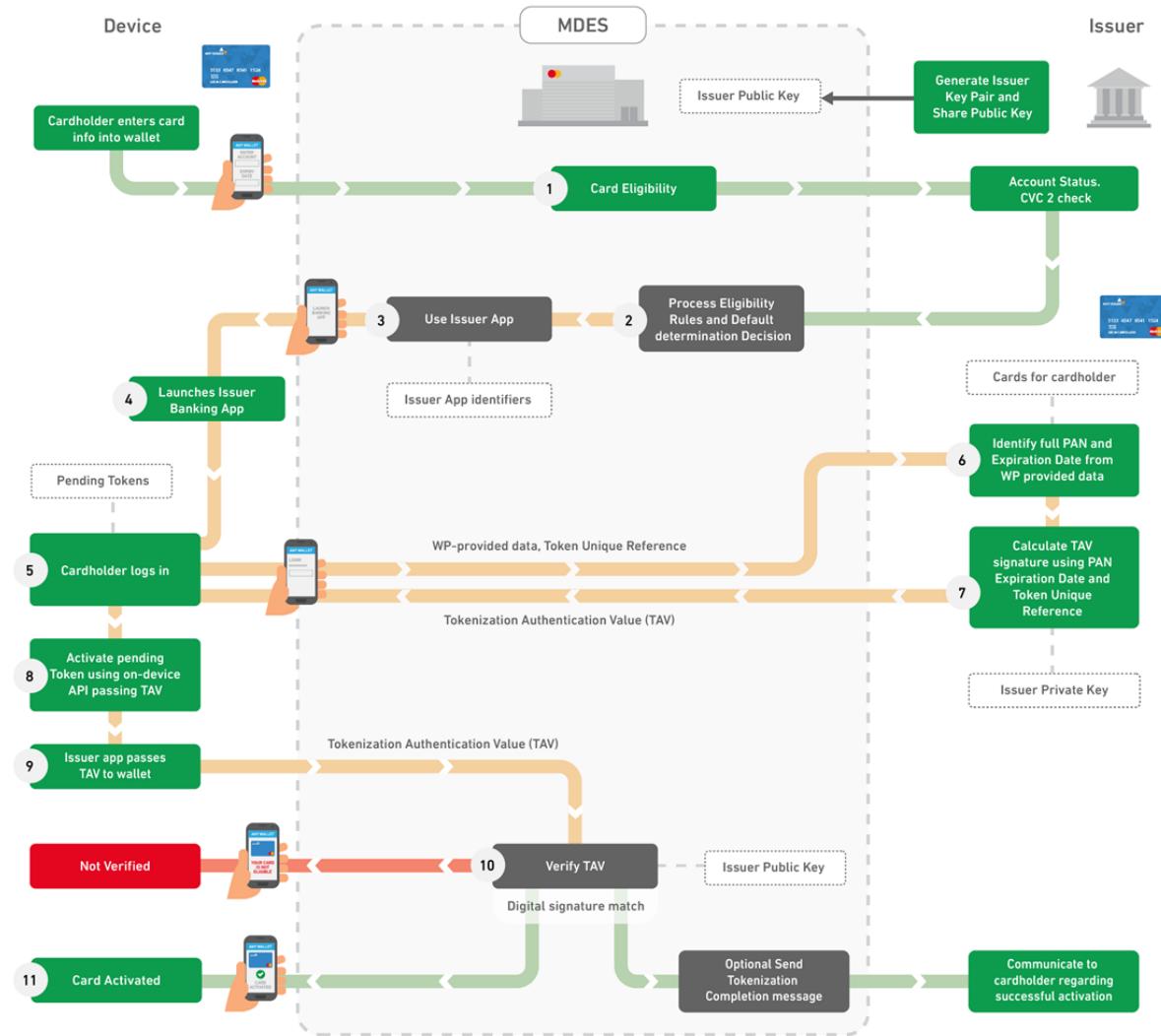
The issuer’s app would retrieve information from the wallet to identify a card for which digitization has been approved but requires authentication prior to activation. The exact method would be determined between the issuer and the Wallet Provider. However, the information passed should enable the issuer to determine the Account PAN of the card digitized, because this information is required for the calculation of the signature within the TAV.

The information passed from the wallet to the issuer’s app should include the following:

- The Expiration Date, if the card expiry date known to the cardholder matches the latest expiry date known to the issuer
- The Token Unique Reference, if the issuer wants to authorize the activation of a specific token

Mastercard recommends that issuers include the Expiration Date and/or the Token Unique Reference within the signed data wherever possible.

The following diagram shows an example of how activation using a TAV can be implemented.



**NOTE: Details on the creation of a TAV and the Key Management processes required to support this method of activation are provided in the Issuer-Initiated Digitization—Tokenization Authentication Value (TAV) section.**

MDES uses the predefined public key associated with the Account Range of the PAN to verify the signature contained in the TAV. If the signature is correct, MDES activates the token. Otherwise, MDES advises the Wallet Provider of an error and the token remains suspended, awaiting activation.

MDES implements a velocity count on activation attempts using a TAV and permits only three invalid attempts at activation. Further attempts, even with a valid TAV, results in the Wallet Provider being advised of an error. This prevents a brute force attack on the cryptographic key used to create the signature. After three invalid attempts, a token may only be activated using the Customer Service Tools (Application or API).

## **Issuer App Token Activation via Customer Service API**

An issuer may authenticate cardholders using the issuer's own mobile app and then activate tokens using the MDES Customer Service API.

To activate a token via the Customer Service API, an issuer must perform the following tasks:

- **Identify the Issuer App as the Activation Method**—This can be achieved by either:
  - Setting it as the default Activation Method, during issuer enablement
  - Including it in the 'Approve, but require authentication' eligibility or authorization responses that the issuer systems return to MDES (as TER or TAR network message responses, or Authorize Service API responses)
- **Add cardholder authentication functionality to the Issuer App**—Add functionality that enables a cardholder to verify their identity and passes the authentication result to the issuer systems.
- **Adapt the Issuer App to query the wallet application about tokens awaiting activation**—Each wallet will provide a unique API to perform this function. The Issuer App must obtain the Token Unique Reference from the wallet application and pass it to the issuer systems.

As an alternative, the Issuer App can query MDES via the Search API to find all tokens associated with a PAN. This may be useful when the Issuer App is a wrapper to an online banking service and does not have access to the on-device wallet APIs. The API response will include the Token Unique Reference and Token Status for each token, with a CurrentStatusCode value of 'U' (unmapped) and ProvisioningStatusCode of 'A' (awaiting activation) assigned to tokens awaiting activation.

**NOTE: If the provisioning status is any of the following values, the token cannot be activated and an attempt to activate it will fail:**

- **T = awaiting cardholder acceptance of Terms and Conditions**
- **P = token and credentials being prepared**
- **D = token and credentials being delivered to Wallet Provider or device**
- **S = provisioning successful**
- **F = failed**

Issuers should be aware that if there are multiple tokens in an unmapped status with an 'awaiting activation' provisioning status, they must determine and activate the correct token on the correct device.

The issuer might need to implement retry logic with the Search API if a token is not yet in a state to be activated. Any retry logic should minimize the time a cardholder waits for a response in the user interface, and cardholders should be informed that their token will be activated later if it cannot be activated immediately. The detailed design and behavior of this user experience must be determined by the issuer.

- **Adapt the issuer systems to use the Token Activate API for token activation**—Adapt the issuer systems to send a Token Activate API request, containing the Token Unique Reference, to MDES to activate the token awaiting activation.

**NOTE: The issuer must be capable of handling the error situation where a token is not in the appropriate state to be activated, and perform retry logic. This might involve multiple retry attempts, because provisioning can sometimes take a significant period of time and so the token might not be ready for activation.**

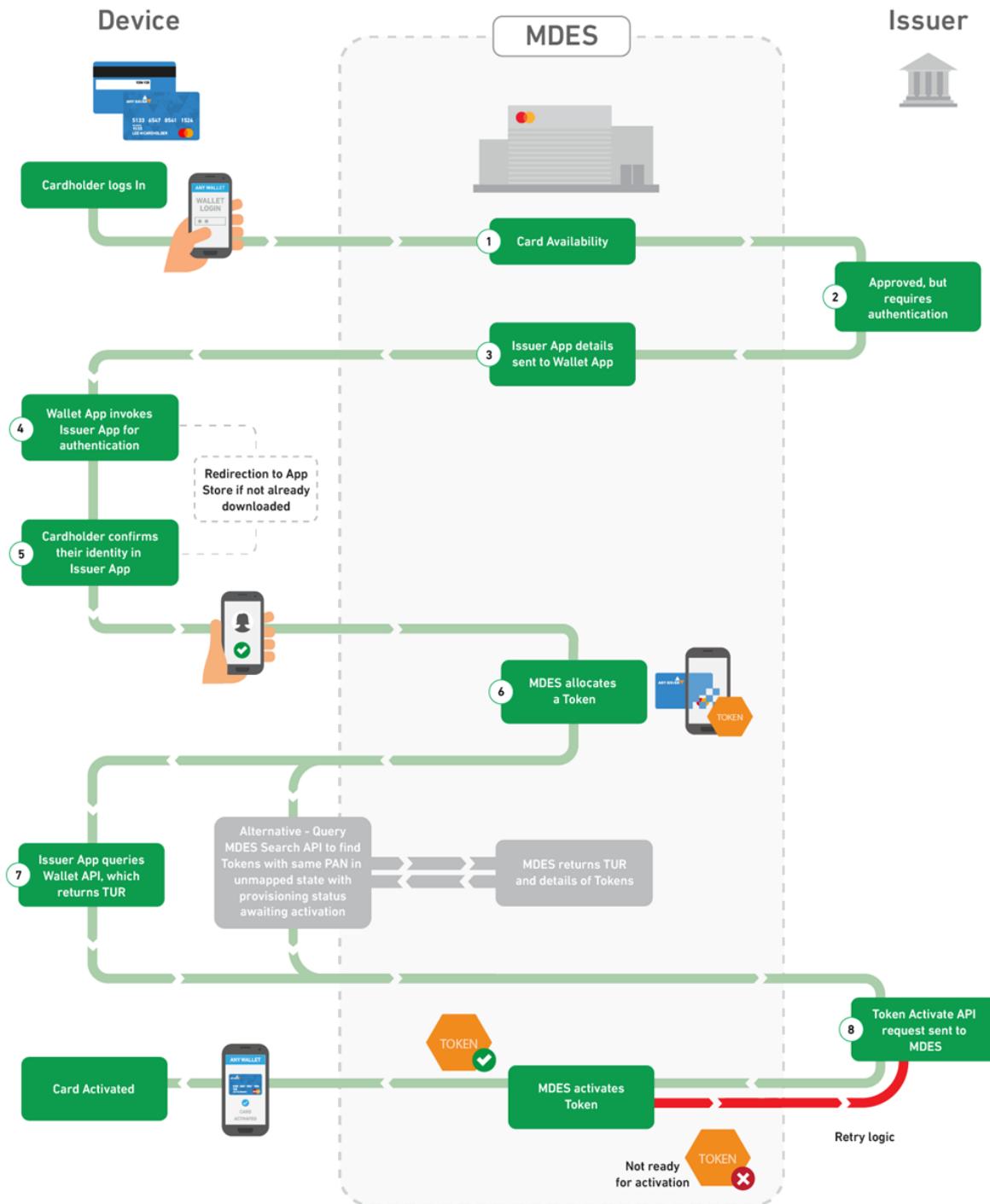
If the Token Activate API fails, it may report that the token is not in the 'awaiting activation' state. This might occur if an issuer uses the Token Activate API before the Wallet Provider has completed the provisioning of the token to the device. Mastercard strongly recommends that the issuer checks the token status before using the Token Activate API. The token should have a CurrentStatusCode value of 'U' (unmapped) and ProvisioningStatusCode of 'A' (awaiting activation) before attempting activation.

**NOTE: The Token Activate API and Search API are features of the MDES Customer Service API. For further information, refer to the Mastercard Developers site (<https://developer.mastercard.com>).**

The issuer determines how their app authenticates cardholders. For example, the app could require a cardholder to log in with their online banking credentials and click an activation button, which sets an authentication flag for their online account.

When implemented, the authentication and activation method includes the following activities, which are shown in the following diagram:

1. The cardholder uses the wallet application on their device to request digitization of a card.
2. During the card eligibility check or authorization check stages, the issuer systems respond to MDES with 'Approve, but require authentication' and the Issuer App name.
3. MDES sends the Issuer App details to the wallet application.
4. The wallet application opens the Issuer App or directs the cardholder to the app store, if the Issuer App is not installed.
5. The cardholder verifies their identity using the Issuer App, which notifies the issuer systems.
6. MDES allocates a token for the card PAN and provisions it to the device.
7. The Issuer App obtains the Token Unique Reference from the wallet application and sends it to the issuer systems.
8. The issuer systems send a Token Activate API request to MDES to activate the token. An error might be returned if the token is not in a state to be activated, and appropriate retry logic must be implemented.



## Activation by Activation Code

Issuers may select an authentication process that uses an Activation Code (a random value), which is sent to the cardholder using a trusted channel for entry into the wallet application.

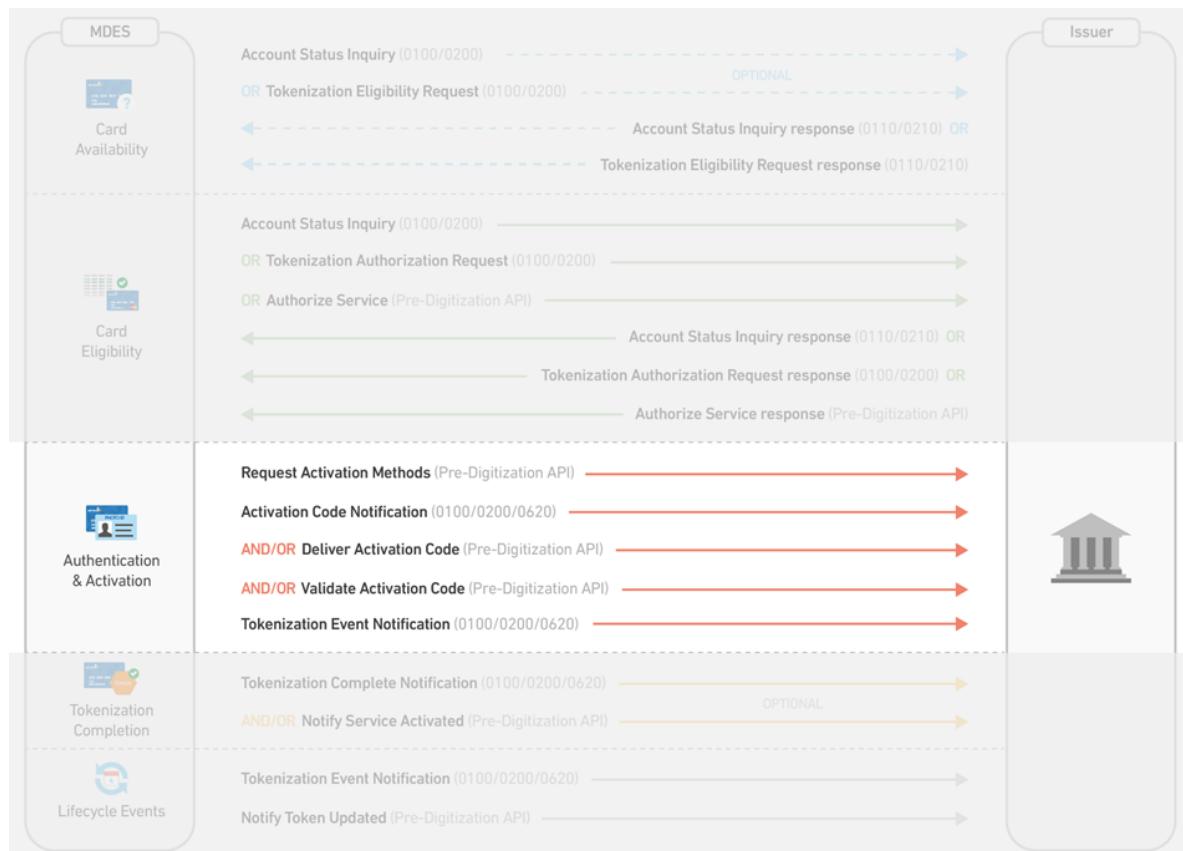
Activation Code generation and validation can be controlled by either:

- **MDES**—This is the default method, where MDES generates and provides each code (with an Expiration Date and Time) to the issuer for sending to the cardholder. MDES checks the cardholder-entered code and provides the result to the issuer.
- **Issuer**—This method uses Pre-Digitization API messages and is configured during issuer enablement. The issuer generates and sends each code to the cardholder. MDES passes the cardholder-entered code to the issuer, who checks it and provides the result to MDES.

**NOTE: Follow the trusted channel's communication requirements to support the delivery of the Activation Code as an authentication method. The Activation Code is sometimes known as an Authentication Code, usually when the code is used only to indicate successful authentication of a cardholder.**

The following diagram shows the pre-digitization messages that can be sent during Cardholder Authentication and Token Activation.

**Figure 16: Message Flows for Cardholder Authentication and Token Activation**



The Activation Code can be entered into the wallet application either:

- Manually, by the cardholder
- Automatically, if the code is distributed directly to the mobile device by text message (or an equivalent) and the Wallet Provider and mobile device operating system support this functionality

### **MDES Controls Activation Codes**

By default, MDES generates and validates the Activation Codes used to authenticate cardholders. MDES Activation Codes are random 6-digit numeric values.

When a cardholder selects an authentication method that requires an Activation Code, the Wallet Provider informs MDES of the cardholder's selected communication channel. MDES sends the issuer an Activation Code Notification (ACN) network message and/or a Deliver Activation Code API message (depending on what was chosen during issuer enablement). The message contains:

- Activation Code
- Expiration Date and Time for the code
- Cardholder's selected communication channel

The issuer provides the Activation Code and its Expiration Date and Time to the cardholder using the selected communication channel. The code value entered into the wallet application is relayed to MDES, where it is checked. If the Activation Code has expired, it is rejected. Otherwise, the entered value is compared to the MDES-generated code. Three attempts at entering the Activation Code correctly are permitted before the code is invalidated; no further attempts are permitted.

### **Validity Period**

The issuer can define an Activation Code validity period for each account range during issuer enablement. The validity period can be specified in minutes (1–59), hours (1–23), or days (1–30). An Activation Code's Expiration Date and Time is calculated, using the relevant validity period, when the code is sent to the issuer.

The cardholder must complete the activation process before the Activation Code expires. Therefore, when defining the validity periods, the issuer should:

- Allow enough time for a cardholder to receive the Activation Code and enter it into their device
- Be aware that, even though the cardholder can contact the issuer to generate a new Activation Code, the wallet user interface might not present an option for the cardholder to receive and enter the new code

### **Resending Activation Codes**

The MDES functionality enables Wallet Providers and issuers to build implementations that allow for the resending of Activation Codes while they are still valid. This enables a cardholder to request the code again if they lost it or did not receive it via the chosen delivery channel.

Depending on the implementation:

- The Wallet Provider may allow the cardholder to request a resend from the wallet user interface.  
When the Wallet Provider requests the resend from MDES, MDES will send the Activation Code (with the **same** Expiration Date and Time) and chosen delivery channel to the issuer. The issuer systems must resend the code to the cardholder, using the delivery channel, and the wallet application must allow for the entry of the re-sent code.
- The issuer may allow the cardholder to request a resend directly from the issuer, such as by calling issuer customer services.  
The issuer can use the Customer Service Tools to resend the Activation Code (with a **new** Expiration Date and Time) using a particular delivery channel; see Token Activation. The wallet application must allow for the entry of the re-sent code.

When an Activation Code is invalidated or has expired, it cannot be resent.

### **Token Activation**

When a valid Activation Code is entered within a valid timeframe, MDES activates the token. When the Activation Code is invalidated or has expired, the cardholder must contact the issuer to complete activation.

If the issuer chose to receive Tokenization Event Notification (TVN) network messages, it is sent TVN messages during the activation process (with an appropriate reason code) when:

- An incorrect Activation Code value is entered on the first and second attempts
- The number of invalid attempts has been exceeded on the third attempt
- The Activation Code is invalidated or expired, either on a fourth attempt or an attempt after the validity period has expired

For information on the TVN message, refer to the Lifecycle Events section.

Using the Customer Service Tools, the issuer can:

- **Resend an Activation Code**—A code can be re-sent up to three times while it is still valid; the code's Expiration Date and Time is reset each time it is sent.
- **Generate and send a new Activation Code**—A new code (with a new Expiration Date and Time) can be generated any time, up to 30 days after the token was allocated (the number of days is subject to change at the discretion of Mastercard)
- **Activate the token immediately** (without needing to send a new code)

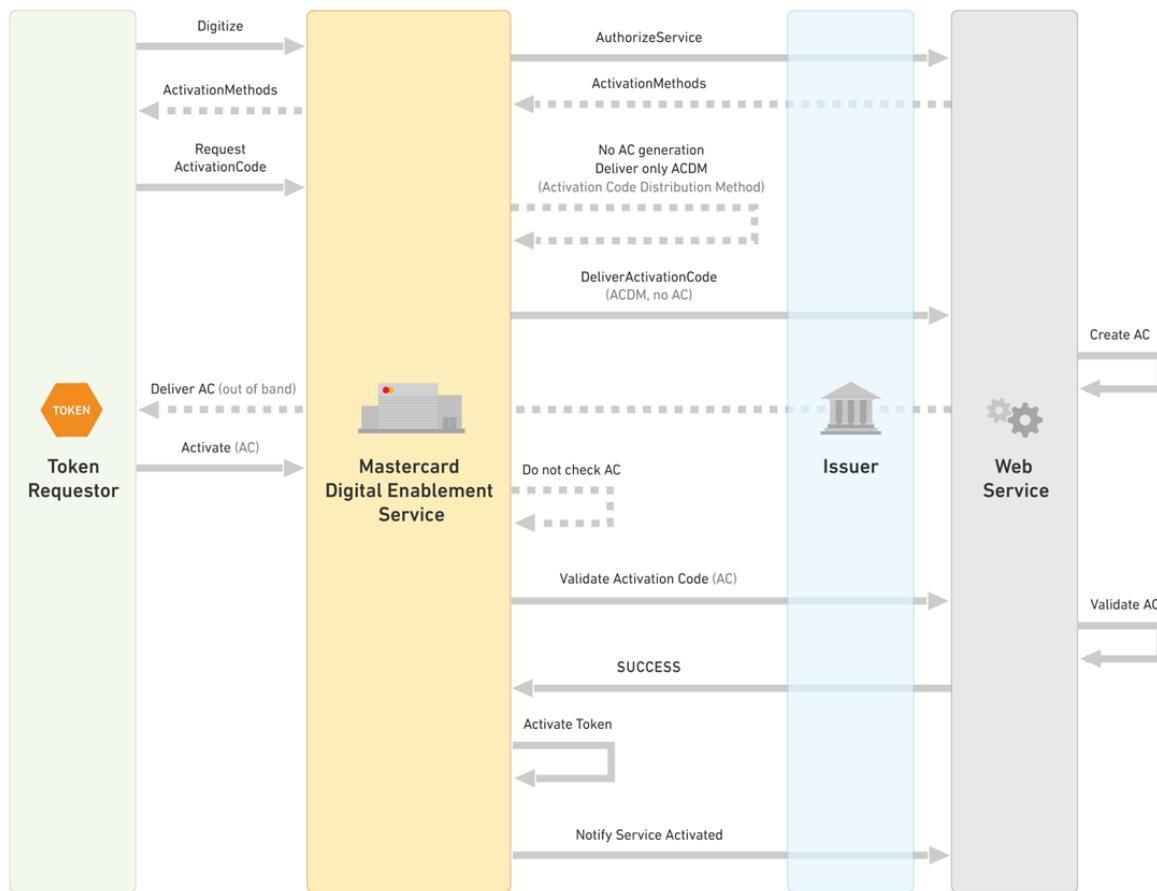
**NOTE: To reduce the risk of unauthorized digitization, Mastercard recommends that the issuer uses a robust process to confirm the identity of the cardholder prior to distributing the Activation Code or prior to activating the token using the Customer Service Tools.**

## Issuer Controls Activation Codes

The issuer can chose, during issuer enablement, to generate and validate its own Activation Codes. Issuer-generated Activation Codes can be an alphanumeric string of up to 32 characters.

**NOTE: The issuer should consider the wallet programs it is supporting when determining its Activation Code generation algorithm. For example, some Wallet Providers might only support 6-digit codes.**

The following diagram shows an overview of the Activation Code process.



1. MDES relays the digitization request from the Wallet Provider (Token Requestor) to the issuer. When additional cardholder authentication is required, MDES provides the possible authentication methods to the Wallet Provider.
2. When a cardholder selects an authentication method that requires an Activation Code, MDES sends the issuer a Deliver Activation Code API message containing the cardholder-chosen Activation Code Distribution Method (ACDM). No MDES Activation Code is supplied.

3. The issuer's web service generates the Activation Code and an optional Expiration Date and Time, and sends them to the cardholder out of band, using the channel indicated by the chosen ACDM.
4. The Activation Code value entered into the wallet application is relayed to MDES, which sends the value to the issuer using a Validate Activation Code API request message. MDES does not check the cardholder-entered value because it does not know the issuer-generated code and associated Expiration Date and Time.
5. The issuer web service checks the cardholder-entered code and sends the validation result to MDES in the Validate Activation Code API response message.
6. If MDES receives a SUCCESS result, MDES activates the token and notifies the issuer of the activation using the Notify Service Activated API message.

Typically, three attempts at entering the Activation Code correctly are permitted before the code is invalidated; no further attempts are permitted. When the Activation Code is invalidated or has expired, the issuer might allow the cardholder to request a new Activation Code directly from the issuer. This depends on the issuer implementation and is out of scope of this document.

### **Activation Code Notification (ACN) Message**

Issuers can choose to receive this network message when they need MDES to generate an Activation Code for authenticating a cardholder.

Issuers may also receive this network message (if chosen) when a cardholder requests a resend of their Activation Code from the wallet user interface, if the Wallet Provider has implemented such functionality. For more information, see Resending Activation Codes.

ACN messages can be sent as one of several message types. The issuer can choose to receive either:

- Administrative Advice/0620 message type
- Authorization Request/0100 or Financial Transaction Request/0200 message types (the type depends on whether the issuer is connected to the Dual Message System or Single Message System, respectively)

### **Message Request Details**

The ACN network message contains the following:

- Card Account PAN
- Card Account PAN Expiration Date
- The type of device initiating the digitization request, when supported by the Wallet Provider
- Wallet ID (WID)
- Token Requestor ID (TRID)

The ACN message also contains the Activation Code to be used to activate a specific token. This additional data is as follows.

<b>Data</b>	<b>Description</b>
Correlation ID	A unique value assigned to a card digitization, enabling issuers to link the pre-digitization messages relating to that digitization. For example, if a cardholder enters an invalid CVC 2 during digitization, the multiple Card Eligibility request messages will have the same Correlation ID.
Activation Code	The Activation Code to be delivered to the cardholder by the issuer.
Activation Code Expiration Date and Time	The date and time that the Activation Code expires, specified in Coordinated Universal Time (UTC) as YYMMDDhhmm. The cardholder should be informed of the Expiration Date and Time so that they can complete activation in a timely manner.
Cardholder's Activation Method Preference	The channel or method selected by the cardholder if a choice was offered by the Wallet Provider. An issuer may request to distribute the Activation Code to one or more cardholder-specific channels when this data is not provided.

### **Message Response Details**

The response to the ACN is not used by MDES. Although a response message is required, the response code shall be ignored. It is advised that issuers respond with DE 39 = 00.

### **Deliver Activation Code API Message**

Issuers can choose to receive this API message when an Activation Code is used for authenticating the cardholder.

The Deliver Activation Code API request message contents depend on who generates the code (see Activation by Activation Code):

- **MDES** (default method)—The message contains the MDES-generated Activation Code, its Expiration Date and Time, and the cardholder-chosen Activation Code Distribution Method (ACDM). The details are the same as those provided in an Activation Code Notification (ACN) network message.  
Issuers may also receive this message (if chosen) when a cardholder requests a resend of their Activation Code from the wallet user interface, if the Wallet Provider has implemented such functionality. For more information, see Resending Activation Codes.
- **Issuer**—The message contains the ACDM.

For information on the Deliver Activation Code API message and its parameters, refer to the MDES Pre-Digitization API documentation on the Mastercard Developers site.

### **Validate Activation Code API Message**

Issuers can choose to receive this API message when they need to validate a cardholder-entered Activation Code prior to token activation.

The Validate Activation Code API message is used by issuers who are generating and validating their own Activation Codes (see Activation by Activation Code):

- The request message provides the Activation Code value entered into the wallet application to the issuer so it can validate the code.
- The response message provides the issuer's validation result to MDES.

If the validation is successful, MDES activates the token.

Typically, three attempts at entering the Activation Code correctly are permitted before the code is invalidated; no further attempts are permitted. When the Activation Code is invalidated or has expired, the issuer might allow the cardholder to request a new Activation Code directly from the issuer. This depends on the issuer implementation and is out of scope of this document.

For information on the Validate Activation Code API message and its parameters, refer to the MDES Pre-Digitization API documentation on the Mastercard Developers site.

## Activation by Call Center

Issuers may select an authentication process that requires the cardholder to contact the issuer's call center, which can verify the cardholder's identity before activating their token.

This method of authentication is labor intensive and could provide a poor customer experience. Mastercard recommends that issuers use other authentication methods instead, and only consider this method for specific circumstances where they need to talk to the cardholder, for example when there has been suspicious account activity.

To use this method of authentication and activation:

- The issuer includes their call center phone number as an Activation Method in the 'Approve, but require authentication' eligibility or authorization responses that the issuer systems return to MDES (as TER or TAR network message responses, or Authorize Service API responses).
- After confirming the cardholder's identity, the issuer's call center uses the MDES Customer Service Tools to activate the token. For information on the Customer Service Tools, refer to the Operational Management chapter.

**NOTE: It is recommended that a robust cardholder authentication process is performed prior to activating the token using the Customer Service Tools to reduce the risk of unauthorized digitization.**

## Tokenization Completion

Tokenization Completion activates the token so that it can be used to make payments.

### Overview

When the eligibility decision is 'Approve' or 'Approve, but require authentication,' the card is tokenized and digital account credentials are delivered to the target device, server or solution.

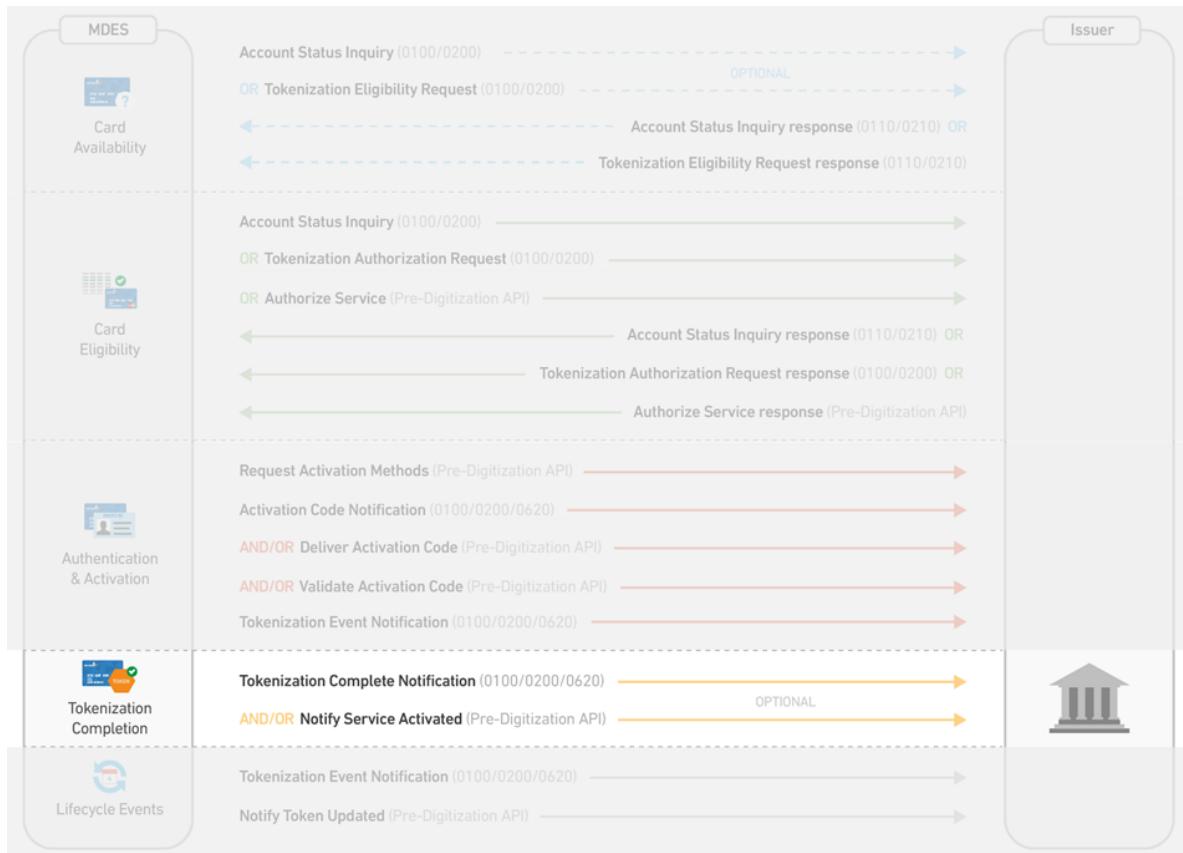
### Token Mapping

When cardholder authentication is not required or is optional, the token is activated immediately by establishing the token to PAN mapping relationship. Otherwise, the mapping does not occur until authentication and activation are completed by the cardholder or issuer as described in Cardholder Authentication and Token Activation. The active token is then ready to perform transactions.

The token to PAN mapping relationship is established within the MDES Transaction Processing component. When the token is used for transactions, MDES replaces the token with the PAN in the transaction data it sends to the issuer.

### Issuer Notification

Once the tokenization process is complete, MDES can send the issuer a Tokenization Complete Notification (TCN) network message and/or Notify Service Activated API message (depending on what was chosen during issuer enablement), which identifies the token.

**Figure 17: Message Flows for Tokenization Completion**

The issuer is not informed when MDES declines a digitization due to an eligibility rule; see Declined Digitization.

For merchant and commerce platform tokenization, additional cardholder authentication is optional. If it is performed, it will be after tokenization (not before, as with wallet programs). Therefore, issuers should be aware that the TCN or Notify Service Activated API message will be received before a Request Activation Methods API message, an Activation Code Notification (ACN) message, or Deliver Activation Code API message.

## Tokenization Complete Notification (TCN) Message

Issuers can choose to receive this network message when the card has been digitized successfully.

TCN messages can be sent as one of several message types. The issuer can choose to receive either:

- Administrative Advice/0620 message type
- Authorization Request/0100 or Financial Transaction Request/0200 message types (the type depends on whether the issuer is connected to the Dual Message System or Single Message System, respectively)

## Message Request Details

The TCN network message contains the following:

- Card Account PAN
- Card Account PAN Expiration Date
- The type of device initiating the digitization request, when supported by the Wallet Provider
- Wallet ID (WID)
- PAN Mapping File Information, containing:
  - Token
  - Token expiration date
  - Token Assurance Level
  - Token Requestor ID (TRID)
  - Storage Technology

The TCN message can also contain the following information relating to the tokenization process.

Data	Description
Correlation ID	A unique value assigned to a card digitization, enabling issuers to link the pre-digitization messages relating to that digitization. For example, if a cardholder enters an invalid CVC 2 during digitization, the multiple Card Eligibility request messages will have the same Correlation ID.
Number of Active Tokens for the Account PAN	The number of active or suspended tokens for the Account PAN digitized to devices (including the token requested).
Issuer Product Configuration ID	The value selected by MDES and communicated to the Wallet Provider. The Issuer Product Configuration ID can be right-padded and left-padded with spaces.
Cardholder Language	The selected language of the mobile device (when supplied by the Wallet Provider).
Device Name	The cardholder's own name for their device (when supported by the device and Wallet Provider).

**NOTE: The Device Name received from the Wallet Provider may contain special characters that are not supported by the Mastercard Network. Such characters are replaced with a period ('.') character. Issuers should be aware that this may result in the Device Name consisting of all periods when non-Latin languages are selected by the cardholder within the device.**

Data	Description
Final Tokenization Decision	The final eligibility decision, either: <ul style="list-style-type: none"><li>• 1 = Approve</li><li>• 2 = Approve, but require additional authentication</li></ul>
Final Tokenization Decision Indicator	The element of MDES that determined the eligibility decision: <ul style="list-style-type: none"><li>• 1 = Tokenization Eligibility Response</li><li>• 2 = Tokenization Authorization Response</li><li>• 3 = Issuer pre-defined tokenization rules</li><li>• 4 = Mobile Application</li></ul>
Terms and Conditions Identifier	The value of the Terms and Conditions agreed on by the cardholder (when supported by the Wallet Provider).
Terms and Conditions Date and Time	The date and time of the cardholder's agreement, specified in Coordinated Universal Time (UTC) as YYMMDDhhmm.
Number of Activation Attempts	The number of Activation Code entry attempts by the cardholder. Not supplied if a code has not been entered.  For merchant and commerce platform tokenization, the token is activated automatically, so this value will be set to 0.
Token Unique Reference	A unique value that identifies the token designated. It is used by the Transaction Detail Service (TDS) or an issuer's TDS, and may be used for requests using the Customer Service Tools.  The token has the same Token Unique Reference throughout its life, even if the Account PAN is updated due to card re-issue; see Token Designation Service. The value only changes when the token is recycled and re-allocated.
Primary Account Number Unique Reference	A unique value that identifies the Account PAN at the wallet level. If a wallet has multiple payment applications, there will be a single Primary Account Number Unique Reference for a PAN across all those applications.  This value is not the Payment Account Reference (PAR).
Token Type	The value indicating the type of token: <ul style="list-style-type: none"><li>• C = Mastercard Cloud-Based Payments (MCBP)</li><li>• S = Embedded Secure Element</li><li>• F = Card on File</li></ul>

### Message Response Details

The response is not used by MDES. Although a response message is required, the response code is ignored. Issuers should respond with DE 39 = 00.

## Notify Service Activated API Message

Issuers can choose to receive this API message when the card has been digitized successfully.

The Notify Service Activated API message includes all the information that is provided in the Tokenization Complete Notification (TCN) message.

For information on the Notify Service Activated API message and its parameters, refer to the MDES Pre-Digitization API documentation on the Mastercard Developers site.

## Issuer-Initiated Digitization with MDES Token Connect

---

Issuer-initiated digitization provides a digitization experience driven by the issuer, from the issuer's app or website. The issuer pushes an account number to the Token Requestor's environment to create a token. Issuer-initiated digitization is also referred to as Push Provisioning.

MDES Token Connect is a framework that allows MDES issuers to connect with open-loop MDES Token Requestors such as wallets storing tokens on a mobile device or an IoT device, commerce platforms or merchants, for Push Provisioning.

**NOTE: Further information about MDES Token Connect framework is available in Mastercard Developers at <https://developer.mastercard.com/page/push-provisioning>**

### Consumer Experience

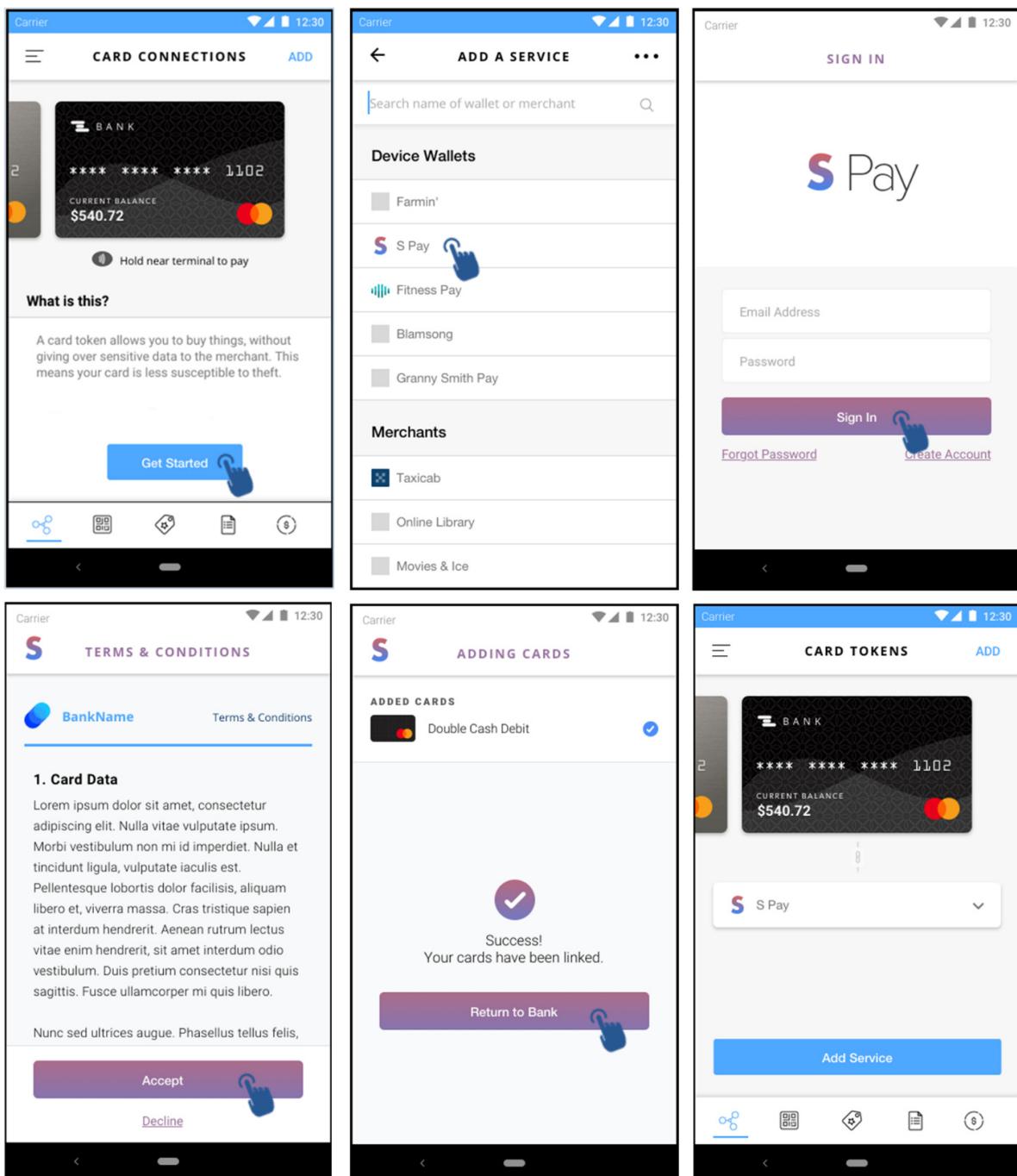
Once logged into their issuer application or website, the consumer is presented with the list of Token Requestors enabled to receive Token Connect provisioning requests. The cardholder chooses the target Token Requestor, then selects one or more card accounts to be pushed to this target.

The consumer is further taken to the Token Requestor's app or website where they are asked to sign in or sign up, so that the Token Requestor can associate the card being pushed with one of their customer accounts. Upon successful consumer login, the Token Requestor proceeds with the tokenization of the account.

**NOTE: Depending on the issuer configuration, cardholder authentication may be required to activate the new token.**

When the tokenization is completed, the consumer can choose to go back to the issuer's website or application and repeat the process with more Token Requestors.

The figure below illustrates a possible user experience for tokenization using Token Connect:



MDES Token Connect may support multiple user experiences such as:

- Web-to-web on mobile as well as desktop devices
- Web-to-app on Android and iOS mobile devices
- App-to-app on Android and iOS mobile devices

## Benefits of Token Connect

Push Provisioning offers a better user experience where the consumer simply selects one or more card(s) proposed by their issuer to be digitized rather than enter their card details manually (account number, expiry date, CVC2).

Push Provisioning has several advantages when compared to a traditional card account provisioning initiated from the Token Requestor's environment. They are listed below:

- It significantly increases tokenization success rates. As the tokenization is triggered by a MDES issuer that has enabled the Account Ranges and Token Requestors that they suggest to their cardholders, the MDES eligibility check will be successful almost all the time.
- For Token Requestors, it is the opportunity to get more visibility for their brand through the issuer's interface, and acquire new accounts from the issuer.
- Issuers can enable Instant Digital Issuance. Cardholders can use the digital card account as soon as they have been approved for the FPAN and even before the plastic card is shipped or active.
- For issuers, it is the opportunity to offer more services in their banking app/website and increase consumer engagement on these digital applications.

MDES Token Connect combines the benefits of Push Provisioning with the scalability of an interoperable framework. There is no need for multiple proprietary APIs between issuers and Token Requestors, no costly one-to-one integration between each issuer and Token Requestor. Once their connection to MDES Token Connect framework is enabled, a MDES issuer can connect with any MDES Token Requestor that has implemented Token Connect.

## Security Guidelines

While MDES Token Connect offers an optimized consumer experience for digitization, it also creates security challenges that need to be addressed by the issuer.

### Security Risks associated with MDES Token Connect

This section details these security risks and associated mitigation recommendations. The consumer's login to the issuer's environment constitutes a pre-authentication of the cardholder where re-authenticating the cardholder later in the process seems unnecessary.

The usage of MDES Token Connect framework without further cardholder authentication must be thoroughly managed to avoid fraud risks such as the following:

- Push provisioning with MDES Token Connect is a card-not-present operation. Consumers do not enter their CVC2 security code, even if a CVC2 is applicable for the card being digitized. A significant part of the value proposition of Token Connect for the consumer consists of simplifying their digitization experience by avoiding manual entry of card details. A possible risk is that Token Connect may allow a fraudster to digitize their victim's card into their own Token Requestor account, if they have obtained access to their victim's issuer account via a phishing attack.
- The URL that toggles the consumer from the issuer interface to the Token Requestor interface is highly sensitive. First, it contains the pushAccountReceipt(s) that act as a "voucher to tokenize" a particular card/financial account. Secondly, it generally embeds the issuer callback URL to return to the issuer app/web site. That sensitive URL is meant to

remain and be used locally by the cardholder on the same device where the issuer interface is running. Yet this URL may be divulged accidentally by the cardholder or captured maliciously by a fraudster. In the absence of countermeasures, this may allow the fraudster to digitize their victim's card into their own Token Requestor account, or even get access to their victim's account in the issuer app/web site.

To mitigate these risks, MDES has implemented restrictions for tokenizations triggered with a pushAccountReceipt:

- A pushAccountReceipt is valid exclusively for the card or financial account and for the Token Requestor (TRID) for which it was generated
- A pushAccountReceipt expires thirty minutes after its issuance. This gives reasonable margin for the consumer to sign in, or even sign up, to the Token Requestor's environment before completing tokenization
- A pushAccountReceipt can be used successfully only once (no replay)

For these restrictions to be entirely efficient, issuers must include complementary mitigation actions as part of their Token Connect implementation.

### **Consumer Login in Issuer's Interface**

Push provisioning with Token Connect is triggered from the issuer's interface where the cardholder is logged in, and a successful login may constitute a pre-authentication of the cardholder for the tokenization operation.

The security of the operation is highly dependent on the security of the login method in the issuer's environment. Issuers should support secure login methods that are resistant to attacks such as phishing and keystroke logging. Timeout before logout should also be considered.

### **Device Binding**

An efficient way for issuers to secure tokenization with MDES Token Connect is to implement device binding. For the vast majority of cases, the device from which the user accesses the issuer interface to trigger the tokenization is the same device from which the Token Requestor completes tokenization.

By extension, the device IP address in the triggering issuer interface and in the target Token Requestor interface should generally be identical. A matching IP address is an excellent indicator of normal Token Connect path followed by the genuine cardholder.

On the contrary, a mismatch between device IP address can be due to:

- A compromise of the URL when toggling from issuer to Token Requestor interface
- A legitimate digitization initiated from a desktop computer but completed on the mobile device, if the device-based wallet supports a proprietary desktop-to-mobile digitization path in their Token Connect implementation
- A change of dynamic IP address of the device while toggling from issuer to Token Requestor interface (for instance, if the user is traveling or switching data network)

For Token Connect, Mastercard requests that Token Requestors supply the IP address of the device initiating the tokenization, so that issuers can receive this information in the

---

tokenization authorization message (ISO-based TAR, or AuthorizeService request in Pre-digitization API).

**NOTE: Issuers that receive the tokenization authorization message as an Account Status Inquiry (ASI) cannot receive the IP address information from the Token Requestor, and should consider changing their configuration to support Token Connect and device binding.**

To mitigate the risk of URL compromise with Token Connect, Mastercard recommends that the issuer implements the following algorithm:

- After receiving pushAccountReceipt(s) from MDES, and before driving the consumer to the Token Requestor's interface, log the minimum following information on their back-end server:
  - pushAccountReceipt
  - card/financial account number
  - Token Requestor ID (TRID)
  - Device IP address
- While processing the tokenization authorization message, if the account source is "account added via application", and the { FPAN, TRID } in the message matches one of the logged { pushAccountReceipt, account number, TRID, IP address } combinations:
  - If the device IP address is provided and matches the logged device IP address: approve the request (or go on decision algorithm)
  - If the device IP address is not provided, or is provided but doesn't match the logged device IP address:
    - For a device-based token (paymentApplInstanceld parameter is present): require additional authentication
    - Otherwise (server-based or static token): decline the request

**NOTE: When they use AuthorizeService (Pre-digitization API), issuers may also receive additional information about the target device for device-based wallets such as: device serial number, MSISDN or IMEI. Issuers may use these data elements to reinforce their device binding algorithm by comparing these data elements with information from the device hosting the issuer interface. However, this information is optional.**

### **Issuer Callback URL**

Most issuers will want to drive the consumer back to their app or web site upon completion of tokenization with Token Connect.

When this is the case, the issuer appends a "callback URL" as parameter to the URL that redirects the consumer from the issuer to the Token Requestor's environment ("redirection URL").

**NOTE: Further information about MDES Token Connect framework is available in Mastercard Developers at <https://developer.mastercard.com/page/push-provisioning>**

As discussed above, this redirection URL may be divulged accidentally by the consumer or captured maliciously by a fraudster. If this happens, the embedded issuer callback URL would be equally compromised.

Issuers that supply a callback URL must ensure that their systems are not vulnerable to a compromise of this callback URL. In other words, their implementation must ensure that the callback URL is worthless to anyone that is not the genuine cardholder. They shall not include any sensitive parameters in the callback URL.

As an example, if the issuer wants to include a session identifier in the callback URL to avoid the hassle of a new sign in, they must ensure that the supply of the session identifier is not enough to waive the sign in operation. It must be coupled with additional measures such as device fingerprint matching, IP matching, and timeout checking.

### **Card Eligibility Decision**

Although your Token Connect implementation is secured with device binding and a safe callback URL, such protective measures are ineffective if a fraudster gets access to a genuine cardholder's issuer account and trigger tokenization, for instance, through phishing or keystroke logging.

Besides revising the consumer login method itself, if you need to secure your Token Connect implementation against login attacks, the best protection is to require additional authentication during card eligibility, and to propose exclusively out-of-band authentication methods such as a message to a mobile number or email address. Activation via an issuer app or issuer web site should not be proposed. An additional out-of-band authentication will obviously impact the consumer experience, although it offers protection against both phishing attacks and a compromise of the redirection URL.

As a reminder, the final card eligibility decision is a combination of the issuer's response to the tokenization authorization message (ISO Account Status Inquiry, ISO Tokenization Authorization Request, or AuthorizeService request from MDES Predigitization API) and the issuer predigitization eligibility rules parameterized for the account range in MDES, if any.

**NOTE: See [Card Eligibility](#) for further details.**

When enabling Token Connect, issuers should review and adjust their decision algorithm for the tokenization authorization message as well as the eligibility rules that they have parameterized for their account ranges enabled in MDES. They must be ready to process situations such as the absence of CVC2 and IP mismatch.

### **Predigitization Eligibility Rules**

When implementing MDES Token Connect, issuers may need to revise their MDES Pre-digitization Eligibility rules.

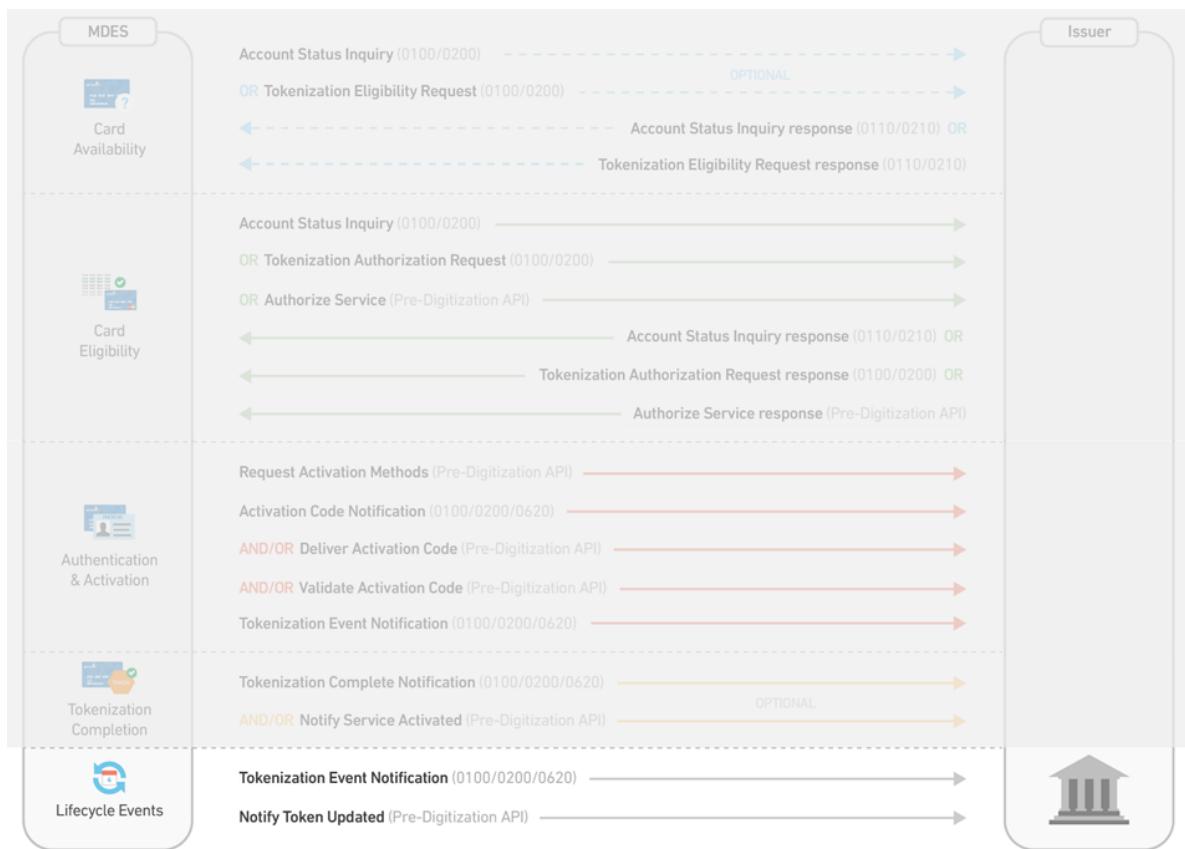
With the introduction of the MDES Token Connect framework, Mastercard makes a new condition available for issuers to create eligibility rules, based on the presence or absence of a Push Account Receipt. Issuers wishing to create eligibility rules specifically for Token Connect digitizations simply need to include a condition "Push Account Receipt Present = Yes" to their rule.

## Lifecycle Events

MDES can send issuers Tokenization Event Notification (TVN) and/or Notify Token Updated messages when there are significant token changes. This includes changes to information about the token, its state (such as activation or suspension) and its Product Configuration.

The notifications, shown below, depend on the message types selected during issuer enablement (refer to the Issuer Enablement section).

**Figure 18: Message Flows for Token Lifecycle Events**



**NOTE: MDES allows predigitization messages to be configured at the account range level and if necessary, at the Wallet level.**

This allows some wallets/programs to be configured with an alternative or a simpler message flow (for example, just having ASI eligibility for M4M).

## Tokenization Event Notification (TVN) Message

Issuers can choose to receive this network message when there are unsuccessful Activation Code entry attempts (during Cardholder Authentication) or significant changes to the token (after digitization).

TVN messages can be sent as one of several message types. The issuer can choose to receive either:

- Administrative Advice/0620 message type
- Authorization Request/0100 or Financial Transaction Request/0200 message types (the type depends on whether the issuer is connected to the Dual Message System or Single Message System, respectively)

### Message Scenarios

A TVN is sent to the issuer systems when a change to a token status occurs. The following scenarios may apply:

Scenario	TVN Sent?	Reason
Token updated via Customer Service API or the Customer Service Application	No	The TVN is not sent to the issuer because the request for token update via Customer Service API or Customer Service Application is initiated by the issuer.
Token updated by the wallet	Yes	The TVN serves to inform the issuer and allows the issuer systems to be updated.
Token updated by the consumer	Yes	The TVN serves to inform the issuer and allows the issuer systems to be updated.
Token updated by a 0302 network message or batch file	No	A TVN is not required if the issuer systems generate a 0302 message. If a 0302 message fails, the TVN is not sent (only a 0312 message with an erroneous response code is sent to the issuer).

**NOTE: A TVN message is never sent to the issuer if the token has never been activated (it remains unmapped after 30 days in the 'awaiting activation' state). However, the issuer might receive TVN messages for unsuccessful Activation Code entry attempts, if they chose to be informed of them.**

### Message Request Details

The TVN network message contains the following:

- Card Account PAN
- Card Account PAN Expiration Date
- Wallet ID (WID)
- PAN Mapping File Information, containing:
  - Token

- Token expiration date
- Token Requestor ID (TRID)

A TVN message contains the details of an event occurring for a token on the service. An issuer may use this notification to trigger communication to the cardholder to assist their successful completion of the activation process.

Data	Description
Correlation ID	A unique value assigned to a card digitization, enabling issuers to link the pre-digitization messages relating to that digitization. For example, if a cardholder enters an invalid CVC 2 during digitization, the multiple Card Eligibility request messages will have the same Correlation ID.
Tokenization Event Indicator	This indicates the event that has occurred for the token: <ul style="list-style-type: none"><li>• 3 = Deactivate</li><li>• 4 = Deleted from consumer device</li><li>• 6 = Suspend</li><li>• 7 = Resume</li><li>• 8 = Tokenization Exception Event</li><li>• 9 = Replacement (token re-digitization)</li></ul> <p>Only event type 8 occurs during pre-digitization processing; the other types are token lifecycle events.</p>
Tokenization Event Reason Code	In case of a Tokenization Exception Event, indicates to the issuer which pre-tokenization exception event has occurred. The following values are supported: <ul style="list-style-type: none"><li>• 00 = Activation Code retries exceeded</li><li>• 01 = Activation Code expired or invalidated</li><li>• 02 = Activation Code entered incorrectly by the cardholder</li></ul>
Event Requestor	This indicates who or what caused a token status update (deactivate, suspend or resume): <ul style="list-style-type: none"><li>• 0 = Wallet Provider or Token Requestor</li><li>• 1 = Funding Account issuer</li><li>• 2 = Cardholder</li><li>• 3 = The Tokenization Event was requested in relation to a systematic event triggered by Mobile PIN Validation security (applicable to Tokenization Event Indicator value of 6 [Suspend] or 7 [Resume] only)</li><li>• 4 = The Tokenization Event was requested in relation to a systematic event triggered by Mobile PIN Change Validation security (applicable to Tokenization Event Indicator value of 6 [Suspend] or 7 [Resume] only)</li></ul>

## Message Response Details

The response is not used by MDES. Although a response message is required, the response code is ignored. Issuers are advised to respond with DE 39 = 00.

## Notify Token Updated API Message

Issuers can choose to receive this API message when there are significant changes to the token.

The Notify Token Updated API message contains details of an event occurring for a token on the service. The event details are similar to those provided in a Tokenization Event Notification (TVN) network message. An issuer may use these details to trigger communication to the cardholder to assist their successful completion of the activation process.

**NOTE: The Notify Token Updated API message does not communicate unsuccessful Activation Code entry attempts (during Cardholder Authentication). If the issuer is validating its own Activation Codes, it communicates unsuccessful attempts to MDES in the Validate Activation Code API response message.**

For information on the Notify Token Updated API message and its parameters, refer to the MDES Pre-Digitization API documentation on the Mastercard Developers site.

## Cardholder-Initiated Token Deactivation for Apple Pay

There is a special case for the Apple Pay wallet program regarding cardholder token deletion.

**NOTE: When a cardholder deletes their card from the Apple Pay wallet program, Token Event Notification (TVN) network messages and Notify Token Updated API messages (indicating token deactivation) are not sent to the issuer, and the MDES token to Account PAN mapping remains active so that future merchant-initiated transactions will be processed as normal.**

**Token deactivations initiated by other parties or for any other wallet program will result in the deactivation message being sent to the issuer and the token being deactivated, so no further transactions can be processed.**

## Halting Digitization

---

Issuers can halt all digitization quickly until further notice.

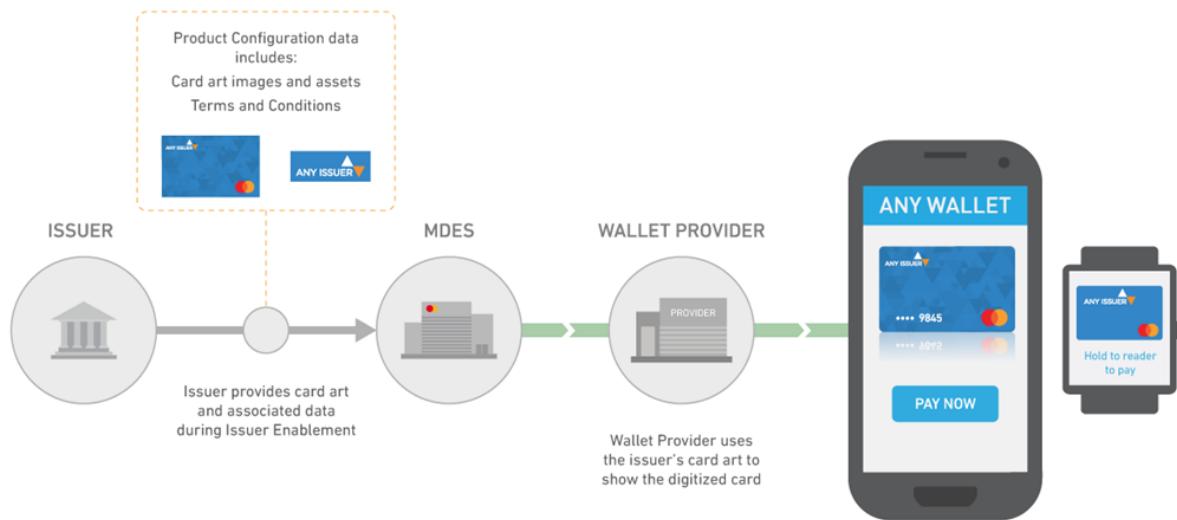
To do this, an issuer can either:

- Decline all Account Status Inquiry (ASI), Tokenization Authorization Request (TAR), or Authorize Service pre-digitization messages
- Remove any Rule Sets present from the account ranges for which they wish to halt digitization, and amend the default eligibility decision for these account ranges to 'Decline'

Performing either of these actions ensures that digitization is halted immediately (this may take up to a day). An issuer can also indicate if the date needs to be in the future for this purpose.

## Card Art Support and Associated Data

Wallet Providers are expected to provide a rich visual experience in their wallet application or user interface, by displaying issuer-provided card art, card text, and service Terms and Conditions for the cardholder's digitized card. Depending on the Mastercard digital brand guidelines, the card art may be related to the physical card or an issuer's digital brand.



Issuers provide the card art and associated data when enabling and maintaining their card ranges in MDES. Examples of associated data include:

- Terms and Conditions
- Issuer's contact information, such as a phone number for their call center
- Technical data, such as a link to the issuer's mobile banking app

**NOTE: Cardholders might not be present during merchant or commerce platform tokenization, so those MDES program participants do not provide issuer Terms and Conditions to their cardholders during digitization.**

Images and associated data are stored and managed in the Card Image Repository (CIR).

MDES supports multiple Wallet Providers and each may represent digitized cards in different ways—some may use images representing physical cards, others may break with traditional form factors and present cards in a more abstract way. To facilitate this, issuers should consider the following:

- Issuers may provide either:
  - A single combined card background image, which already includes the issuer logo, Mastercard brand logo, and so on
  - Separate image assets for the different card components, which allows Wallet Providers greater flexibility for card layout

**NOTE: For information about these different options, see Card Art Image Assets.**

- Individual assets (image and text) may be assigned to one or more Product Configurations.
- Product Configurations can be assigned to one or more card product ranges.
- A given Product Configuration can be assigned to an Account Range as the default to use during digitizations in that Account Range.
- Issuers may override the default Product Configuration for individual digitizations by specifying the desired issuer Product Configuration in DE 124 of the TER or TAR response network message (if opted into network messages).

As part of the issuer enablement process, the issuer configures all Product Configuration data, including the card art required for the Wallet Provider to display on the cardholder device. For more information, refer to the Card Art and Associated Data for MDES appendix.

**NOTE: Product Configuration data is provided to the Wallet Provider when the token is provisioned. Updates to Product Configuration data after provisioning can also be pushed to the mobile device for existing tokens.**

**Related Concepts**

[Card Art and Associated Data for MDES](#)

## Chapter 5 Token Management

*This section describes token management for MDES.*

---

What is a Token?.....	150
Token Designation Service.....	151

## What is a Token?

A token is an alternative value for the primary account number (PAN) used by a payment card issuer to identify a payment card account. Tokens are issued in compliance with the *EMV Payment Tokenization Specification Technical Framework*, and they pass the basic validation rules for a PAN, including the Luhn Formula for Computing Modulus 10 Check Digit.

MDES allocates a token (from the issuer's token pool) and provisions it to the target, such as a device's SE, a cloud-based Host Card Emulation (HCE) solution, or a secure server. This token is the digital representation of the consumer account for digital transactions.

The Card on File token type enables a Token Requestor to replace cardholder PANs (and associated expiration dates) stored on file with static tokens for e-commerce transactions. For information on supporting Card on File token issuance, management and transaction processing, contact your Mastercard representative.

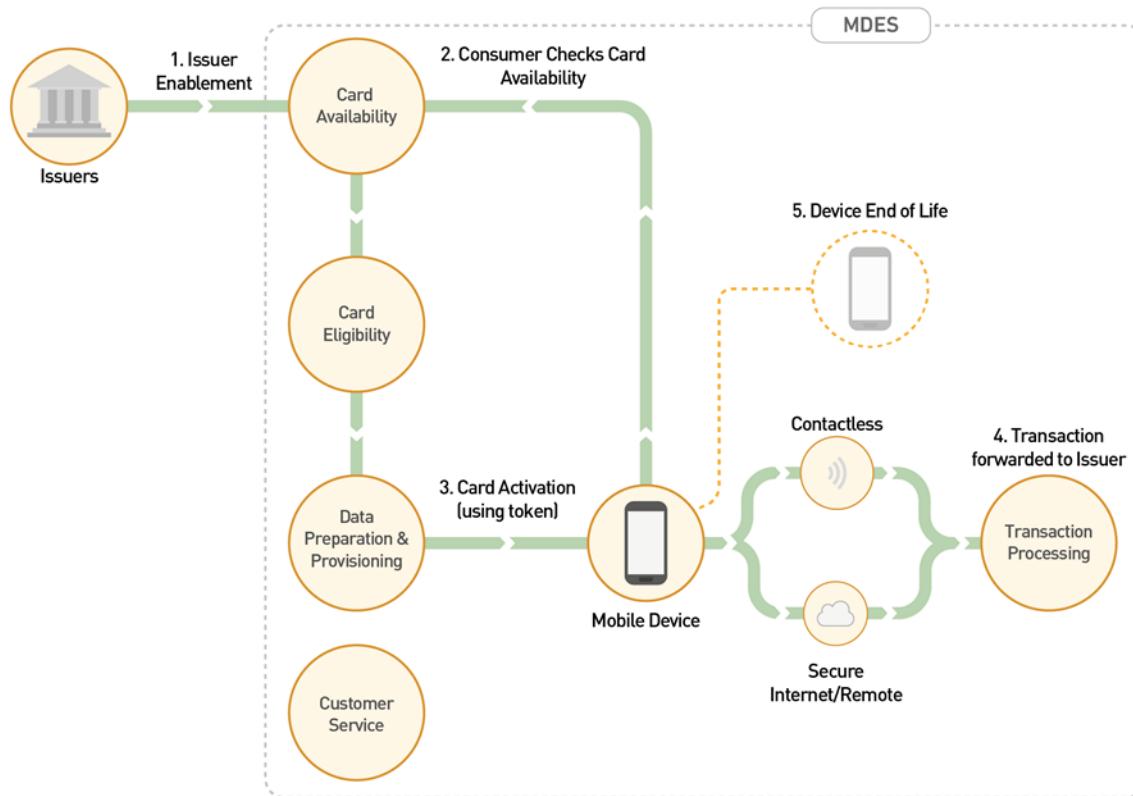
**NOTE: MDES can only allocate the Card on File token type for Mastercard consumer product and acceptance brands, and Debit Mastercard.**

During transaction processing, Mastercard validates the token and accompanying data in the following message types, and maps the token to the cardholder's Account PAN:

- Authorization Request/0100
- Authorization Advice/0120
- Financial Transaction Request/0200
- Financial Transaction Advice/0220
- Reversal Request/0400
- Reversal Advice/0420
- Acquirer Reversal Advice/0420
- Issuer Reversal Advice/0422

The transaction is then forwarded for authorization by the issuer using the Account PAN.

**Figure 19: Token Use (Illustrative)**



## Token Designation Service

The MDES Token Designation Service manages the availability and lifecycle of each token. It is a business service of the MDES platform, used during issuer enablement, through provisioning, to token recycling. Issuers do not need to enable or configure it during issuer enablement.

The service can designate the following number of tokens per Account PAN.

Token Type	Maximum Number of Active or Suspended Tokens (Token Limit)
SE and cloud-based (for digitizing to consumer devices)	Unlimited, although the number of tokens reported will have a maximum value of 99. For example, 129 active or suspended tokens will be reported as 99.
Card on File (for digitizing to servers)	99 per Token Requestor

For wallet programs other than Apple Pay, there can be one active/suspended token to PAN mapping per Account PAN for a particular wallet application instance; in other words, a card can be digitized once to a particular wallet application instance, unless that token expires or is deactivated. For Apple Pay, if a cardholder deletes their card, the MDES token to Account PAN mapping remains active so that future merchant-initiated transactions will be processed as normal; see Cardholder-Initiated Token Deactivation for Apple Pay. This means that there can be multiple active tokens for the same Account PAN (in Apple Pay), if the cardholder redigitizes their card.

When a token expires or is deactivated via MDES Customer Service Tools (Application or API), the token is recycled 540 days after the last transaction activity and made available again in the issuer's token pool.

### **Token Account Ranges**

The issuer identifies Account PAN ranges to be digitized. MDES then designates token account ranges on behalf of the issuer to the selected card account ranges. Mastercard is responsible for the designation and management of these tokens as follows:

- The token account range configuration matches the Account PAN range configurations. Attributes such as brand, product, and country of issue are the same so that transactions performed using the mobile device are processed and accounted for correctly by merchants and acquirers through authorization and clearing systems.
- A token account range does not contain any issued Account PANs. The token account range is (re)designated exclusively for use by MDES.
- Multiple token account ranges may be associated with the Account PAN range. This depends on the portfolio size for cards issued and number of tokens associated to it.

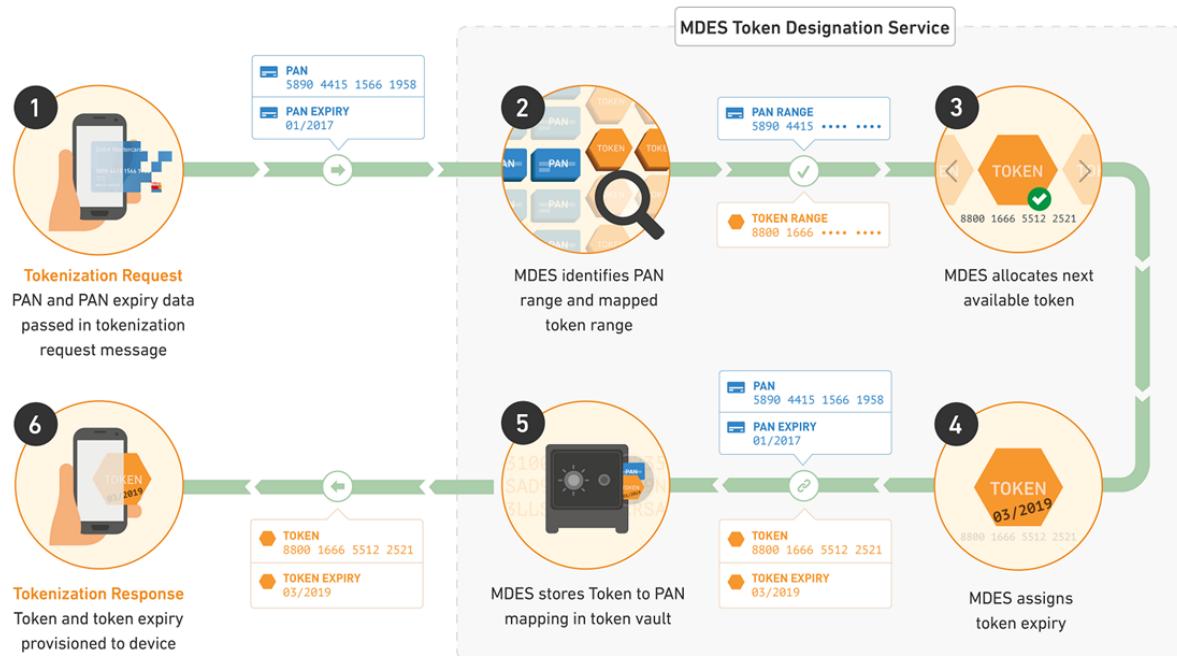
### **Token Designation**

Token account ranges are identified and designated to Account PAN ranges by MDES on behalf of the issuer during the issuer enablement process (see [Issuer Enablement](#)).

As the following diagram shows, when the tokenization of an Account PAN is requested, the next available token from the appropriate token range is designated for that digitization.

Tokens are not necessarily designated in ascending sequential order, so issuers should not rely on the latest token designated to infer how many tokens are remaining in the pool.

**Figure 20: Token Allocation for a Digitization Request**



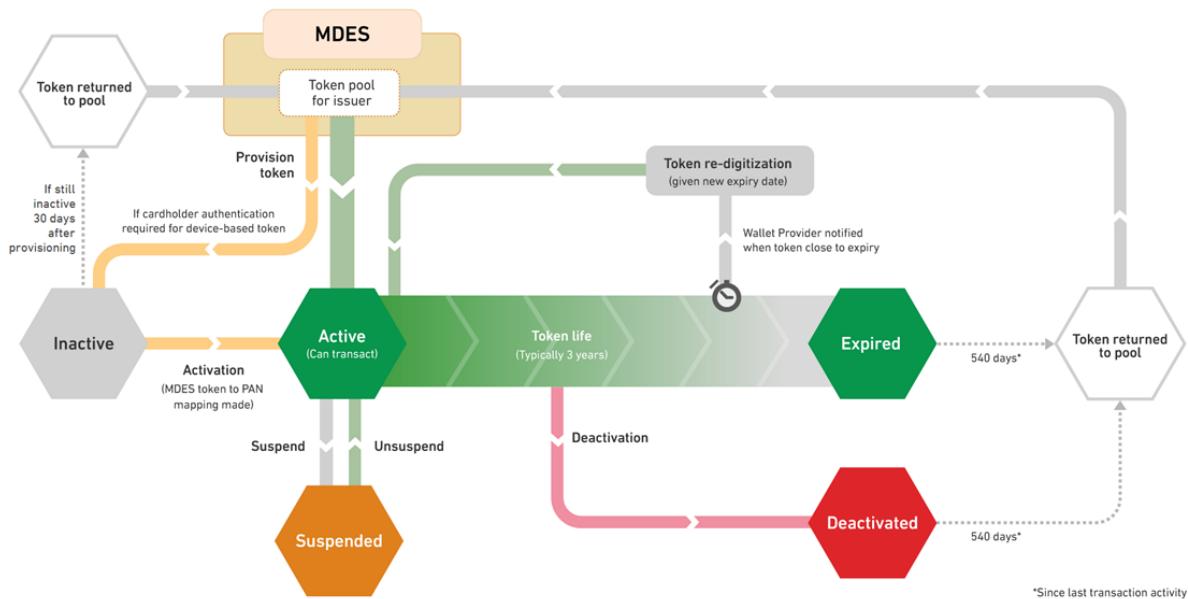
An issuer is not informed that a token is designated for a tokenization or digitization event until the token is activated within MDES. Until this point, the token is inactive and unable to perform financial transactions.

If the issuer chose to receive the Tokenization Complete Notification (TCN) network message, that message informs them of the token designation. Otherwise, they are informed on the first authorization or financial transaction request initiated with the token.

## Token Maintenance

A token has an expiration date of typically three years from the date of digitization, and can have different statuses, as shown in the following diagram. Updating the token status is possible using the Customer Service Tools or 0302 Issuer File Update network messages, where it can be 'deactivated' from the Account PAN to which it was mapped. The token is returned to the issuer's token pool and made available for tokenization again, five hundred and forty (540) days after the last transaction activity,

**Figure 21: Token Lifecycle**



**NOTE: A token can be deleted at any stage of its lifecycle.**

Tokens can be re-digitized by the Wallet Provider, see Token Re-Digitization. If they are not re-digitized, they eventually expire.

While a token is digitized on a device or server, it can be suspended independently by each party:

- Wallet Provider or Token Requestor
- Funding Account issuer
- Cardholder
- MDES, due to a systematic event triggered by the entry of an invalid Mobile PIN or failure of locally-verified CDCVM (not relevant to merchant or commerce platform tokenization)

For reversing the suspension, each party will have to resume the token. For example, if a token is suspended by the Wallet Provider and the issuer, both need to resume the token to revert to a token active status.

Special case for Apple Pay:

- If the issuer suspended the token, only the issuer can resume it.
- If the cardholder suspended the token, either the cardholder or the issuer can resume it.

**NOTE: A deactivated or expired token does not count against the active token limit. However, a suspended token does count against the token limit, because the suspension can be reversed.**

When a token is digitized to a device, the token to Account PAN mapping relationship is loaded into the MDES Mapping Service. If the Account PAN expires, the issuer can update the Mapping Service with the replacement Account PAN data using the Customer Service Tools or the Issuer File Updates network messages.

**NOTE: It is the issuer's responsibility to maintain the Account PAN expiration date in MDES. Mastercard does not validate the Account PAN expiration date retrieved from the Mapping Service prior to passing it to the issuer in an authorization or financial transaction request.**

### Inactive Tokens

When a provisioned token is awaiting activation in MDES, typically while additional cardholder authentication is being performed, the token is in an inactive state and cannot perform transactions.

If the token is not activated within 30 days of being allocated, it will be returned to the token pool and made available for tokenization again. This duration is subject to change at the discretion of Mastercard and is irrespective of the Expiration Date and Time of the Activation Code (if that Activation Method is being used).

### Token Expiration Date and Transaction Processing

The token expiration date is set to 3 years from the provisioning date. When the token expires, it is held until 540 days after the last transaction activity to ensure any clearing and exception processing activity can occur successfully. Mastercard validates the token expiration date in the transaction and if it has expired, declines the transaction.

When a token expires, it can no longer transact. For an expired device token, the issuer should advise the cardholder to delete the token from their mobile device and re-digitize their card (which allocates a new token for the Account PAN). Similarly, for an expired server-based token (for merchant or commerce platform), the server token must be deleted and the card re-digitized.

### Token Re-Digitization

When a token is within thirty days of expiring, MDES notifies the Wallet Provider so that they can request re-digitization of the token before it expires. Token re-digitization extends the life of the token, making it valid for another three years, avoiding any inconvenience to the cardholder. The re-digitized token has the same number. If multiple re-digitizations are attempted on the same token, an additional month will be added to the previous expiration date. Only a certain number of re-digitizations will be allowed within a given time period.

When a token is re-digitized successfully, MDES sends the issuer a Tokenization Event Notification (TVN) message and/or Notify Token Updated message (if the issuer chose to receive them). These request messages include the reason for the token update and the new token expiration date.

**NOTE: Expired tokens cannot be re-digitized. If a token expires naturally, it is no longer valid for making payments and the only course of action (after expiry) is to re-digitize the card (not the token), resulting in a new token with a different number.**

## Token Recycling

Token reuse or recycling is the MDES feature that returns the token to the issuer's token pool to make it available again for future provisioning to another device and mapping to a new Account PAN. Recycling tokens allows for the maximum utilization of the issuer's available tokens and minimizes the need to designate new token account ranges.

A token may be recycled for several reasons, including token expiration, token deactivation, or the failure of a digitization attempt. A token cannot be recycled for at least five hundred and forty days (excluding when digitization fails) to allow for any applicable clearing and exception processing activity.

## De-activated or Expired Tokens

Depending on the implementation, a token can be deactivated by different parties, including the Wallet Provider or Token Requestor, Funding Account issuer, or cardholder.

If the token has expired or been deactivated, using the Customer Service Tools (Application or API) or network message, no authorization transactions are possible. The token is returned to the issuer's token pool and made available for digitization again, five hundred and forty days after the last transaction activity.

**NOTE: A deactivated or expired token cannot initiate financial transactions other than refunds.**

## Managing Account PAN Updates as a Result of Lost or Stolen Mobile Devices and Cards

**NOTE: When a FPAN is replaced by another FPAN it must be from the same FPAN range so that the original token can be maintained.**

If a cardholder's mobile device is lost or stolen, the associated token remains mapped to the PAN in MDES until the issuer changes the status of the token using the Customer Service Tools or 0302 Issuer File Update network messages. Changing the token status to 'deactivated' or 'expired' allows it to be eligible for recycling as described above. In this situation, the issuer may or may not replace the Account PAN. The cardholder would then need to redigitize a new token to their replacement device. MDES does not re-provision a token from a lost/stolen device to the replacement device.

In the case of a lost physical card or a re-issued card with a different Account PAN for any other reason (for example, suspected account data compromise), an issuer **must** update the Account PAN stored in MDES using the Customer Service Tools or 0302 Issuer File Update network messages. The cardholder will not need to provision a new token, and so recycling does not apply.

A single Account PAN update can apply to all tokens or a single token. It is advised that when an Account PAN is updated due to card re-issue, all tokens are updated using one Account PAN update. MDES updates all tokens from all Wallet Providers and Token Requestors to ensure that token transactions continue without interruption and impact to cardholders. MDES advises all Wallet Providers and Token Requestors of the updated Account PAN's last 4 digits so that cardholders will recognize their new card within the user interface.

If an issuer advises Mastercard of card replacement using the Automated Billing Updater service, these card updates are reflected in MDES and further use of the Customer Service Tools or 0302 Issuer File Update network messages is not necessary.

**NOTE: In regions where participation in the Automated Billing Updater service is optional, it is mandatory that issuers provide notice of Account PAN updates due to card re-issue or replacement so that token mapping remains current and token transactions continue to process correctly. Issuers may choose to use the Customer Service Tools or 0302 Issuer File Update network messages, or participate in the Automated Billing Updater service.**

If an issuer re-issues a physical card with the same Account PAN, the token continues to operate and may perform transactions normally. There is no need to delete the token from the mobile device and re-digitize the card.

### **Managing Card on File (COF) Tokens When Cards are Lost/Stolen**

In the case of MDES for Merchants (M4M) tokens, when fraud is detected, or a card is reported lost or stolen to the issuer, the issuer should:

- Confirm that fraudulent activity exists, using their internal Business As Usual (BAU) process
- Identify the fraudulent activity associated with these tokens, using the MDES Customer Service Portal and Customer Support APIs, in the following ways:
  - The issuer's Customer Service Representative (CSR) uses the Search function within the MDES Customer Service Portal to check:
    - if any tokens are associated with that fraudulent activity
    - when those tokens were created
    - if the tokens were associated with either M4M or Device based Wallets
  - The CSR identifies and confirms with cardholders if any fraudulent tokens have been created that have not yet been used for transactions.

**NOTE: Issuers are able to use the MDES Customer Support API to automate token support processes, which greatly reduces the need for the CSR to manually search for a token status**

- Once the scope of the fraudulent activity is verified with the customer, the issuer takes action on the illegitimate tokens by using the **DELETE** function to remove the tokens in question (with associated merchants or wallets)
- After the tokens in question are deleted, the issuer updates the customer's account number and re-issues the card
- Once the customer's card number is re-issued, the Lifecycle Management (LCM) PAN mapping is applied to just those legitimate tokens that were left in an ACTIVE state, thus

preserving the customer's legitimate merchant/wallet accounts and the issuer's card preference in those experiences

### Re-issuing a Card as a Different Product

When an issuer re-issues a card and also upgrades (or downgrades) the cardholder to a different product, for example moving from a standard card product to a premium card product, the issuer may either:

- Use the Product Configuration push capabilities, offered through issuer enablement/maintenance and Customer Service Tools, to update the card
- For device tokens, advise the cardholder to delete the token from their mobile device and digitize the new card with the new Account PAN

This is to ensure that the new token product attributes match the new card and the correct fees are applied when the token performs transactions.

**NOTE: When a re-issued card is updated to include additional security features, such as contactless or Chip & PIN/Signature technology, a token in a mobile device linked to the Account PAN is unaffected by the change of card features and no token management actions are necessary. This is likely to occur throughout an EMV migration program.**

If the cardholder wants to suspend the token temporarily, such as when the device is under repair, the issuer would use the Customer Service Tools to manage the temporary suspension. For information on the Customer Service Tools and 0302 Issuer File Update network message capabilities, refer to the Operational Management chapter.

### Failed Digitization

During digitization, several processes occur simultaneously, such as pre-digitization, provisioning, and token designation. If any of these processes fail for technical, connectivity, or eligibility reasons, the digitization of the token onto the device or server also fails. In this scenario, it is not possible for the device or server to initiate a transaction, so MDES can recycle the token immediately.

### Using a Token's Designated Number Within Issuer Systems

Issuers must understand that the value designated for a specific token (the 'up to 19 digit' number) is only designated to the token *temporarily*, even though it may be for a period exceeding four-and-a-half years. When a token is recycled, 540 or more days following deactivation or expiration, the number is available for re-designation by Mastercard. Issuers should ensure their systems:

- Do not use this value as an identifier of a specific token that would be permanently linked to a PAN
- Can handle the same number being associated with more than one Account PAN over time

MDES does *not* advise an issuer when the token's number is released for recycling unless the issuer receives a TCN network message. Therefore, issuers should expect to receive

transactions for a PAN that contains a token previously associated with a different PAN. This would be an indication that the number has been recycled and re-designated to a different Account PAN, during a subsequent digitization.

## Chapter 6 Payment Account Reference (PAR)

*This section describes the Payment Account Reference (PAR) support in MDEN.*

---

What is PAR?.....	161
When Mastercard is the BIN Controller.....	161
When Mastercard is Not the BIN Controller.....	164

## What is PAR?

Payment tokenization brings several benefits to the payment industry while, at the same time, it creates new challenges for entities that rely on a PAN to drive payment processing and value-added services. EMVCo's Payment Account Reference (PAR) provides an industry-aligned solution.

With payment tokenization, a cardholder PAN is replaced with a unique value (a token) that looks and functions like a PAN but is not the cardholder's actual PAN. Because each payment token is issued for a unique environment, device or Token Requestor, the cardholder may be issued many payment tokens representing a single PAN. This means that a merchant, acquirer and the payment networks can receive transactions using different payment tokens for the same underlying PAN, but the merchant or acquirer has no way to link those token transactions.

PAR provides an industry-aligned approach designed to help link PAN-based transactions to transactions using associated payment tokens, without using the PAN as the linkage mechanism. A PAR is a unique non-financial reference assigned to each unique PAN.

BIN Controllers determine the rules for use of the Issuer Identification Numbers (IINs, commonly referred to as BINs) under their control. A BIN Controller is either:

- An ISO-recognized blockholder with allocated BINs
- An ISO-recognized card issuer with allocated BINs

Mastercard is an ISO-recognized blockholder that sublicenses or otherwise assigns allocated BINs for use by card issuers. Mastercard is a *Registered BIN Controller* with EMVCo and, as such, determines the governance of the PAR Field and PAR Data for all the BINs under its jurisdiction, including assignment and lifecycle management.

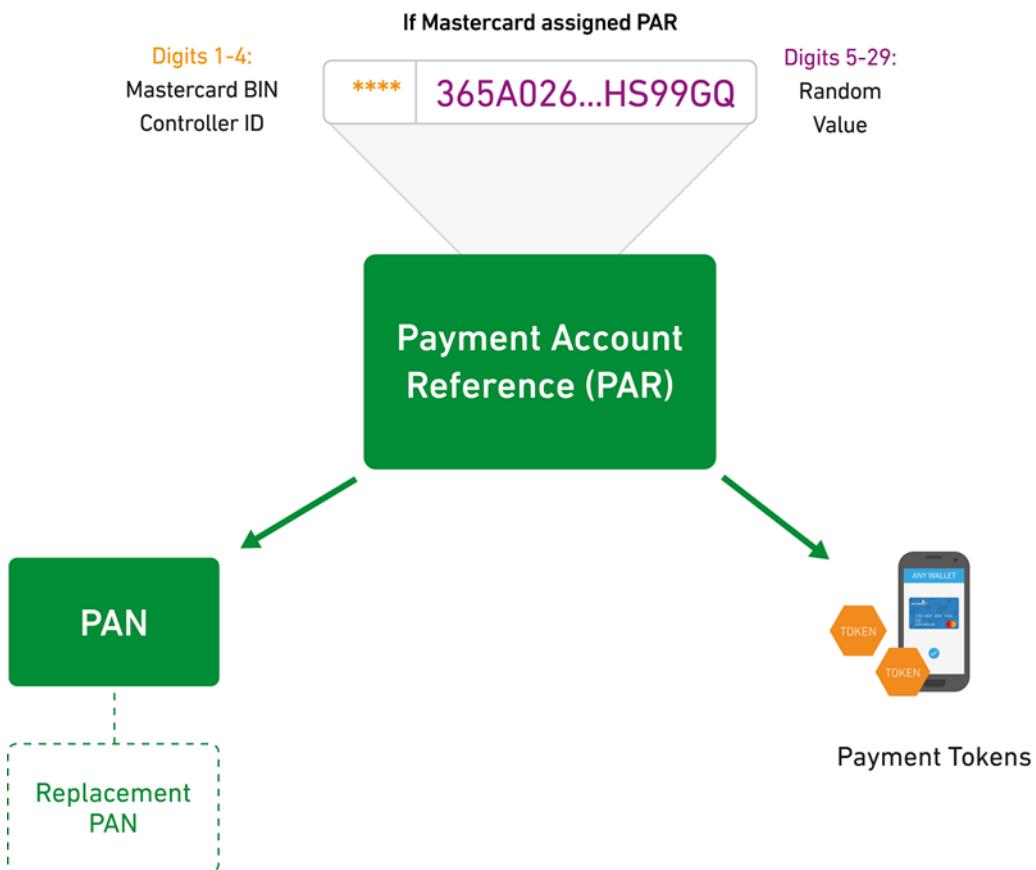
Mastercard has registered with EMVCo for supporting PAR as a linkage mechanism and has been granted the BIN Controller Identifier '5001'.

## When Mastercard is the BIN Controller

When Mastercard is the BIN Controller, MDES will generate PAR values for tokenized Account PANs and maintain the PAR to PAN mappings within the Mastercard PAR Vault.

Mastercard generates a PAR as a 29-character value, where:

- The first 4 characters represent the BIN Controller Identifier that is assigned to Mastercard by EMVCo, which is '5001'
- The last 25 characters represent a Globally Unique Identifier, which is an alphanumeric string with all uppercase characters



As part of the initial PAR assignment phase, Mastercard will create and map PARs to all the PAR-eligible PANs that have at least one MDES token in active or suspended status. The PAR to PAN mappings will be maintained within the Mastercard PAR Vault.

After the PAR ecosystem initialization, each *first* request to MDES for a card digitization or tokenization (by a Token Requestor) generates a PAR for the card PAN and records the associated PAR to PAN mapping in the PAR Vault. All subsequent digitization or tokenization requests for the *same* card retrieve the PAR from the existing PAR to PAN mapping in the PAR Vault.

The PAR corresponding to a digitized PAN will be used in:

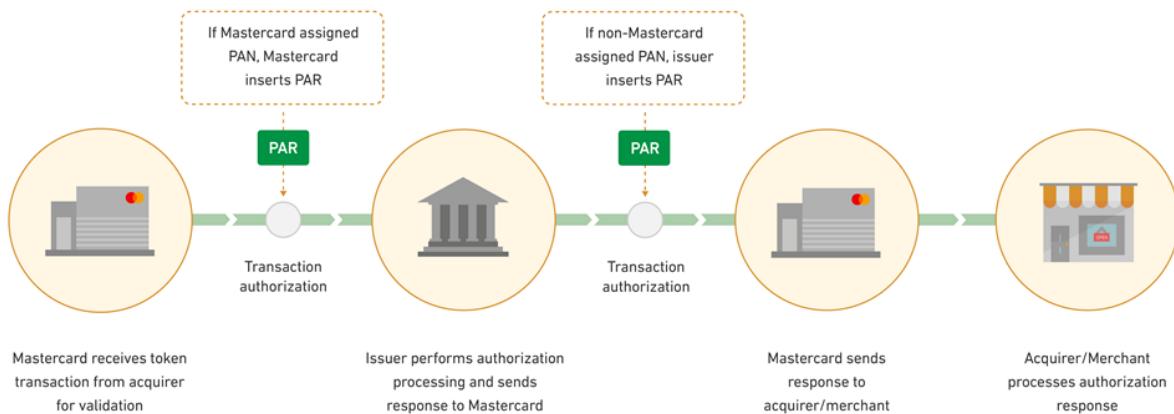
- Pre-digitization network messages and APIs
- Transaction-related network messages

After the PAR is generated or retrieved from the PAR Vault, the PAR value is provided to the issuer for its convenience (for example, for use in card personalization):

- The PAR is included in the following pre-digitization messages (depending on the message profile chosen by the issuer for that account range during issuer enablement):
  - In DE 56 of the Tokenization Complete Notification (TCN) network message

- In DE 56 of the Administrative Advice/0620—Issuer Token Notification Advice, with DE 60 = 0251, for Tokenization Complete Notification
- In the CardAndTokenInfo encrypted data structure (with the Issuer Encryption Public Key) in the NotifyServiceActivated API request  
The CardAndTokenData data structure includes a paymentAccountReference field, which allows the transfer of the PAR parameter to the issuer when Mastercard is the BIN Controller.
- When a transaction request is initiated by an acquirer with a token or PAN for which the PAR is in the PAR Vault (whether with an Authorization Request/0100 message on the Dual Message System or with a Financial Transaction Request/0200 on the Single Message System), MDES will retrieve the corresponding PAR from the PAR Vault. MDES will include the PAR value in the transaction message (Authorization Request/0100 or Financial Transaction Request/0200) it creates for the issuer.

**Figure 22: PAR Value Inserted into the Transaction Authorization Message**



MDES issuers can already send PAN swap requests through the Customer Service Application or Customer Service API (Token Management function) to update the token to PAN mapping in the Token Vault. In addition, MDES might generate a separate request to the PAR Vault as follows:

- When there is at least one mapped token with the old PAN in active or suspended status, there will be a separate request to update the PAR to PAN relationship after successful update of at least one token to PAN mapping.
- When all the tokens mapped to the old PAN are in deactivated status, there will be a separate request to update the PAR to PAN relationship.
- When there are no tokens mapped to the old PAN, there will be no separate requests to update the PAR to PAN relationship.

The PAR to PAN relationship will be updated when:

- Issuers participating in MDES initiate a token to PAN mapping update by using Issuer File Update Request/0302 – Maintenance (Token/PAN Update MCC106) or R311 Bulk File Update

- Issuers submit PAN updates using the Automatic Billing Updater (ABU) or Payment Account Management API

Issuers can use the Payment Account Management API to retrieve PAR values for PANs and tokens related to their accounts. The API is accessed through the Mastercard Developers site (<https://developer.mastercard.com>).

## When Mastercard is Not the BIN Controller

---

When Mastercard is not the BIN Controller, Mastercard does not assign or generate PAR values. The issuer or third-party entity assigns the PAR value.

After the PAR is generated by the issuer or retrieved from their PAR Vault, the PAR value is provided to MDES for token personalization in pre-digitization network messages and API messages (depending on the message profile chosen by the issuer for that account range during issuer enablement):

- In DE 56 of the Tokenization Authorization Request (TAR) response network message
- In DE 56 of the Account Status Inquiry (ASI) response
- In the paymentAccountReference field of the AuthorizeServiceResponseData object, which is encrypted with Mastercard Encryption Public Key and included in the encryptedPayload returned in the Authorize Service API response, when Mastercard is not the BIN Controller

When a transaction request is initiated by an acquirer with a token or PAN for which the PAR is not in the Mastercard PAR Vault but is kept by the issuer in their PAR Vault, issuers must prepare to send DE 56 with the PAR value in the transaction response message, as shown in the 'PAR Value Inserted into the Transaction Authorization Message' diagram (in the When Mastercard is the BIN Controller section). Mastercard will relay that PAR to the acquirer.

## Chapter 7 Provisioning

*This section describes the provisioning process for MDES.*

---

What is the Provisioning Service?.....	166
Mastercard Provisioning Service Security for Secure Elements.....	167

## What is the Provisioning Service?

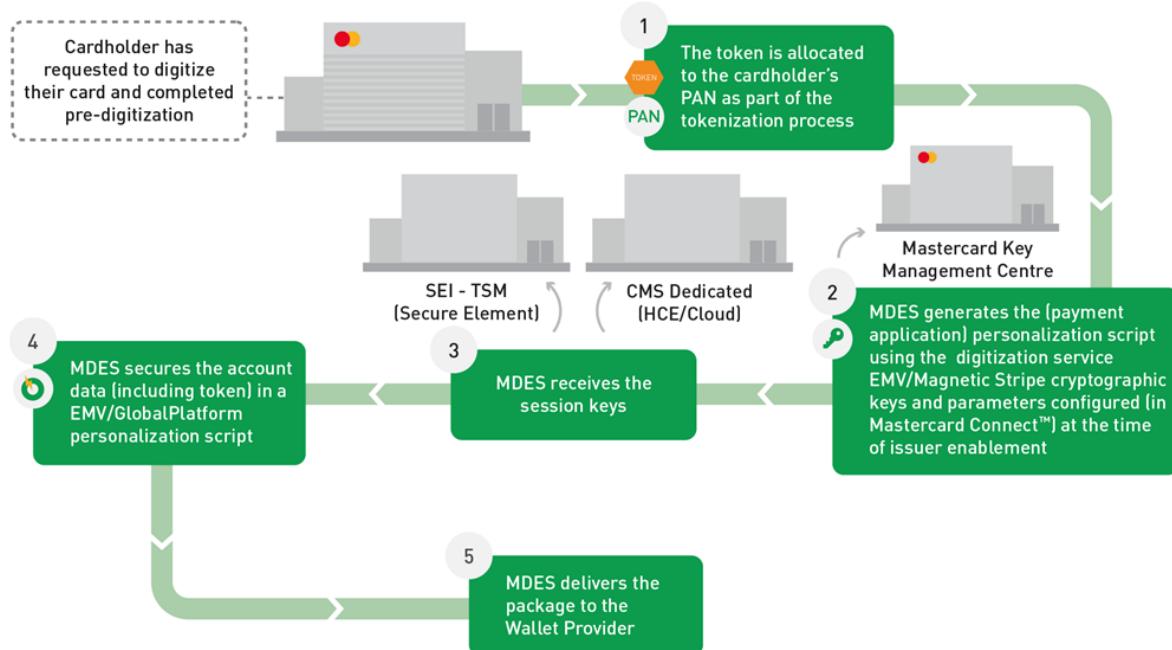
The provisioning service activates secure payments on cardholder mobile devices or Wallet Provider (Token Requestor) servers initially by personalizing the device or server with account data and a token Over the Air (OTA).

For example, device provisioning includes the following:

- Personalized Data Preparation—MDES performs aggregation of the personalization data required to enable tokens. Data preparation is performed in line with the requirements of M/Chip Mobile specifications. This includes (EMV) key generation, which is necessary for transaction validation.
- Script Generation—MDES encapsulates personalization data inside GlobalPlatform scripts for secure distribution. For devices with a Secure Element (SE), GlobalPlatform scripts are prepared using confidential keys to satisfy the secure access conditions.
- Package Distribution—MDES prepares and delivers a package to perform digitization. This is provided by MDES to the Secure Element Issuer Trusted Service Manager (SEI TSM), Credentials Management System (CMS) Dedicated or Wallet Provider for further transmission to the device.

### The Provisioning Flow for Devices (Illustrative)

When a cardholder's mobile device has been through pre-digitization (refer to the Pre-digitization chapter) the mobile device can be provisioned.



## **Mastercard Provisioning Service Security for Secure Elements**

MDES has adopted the GlobalPlatform (GP) framework, as this is the main card management environment used in the mobile industry for provisioning Universal Integrated Circuit Cards (UICC) and Secure Elements (SEs).

To ensure that only appropriate parties can access applications inside the SE, the GP framework provides control mechanisms that restrict access only to authorized parties. Access rights are controlled by the Secure Element Issuer (SEI), which can grant or withdraw restricted SE access to Service Providers (in this case, Mastercard).

MDES then enables different application providers to install applications in the same SE and manage those applications independently of each other, in full isolation. MDES provides secure remote communication using GP secure channel protocols to protect the remote transmission of sensitive data (token and cryptographic information) to and from the SE. This protects end-to-end security using SE keys. The SE keys are also used to set up a secure channel between MDES and the SE known only to MDES. During provisioning, MDES establishes a secure channel with the SE to securely transmit the token information.

## Chapter 8 Wallet Providers and Token Requestors

*This section describes Wallet Providers, Token Requestors, their unique identifiers (IDs), and their interactions with MDES.*

---

What is a Token Requestor?.....	169
Token Requestor Functions.....	169
Token Requestor ID and Wallet ID.....	171
Token Requestor Models.....	172

## What is a Token Requestor?

Token Requestors integrate with MDES to request tokens for Mastercard payment cards, which can then be used for digital payments (token transactions) instead of Account PANs.

Example Token Requestors:

- **Issuers** and **Wallet Providers**, who provide wallet applications for cardholders to digitize cards into smart devices, which might be manufactured by them or partner OEMs
- **MERCHANTS**, who digitize the consumer Account PANs stored on their servers (typically without cardholder interaction)

For more information, refer to MDES Participants and Interactions. For example implementations, see Token Requestor Models.

The Token Requestor manages and communicates how tokens are made available to the issuer's cardholders. This process can differ for each Token Requestor, but each must support a number of integration messages with MDES to ensure that cardholders' cards are eligible for digitization and (where relevant) that target devices can be digitized to.

Depending on the implementation, the Wallet Provider or Token Requestor is responsible for the following:

- Managing the cardholder's digital wallet—Providing the digital wallet application to the cardholder with available functions for digitization.
- Token lifecycle management functions—Depends on features made available to the cardholder in the wallet application or user interface, and relates to token management options such as status changes (for example, lost or stolen).
- Along with Mastercard, managing the pre-digitization and digitization process—Different Token Requestors have a variety of risk management methods and rating information to be used during the pre-digitization process.
- Development of a Token Implementation Plan and the Terms and Conditions under which issuers may participate in the Token Implementation.

## Token Requestor Functions

---

This section describes digitization and token management functions for Wallet Providers and Token Requestors.

### Digitization

Depending on the implementation, the Wallet Provider or Token Requestor interacts with MDES to perform several checks supporting pre-digitization:

- **Card availability check**—The Token Requestor checks MDES to see if the cardholder's Primary Account Number (PAN) is within a range that is available for digitization.

- **Device compatibility check**—The Token Requestor checks MDES to see if the device is compatible with digitization. This check is not relevant to merchant or commerce platform tokenization.
- **Pre-digitization eligibility check, including optional Cardholder Authentication**—  
The Token Requestor passes the card's Card Validation Code (CVC 2, when available), address (when available), and other data to MDES to check if the specific Account PAN is eligible and approved (by the issuer) for digitization.  
The Wallet Provider-supplied account data can include additional information (where available) about the card or cardholder, to support the digitization request. The issuer may use this information to determine the eligibility decision, refer to Eligibility Rules.

For wallet implementations, the Wallet Provider is also responsible for confirming acceptance of issuer Terms and Conditions and for displaying Issuer Service brand art, the equivalent of the card art, to the cardholder. The cardholder must accept the issuer's Terms and Conditions through the wallet or user interface before digitization can be performed.

**NOTE: Cardholders might not be present during merchant or commerce platform tokenization, so those MDES program participants do not provide issuer Terms and Conditions to their cardholders during digitization.**

## Token Management

The Token Requestor might provide a platform or functionality that enables cardholders to manage the lifecycle of their token. MDES separately provides issuers with an API and Customer Service Tools that enable issuers to manage the lifecycle of their tokens. Depending on the implementation, available functions may include:

- **Suspend a token**—Performed by the cardholder through the wallet or user interface or by contacting the Token Requestor's or issuer's Customer Services.
- **Resume a token**—Performed by the cardholder or the issuer, depending on who suspended the token. The party that suspends the token can resume it.
- **Delete a token**—Enables a cardholder to delete the token from their mobile device in two ways:
  - Contacting the issuer, who then uses the Customer Service Tools to make the change.
  - Using their wallet or user interface to request the deletion, and the request is received via the Token Requestor. When the Token Requestor deletes a token from the wallet, the token remains active and merchant-initiated transactions may continue to be processed.

## Token Requestor ID and Wallet ID

Token Requestor IDs (TRIDs) and Wallet IDs (WIDs) are included in some of the MDES messages to identify the distinct entities requesting or using a token.

MDES can be used by many types of Wallet Providers and Token Requestors for different implementations. The implementation model determines which entities are assigned the TRID and WID, see the Token Requestor Models section.

ID	Length	Description
TRID	11 digits	<p>This ID uniquely identifies a Token Requestor (and Token Domain) that is directly integrated with MDES and using it for tokenization, such as a Wallet Provider, merchant, or issuer.</p> <p>When the Token Requestor is a Wallet Provider with OEMs, this ID also indicates whether the target device has Consumer Device Cardholder Verification Method (CDCVM) capabilities. See the Token Requestor Models section.</p> <p>The ID is assigned by the Token Service Provider (TSP). The first three digits identify the TSP; the MDES TSP code is <b>501</b>.</p>
WID	3 digits	<p>For many implementations, this ID typically identifies a program or service, such as:</p> <ul style="list-style-type: none"><li>• A Wallet Provider's or issuer's wallet program</li><li>• The MDES for merchants program (which has the WID <b>327</b>)</li><li>• A commerce platform</li></ul> <p>The ID is assigned by Mastercard Franchise Development.</p>

The IDs are included in these messages: TER, TAR, ACN, TCN, TVN, Authorize Service, Request Activation Methods, Notify Service Activated. The WID is also in Deliver Activation Code messages.

The IDs are used across all token types, and provide visibility to issuer systems for their risk management and customer service processes. For example, the IDs in a TER message identify the party requesting tokenization (TRID) and typically the program or service that will use the token (WID).

The WID is included in the transaction data that is sent to the issuer for token transactions. The WID can also be used to identify non-tokenized wallet transactions.

**NOTE: Issuers participating in the MDES for merchants program (WID 327) are automatically integrated with all merchants using that program, so issuers will see new TRIDs as merchants join the program (Mastercard will assign the TRIDs without prior notice). Issuer systems must allow new TRID values to be accepted during (but not necessarily limited to) pre-digitization and transaction processing. This will avoid digitization requests and payments being declined only on the basis of a new TRID.**

For further information on these IDs, contact your Mastercard representative.

## Token Requestor Models

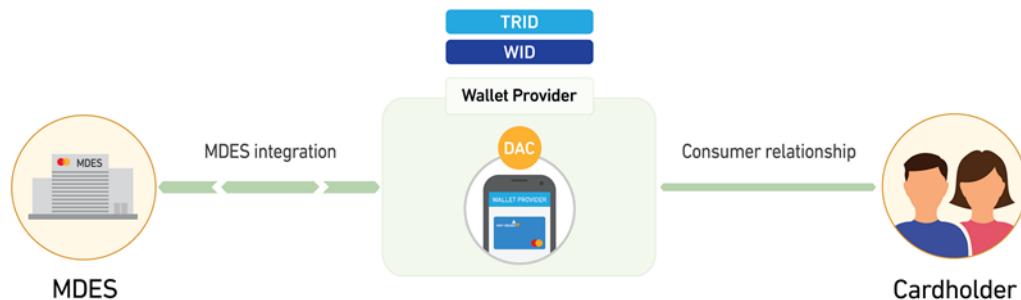
The Token Requestor implementation model determines which entities are assigned the TRID and WID. This section shows some example implementation models.

### Device Wallet

As shown below, when a Wallet Provider integrates with MDES directly to digitize cards for its device wallets:

- TRID = Wallet Provider (the Mastercard Digital Activity Customer, DAC)
- WID = Wallet Provider's wallet program

The IDs enable an issuer to identify the Wallet Provider and its wallet program.



### Wallet Provider with OEMs

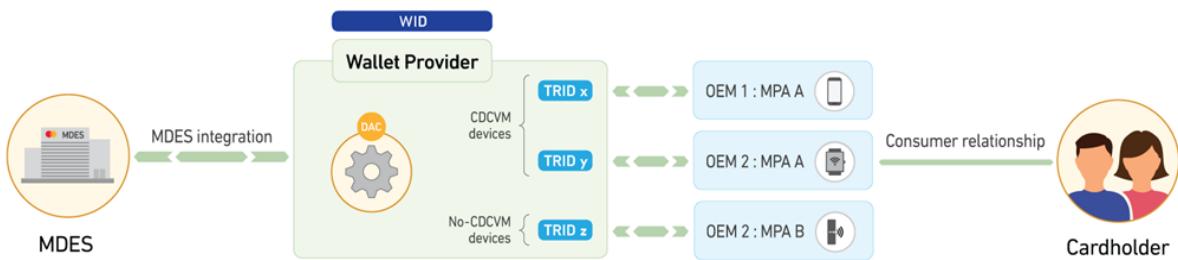
As shown below, when a device manufacturer (OEM) connects to MDES via a Wallet Provider to get payment tokens for its devices:

- WID = Wallet Provider (DAC)
- TRID = Device manufacturer (OEM). An OEM integrated by a Wallet Provider may be assigned one or two TRIDs; the usage of one or the other TRID value indicates whether the target device has Consumer Device Cardholder Verification Method (CDCVM) capabilities:
  - CDCVM—There is one TRID for OEM devices that have CDCVM capabilities, which allow users to verify their identities (such as PIN entry or biometric authentication).
  - No CDCVM—There is one TRID for OEM devices that do not have CDCVM capabilities.

A TRID is associated to a unique Wallet Provider (WID). An OEM integrated to MDES through multiple MDES Wallet Providers will receive different TRIDs for each Wallet Provider.

**NOTE: This two-TRID solution is a temporary arrangement until CDCVM-related data is passed in transaction messages. At that point, there might be a single TRID for each OEM.**

The WID enables an issuer to identify the Wallet Provider requesting tokens (for its OEMs), and the TRID can help the issuer determine whether cardholder authentication can be used at a target device (where a token will be used).

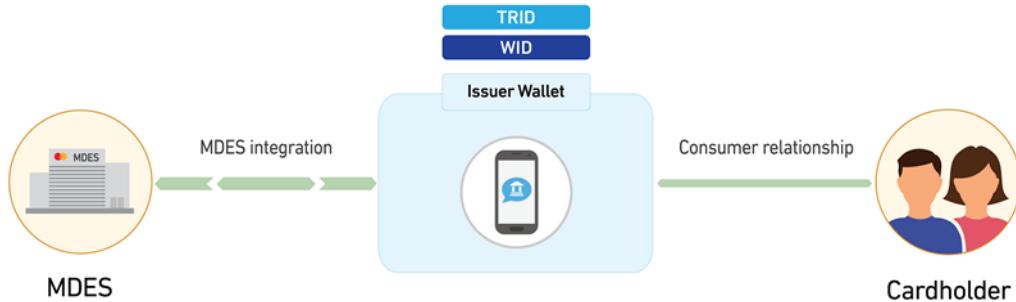


### Issuer Wallet

As shown below, when an issuer integrates with MDES directly to digitize cards for its wallets:

- TRID = Issuer
- WID = Issuer's wallet program

The IDs enable an issuer to identify requests from its wallet program.

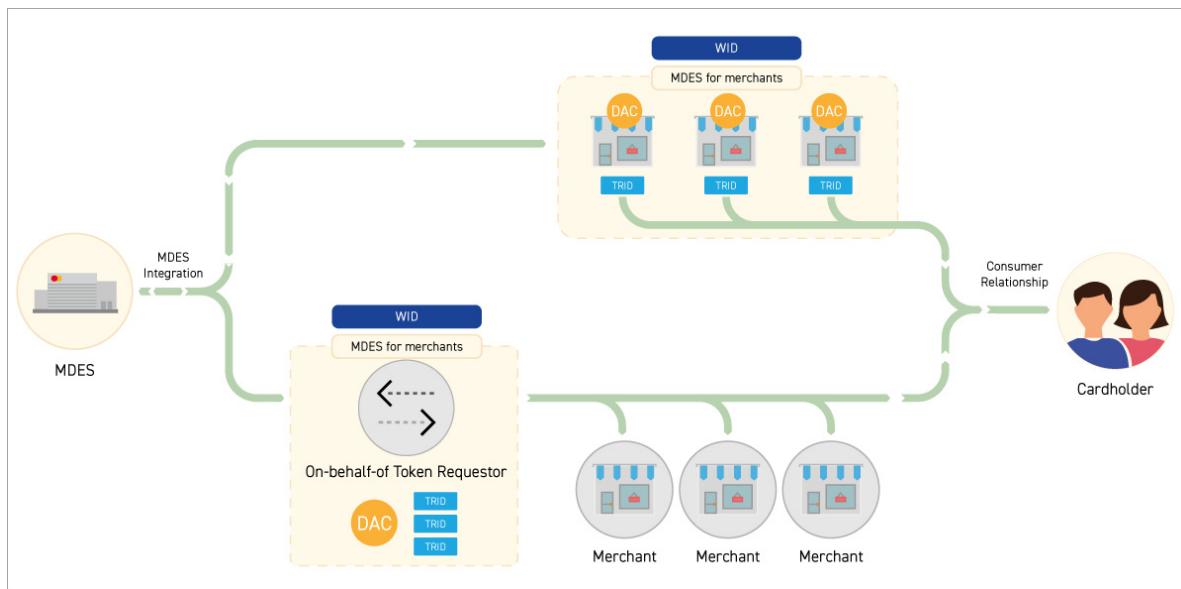


### MDES for Merchants

As shown below, when a merchant integrates directly with MDES or via an On-Behalf-of Token Requestor (OBOTR), to digitize their consumers' Account PANs stored on either entity's servers:

- TRID = Merchant
- WID = **327** (fixed value), which identifies the merchant tokenization program

The TRID enables an issuer to identify the merchant, and the WID enables issuer systems to track digitization requests and transactions relating to merchant tokenization.

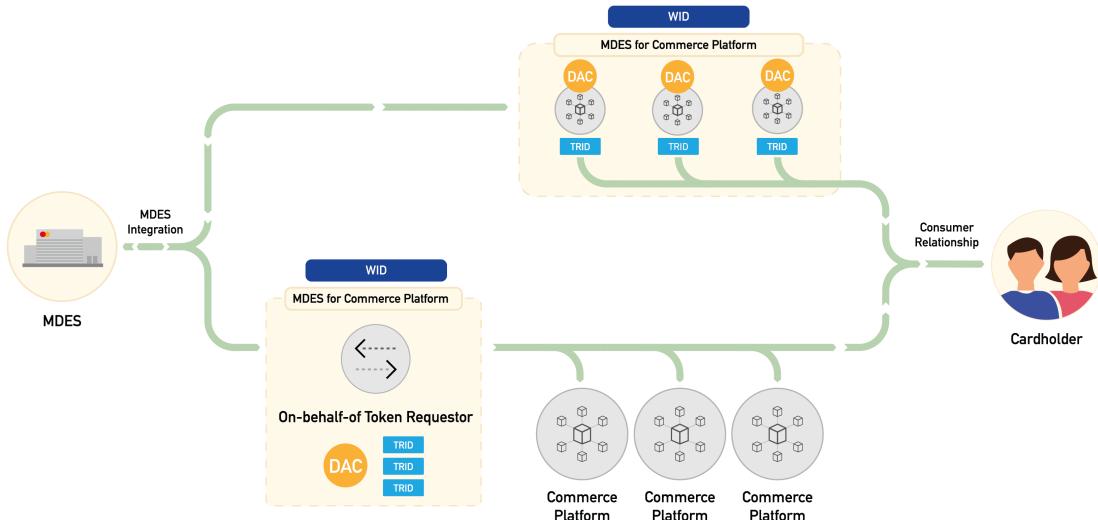


### MDES for Commerce Platforms

As shown below, when a commerce platform integrates with MDES directly to digitize its users' Account PANs:

- TRID = Commerce platform
- WID = **327** (fixed value), which identifies the merchant tokenization program

The IDs enable an issuer to identify the commerce platform.

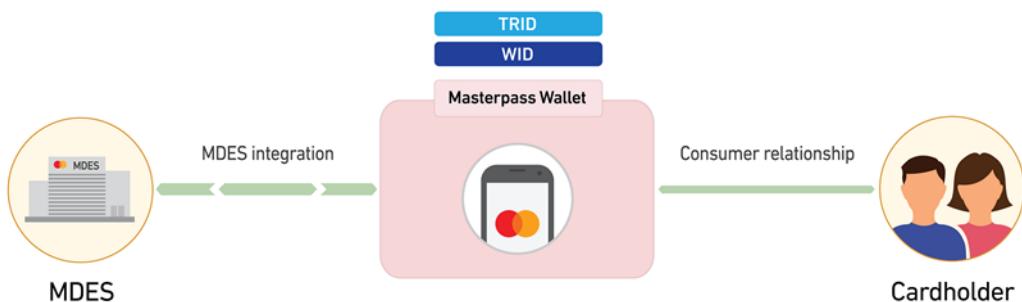


## Masterpass by Mastercard

As shown below, when the wallet program is Masterpass by Mastercard:

- TRID = Masterpass
- WID = Masterpass

The IDs enable an issuer to identify the Masterpass program.

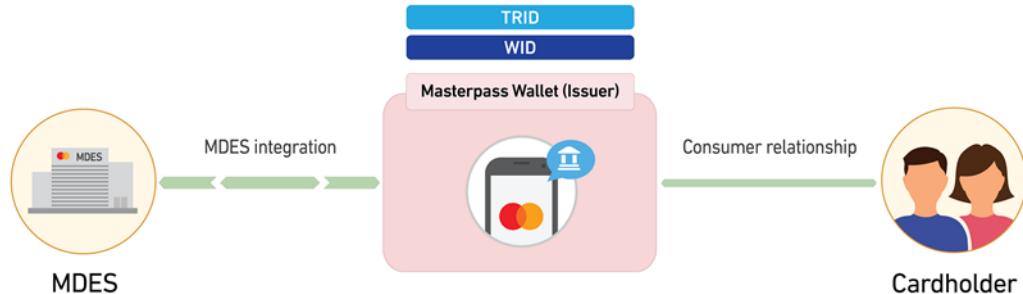


## Masterpass Issuer Wallet

As shown below, when an issuer uses Masterpass Software Development Kits (SDKs) and functionality to build its wallet program:

- TRID = Issuer
- WID = Issuer's wallet program

The IDs enable an issuer to identify requests from its Masterpass wallet program.



---

## Chapter 9 Mastercard Cloud-Based Payments (MCBP)

*This section describes the Mastercard Cloud-Based Payments (MCBP) support in MDES.*

---

User Experiences Supported by MCBP.....	178
Wallet Configurations Supported by MDES.....	185
Warning about MDES Security Controls for MCBP 2.0.....	187

## What is MCBP?

Mastercard Cloud-Based Payments (MCBP) enables a card to be digitized into a wallet application on a mobile device and used for payment without the need for a Secure Element (SE) or a Trusted Execution Environment (TEE) to protect the card's sensitive assets, such as the keys needed for calculating the Application Cryptogram.

To achieve this, the Master Keys for the digitized card are kept securely on remote servers, hence the term 'cloud-based payment,' and a limited number of keys (where each key can only be used to perform a single transaction) are downloaded to the wallet application on an as-needed basis. These keys are stored in an encrypted format. After a key has been used to perform a transaction, the key is erased and when the number of available keys in the wallet application goes below a predefined threshold, additional keys are downloaded to enable the wallet application to continue to perform transactions.

MCBP is designed to support ATM, in-store and e-commerce transactions:

- ATM transactions between an ATM terminal and an MCBP-enabled wallet application can be contactless magnetic stripe or contactless EMV transactions.
- In-store transactions between a merchant contactless terminal and an MCBP-enabled wallet application can be contactless magnetic stripe or contactless EMV transactions.
- E-commerce transactions between a remote merchant system and an MCBP-enabled wallet application can be Digital Secure Remote Payment (DSRP) transactions.

An MCBP wallet implementation may support contactless transactions, DSRP transactions, or both. For contactless implementations, contactless EMV transactions must always be supported, but support for contactless magnetic stripe transactions depends on the payment brand.

## User Experiences Supported by MCBP

---

MCBP supports various user experiences when performing contactless and DSRP transactions.

### Cardholder Verification Method (CVM) Basic Concepts

As part of the user experience, there is a need to deliver a form of Cardholder Verification Method (CVM) in addition to the implicit or explicit consent of the cardholder to perform the transaction:

- **Consumer Device Cardholder Verification Method (CDCVM)**—Aims to deliver a form of CVM where the cardholder will use their mobile device to support the authentication process. The CDCVM can be delivered using:
  - A Mobile PIN that is validated online by MDES during the authorization process
  - CDCVMs validated by the cardholder's mobile device, for example device PIN, pattern, password or biometric methods (such as fingerprint, iris or facial recognition)These methods (also known as locally-verified CDCVM) are commonly associated with a device unlock process and are validated on the cardholder's mobile device. The payment component embedded in the wallet will use the outcome of this authentication process.

The Wallet Provider determines the support and choice of CDCVM when configuring its mobile wallet application.

Mobile PIN and locally-verified CDCVM are mutually exclusive. The Wallet Provider must select one method when CDCVM is supported for a given mobile wallet application. It is not allowed to enable Mobile PIN for one use case (such as Contactless or DSRP) and locally-verified CDCVM for the other use case; the same method must be used for both use cases when supported by the mobile wallet application.

- **CVM**—Aims to deliver a form of CVM at the payment terminal (POS device) or ATM terminal. The issuer determines the configuration of the CVM options using the CVM List.

**NOTE: Online Pin ATM has been added as the first option in all CVM lists (MCBP and non-MCBP) to ensure an optimal experience at the contactless ATM terminals.**

**NOTE: 'No CVM required' is considered as a valid CVM in some configurations and use cases, such as low-value transactions (LVTs). When this CVM is selected for a contactless transaction, the POS device does not require any cardholder authentication to proceed.**

### User Experiences for Contactless Transactions

For contactless transactions, a wallet may use one of the following user experiences (also known as CVM models).

User Experience	Description
Card-Like	<p>Requires cardholder authentication similar to that used for traditional plastic card contactless transactions. The CVM will be performed on the contactless terminal (POS device).</p> <p>When using a Card-Like user experience, a POS device that supports CDCVM cannot delegate the cardholder authentication to the mobile device when authentication is required for high-value transactions (HVTs). Similarly, a POS device that supports CDCVM cannot leverage any CDCVM that could have been performed on the cardholder's mobile device when the Card-Like user experience is enabled (that is, no support of CDCVM is exposed in the information contained in the card profile of the token used to transact).</p> <p>Transaction notes:</p> <ul style="list-style-type: none"><li>• For transit transactions, the cardholder's wallet and the transit gate are not expected to request cardholder authentication.</li><li>• For low-value transaction (LVTs), the POS device will not perform any cardholder validation. However, the Card-Like user experience can be enabled with or without Lost &amp; Stolen support for LVTs.</li></ul> <p>The Lost &amp; Stolen feature uses counters stored in the cardholder's wallet to control the number of LVTs allowed before requiring cardholder authentication. This limits fraud risk if the cardholder's mobile device is lost or stolen.</p> <p>When a wallet supports the Lost &amp; Stolen option with a Card-Like user experience, the authentication is expected to use a CVM that can be validated on the mobile device (CDCVM), and Mobile PIN is not eligible for this process.</p> <ul style="list-style-type: none"><li>• For HVTs, the POS device (not the cardholder's wallet) must perform cardholder authentication when required, using Online PIN ATM, Online PIN POS, Signature, (No CVM Required), depending on the configuration of the CVM List of the selected application and the capabilities of the POS device.</li></ul>

User Experience	Description
Flexible CDCVM	<p>Allows a POS device that supports CDCVM to delegate cardholder authentication to the mobile device when required for HVTs.</p> <p>Transaction notes:</p> <ul style="list-style-type: none"><li>For transit transactions, the cardholder's wallet and the transit gate are not expected to perform cardholder authentication.</li><li>For LVTs, the POS device will not perform any cardholder validation. However, the Flexible CDCVM user experience can be enabled with or without Lost &amp; Stolen support for LVTs, using the same CDCVM as for HVTs.</li></ul> <p>The Lost &amp; Stolen feature is described in the Card-Like Transaction notes above. When a wallet supports the Lost &amp; Stolen option with a Flexible CDCVM user experience, the authentication is expected to use the same CDCVM as configured for HVTs. Even if a CDCVM validated on the mobile device has the advantage of delivering immediate feedback to the cardholder, a Mobile PIN is still eligible for this process to deliver a consistent user experience between contactless LVT and HVT transactions.</p> <ul style="list-style-type: none"><li>For LVTs using magnetic stripe on some legacy devices, it is possible that the wallet is not able to determine whether the transaction is an LVT. In this situation, the cardholder can be asked to authenticate on the device (if not yet done) in order to perform the transaction.</li><li>For HVTs originating from a POS device not supporting CDCVM, cardholder authentication is required using Online PIN ATM, Online PIN POS, or Signature, (No CVM Required), depending on the configuration of the CVM List and the capabilities of the POS device, regardless of whether the cardholder has already been authenticated by the mobile device.</li></ul> <p>If the wallet application can request CDCVM for HVTs, it is acceptable that the CVM List excludes Online PIN ATM, Online PIN POS, Signature, (No CVM Required) or both methods. In this situation, issuers (and Wallet Providers) are recommended to validate commonly-used terminals to ensure that there are no interoperability issues arising from omitting one or both items from the CVM List.</p> <ul style="list-style-type: none"><li>For HVTs originating from a POS device supporting CDCVM, the POS device can delegate cardholder authentication to the mobile device, with no further POS device authentication required.</li></ul>

User Experience	Description
CDCVM Always	<p>Requires the cardholder's mobile device to authenticate the cardholder for all transactions. CDCVM can be performed using either a Mobile PIN or a locally-verified CDCVM.</p> <p><b>NOTE: The wallet application is expected to decline any transaction for which cardholder authentication is not performed or is unsuccessful.</b></p> <p>A POS device that supports CDCVM will delegate cardholder authentication to the mobile device when required for HVTs.</p> <p>Transaction notes:</p> <ul style="list-style-type: none"> <li>For transit transactions, the wallet always requires cardholder authentication. Cardholders must be trained appropriately to authenticate before the contactless tap at the transit gate.</li> <li>For LVTs, the POS device will not perform any cardholder validation. The wallet will always require cardholder authentication using the applicable CDCVM.</li> <li>For HVTs originating from a POS device not supporting CDCVM, cardholder authentication is required using Online PIN ATM, Online PIN POS or Signature, (No CVM Required), depending on the configuration of the CVM List and the capabilities of the POS device. Additionally, cardholder authentication using an applicable CDCVM via the wallet is required. It is acceptable that the CVM List excludes Online PIN ATM, Online PIN POS, Signature, (No CVM Required), or both methods. In this situation, issuers (and Wallet Providers) are recommended to validate commonly-used terminals to ensure that there are no interoperability issues arising from omitting one or both items from the CVM List.</li> <li>For HVTs originating from a POS device supporting CDCVM, cardholder authentication using an applicable CDCVM via the mobile device is required. No further POS device authentication is required.</li> </ul>

When enabling an account range for a contactless-enabled wallet application, the issuer is requested to configure the CVM List. For an MCBP wallet application, the CVM List proposed to the issuer depends on the brand and the user experience for the wallet application, as follows:

Brand (Application Identifier [AID])	Wallet User Experience	Issuer Options for the CVM List
Mastercard (AO 00 00 00 04 10 10)	Card-Like	<ul style="list-style-type: none"> <li>Online PIN ATM, Online PIN POS, No CVM Required</li> <li>Online PIN ATM, Online PIN POS, Signature, No CVM Required</li> <li>Online PIN ATM, Signature, Online PIN POS, No CVM Required</li> </ul>

<b>Brand (Application Identifier [AID])</b>	<b>Wallet User Experience</b>	<b>Issuer Options for the CVM List</b>
Mastercard (A0 00 00 00 04 10 10)	Flexible CDCVM or CDCVM Always	<ul style="list-style-type: none"> <li>• Online Pin ATM, No CVM Required</li> <li>• Online PIN ATM, Online PIN POS, No CVM Required</li> <li>• Online PIN ATM, Signature, Online PIN POS, No CVM Required</li> <li>• Online PIN ATM, Online PIN POS, Signature, No CVM Required</li> <li>• Online PIN ATM, Signature, Online PIN POS, No CVM Required</li> </ul>
Maestro (A0 00 00 00 04 30 60)	Flexible CDCVM or CDCVM Always	<ul style="list-style-type: none"> <li>• Online Pin ATM, No CVM Required</li> <li>• Online PIN, No CVM Required</li> </ul>
Private Label (A0 00 00 00 04 91 00)	Card-Like, Flexible CDCVM or CDCVM Always	<ul style="list-style-type: none"> <li>• Online Pin ATM, No CVM Required</li> <li>• Online PIN ATM, Online PIN POS, No CVM Required</li> <li>• Online PIN ATM, Signature, Online PIN POS, No CVM Required</li> <li>• Online PIN ATM, Online PIN POS, Signature, No CVM Required</li> <li>• Online PIN ATM, Signature, Online PIN POS, No CVM Required</li> </ul>

The issuer is *not* requested to configure the CVM List for the following brands and wallet user experiences:

<b>Brand (AID)</b>	<b>Wallet User Experience</b>	<b>CVM List</b>
Maestro (A0 00 00 00 04 30 60)	Card-Like	Online PIN ATM, Online PIN POS, No CVM Required
U.S. Maestro (A0 00 00 00 04 22 03)	Card-Like, Flexible CDCVM or CDCVM Always	Online PIN ATM, Online PIN POS, No CVM Required

**NOTE: Issuers should include their online PIN in their CVM list if they want to support ATM transactions.**

## User Experience for DSRP Transactions

DSRP transactions always use the CDCVM Always user experience with cardholder authentication for every transaction. The CDCVM can be delivered using a Mobile PIN or a CDCVM verified on the cardholder's mobile device.

The choice of CDCVM (Mobile PIN **or** locally-verified CDCVM) must be consistent with the user experience defined for contactless payment when contactless is supported by the wallet.

### MCBP 1.0

MDES associates a CDCVM Always user experience to any token configured to support MCBP 1.0, both for contactless and DSRP transactions.

The MD and UMD cryptograms must be valid for any transaction using an MCBP 1.0 token. Any failure will lead to a declined transaction:

- The entry of a wrong Mobile PIN will cause the generation of an invalid UMD cryptogram because the wrong session key is used.
- An invalid UMD combined with a valid MD will cause MDES to increment a PIN Try Counter. When the PIN Try Counter exceeds the PIN Try Limit, the token is suspended.
- A valid UMD combined with a valid MD will reset the PIN Try Counter in MDES.

Mobile PIN is the mechanism commonly used to deliver CDCVM when using MCBP 1.0.

### MCBP 2.0

MCBP 2.0 aims to address market needs and deliver an improved and consistent user experience for all cards within a wallet.

Wallet Providers (and issuers acting in the role of Wallet Providers) supporting contactless transactions can select any user experience (Card-Like, Flexible CDCVM, or CDCVM Always) when onboarding a new wallet to MDES. The user experience for DSRP is CDCVM Always.

To deliver a consistent user experience, the wallet application supports the same type of CDCVM for contactless and DSRP transactions, when applicable. For example, the cardholder cannot be expected to authenticate using a Mobile PIN when performing DSRP transactions while a locally-verified CDCVM is used for contactless payment when CDCVM is required to perform a transaction.

MDES also introduces the concept of **Transaction Analysis** when performing transactions using a token configured with MCBP 2.0. One of the objectives is to mitigate the security risk associated with user experiences (such as Card-Like or Flexible CDCVM) relaxing the rules related to authenticating the cardholder performing a contactless transaction. For information on MDES Transaction Analysis, refer to the Transaction Analysis chapter and the Transaction Analysis Technical Details appendix.

## Wallet Configurations Supported by MDES

MDES supports several wallet configurations. When a Wallet Provider onboards its wallet application, it indicates the application's configuration: the MCBP version, wallet use, user experience, CDCVM, and other contactless options.

### MCBP Version

MDES supports MCBP 1.0 and MCBP 2.0.

### Wallet Application Use

MDES supports the following uses:

- Contactless only
- Contactless and DSRP
- DSRP only

### User Experience

For any token associated with MCBP 1.0, MDES uses CDCVM Always (with Mobile PIN).

For MCBP 2.0, MDES supports the following configurations.

Configuration	Means that...
Card-Like user experience with <b>optional</b> support of Lost & Stolen	<ul style="list-style-type: none"><li>• Lost &amp; Stolen support is an optional feature managed by the wallet</li><li>• When Lost &amp; Stolen is enabled it can optionally report CDCVM information to MDES</li><li>• The concept of conditional UMD validation means for MDES that when CDCVM is reported as performed in the transaction data, the Mastercard Authorization System expects to receive a valid UMD cryptogram (and a valid MD cryptogram)</li><li>• Locally-verified CDCVM must be used to deliver Lost &amp; Stolen CDCVM; Mobile PIN is not eligible for this Lost &amp; Stolen process</li><li>• The token does not expose any support of CDCVM to the POS device</li></ul>

Configuration	Means that...
Flexible CDCVM user experience with <b>optional</b> support of Lost & Stolen	<ul style="list-style-type: none"> <li>Lost &amp; Stolen support is an optional feature managed by the wallet</li> <li>When Lost &amp; Stolen is enabled it can optionally report CDCVM information to MDES</li> <li>The concept of conditional UMD validation means for MDES that when CDCVM is reported as performed in the transaction data, the Mastercard Authorization System expects to receive a valid UMD cryptogram (and a valid MD cryptogram)</li> <li>Mobile PIN or Locally-verified CDCVM can be used to deliver CDCVM (one method must be chosen at time of wallet onboarding)</li> <li>The token exposes support of CDCVM to the POS device and 'POS with CDCVM support' can leverage authentication performed on the cardholder's device (using Mobile PIN or locally-verified CDCVM)</li> </ul>
CDCVM Always user experience	<ul style="list-style-type: none"> <li>Mobile PIN or locally-verified CDCVM can be used to deliver CDCVM (one method must be chosen at time of wallet onboarding)</li> <li>The token exposes support of CDCVM to the POS device and 'POS with CDCVM support' can leverage authentication performed on the cardholder's device (using Mobile PIN or locally-verified CDCVM)</li> </ul>

## CDCVM and Mobile PIN

MDES supports the following types of CDCVM: Mobile PIN and locally-verified CDCVM.

The Mobile PIN value is:

- A 4–8 digit PIN value
- Known by the cardholder and the Credentials Management System (CMS-D) and shared during wallet initialization
- Never stored on the mobile device; it is entered by the cardholder for every transaction requiring an authentication on the mobile device
- Validated online by MDES during the cryptogram validation of the authorization process
- Never validated by the mobile device, the wallet, or the MPA
- Never sent as part of transaction data
- Used to deliver instant cardholder authentication; it is not eligible for prolonged or persistent cardholder authentication
- Used by the MPA to retrieve the UMD Session Key from a Single Use Key; the Mobile PIN is securely deleted from memory as soon as this operation has been performed on the device

Locally-verified CDCVM is:

- Entered on and validated by the consumer's mobile device
- A method commonly associated with a device unlock process, for example device PIN, pattern, password or biometric methods (such as fingerprint, iris or facial recognition)  
Swipe is not a valid CDCVM for MDES MCBP wallets. Setting the device unlock to 'No device unlock' is also not valid for MDES MCBP wallets.

- Used by the payment component embedded in the wallet using the outcome of this authentication process

**NOTE: The wallet registration (set-up) process determines the type of CDCVM supported by the wallet: either Mobile PIN or locally-verified CDCVM, but not both at the same time. This means that a Wallet Provider looking to provide the option for the cardholder to select either type must register two mobile wallet applications, one of which will be used when installing the wallet on the cardholder's device.**

## Mobile PIN Management

The MDES Digitization service supports two different Mobile PIN models:

- **Token-specific Mobile PIN**—The cardholder chooses a different Mobile PIN value for every token.  
The cardholder chooses a Mobile PIN value using the wallet application when their card is first digitized. As with a PIN on a physical card, the cardholder has the option of changing their Mobile PIN from time to time, and they may also contact issuer Customer Services to reset their Mobile PIN (for example, if they forget it). The change of Mobile PIN will securely store the new Mobile PIN in the Credentials Management System (CMS) Dedicated and new payment credentials will be provisioned to the cardholder's mobile device.
- **Wallet-level Mobile PIN**—The cardholder chooses a single Mobile PIN value for all tokens within the same wallet.  
The cardholder chooses a Mobile PIN value when they first sign up for the service. In general, the Wallet Provider's server is responsible for managing the Mobile PIN on behalf of the wallet application. The Wallet Provider is responsible for authenticating the user before allowing a new Mobile PIN to be set.

**NOTE: Only a wallet-level Mobile PIN may be set at registration time. A token-specific Mobile PIN is set when the card is digitized.**

## Other Contactless Options

MDES supports the following features when defining the setup of a wallet:

- Support of transit transactions
- Downgrade to magnetic stripe mode at legacy U.S.-based contactless readers
- Support a downgraded mode for magnetic stripe readers

## Warning about MDES Security Controls for MCBP 2.0

---

The current implementation of MDES for MCBP 2.0 tokens has several security controls that cannot be disabled.

The MD cryptogram must be valid for any transaction using an MCBP 2.0 token. Any failure will lead to a declined transaction, unless there is an issuer override of the Mastercard default decision (Fraud Control).

The validation of the UMD is conditional to the identification by MDES that CDCVM was performed:

- Any EMV-based transactions, such as Contactless M/Chip or DSRP with full EMV/Chip data or DSRP with UCAF data, carry the information using the Card Verification Results (CVR). In this situation, if CVR (Byte 1 bit 3) reports that CDCVM was performed, the UMD cryptogram must be valid for any transaction using an MCBP 2.0 token. Any failure will lead to a declined transaction, unless there is an issuer override of the Mastercard default decision (Cardholder Verification).
- Any magnetic stripe transactions performed using a V3 POS device carry the information in the nUN value. In this situation, if nUN reports that CDCVM was performed, the UMD cryptogram must be valid for any transaction using an MCBP 2.0 token. Any failure will lead to a declined transaction, unless there is an issuer override of the Mastercard default decision (Cardholder Verification).
- A V2 POS device is not able to update the nUN value in order to report that CDCVM was performed:
  - The availability of a valid UMD cryptogram is used to determine that CDCVM was performed when a magnetic stripe transaction is performed using a V2 POS device.
  - When a magnetic stripe transaction is performed using a V2 POS device, it is not possible to distinguish between a case when CDCVM was not performed (and no valid UMD was generated) and a case when CDCVM was performed but the UMD cryptogram was invalid (such as when a wrong Mobile PIN value is provided by the cardholder). In this situation, it is not possible for MDES to increment the PIN Try Counter because MDES cannot determine whether CDCVM was performed:
    - When using a Card-Like user experience there is no impact, unless Lost & Stolen was used and the transaction data reports that CDCVM was performed and a failed locally-verified CDCVM generating an invalid UMD was not blocked by the wallet.
    - When using a Flexible CDCVM user experience combined with the use of Mobile PIN, this can lead to a potential security risk that can be mitigated by the CVM used at the POS level for HVTs (such as Online PIN) and ad hoc monitoring that can be implemented by the issuer.
    - When using a CDCVM Always user experience, the transaction will be declined because the UMD validation failed (unless there is an issuer override of the Mastercard default decision).
  - Mastercard published a mandate for V3 POS devices as part of the *Global Operations Bulletin No. 11*, 3 November 2014. This article announces a new requirement for acquirers to migrate all contactless-enabled terminals to *Mastercard Contactless Reader Specification version 3.0* (MCL 3.0). The effective dates are:
    - 1 January 2016—for new contactless reader deployments
    - 1 January 2019—for all currently deployed contactless readers

## Chapter 10 Shared Cardholder Verification Method on a Cardholder-Owned Device

*This section describes Shared Cardholder Verification Method (CVM) for secure payments from a mobile device.*

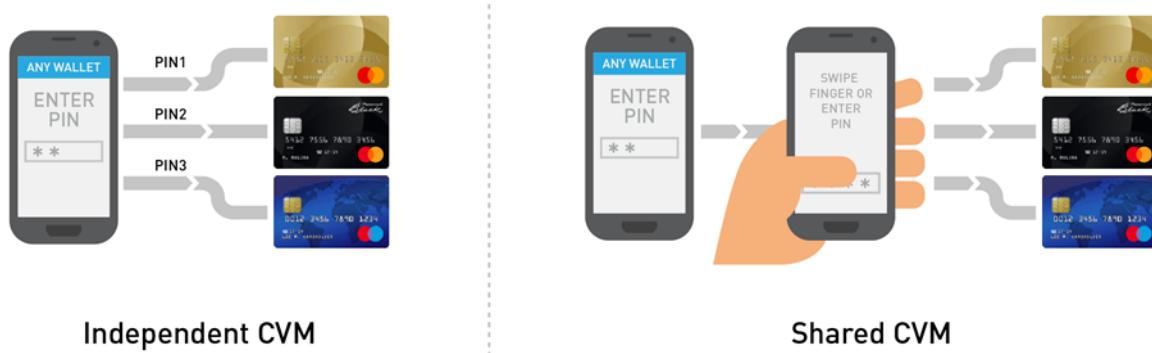
---

What is Shared CVM?.....	190
Cardholder Verification Methods.....	190
How Shared CVM Works.....	193
Cardholder Experience at the Point of Sale.....	194
Security Considerations.....	194
Issuer Considerations.....	195

## What is Shared CVM?

A Shared Cardholder Verification Method (Shared CVM) is an alternative to Secure Element-based Mobile PIN (mPIN), where the mobile device provides a single, shared cardholder verification method for all digitized payment cards on a consumer device, compared with the method where each digitized payment card performs its own cardholder verification.

**Figure 23: Independent CVM versus Shared CVM (Illustrative)**



In most cases it is expected that the Shared CVM initially uses a fingerprint biometric with a device password acting as backup at times where the biometric cannot be validated or has not been enrolled.

Issuers permit the use of a particular Shared CVM solution by agreeing to allow their cards to be digitized into a particular wallet on such a device. MDES permits issuers to decide whether their cards are available and eligible to be digitized into particular wallets.

## Cardholder Verification Methods

Cardholder Verification Methods (CVM) for card payments include signature, online PIN, and offline PIN. For contactless transactions, an additional 'no CVM' method is included to facilitate low value transactions which complete without online PIN or signature.

- Mastercard has pioneered the addition of payment capabilities into mobile devices and recognized well in advance that these devices allowed cardholder verification into mobile devices without the need for signature capture or a terminal for PIN capture. This is known as Consumer Device CVM (CDCVM). An example of CDCVM is mobile PIN (mPIN) where the PIN is verified by the Mastercard application inside the Secure Element or Host Card Emulation (HCE) solution of the mobile device. If CDCVM is supported by both the terminal and the payment application the CVM processing will not be performed.  
When CDCVM is not supported by the wallet and/or Point of Sale (POS) terminal, the CVM List (legacy solution) represents your verification preferences for contactless transactions. The POS terminal will use the first matching CVM it supports. For example, for Signature preferring CVM List, the terminal will use the first preference, "Signature", unless the terminal does not have that capability, such as a vending machine, in which case it will use

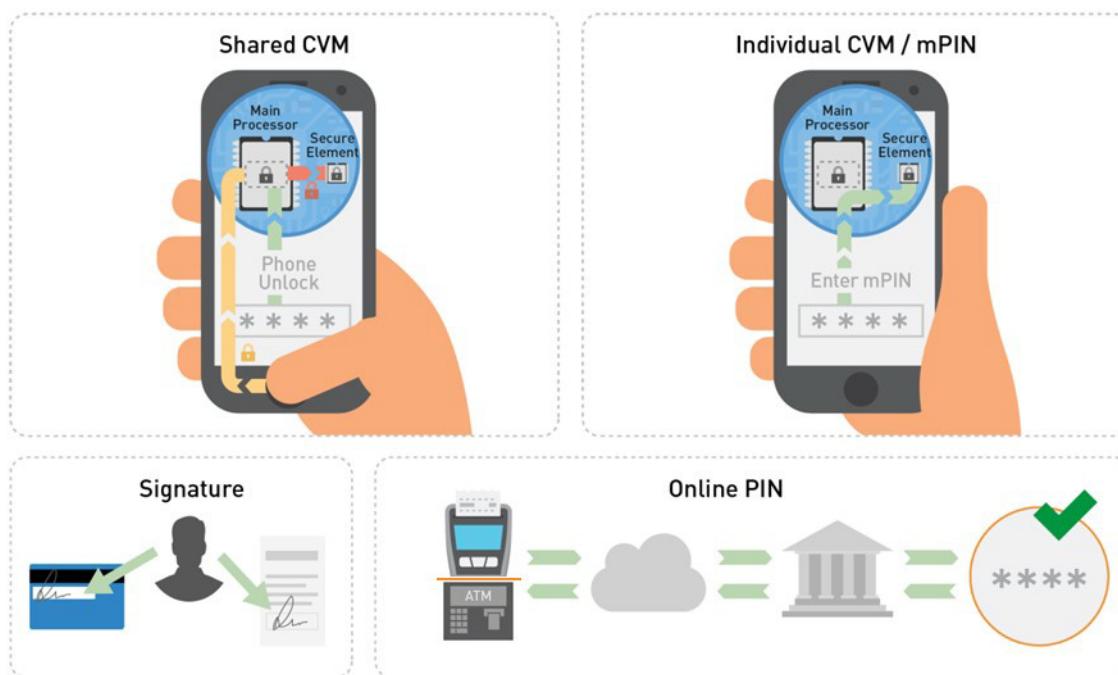
“Online PIN”, if supported. The terminal will only support the “No CVM Required” capability when performing a low value transaction. If the terminal does not support any of the methods in the CVM List, it will decide how to proceed based on the Terminal Action Codes (see [EMVCo EMV Book 4](#)).

Key reasons for a move to on-device cardholder verification include:

- Allowing the device to be used for transactions without a physical PIN pad (for example, transactions on the web, in applications, and in the aisle)
- Allowing the user to verify themselves before tapping on the terminal, enabling a faster experience for both the consumer and the merchant clerk for both low and high-value transactions

To support backwards compatibility of mobile payments with existing card terminals at the point of sale, Mastercard has allowed use of card-based verification methods while the migration to fully-digital device payments occurs. The three methods are shown in the following diagram:

**Figure 24: CVM and Where They are Validated (Illustrative)**



With cardholders already using passcodes and biometrics to unlock their mobile devices, and the launch of digital wallets with multiple payment card support, it makes sense to allow cardholders to use these verification methods (such as Shared CVMs) to verify themselves to the wallet applications to simplify the payment experience.

CVM	Captured by	Verified by
Signature	Receipt	Merchant
Online PIN	Point of Sale (POS)	Issuer host
Offline Card PIN	POS	Chip-based M/Chip application
Offline Mobile PIN (mPIN)	Mobile	Secure Element or Host Card Emulation-based M/Chip Mobile Application
Shared CVM	Mobile	Mobile device processor Secure Enclave

**NOTE: Issuers should include their 'online PIN' for the CVM in the CVM list for the account ranges that they would like to use for supporting contactless ATMs. They can do so by either changing their MDES Settings in MDES Manage My Accounts or by requesting the change via their regional CIS representative.**

### CVM Lists

- The payment device is configured with a list of CVMs, which is selected by the issuer during enablement that meets the consumer experience required at point of sale. MDES supports the following groups:
  - Low value transaction only: Online PIN at ATM (42/01) & No CVM (1F/03)
  - Online PIN only: Online PIN at ATM (42/01), Online PIN (42/03) & No CVM (1F/03)
  - Signature only: Online PIN at ATM (42/01), Signature (1E/03) & No CVM (1F/03)
  - Online PIN preferring: Online PIN at ATM (42/01), Online PIN (42/03), Signature (1E/03) & No CVM (1F/03)
  - Signature preferring: Online PIN at ATM (42/01), Signature (1E/03), Online PIN (42/03) & No CVM (1F/03)
- Each selection is a prioritized list of CVMs that will be shared with the point of sale (POS) terminal and the highest priority compatible CVM will be used. If no compatible CVM is found, the terminal following the '**No CVM found**' logic as per EMV Specs, will be used.
- The CVM entry states in brackets the CVM code (42 = online PIN, ...) and Condition Code (01 = at unattended cash, ie. ATM), see [EMVCo EMV Book 4](#)

#### NOTE:

- Purchase with Cash Back (PWCB) requires to include Online PIN (42/03)**
- NOTE: All lists include No CVM. Digitization and Re-digitizations will include Online PIN at ATM from April 2019**

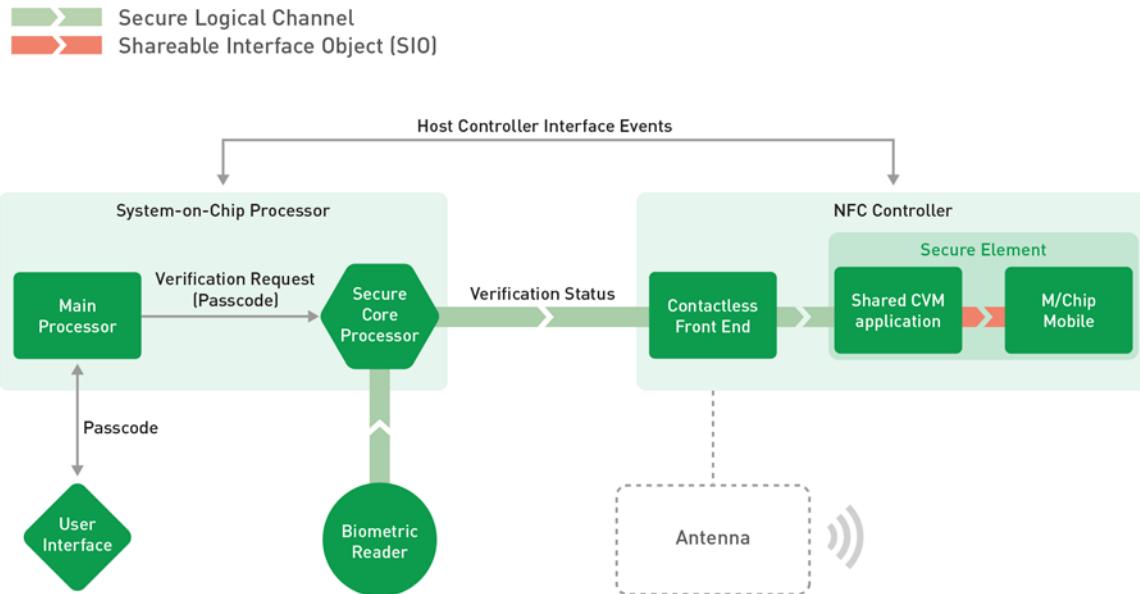
## How Shared CVM Works

A shared CVM is provided by the mobile device and makes use of the device's built-in security features to verify the cardholder.

The device supports both passcode and fingerprint biometrics as methods for verifying the cardholder. If a fingerprint biometric has been registered on a device, the verification process prioritizes the fingerprint biometric verification over passcode verification, although a cardholder is able to opt for passcode verification on every verification request.

Initially, the cardholder sets a device passcode and enrolls their biometric credentials on their mobile device. These may be used for purposes other than confirmation of payment (for example, unlocking the device).

The following diagram shows an example of a mobile device hardware architecture with a biometric subsystem using secure channels for communication between components.



The following steps occur when a cardholder initiates a transaction by opening the mobile wallet:

1. The cardholder presents a finger to the biometric sensor.
2. A biometric sample is captured and, using a secure mechanism, communicated to the secure co-processor where it is matched against existing biometric templates securely stored in protected memory accessible only by the secure co-processor.
3. A successful match is communicated using a secure mechanism to a Shared CVM application within the Secure Element capable of processing information about the Shared CVM.
4. The secure communication mechanism ensures an attacker cannot manipulate the Shared CVM application into registering that a cardholder was verified.

5. The Shared CVM application communicates to the M/Chip Mobile application internally within the Secure Element indicating the success of the verification.
6. The M/Chip Mobile application sets the PIN Verification Status (PVS) to 'verified' indicating that the cardholder was verified. This is the same data element used for mPIN verification.

## Cardholder Experience at the Point of Sale

---

Depending on terminal capabilities, the cardholder experience may vary slightly for high-value transactions (HVTs) or where an alternative network is selected.

For example diagrams of cardholder experiences using CVM, see the U.S. Soft Limit Terminals and Hard Limit Terminals sections in the Token Transaction Flows appendix.

Issuers should advise their cardholders that when transacting in markets that implement 'Hard CVM limits' for contactless payments, they are unable to use their mobile device for HVTs. For example, in the United Kingdom, any payment above GBP 30 cannot be made as a contactless transaction.

## Security Considerations

---

Although security has been at the forefront of the design of the biometric matching and password validations systems, these systems are still subject to attack.

Components involved in providing the Shared CVM are subject to review within the scope of the Mastercard Compliance Assessment and Security Testing (CAST) process. This gives all parties a high assurance as to the security and reliability of these components and the data generated by them.

Mastercard works with each provider to review the components and process of the Shared CVM solution ensuring that they offer issuers a reliable cardholder verification solution.

### Risks to Passcodes

Device passcodes are validated by the mobile devices using various protection mechanisms specific to devices. However, if the user 'jailbreaks' or 'roots' their device and deliberately or accidentally installs malware on the device, the device passcode could potentially be snooped by such programs. This risk is no greater than if mPIN were used for cardholder verification, since this could also be snooped by the malware.

Passcodes, similar to mPINs, are also vulnerable to shoulder surfing attacks, where criminals could observe a cardholder enter their passcode on their device, as a result compromising the passcode. If the device were then stolen, the criminal could potentially use the passcode to authorize a transaction.

**NOTE: Jailbreak or root: defined as a form of privilege escalation on a mobile device operating system that allows the user to obtain privileged control ('root access'). These elevated privileges allow the user to perform actions that are normally prevented by the device manufacturer or network operator.**

### Risks to Fingerprint Biometrics

Fingerprint biometrics can be spoofed. The process involves making a mold of an enrolled fingerprint from a latent print of an actual user's finger.

This is, however, not a scalable type of attack; this situation is not similar to a mass attack where millions of passwords are compromised. It is a threat that requires the perpetrator to first have physical access to the device, and then create a spoofed fingerprint from a print left behind by the actual owner of the device. Once the spoofed fingerprint is created, only that device is compromised. This is analogous to the PIN being revealed on a single card.

## Issuer Considerations

---

Since the mobile device is providing the Shared CVM service for use by all payment applications on the device, the issuer has no ability to manage the passcode or the biometric credentials as these are managed by the user on their own device. Issuers are unable to change or manage the CVM credentials in the same manner they would be able to do with a PIN or mPIN.

To use the Shared CVM provided by the device, at a minimum, the cardholder needs to set up a passcode and then, optionally, enroll at least one fingerprint, following the operating system's prompts and requirements. An issuer should communicate to their cardholders about the new type of CVM.

The following points should be considered:

- Offering advice on selecting and setting secure device passcodes, suggesting minimum lengths and complexity guidelines.
- Warning cardholders that enrolling another person's biometric into their mobile device should be considered the same as sharing a PIN or mPIN, and would allow that individual to perform a fully-verified transaction.
- Issuers should be aware that if a cardholder removes the device passcode from their device or deletes their Wallet Provider account, all digitized cards are removed from that device, requiring them to re-provision their cards to their device.
- Advising customers to not 'jailbreak' or 'root' their mobile device, since this would mean the device is more vulnerable to attack and fraud.
- Directing cardholders who have forgotten their passcodes, or who have disabled devices, to the support site of the mobile device manufacturer.
- Advising cardholders about being aware of their surroundings when entering their device passcodes, to ensure they are not being observed.

## Chapter 11 Digital Secure Remote Payment (DSRP)

*This section describes DSRP from implementation to support.*

---

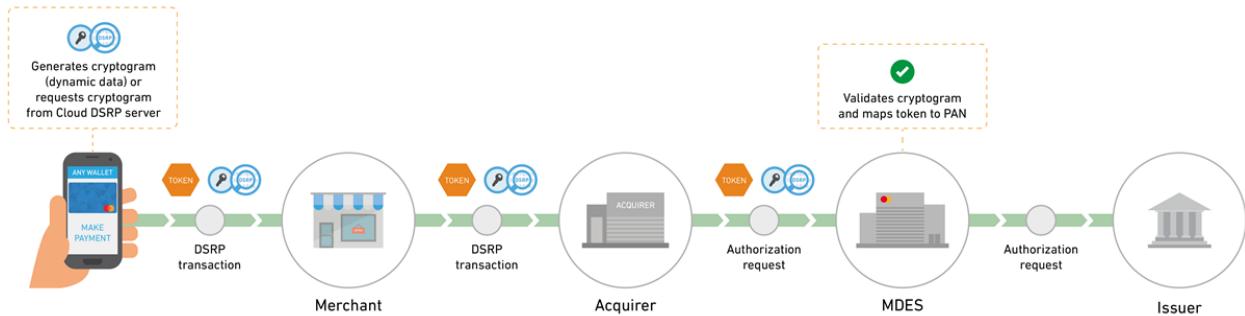
Benefits for Issuers.....	198
DSRP Support.....	199
Partial Shipments, Recurring Payment Transactions and Incremental Authorizations.....	201
Implementation.....	202

## What is DSRP?

DSRP is a payment solution that allows Card Not Present merchants to benefit from the dynamic secure data generated by M/Chip applications. DSRP is the only way to remotely process tokenized cards enabled by MDES.

DSRP transactions have the capability to include dynamic data to provide evidence that cardholder verification has been performed.

**Figure 25: DSRP Transaction Containing a Token and Cryptogram (Dynamic Data)**



DSRP transactions can be initiated from:

- Any device that can perform cardholder verification, including mobile devices and properly secured web-based implementations
- Token Requestors (such as merchants or commerce platforms) that are connected to Mastercard Cloud DSRP

Typical scenarios for these transactions include:

- Mobile e-commerce scenarios where cardholders use either their mobile browsers or a specific merchant application to purchase goods or services
- Merchant tokenization scenarios where cardholders purchase goods or services from a merchant website that participates in MDES for merchants

The use of a mobile application also offers the potential for shopping experiences in which DSRP may be used in circumstances where traditionally a face-to-face transaction at a physical point-of-sale device would have been conducted. For example, a merchant may provide an application that allows the cardholder to use the camera on a mobile device to scan the barcodes of goods in a brick and mortar store. When the cardholder has completed shopping, rather than going to a cashier to check out and pay, the cardholder may pay using DSRP through the mobile application, and leave the store with the goods without going to a cashier to checkout.

Because DSRP enables both e-commerce and replacement of a face-to-face payment in store, the two scenarios are distinguished in the Dual Message System (Authorization) and Single Message System transactions through the use of the POS Terminal Location field.

## Fraud Liability

Depending on the implementation, DSRP transactions may or may not provide fraud liability protection to the merchant. This is indicated in the Dual Message System (Authorization) and Single Message System transactions through the use of different values of Security Level Indicators (Electronic Commerce Security Level Indicator and UCAF Collection Indicator).

DSRP transactions initiated with an MD5 token have the following SLI values (in DE 48, subelement 42, subfield 1):

- 242 indicates issuer liability
- 246 indicates merchant liability

For DSRP partial shipments or recurring payments, the initial transaction defines the liability (the subsequent transaction messages have SLI values of 247).

The liability is based on the Mastercard Rules.

**NOTE: For more information about the SLI values, refer to "AN 1001—Electronic Commerce Security Level Indicator Validation and Usage," Release 17.Q4 article.**

---

## Benefits for Issuers

Securing transactions with DSRP can benefit issuers in many ways.

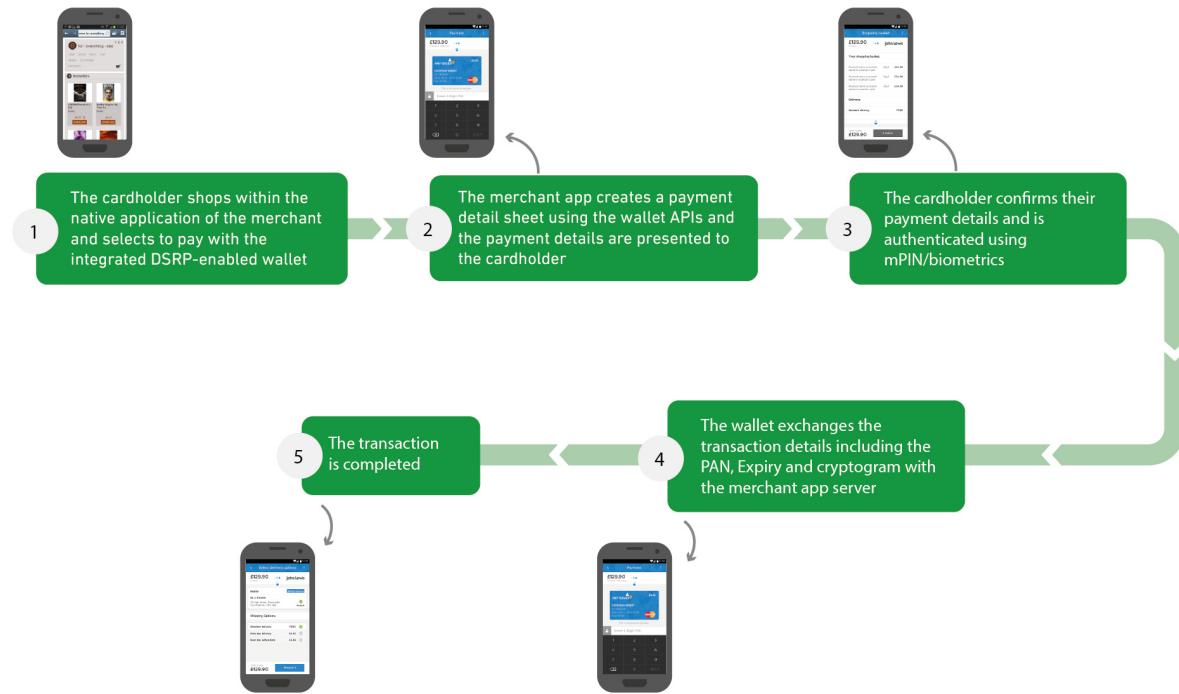
The benefits include:

- Leveraging EMV-based security can help to reduce transaction fraud and potentially increase the usage of card accounts for e-commerce, particularly in markets where consumer concern about the security of using cards on the web has restricted card-based e-commerce
- Enabling cardholder verification using a passcode, pattern, Mobile PIN, mPIN, or biometrics entered into the mobile device and verified by the payment application, provides an additional layer of protection to cardholders from unauthorized transactions
- Enabling more payment options for native, device-based payments (via in-app or mobile web), card on file, and for new purchasing options via QR codes and NFC tags in the physical world
- Authorizing transactions by the same host system as used for standard chip card transactions at the point of sale
- Increasing the value of the issuer's digitized Mastercard cards in the mobile device by enabling it to be used to initiate transactions in multiple environments (contactless at the point of sale, or remote through DSRP)
- Enabling the digitization of the issuer's Mastercard cards in card-on-file portfolios

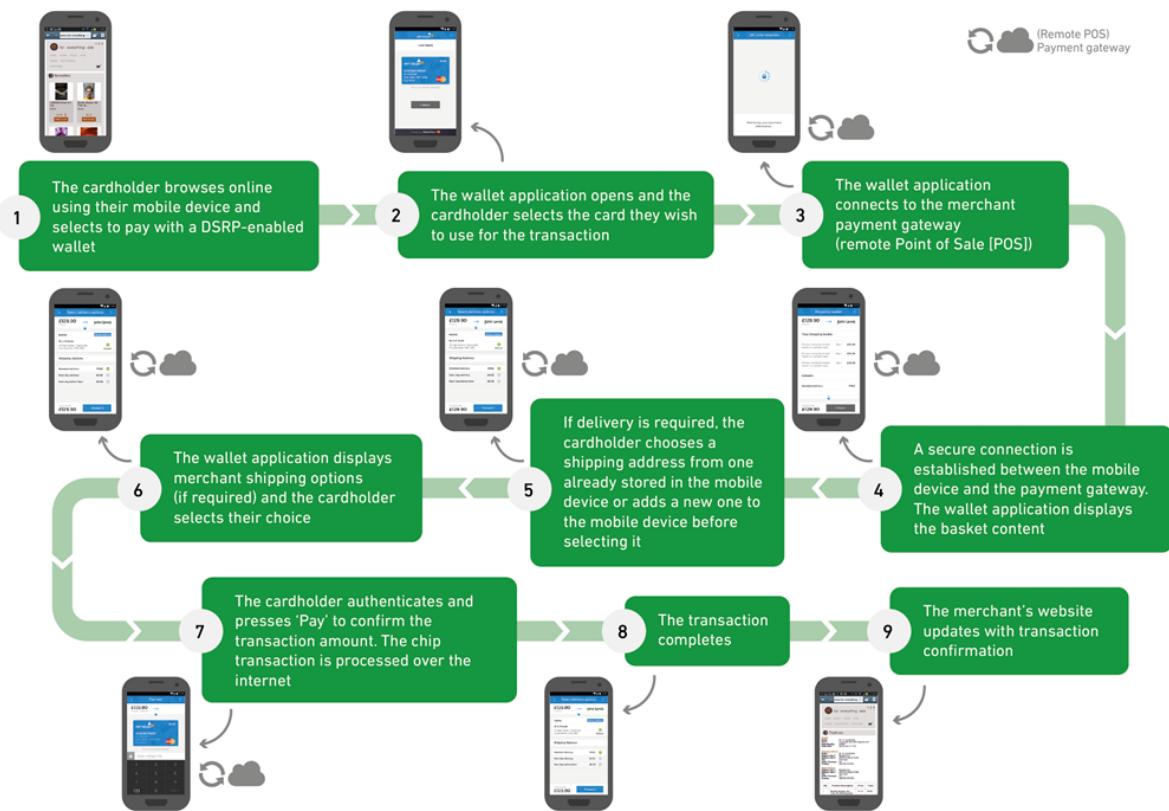
## DSRP Support

The diagrams below provide illustrative examples of the use of DSRP.

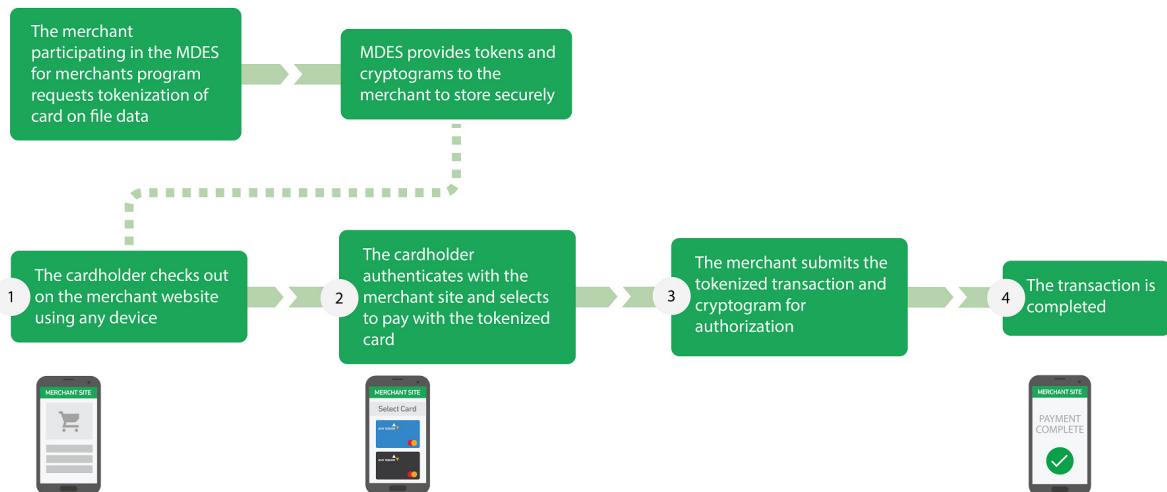
**Figure 26: Shopping from a Mobile App Directly Integrated with a DSRP Wallet**



**Figure 27: Shopping from a Mobile Device Browser**



**Figure 28: Shopping with a Merchant Participating in the MDES for Merchants Program**



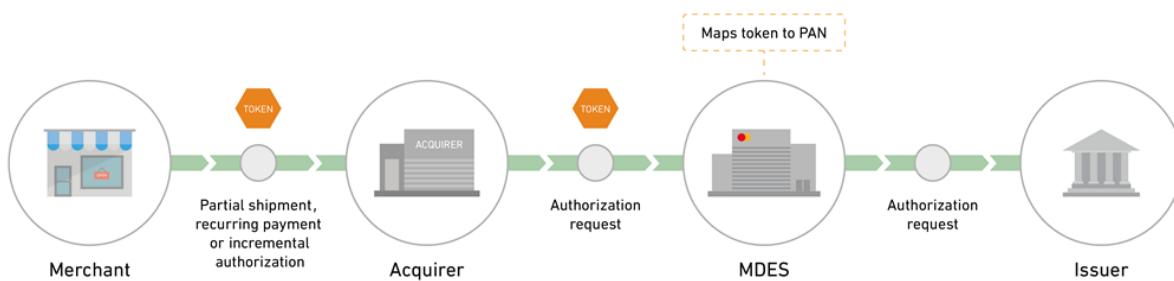
## Partial Shipments, Recurring Payment Transactions and Incremental Authorizations

A partial shipment occurs when an e-commerce merchant needs to ship several items in separate consignments (for example, if some of the purchased items are out of stock, or items are shipping from separate locations). Recurring payments enable a merchant or service provider to collect charges according to a billing cycle. Incremental authorizations enable merchants to increase the total amount that was authorized for a previous transaction.

For DSRP transactions, only the first authorization has cryptographic (chip) data included. For subsequent authorizations, the merchant indicates that they are associated with a previous transaction that was cryptographically authenticated.

Recurring payments that were initiated with a device token, either through a DSRP transaction or through a contactless transaction, only have cryptographic data in the first transaction. Authorizations for recurring payments initiated with a device token must provide an indication that there was an initial transaction with cryptographic data. An incremental authorization looks like a normal authorization but the transaction data includes a reference to the original authorization, so it does not require a cryptogram.

**Figure 29: Subsequent DSRP Partial Shipment, Recurring Payment or Incremental Authorization Transaction Containing a Token (No Cryptogram)**



For partial shipment and recurring payment transactions, the initial transaction may be either a DSRP transaction or a contactless transaction.

Issuers must be prepared to receive authorization requests indicating a partial shipment or recurring payment.

**NOTE: Subsequent authorizations for DSRP transactions are sent as Credential on File transactions (POS Entry Mode set to 10), regardless of whether the initial authorization was sent from the acquirer with full EMV Data (POS Entry Mode of 09) or with UCAF data (POS Entry Mode of 81) or as a contactless transaction.**

Mastercard recommends that issuers do not authorize requests for merchant-initiated transactions indicating partial shipment or recurring payment, unless the initial transaction (to which the partial or recurring transaction relates) was authorized. Initial transactions containing a cryptogram can be identified by the presence of values 51V, 61V, or 62V as on-behalf service results in DE 48, subelement 71.

**NOTE: For more information about on-behalf service results, refer to the *Customer Interface Specification***

Partial shipments and recurring payments for DSRP are supported on the Dual Message System only.

## Implementation

---

When an issuer enables their account ranges for MDSE, the card range is automatically enabled for DSRP. For more information, refer to the Issuer Enablement section.

Issuers must prepare their systems to receive the applicable data elements and values related to DSRP. The following information is available on Publications in Mastercard Connect™ ([www.mastercardconnect.com](http://www.mastercardconnect.com)):

- “AN 1001—Electronic Commerce Security Level Indicator Validation and Usage,” Release 17.Q4 article
- *Global Operations Bulletin No. 10*, 3 October 2016
- “Global 591—Digital Secure Remote Payment Enhancements—Reminder,” Release 15.Q4 article
- “Global 550—Enhancements to Mastercard Digital Enablement Service,” Release 14.Q3 article
- “Global 510—Enhancement to Mastercard Digital Enablement Service,” Release 14.Q2 article

For additional DSRP implementation information, refer to *DSRP—Acquirer Implementation Guide*.

## Chapter 12 Transaction Processing

*This section describes transaction processing using MDES.*

---

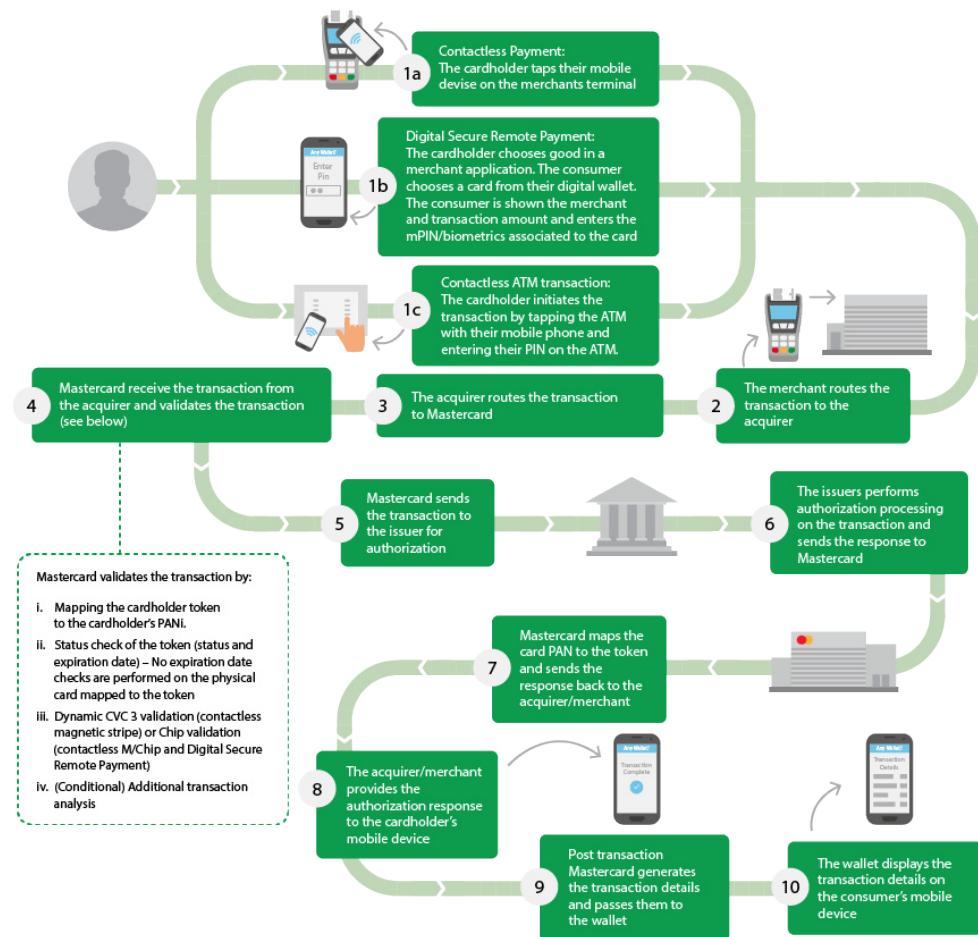
Benefits of Transaction Processing.....	204
Single Message and Dual Message Support.....	205
Transaction Detail Service.....	208
Alternative Routing Solution.....	210

## Benefits of Transaction Processing

A key component of MDES is the ability to process transactions using a token through the Mastercard Network.

One of the benefits of MDES is that it can perform the applicable cryptography validation (chip or dynamic CVC 3) and token to Account PAN mapping, minimizing the impact on the issuer's infrastructure, and enabling faster speed to market.

**Figure 30: Token-Initiated Transaction Flow for a Mobile Device**



In addition to standard Mastercard transaction processing, Mastercard performs the following services for the issuer:

- Map the token in the transaction to the cardholder's Account PAN and the Wallet ID (WID) for routing to the issuer
- In the transaction data sent to the issuer, the WID is in Data Element (DE) 48, subelement 26, subfield 1.

- Check the status of the token and whether the expiration date passed in the transaction is valid and in the future, to either decline or continue processing the transaction
- Validate the Dynamic CVC 3 for transactions initiated as contactless magnetic stripe or Dynamic Magnetic Stripe Data
- Perform Application Transaction Counter (ATC) checks
- Validate the cryptogram for transactions initiated as contactless M/Chip or DSRP with full EMV/Chip data:
  - Mastercard validates the Authorization Request Cryptogram (ARQC) and generates the Authorization Response Cryptogram (ARPC). DE 55 (Integrated Circuit Card [ICC] System-Related Data) is not sent to the issuer.
  - EMV Terminal Verification Results (TVR)/Card Verification Results (CVR) check—Checks the TVR (a set of results provided by the terminal that conducted the transaction to decide whether to accept, decline, or send the transaction online). Checks the CVR (a set of checks performed by the card at the terminal to authenticate the mPIN and risk parameters).
  - The AID value (tag 84) is mandatory when processing a contactless M/Chip transaction using an MCBP 2.0 token.
- Validate the cryptogram for transactions initiated as DSRP with UCAF data:
  - The Wallet Provider must ensure that the correct UCAF Format is used for the product/solution supported by the wallet application. The UCAF Formats are specified in *Digital Secure Remote Payments — UCAF Formats*, which is available from your Mastercard representative
  - Mastercard extracts the ARQC and dynamic transaction data from the UCAF, and validates the ARQC. The UCAF data in DE 48 (Additional Data—Private Use), subelement 43 (Universal Cardholder Authentication Field [UCAF]) is not sent to the issuer. An Authorization Response Cryptogram (ARPC) is not generated.
- Perform additional Transaction Analysis

**NOTE: It is the issuer's responsibility to check the expiration date for the Account PAN. Mastercard does not check the Account PAN expiry date for transactions performed with a token.**

---

## Single Message and Dual Message Support

The issuer/issuer processor needs to make changes to its single message and dual message interface to support MDSE.

MDSE supports the processing of contactless transactions (both magnetic stripe and M/Chip), Dynamic Magnetic Stripe Data transactions and DSRP transactions with full EMV data (DE 55) or UCAF data (DE 48, subelement 43) by performing the following activities:

- Validating the cryptography provided in the authorization (dual message) and financial transaction (single message) messages
- Mapping the token to the Account PAN in authorization and clearing (dual message) and financial transaction (single message) messages

- Mapping the Point of Service Entry Mode (DE 22, subfield 1) submitted by the acquirer to values indicating the use of MDES as shown in the following table:

<b>Message Type</b>	<b>Transaction Type</b>	<b>POS Entry Mode</b>	<b>POS Data Code: Acquirer or Issuer</b>
Authorization and Financial Transaction	Contactless M/Chip	PAN auto-entry via contactless M/Chip	07
	Contactless Magnetic stripe	PAN auto-entry via contactless magnetic stripe	91
	DSRP with EMV data	PAN entry via electronic commerce, including remote chip	09
	DSRP containing UCAF	PAN entry via electronic commerce, including chip	81
	Dynamic Magnetic Stripe Data	PAN auto-entry via magnetic stripe	90
	Card on File	PAN entry via electronic commerce, including chip	81
Clearing	Card on File	PAN auto entry via server	82
	Credential on File	Credential on File	10
	Contactless Magnetic stripe	PAN auto-entry via contactless magnetic stripe	A
	Contactless M/Chip	PAN auto-entry via contactless M/Chip	M
	DSRP with full EMV data	PAN Entry via electronic commerce, including remote chip)	R
	DSRP containing UCAF	Electronic commerce	S

**NOTE: POS Entry Mode 82 may still be used in legacy implementations that have not converted to POS Entry Mode 10 for MDES transactions**

**NOTE: Tokenized contactless ATM transactions processing will be supported from 18Q4.**

**NOTE: As of publication, the transaction time window is -8 and +20 minutes. For more information, refer to "Global 580—Mastercard Digital Enablement Service—Dynamic Magnetic Stripe Data," Release 16.Q1 article.**

## Online PIN Support

MDES enables cardholders to use the same online PIN as their plastic card for transactions initiated by a mobile device using a token. The online PIN is entered into the point of interaction rather than the cardholder mobile device.

When a token is used at the point of interaction, the online PIN block in DE 52 (Personal Identification Number [PIN]) is sent by the acquirer in the authorization or financial transaction request and is based on the token. As part of MDES, Mastercard converts this PIN block to an online PIN block based on the primary account number before sending the authorization or financial transaction request to the issuer.

Issuers that participate in MDES and perform their own PIN validation must be aware that Mastercard does not send track data on dual message authorization or single message transactions to the issuer when MDES has been performed. Therefore, issuers must maintain the PIN offset/PVV in their own systems instead of expecting PIN offset/PVV in the track data.

Additionally, Mastercard currently supports sending the Card Sequence Number for the PAN to the issuer in MDES contactless chip and DSRP EMV transactions if the issuer has:

- Provided the Card Sequence Number for the PAN to Mastercard for association with the token
- Contacted their Mastercard representative to request receipt of the Card Sequence Number for the PAN in MDES transactions

**NOTE: For more information, refer to “Global 534—Card Sequence Number in Mastercard Digital Enablement Service Transactions,” Release 17.Q2. This functionality also applies to MDES contactless chip ATM transactions.**

**Mastercard does not currently support sending the Card Sequence Number for the PAN to the issuer in MDES contactless magnetic stripe transactions, dynamic magnetic stripe data, or DSRP UCAF. Issuers who have opted in to receive the Card Sequence Number as part of their PIN validation processing must determine its impact on their own operations. Mastercard will not send the card sequence number for the token to issuers in MDES transactions.**

Issuers should opt in to receive DE 23 (Card Sequence Number) and be prepared to validate the PIN for contactless ATM transactions.

**NOTE: An opt-in capability to send DE 23 (Card Sequence Number) in transaction messages to the issuer is available in the 17.Q2 release.**

These changes are detailed in the following Mastercard release articles:

“Global 561—New Digital Enablement Service,” Release 13.Q4	Introduction to MDES. The issuer should review the article to understand the mandatory changes required to accept the new fields in dual message (authorization and clearing) and single message transactions for MDES. This update also details the edits to the Mastercard Platform, explaining the behavior of different data elements in the transaction.
--	---

"Global 501—Enhancement to Mastercard Digital Enablement Service," Release 14.Q1	Update to MDES for issuers that support online PIN for transactions using tokens.
"Global 510—Enhancement to Mastercard Digital Enablement Service," Release 14.Q2	Pre-digitization network message support relating to the tokenization message support. This update also includes support for DSRP (formerly Chip Secured Remote Payment) performed with tokens.
"Global 550—Enhancements to Mastercard Digital Enablement Service," Release 14.Q3	Information on DSRP with UCAF, as well as updated layouts for pre-digitization network messages support.

Issuers are also advised to regularly check the MDES Information Center on Publications in Mastercard Connect™ ([www.mastercardconnect.com](http://www.mastercardconnect.com)) for the latest updates to the Mastercard release documents and articles.

## Transaction Detail Service

MDES allows transaction details to be retrieved by the cardholder's device either directly or via the Wallet Provider in real-time when a transaction is performed using a token.

The Transaction Detail Service (TDS) manages the interactions between Mastercard, the Wallet Provider, and the cardholder's device for the registration, notification and delivery of transaction details. It requires no implementation by the issuer.

**NOTE: The TDS is not currently available to merchants using MDES for tokenization.**

**Figure 31: High-Level User Experience for a Contactless Payment Followed by Transaction Details**



1. The cardholder verifies themselves to their mobile device.
2. The cardholder taps their mobile device to the contactless terminal.

3. The cardholder is notified immediately that their mobile device has completed the transfer of payment data to the terminal (the message originates by the handset detecting it has completed a tap on a terminal).
4. The cardholder is notified of the transaction outcome and associated details via the message coming from the TDS.

For remote payments using DSRP, steps 1 and 2 may also be performed by the cardholder making a website purchase using their mobile device, or on a PC, tablet, or TV.

To provide a consistent user experience regardless of merchant terminal capabilities or whether the transaction was captured via a contactless or remote interface, the TDS provides transaction details to the cardholder's device after online authorization.

### **Key Features**

- Only the device containing the token may receive transaction details for that specific token.
- All transaction details are retrieved by the cardholder's device directly or via the Wallet Provider from the TDS.
- Transaction data stored on the cardholder's device is encrypted to the cardholder's Wallet Provider account and must be treated as personal data by the Wallet Provider.  
The Wallet Provider is responsible for ensuring that any transaction details (for example, date-time, amount, currency, merchant name, or issuer decision) retrieved from MDES are securely stored in accordance with applicable laws for the cardholder's use only.

For purposes of clarity, the TDS delivers transaction details to the cardholder's device, not to the issuer of the card that was digitized.

#### **NOTE:**

- **Mastercard stores transactions for 30 days.**
- **In Mastercard dual message systems, refunds are processed only as clearing messages (with some rare exceptions). Therefore, a consumer will not receive immediate notification of a refund transaction. Instead, they will receive a notification when Mastercard has received and processed the refund in the clearing files, which may be several days or weeks later.**

**NOTE: Our TDS notifications are processed in batches due to which we cannot guarantee immediate delivery of the notifications. While the notifications are delivered within a reasonable time, partners should not anchor time-sensitive business logic off these notifications**

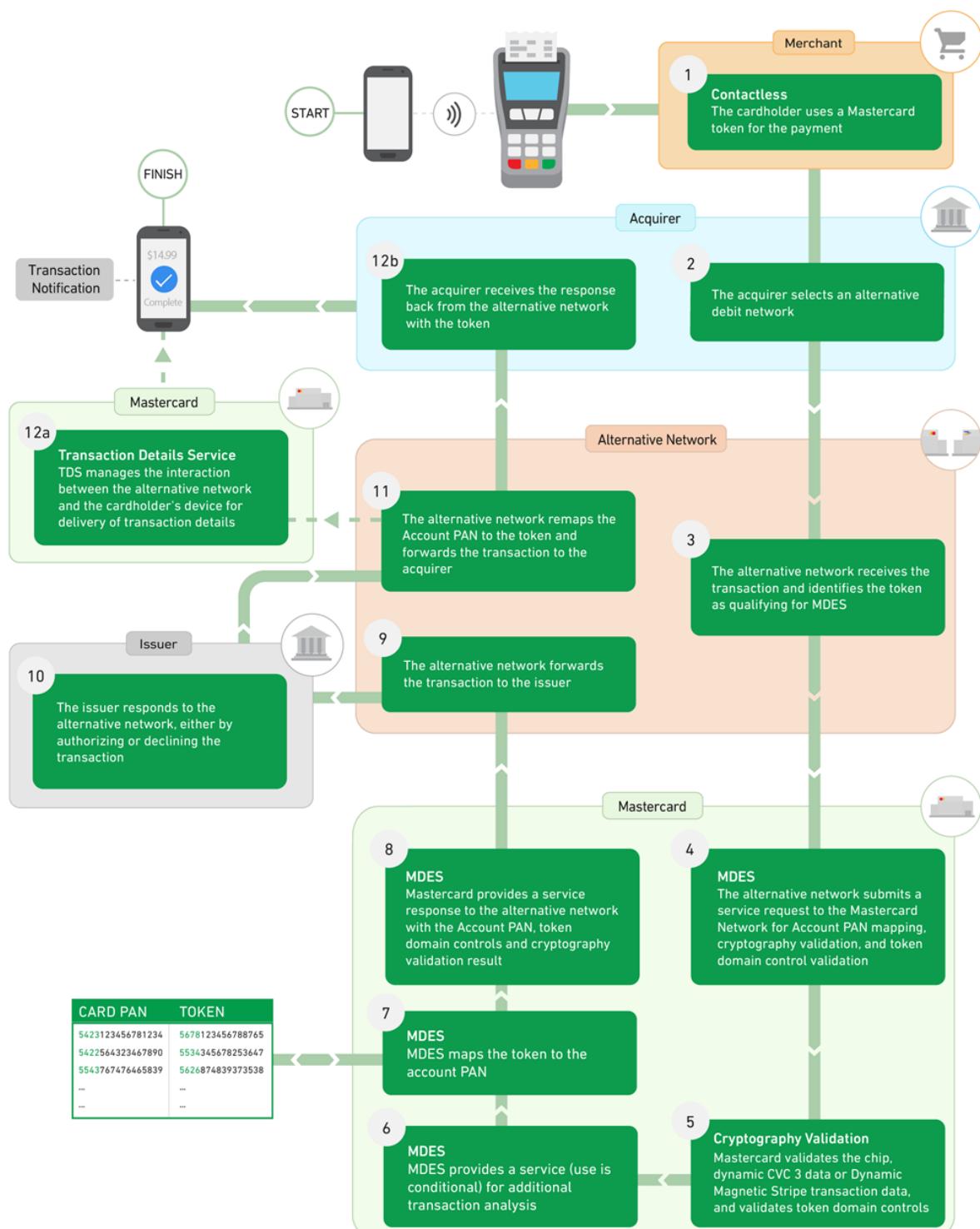
## Alternative Routing Solution

---

The MDES alternative routing solution uses modified Authorization Request/0100 and Authorization Advice/0120 message formats to validate cryptography, apply token controls and provide token to PAN mapping, and provide transaction history to the consumer.

### Message Flow of a Mastercard Token Processed by a Network

Mastercard sends and receives network messages via a specified network connection commonly agreed on by Mastercard and the other network.



MDES provides an alternative network with two primary functions for Mastercard tokens not processed on the Mastercard Network:

- Service request and response messages allow an alternative network to access MDES including chip or dynamic CVC 3 validation, token to Account PAN mapping services, and optional token domain controls.
- Accept transaction history advice messages from the alternative network so that real-time notifications can be pushed to the cardholder's device or the Wallet Provider's server (depending on the implementation). This ensures a consistent user experience for the cardholder regardless of whether the Mastercard token is processed on the Mastercard Network.

### **Service Request and Response**

An alternative network can initiate requests to MDES to use multiple token services, as detailed below. The Mastercard response to the alternative network contains the results of services performed:

- **Token to Account PAN Mapping**—MDES translates the token presented at the point of sale (POS) to the Account PAN as recognized by the issuer's systems.
- **Token Domain Controls**—MDES enforces the appropriate token use based on a defined set of parameters. When requested, MDES invokes token controls based on the point-of-service entry mode values provided in MDES request message.
- **Cryptography Validation**—MDES validates the Authorization Request Cryptogram (ARQC-EMV) or dynamic CVC 3 when an alternative network provides the relevant data in MDES request.

### **Transaction Detail**

After the alternative network processes the authorization request, it sends a transaction history advice message to Mastercard including details such as whether the transaction was approved or declined, the transaction amount and the merchant name. Unless the issuer is providing their own transaction details service, the Mastercard Transaction Detail Service (TDS) pushes a real-time notification to the device or server, allowing it to retrieve the transaction details and present them to the cardholder.

**NOTE: Mastercard stores transactions for 30 days.**

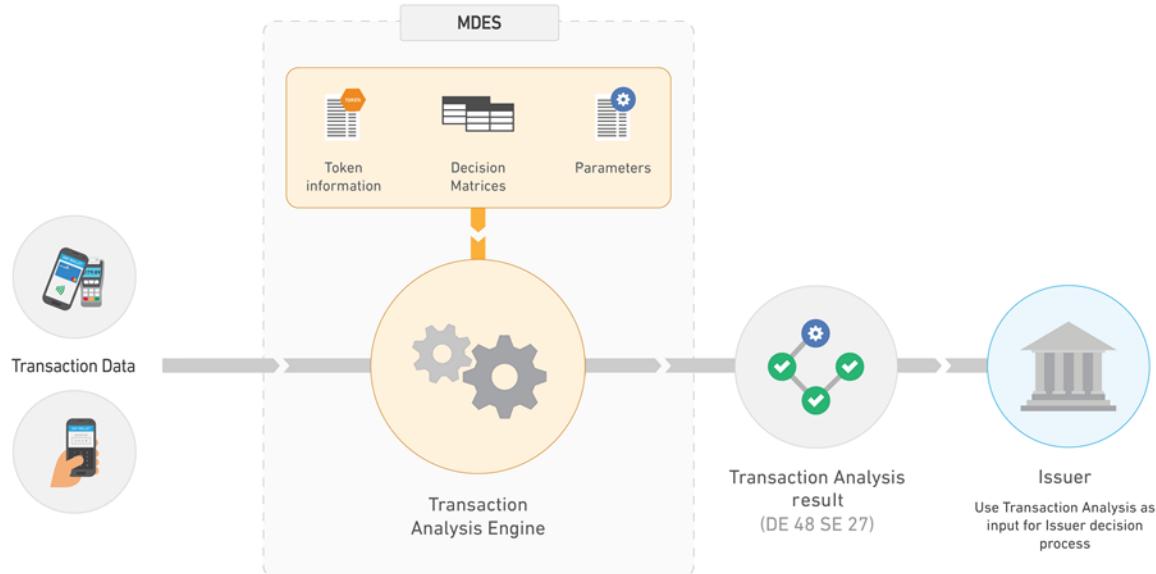
## Chapter 13 Transaction Analysis

*This section describes MDES Transaction Analysis.*

---

What is Transaction Analysis?.....	214
Wallet Provider Options for Transaction Analysis.....	216
Issuer Options for Transaction Analysis.....	217
List of Real-Time Validations.....	218
Impact on the Issuer Decision Process.....	221

## What is Transaction Analysis?



In the “Global 542—Mastercard Digital Enablement Service Enhancements Supporting New Transaction Analysis Capabilities and CVM Models for MCBP Tokens” Release 17.Q2 announcement, Mastercard announced the mandatory support of Transaction Analysis for issuers participating in MDES and in a wallet that uses MCBP 2.0 tokens. In the “AN 1410—Additional Controls in Transaction Analysis” Release 18.Q2 announcement, Mastercard announced the addition of two new controls in the transaction analysis performed by MDES on transactions using MCBP 2.0 tokens.

## What is Transaction Analysis?

Transaction Analysis is a service provided by MDES. MCBP 2.0 is the first product to use Transaction Analysis.

### Objectives

Transaction Analysis has several objectives, which include the following:

- Provide the issuer with detailed information about a transaction while hiding all the technical complexity for retrieving and analyzing the information for each product.
- Mitigate the security risk associated with user experiences (such as Card-Like or Flexible CDCV) relaxing the rules related to the authentication of the cardholder performing a contactless transaction compared to a user experience using CDCV Always where authentication on the device is required for each transaction. The user experiences are described in the Mastercard Cloud-Based Payments (MCBP) chapter.
- Improve the issuer decision on transactions reaching their risk management system when the issuer has to process the transaction in real time for an approval or decline.

- Improve the information delivered to the issuer for post-Transaction Analysis, when the Mastercard Authorization System has declined the transaction.
- Deliver an advanced decision process that uses the following input parameters:
  - The type of transaction:
    - Contactless EMV
    - Contactless magnetic stripe
    - DSRP (using DE55)
    - DSRP (using DE48 – UCAF)
  - The qualification of the transaction (when applicable) between a low-value transaction (LVT) versus a high-value transaction (HVT)
  - The outcome of a list of checks performed by the Mastercard Authorization System, including:
    - System checks for integrity, data consistency, and abnormal use of a product
    - Control of use of Consumer Device Cardholder Verification Method (CDCVM) and user consent to the transaction
    - Validation of Cardholder Verification on the device and on the POS device, when applicable
    - Fraud control using Application Transaction Counter (ATC) checks, cross-channel detection, fuzzing and key compromise
    - Additional checks including token authentication to the terminal and detection of any wallet overrule of the Mastercard decision on CDCVM
  - The context of the decision; whether it is the primary decision made by the Mastercard Authorization System, or by the Mastercard Authorization System when Stand-In processing applies
- Adapt the decision parameters for each tokenized card:
  - Define a default Mastercard configuration for a given product, such as MCBP 2.0.
  - Customize the default configuration based on the user experience supported by the wallet.
  - Allow the issuer to adjust the decision process to their needs during issuer enablement:
    - Override the Mastercard decision related to Cardholder Verification
    - Override the Mastercard decision related to Fraud Control
    - Strengthen the Mastercard decision related to Token Authentication to Terminal
    - Strengthen the Mastercard decision related to Wallet Overrule

## Results Delivery to Issuers

The Mastercard Authorization System uses DE 48 subelement 27 to deliver the Transaction Analysis results to the issuer:

- Using Authorization Request/0100 message: Continue processing decision
- Using Authorization Advice/0120 message:
  - Decline decision
  - Stand-In processing

The Transaction Analysis Technical Details appendix provides a detailed description of the information delivered to the issuer using:

- The Transaction Analysis Overview value, delivered using DE 48 subelement 27 subfield 1, which can be one of the following values:
  - Continue with Information (CI)
  - Continue with Warning (CW)
  - Decline Issuer Decision (DI)
  - Decline Suspicious (DS)
- The list of Test Result Codes, delivered using DE 48 subelement 27 subfield 2, which can include the following values (codes):

<b>Category</b>	<b>Values/Codes</b>
Fixed values defined by Mastercard	NMK, UTP, FER, DNC, EXP, CVF, PPP, SNA, ICT, CVX
Values depending on wallet user experience	OVU, OVP
Issuer-configurable decision for Cardholder Verification	OVF, OVE, CVU, PTB, PWE, CRN
Issuer-configurable decision for Fraud Control	CAM, DMM, FUZ, SKC, REP, CCH, PKC
Issuer-configurable decision for Token Authentication to Terminal	DAU, DAF
Issuer-configurable decision for Wallet Overrule	WOC

For code descriptions, refer to List of Real-Time Validations.

## **Wallet Provider Options for Transaction Analysis**

The wallet registration process uses a list of questions to determine the configuration of a wallet supporting MCBP 2.0.

The starting point is the product definition that is associated among others with the Mastercard default decision matrix for the new Transaction Analysis process.

The following questions relating to Transaction Analysis are asked during the wallet registration process:

<b>Question</b>	<b>Choice</b>
What is the version of MCBP?	<ul style="list-style-type: none"> <li>• MCBP 1.0</li> <li>• MCBP 2.0</li> </ul>

<b>Question</b>	<b>Choice</b>
What is the use of the product?	<ul style="list-style-type: none"> <li>• Contactless Only</li> <li>• Contactless and DSRP</li> <li>• DSRP only</li> </ul>
What is the user experience to be used for contactless?	<ul style="list-style-type: none"> <li>• Card-Like</li> <li>• Flexible CDCVM</li> <li>• CDCVM Always</li> </ul>
<b>NOTE: CDCVM Always is the user experience systematically used for DSRP.</b>	
The Card-Like, Flexible CDCVM and CDCVM Always user experiences are described in the Mastercard Cloud-Based Payments (MCBP) chapter.	

The following questions are also asked, but they do not impact Transaction Analysis:

- What is the type of CDCVM?
- Are transit transactions supported by the wallet?
- Do you want to downgrade to magnetic stripe mode at legacy U.S.-based contactless readers?
- Do you want to favor contactless magnetic stripe transactions?

The support of MCBP 2.0 triggers the use of Transaction Analysis by the Mastercard Authorization System.

The selection of CDCVM Always as the user experience for contactless changes the setting of the decision matrix, as described in the Transaction Analysis Technical Details appendix.

## Issuer Options for Transaction Analysis

The issuer enablement process uses a list of questions to customize the Transaction Analysis configuration of a wallet supporting MCBP 2.0.

When an issuer enables an account range for an MCBP 2.0 wallet application, it is asked to configure the behavior of the Mastercard Authorization System when the following situations are detected by the Transaction Analysis process:

<b>Situation</b>	<b>Choice</b>
One or more failures detected in Cardholder Verification	<ul style="list-style-type: none"> <li>• Continue</li> <li>• Decline (the default)</li> </ul>
One or more failures detected in Fraud Control	<ul style="list-style-type: none"> <li>• Continue</li> <li>• Decline (the default)</li> </ul>

Situation	Choice
Token authentication to Terminal (ODA) failed or not performed	<ul style="list-style-type: none"><li>• Continue (the default)</li><li>• Decline</li></ul>
Wallet Overrule of Mastercard decision on CDCVM	<ul style="list-style-type: none"><li>• Continue (the default)</li><li>• Decline</li></ul>

The issuer option to continue aims to avoid a transaction being declined by Mastercard during Transaction Analysis when one of the Test Result Codes (associated with a decline) is triggered. That way, the issuer can make its own decision with their risk management process using the information provided by the MDES Transaction Analysis service with DE 48 subelement 27.

For example, under some conditions an issuer may want to approve a transaction using an invalid Mobile PIN or failure of locally-verified CDCVM (OVF will be raised) when the user provided a valid Online PIN using the PIN Pad of the POS device while performing that transaction.

The issuer should be aware that:

- The issuer's answer to these questions affects the Mastercard decision process during Transaction Analysis, but it does not change the user experience supported by the wallet.
- Any change to the default settings has a direct impact on the security of the payment solution and it is assumed that the issuer will enable all the required controls on the transaction data and input provided by Transaction Analysis when approving the transaction.
- Those changes only apply to the primary decision matrix.  
The alternative decision matrix (used for Stand-In processing) uses the default Mastercard setting in order to avoid approval of transactions that would most probably have been declined by the issuer as result of their risk analysis.

Detailed information about the configuration of the decision matrix is provided in the Transaction Analysis Technical Details appendix.

## List of Real-Time Validations

These tables provide a high-level description of each real-time validation supported by MDES Transaction Analysis. The Transaction Analysis Technical Details appendix contains detailed

information about each check performed by the Mastercard Authorization System when Transaction Analysis is performed on tokenized transactions using MCBP 2.0.

### **Checks Associated with Fixed Decision Defined by Mastercard**

<b>Code</b>	<b>Name</b>	<b>Short Description</b>
NMK	No Matching Key File/KDI Combination	The cryptographic material required to validate the transaction cannot be retrieved.
UTP	Unable to process	Detection of a fatal error in the transaction data. The transaction cannot be processed.
FER	Format error	Detection of a format error in a DSRP transaction containing DE48 subelement 43 (UCAF).
DNC	Data not consistent with application or product	Detection of data present in a contactless EMV transactions that is inconsistent with the application or product.
EXP	Token Expired	The payment terminal has reported that the token is expired.
CVF	Cardholder verification (on terminal) was not successful	The payment terminal has reported that cardholder verification (on the terminal) was unsuccessful.
PPP	PIN Pad Problem	The payment terminal has reported that there was a problem with the PIN pad during an HVT.
SNA	Requested service not allowed for this product	The payment terminal has reported that the requested service is not allowed for the given product.
ICT	Not a valid Cryptogram Type	Detection of an EMV cryptogram type that is not an Authorization Request Cryptogram (ARQC).
CVX	Status CVM unknown	The status of the CVM cannot be determined.
<b>NOTE: This CVX code is never triggered in the <i>current</i> implementation of MDES Transaction Analysis.</b>		

### **Checks with Decision Determined by the Wallet User Experience**

<b>Code</b>	<b>Name</b>	<b>Short Description</b>
OVU	CDCVM Not Performed	Detection that CDCVM was not performed.
OVP	CDCVM (was possible but) not performed	Detection that CDCVM was possible but not performed.

### **Checks with Decision Configurable by the Issuer—Cardholder Verification**

The issuer can soften (override) the Mastercard default setting during the issuer enablement/maintenance process:

<b>Code</b>	<b>Name</b>	<b>Short Description</b>
OVF	CDCVM Failed	Detection that CDCVM was performed and the validation of the User and Mobile Device (UMD) authentication cryptogram (AC) has failed.
OVE	CDCVM retry exceeded – Token Suspended	Detection that CDCVM was performed and the validation of the UMD cryptogram has failed.  The number of CDCVM failures has exceeded the threshold value defined in the configuration for the token associated with MCBP 2.0. The token has to be suspended.
CVU	CVM Requirements not fulfilled	Detection that the CVM requirements were not fulfilled.
PTB	PIN on Terminal Bypass	The payment terminal has reported that PIN entry was bypassed for a high-value EMV contactless transaction.
PWE	Possible wedge attack	Detection of conditions indicating a possible wedge attack.
CRN	Consent requirement not fulfilled	Detection that wallet reported that no user consent was provided at time of the transaction

### **Checks with Decision Configurable by the Issuer—Fraud Control**

The issuer can soften (override) the Mastercard default setting during the issuer enablement/maintenance process:

<b>Code</b>	<b>Name</b>	<b>Short Description</b>
CAM	Invalid card authentication	Detection that the validation of the Mobile Device (MD) authentication cryptogram has failed.
DMM	Data mismatch	Detection of mismatch between information present in transaction data against information stored in the configuration of the token.
FUZ	Fuzzing	Detection of a fuzzing attack.  A fuzzing attack occurs when invalid, unexpected, or random data is intentionally provided as input to a payment application.
SKC	Key Compromised	Detection that a payment key was compromised.
REP	ATC Replay – Same UN	Detection of ATC replay.

<b>Code</b>	<b>Name</b>	<b>Short Description</b>
CCH	Cross Channel	Detection of use of payment application credentials outside of their intended purpose.
PKC	ODA compromised	Detection of compromise of ODA.

### **Checks with Decision Configurable by the Issuer—Token Authentication to Terminal**

The issuer can strengthen the Mastercard default setting during the issuer enablement/maintenance process:

<b>Code</b>	<b>Name</b>	<b>Short Description</b>
DAU	ODA was not performed	The payment terminal has reported that ODA was not performed.
DAF	ODA failed	The payment terminal has reported that ODA failed.

### **Check with Decision Configurable by the Issuer—Wallet Overrule**

The issuer can strengthen the Mastercard default setting during the issuer enablement/maintenance process:

<b>Code</b>	<b>Name</b>	<b>Short Description</b>
WOC	Wallet Overrule of Mastercard decision on CDCVM	Detection that a Wallet Overrule was made for the transaction. The mobile wallet overruled the advice of the Mastercard process running on the mobile device to consider the CDCVM as unsuccessful, and the mobile wallet decided to proceed with the transaction using that CDCVM.

## **Impact on the Issuer Decision Process**

This section describes how the version of MCBP impacts the issuer onboarding process and the decision process for both MDPS and the issuer.

### **Issuer Onboarding**

When using MCBP 1.0, a decision process applies using a legacy decision matrix that is defined **once only** during the initial issuer enablement process, as shown in the following screenshot of the issuer enablement interface (**MCBP 1.0**).

**NOTE: The MCBP 1.0 related values defined at time of issuer enablement for a given Mobile Wallet Application Account Range cannot be changed as part of the issuer maintenance process.**

**Authorization Processing Profile**

**MCBP 1.0**

Note: We will use the following settings when processing on-network Mastercard Cloud Based Payments and stand-in authorization messages. Any out-of-network transactions that fail any authorization will be declined with a response code 05 (Do Not Honor) to the alternative network, regardless of the settings below.

Mobile Device and User (Mobile PIN) Successfully Validated (MD and UMD Valid)	Continue Processing
Mobile Device Successfully Validated; User (Mobile PIN) not Successfully Validated due to Invalid Mobile PIN (MD Valid; UMD Invalid) *	Select Action
Mobile Device not Successfully Validated due to Invalid Device Cryptogram; User (Mobile PIN) Successfully Validated (MD Invalid; UMD Valid)	Decline
Mobile Device and User (Mobile PIN) not Successfully Validated due to Invalid Device Cryptogram and Invalid Mobile PIN (MD and UMD Invalid)	Decline
Impossible to validate cryptogram	Decline
Invalid TVR/CVR	Decline
ATC replay	Decline

**MCBP 2.0**

Note: You can adjust the Mastercard initial settings for how MDES Authorization system will process the token when it detects one or more of the following failures during Transaction Analysis checks:

- If Decline is selected MDES will decline the transaction if the discrepancy is found
- If Continue is selected MDES will route the transaction to the Issuer for an authorization decision

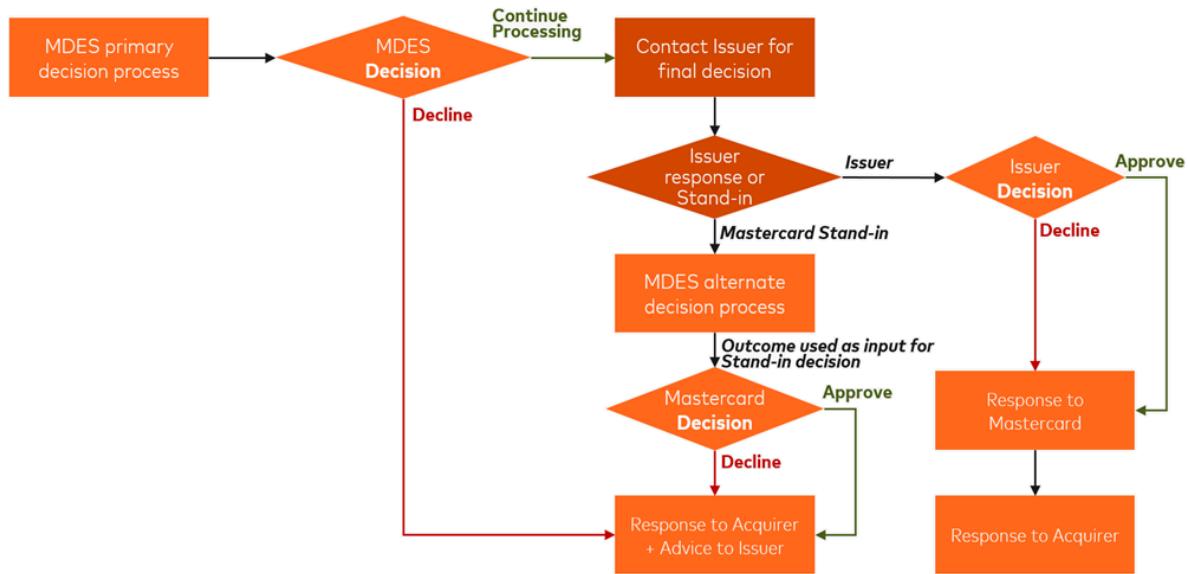
One or more failures detected in Cardholder Verification	Decline
One or more failures detected in Fraud Control	Decline
Token authentication to terminal (ODA) failed or not performed	Continue processing
Wallet overrule of Mastercard decision on CDCVM	Continue processing

When using MCBP 2.0, a decision process powered by MDES Transaction Analysis applies using a new decision matrix. A specific list of questions is defined during the issuer enablement process, as shown in the screenshot above (**MCBP 2.0**).

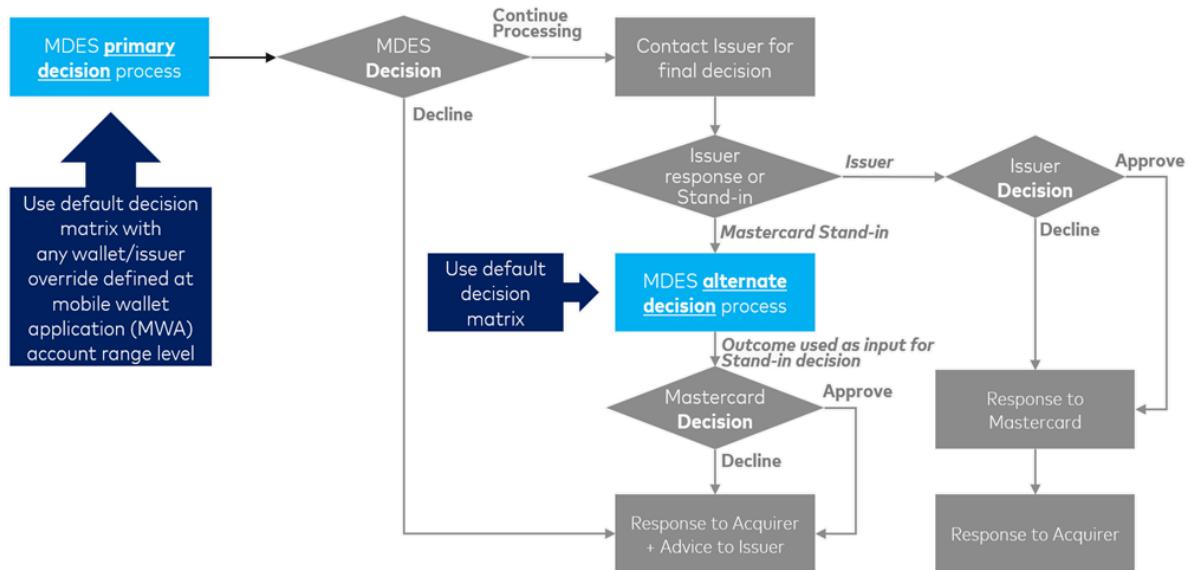
**NOTE: Even if the issuer is onboarding an account range for MCBP 2.0, there is a mandate to define the values for MCBP 1.0. Those values will be used in case the same account range is used for MCBP 1.0.**

## Decision Process

The following diagram shows the decision process when processing MCBP 2.0 transactions.

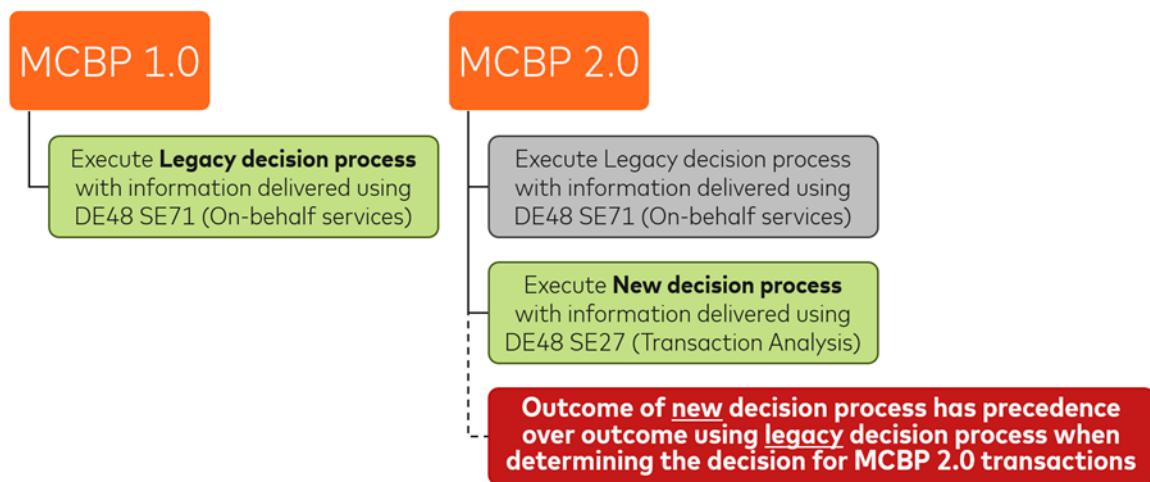


The following diagram highlights the use of the new decision matrix when processing MCBP 2.0 transactions.



For an MCBP 2.0 transaction, the processing decision generated by the Mastercard Authorization System takes into account the results of the new Transaction Analysis exclusively. The MCBP 1.0 decision process is still executed, but its outcome is ignored.

The following diagram shows the logic used for the decision process when using MCBP 1.0 versus MCBP 2.0.



### Impact on MDES and Issuer Decision

A transaction that could have been declined by the MCBP 1.0 decision process can lead to a 'continue processing' when using MCBP 2.0. For example, UMD cryptogram validation is *conditional* when using MCBP 2.0, whereas it was mandated when using MCBP 1.0 supporting only a CDCVM Always user experience.

The new Transaction Analysis aims to determine if the failed UMD validation is associated with "CDCVM was not performed." In practice, it means that an issuer can receive an authorization request containing DE 48 subelement 71 subfield 2 set to value 'P' (Valid MD AC; Invalid UMD AC) and decide to approve the transaction if DE 48 subelement 27 indicates that CDCVM was not performed. An LVT can be performed without an authentication of the cardholder in the context of a Card-Like or Flexible CDCVM user experience. The validation of the UMD cryptogram will fail in this situation, assuming that no CDCVM has been performed and no valid UMD cryptogram has been generated at the time of the transaction.

**NOTE: Issuers are strongly advised to use DE 48 subelement 27 when available (instead of relying solely on DE 48 subelement 71) to make a decision about the transaction (approve or decline).**

The issuer can also leverage Transaction Analysis to distinguish several use cases when, for example, using a wallet configured with a Flexible CDCVM user experience and Mobile PIN:

<b>Use Case</b>	<b>Data and Issuer Options</b>
Transaction performed without Mobile PIN	<p>DE 48 subelement 71 subfield 2 = P DE 48 subelement 27 subfield 2 to include 'OVU' ('OVP') Issuer can:</p> <ul style="list-style-type: none"> <li>• Use the Transaction Analysis Overview information to detect that some checks failed but continue processing with information (<b>CI</b>) is the outcome of the decision process</li> <li>• Approve the transaction (Response Code 00)</li> <li>• Decline for insufficient funds (Response Code 51)</li> <li>• Decline using their own hosted Lost &amp; Stolen risk management process (Response Code 65)</li> </ul>
Transaction performed with a valid Mobile PIN	<p>DE 48 subelement 71 subfield 2 = V or T DE 48 subelement 27 subfield 2 does not include 'OVU', 'OVP', 'OVF', or 'OVE' Issuer can approve the transaction (Response Code 00)</p>
Transaction performed with a wrong Mobile PIN	<p>DE 48 subelement 71 subfield 2 = P or M DE 48 subelement 27 subfield 2 to include 'OVF' (or 'OVE') Issuer can:</p> <ul style="list-style-type: none"> <li>• Leverage the issuer enablement process with the override of Mastercard decision for Cardholder Verification in order to use their own risk management process</li> <li>• Use the Transaction Analysis Overview information to detect that some checks failed and continue processing with warning (CW) is the outcome of the decision process</li> <li>• Decline the transaction and manage their own PIN Try Counter / PIN Try Limit (Response Code 89)</li> <li>• Decline the transaction as the PIN Try Counter is exceeded (Response Code 75)</li> </ul>

A wallet supporting a Card-Like user experience and Lost & Stolen countermeasure for LVTs can optionally report use of CDCVM as part of the transaction data. The issuer can use the results of the Transaction Analysis to determine whether CDCVM was performed in the context of Lost & Stolen. In that situation, the Transaction Analysis will **not** report that "CDCVM was not performed."

Another example is a DSRP transaction performed using a wallet configured to support MCBP 2.0 but not using UCAF Format 0+. Even if DE 48 subelement 71 subfield 2 may report a 'V' value, assuming that cryptographic validation is successful and CDCVM was performed for delivery of a valid UMD, this transaction will be always declined by Mastercard. When a format error is detected (that is, the use of an invalid UCAF Format), the new Transaction Analysis process triggers an 'FER' Test Result Code. It is associated with decline and Transaction Analysis Overview set to Decline Suspicious (DS).

## Recommendations for Issuers

It is important for issuers to integrate the information delivered using Transaction Analysis into their decision process. When token ranges are onboarded on wallets supporting MCBP 2.0, the decision process should not be focused solely on DE 48 subelement 71 subfield 2, but must consider the information delivered using DE 48 subelement 27 when it is provided.

**NOTE: There is no change in the processing of transactions performed using MCBP 1.0.**

The issuer must be aware that:

- A perfect transaction is a transaction without any failed checks.  
The authorization request for a perfect transaction does **not** contain DE 48 subelement 27.
- A transaction performed using a suspended token will not return DE 48 subelement 27.  
In this situation, the token to PAN mapping fails and no further cryptographic validation can be performed. Value 50U (MDES PAN Mapping—Unable to process) will be sent to the issuer as part of the Authorization Advice/0120 message.
- When processing transactions from an alternative network, the Mastercard Authorization System:
  - Does **not** deliver DE 48 subelement 27
  - Declines any transaction that is not a perfect transaction or a transaction with the Transaction Analysis Overview set to Continue with Information (CI)

## Chapter 14 Affiliate Range Information

*This section describes the Affiliate Range information that should be identified during issuer enablement.*

---

Affiliate Range Identification and Maintenance Obligation.....	228
Affiliate Range Process.....	228

## Affiliate Range Identification and Maintenance Obligation

If you are a Principal Customer with Affiliates, as part of your MDES obligations you must indicate your Affiliate Range information via the Affiliate Range process under Manage My company within Mastercard Connect™.

You must maintain this information on a go-forward basis so it remains accurate. This information is critical for Mastercard to help you complete your reporting obligations to some Wallet Providers. Additionally, the information is also used to provide a manual (select event) MDES "Affiliate Report" for the MDES fees, if your organization chose to receive the "Affiliate Billing Report."

Principal Customers should use the Affiliate Range process under Manage My Company within Mastercard Connect™ to update or validate their affiliate range information. Customers can use filters to select a BIN or just enter the BIN number directly. After a BIN is selected, the system displays existing affiliate range information for that BIN and allows the Principal to add, modify, or delete ranges.

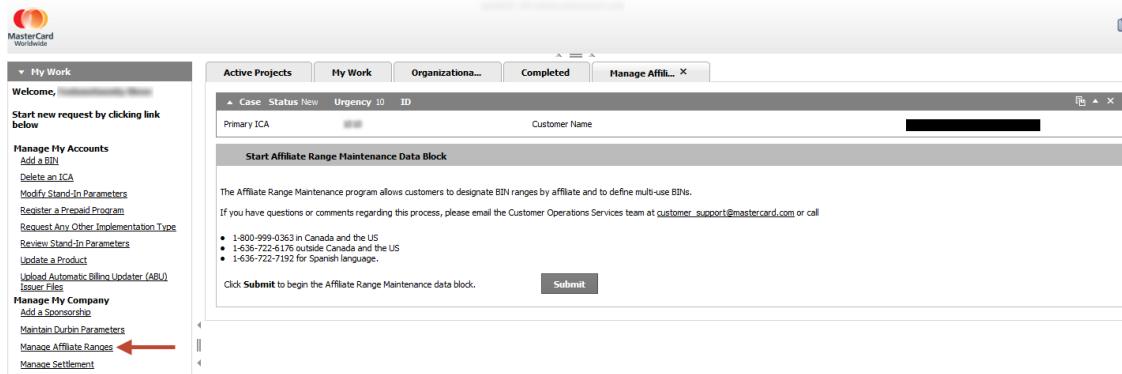
**NOTE: Token ranges may appear on the 'Affiliate Activity Report' in select cases, such as when a token cannot be mapped or there is a format error.**

## Affiliate Range Process

This section describes how to start the Affiliate Range process for Principal customers using MDES. After the initial setup, modifications can be made in the same manner.

### Procedure

1. Click **Manage Affiliate Ranges** link on the left-hand panel.



2. Click **Submit** to start the Affiliate Range process.

The Affiliate Range Maintenance program allows customers to designate BIN ranges by affiliate and to define multi-use BINs. If you have questions or comments regarding this process, please email the Customer Operations Services team at [customer\\_support@mastercard.com](mailto:customer_support@mastercard.com) or call:

- 1-800-999-0363 in Canada and the US
- 1-636-722-6176 outside Canada and the US
- 1-636-722-7192 for Spanish language.

Click Submit to begin the Affiliate Range Maintenance data block.

3. Click on each of the drop-down boxes to make a selection: **Select Brand**, **Select ICA**, **Select Country**, and **Select BIN**.

**Select BIN Filter**

The Select BIN Filter section can be used to narrow down the list of BIN that will be shown in the Select BIN field. You may select any or all of the various BIN filters or you can begin typing the desired BIN number in the Select BIN field below.

Select Brand: Please Select    Select ICA: Please Select    Select Country: Please Select

\* Select BIN: Please Select

Close    Save & Continue >>

4. Click **Save & Continue** after making all your selections.

**Select BIN Filter**

The Select BIN Filter section can be used to narrow down the list of BIN that will be shown in the Select BIN field. You may select any or all of the various BIN filters or you can begin typing the desired BIN number in the Select BIN field below.

Select Brand: MasterCard    Select ICA: [redacted]    Select Country: United States

\* Select BIN: Please Select

Close    Save & Continue >>

The account range for the BIN selected appears under the heading 'Affiliate Range.'

5. Click **Edit Range** on the right side of the screen.

The screenshot shows a software interface for managing affiliate ranges. At the top, there are tabs for 'Active Projects', 'My Work', 'Organization...', 'Completed', and 'Manage Affili...'. Below these are buttons for 'Case', 'Status New', 'Urgency 10', and 'ID'. A 'Customer Name' field is also present. The main area is titled 'Affiliate Range by BIN'. It includes a 'Select BIN Filter' section with dropdowns for 'Select Brand' (MasterCard), 'Select ICA' (with a blurred value), 'Select Country' (United States), and a 'Clear Filter' button. Below this is a 'Select BIN' dropdown with a blurred value. To the right is a 'Please Select' dropdown under 'Affiliate/Legal Name and Location\*' with a red arrow pointing to it. At the bottom are 'Close', 'Save & Continue >>', and 'Edit Range' buttons.

A list of Affiliate names appear in a drop-down box under the heading 'Affiliate/Legal Name and Location.'

6. Select the Affiliate Name in the drop-down box for which the account range is to be assigned.

This screenshot shows the same software interface as the previous one, but the 'Please Select' dropdown is now populated with a list of affiliate names, indicated by a blurred list. The rest of the interface elements are identical to the first screenshot.

7. After selecting, click **Save & Continue**.

8. A review screen appears. Review the changes and click **Submit**.

9. A request ID is assigned (for example, ARM-952). A final confirmation of the change appears in the 'Affiliate Range Detail' section.

U.S. Principal customers should continue to use the Maintain Durbin Parameters process under Manage My Company to manage affiliate ranges for their Durbin eligible BINs.

**NOTE: If you require the standard Mastercard Affiliate Billing Report for other products,  
continue to submit your Affiliate information to MCBS via Form 235.**

## Chapter 15 Fraud Information

*This section describes chargeback rules for MDES.*

---

Chargeback Rights Associated with Tokenized and DSRP Transactions.....	234
Mobile Contactless Transactions.....	234
DSRP Transactions.....	236
Partial Shipments and Recurring Payment Transactions.....	236

## Chargeback Rights Associated with Tokenized and DSRP Transactions

Tokenization does not introduce new chargeback reasons. A customer may initiate a chargeback for exactly the same reasons, and using the same procedures, as for transactions that do not contain tokenized account data.

However, in some instances, clarification of chargeback applicability is needed due to the introduction of new or different data values to support tokenization and the clarifications impact the fraud family of chargebacks. Other chargeback families (authorization, processing error, cardholder dispute) are not impacted by tokenization.

MDES performs token mapping throughout the lifecycle of a transaction, including dispute cycles if necessary, even if a token has been suspended or deactivated.

## Mobile Contactless Transactions

This section describes liability for mobile contactless transactions generated by the secure element of a mobile device or in the cloud (which may or may not involve tokenized account data and/or on-device cardholder verification methods [CVM] for chargeback message reason 4837 (No Cardholder Authorization), 4870 (Chip Liability Shift), and 4871 (Chip/PIN Liability Shift)).

### Mobile Contactless Transaction Liability

Reason	Merchant POS Terminal	Transaction Amount	CVM	Liability
4837	Dual capability POS Terminal	Any amount	Any CVM	Issuer
4870	Dual capability Hybrid POS Terminal	Any amount	Any CVM	Issuer (Contactless transactions cannot be charged back)
4871	Dual capability Hybrid POS Terminal	Equal to or less than contactless CVM limit	Any CVM	Issuer (Contactless transactions cannot be charged back if equal to or less than limit)
4871	Dual capability Hybrid POS Terminal	Greater than contactless CVM limit	Online PIN	Issuer
4871	Dual capability Hybrid POS Terminal with PayPass Version 3.X	Greater than contactless CVM limit	On-device CVM	Issuer

<b>Reason</b>	<b>Merchant POS Terminal</b>	<b>Transaction Amount</b>	<b>CVM</b>	<b>Liability</b>
4871	Dual capability Hybrid POS Terminal with <i>PayPass Version 3.X</i>	Greater than contactless CVM limit	Online PIN or CVM fallback to signature (for example, due to PIN bypass)	Issuer (POS Terminal prompts for PIN; cannot recognize that on-device CVM occurred or pass data indicating its success to issuer)
4871	Dual capability Hybrid POS Terminal with <i>PayPass Version 2.X</i> and offline PIN-only capability	Greater than contactless CVM limit	Signature	Issuer (U.S.-issued online PIN-only chip card used at offline PIN-only Hybrid POS Terminal cannot be charged back; outside U.S., PIN-preferring chip cards must support offline PIN)
4871	Dual capability Hybrid POS Terminal with <i>PayPass Version 2.X</i> and absent or non-working PIN pad	Greater than contactless CVM limit	Signature	Acquirer
4871	Contactless-only POS Terminal with <i>PayPass Version 2.X</i> and absent or non-working PIN pad	Greater than contactless CVM limit	Signature	Acquirer

**NOTE: Contactless-only POS terminals are typically unattended, follow CAT rules, and if deployed as a CAT 3 (limited amount terminal), have maximum transaction amounts equal to the CVM limit.**

Additional scenarios are as follows:

- Contactless-only device (no contact functionality) used at contact-only terminal—transaction cannot occur.
- Device with both contact and contactless functionality used at contact-only terminal—contact transaction may occur; liability shifts for such transactions apply.

### **Dynamic Magnetic Stripe Data Transactions**

Dynamic Magnetic Stripe Data transactions are electronically-captured token transactions, which include a dynamic cryptogram, and issuers should treat them the same way as contactless token transactions. Therefore, issuers cannot use the following message reason codes to charge back a Dynamic Magnetic Stripe Data transaction:

- 4837 (No Cardholder Authorization) when the transaction occurs at an attended terminal due to ‘you auth, you own’ rule
- 4870 (Chip Liability Shift) because of the dynamic cryptogram

## DSRP Transactions

This section identifies the limitations and uses of the chargebacks in the fraud family of chargebacks for DSRP transactions with full EMV data and with UCAF. All other families of chargebacks are available to the issuer to address valid non-fraud disputes.

Message Reason	Explanation	DSRP Transaction Liability
4837 (No Cardholder Authorization)	Used when a cardholder claims the sale was not made with their permission, or the permission of anyone authorized by the cardholder.	This code may not be used to chargeback DSRP transactions or transactions supported by an authorization with full UCAF.
4849 (Questionable Merchant Activity)	Used when a transaction occurs at a merchant location that is later identified in a fraud program, such as the Questionable Merchant Audit Program or the Global Merchant Audit Program.	This code may not be used to chargeback DSRP transactions or transactions supported by an authorization with full UCAF.
4863 (Cardholder Does Not Recognize—Potential Fraud)	Used when a cardholder does not recognize the merchant name for a card-not-present transaction.	This code may not be used to chargeback DSRP transactions or transactions supported by an authorization with full UCAF.
4870 (Chip Liability Shift)	Used in connection with the relative technologies of the cardholder device and the merchant POS terminal.	Not relevant to a DSRP transaction, which does not involve interaction with a POS terminal.
4871 (Chip/PIN Liability Shift)	Used in connection with the relative technologies of the cardholder device and the merchant POS terminal.	Not relevant to a DSRP transaction, which does not involve interaction with a POS terminal.

## Partial Shipments and Recurring Payment Transactions

With DSRP transactions, chip data is included in the original authorization, which provides issuers with as much information as a card-read EMV transaction would. As such, liability for fraud resides with the issuer, whether goods were shipped in their totality or partially—the same logic applies to EMV card-read transactions today.

When a merchant has multiple shipments to complete one order, the token from the first confirms that fraud chargebacks are not applicable for any shipment for the order. This is important as the subsequent shipment(s) may not be tokenized like the first. But while the

issuer may chargeback the second or third shipment as fraud, the merchant may return the chargeback showing the transaction was from the same tokenized order and remedy the fraud chargeback.

All non-fraud related chargeback reasons still apply (cardholder disputes, processing errors) in the event a merchant does not refund goods not shipped or returned.

## Chapter 16 Operational Management

*This section describes issuer operational management of MD&S.*

---

Customer Service Overview.....	239
Customer Support Model.....	240
Customer Service Tools.....	240
Customer Service Tools Functions.....	241
Issuer File Updates.....	242
Reporting.....	243
Changing Your Product Code.....	243

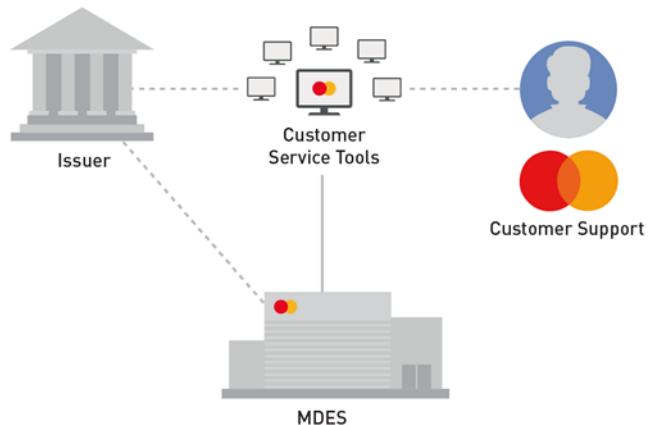
## Customer Service Overview

MDES includes Customer Service Tools that enable issuers to troubleshoot and resolve problems consumers may have when using MDES.

The Customer Service Tools provide functionality for use in addressing issues related to digitization, transaction processing, and lifecycle events. Issuers may opt to access the Customer Service Tools via the API or a hosted application. Issuers have access to the same information and actions regardless of the option they choose.

**NOTE: Mastercard Customer Service Tools are not intended to duplicate or replace functionality already implemented by issuers and Wallet Providers (for example, lost/stolen systems, workflow management, queuing systems, voice response [VR]).**

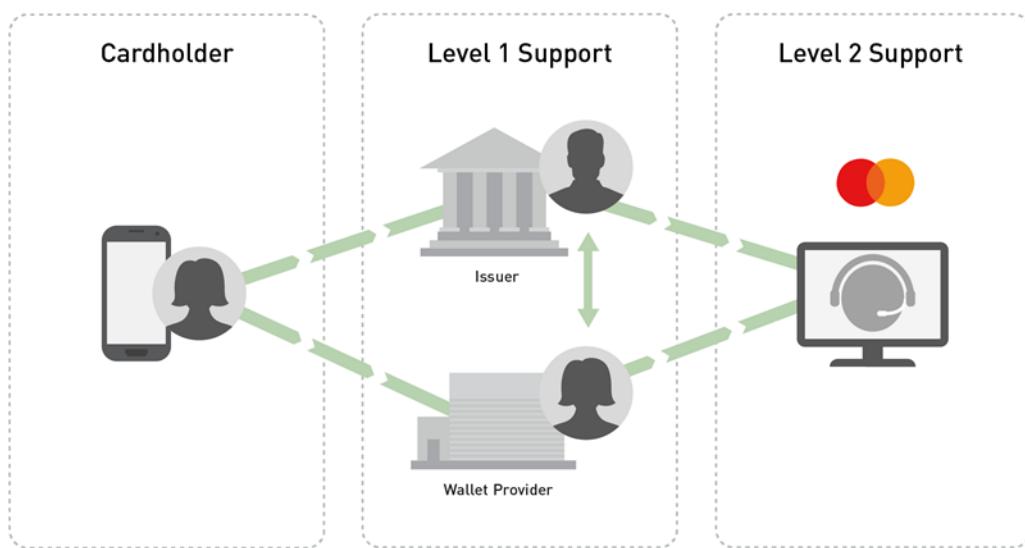
**Figure 32: Customer Service Application (Illustrative)**



## Customer Support Model

If cardholders experience issues with MDES, their first point of contact is the issuer or Wallet Provider.

**Figure 33: Customer Support Model Based on the Issuer and Wallet Provider Owning the Relationship with Cardholders (Illustrative)**



Issuers and Wallet Providers use the tools provided by Mastercard to resolve the problem and only contact Mastercard Customer Operations Services (COS) if they are unable to resolve it on their own.

## Customer Service Tools

The Mastercard Customer Service Application and Customer Service API are available for issuers, to help their representatives or agents address cardholder queries and tokenization issues. Issuers may opt to access the Mastercard application directly or integrate their own application with the API.

MDES Customer Service Tools are designed around a PAN-centric paradigm, where tokens are identified via the PAN or Token Unique Reference(s) and then managed accordingly. Issuers wishing to base customer service functionality around their own identifiers are advised to integrate with the MDES Customer Service API, and create links to the PAN(s) or Token Unique Reference(s) in the API client.

### Customer Service API

The Mastercard Customer Service API enables issuers to:

- Investigate and resolve cardholder issues

- Perform specific actions for cardholders, such as initiate re-provisioning
- Integrate their own support environment with MDES

Mastercard recommends that issuers integrate with the Customer Service Tools using the Customer Service API. The API provides a scalable approach for issuers to support their Customer Service representatives.

The Customer Service API is exposed through the Mastercard Developers site (<https://developer.mastercard.com/>). Issuers must have an account on the site. For account registration instructions and API integration guidelines, visit the site.

## **Customer Service Application**

The Mastercard Customer Service Application is a hosted service that enables issuers to:

- Investigate and resolve cardholder issues
- Perform specific actions for cardholders, such as initiate re-provisioning

The Customer Service Application is accessed through Mastercard Connect™ ([www.mastercardconnect.com](http://www.mastercardconnect.com)). Issuers using the Customer Service Application must have an account on Mastercard Connect™. New users must select the **Sign Up** option and follow the registration process. For the user registration process, refer to the Mastercard Connect™ issuer enablement document.

## **Customer Service Tools Functions**

The Customer Service Tools enable issuers to investigate and resolve cardholder issues and perform specific actions.

The tools support the following functions:

- Provide general system status
- Provide information on a digitization attempt
- Provide information on the status of a token
- Provide information on a device on which the token is digitized
- Provide information on tokens associated to a cardholder's account
- Provide token event history
- Provide token transaction history (last 30 days only)
- Add and retrieve comments
- Restart digitization of a token to a digital wallet
- Delete/deactivate a token
- Suspend and unsuspend (or resume) a token
- Resend an Activation Code
- Activate a token on behalf of a cardholder
- Update the Account PAN mapping information associated with a token
- Update Product Configuration (for example, Card Art)
- Reset Mobile PIN
- View and update the Token Assurance Level (via API only)

For more detailed tools information, refer to the *MDES—Customer Service Application User Guide* on the MDES Information Center on Publications in Mastercard Connect™ ([www.mastercardconnect.com](http://www.mastercardconnect.com)).

## Issuer File Updates

---

Issuers participating in MDES can submit updates to the PAN information associated with a token, as well as updating the token status.

The updates can be made using the following messages, which are both available on the Dual Message and Single Message System:

- Issuer File Update Request/0302 – Maintenance (Token/PAN Update) network messages
- Account Management System File Updates (Bulk File R311)

### PAN Information Updates

Issuers can make the following PAN information updates:

- Replace a PAN
- Replace a PAN expiration date
- Provide a Primary Account Card Sequence Number

These elements can be updated individually or together (in any combination).

When the PAN or PAN expiration date is being replaced, the issuer must indicate whether token mapping information should be updated and if the Wallet Provider or Token Requestor requires notification.

**NOTE: When an Account PAN is replaced, the new Account PAN must be within the same Account Range as the existing Account PAN.**

### Token Status Updates

Issuers can make the following token status updates:

- Deactivate token
- Suspend token
- Resume token

When a token status is updated, MDES is always updated accordingly and the Wallet Provider or Token Requestor is also notified.

Issuers may optionally submit updates to all tokens associated with a PAN or individual tokens. However, if issuers choose to update a single token, they must opt to receive Tokenization Complete Notification (TCN) network messages.

## Reporting

---

Several MDES reports are available for issuers participating in MDES. The reports provide filtered data about different aspects of their service, such as the Wallet Providers servicing their account ranges, tokenization counts, and transaction activity.

The following issuer reports are available:

- MDES Issuer Enablement Summary Report
- MDES Active Wallet Providers by Issuer Report
- MDES Issuer Service Summary Report
- MDES Digitization Report
- MDES Transaction Count by Point-of-Entry Report
- MDES Issuer Transaction Counts and Amount Report
- MDES Issuer Eligibility Decision Report
- MDES Token Activation Metrics Report
- MDES Provisioning Rules Report

These issuer reports are available in Microsoft® Excel and Portable Document Format (PDF) and can be accessed using the PortfolioAnalytics™ service (in Mastercard Connect™). For more information, refer to the *MDES—Issuer PortfolioAnalytics Reports* guide.

## Changing Your Product Code

---

If you have any queries about changing product codes, contact your Mastercard representative.

## Chapter 17 Testing Strategy

*This section provides an overview of the issuer testing and certification processes for MD&ES.*

---

Overview.....	245
Mastercard Test Facility Functions.....	246
Test Scripts—Dual and Single Message.....	246
Customer Service Tools Testing.....	246
Issuer Certification and Account PAN Whitelisting.....	247

## Overview

This section summarizes the parties with roles in the testing strategy for MDES and their responsibilities.

**NOTE: Issuers implementing their own Wallet Programs should refer to the *MDES—Wallet Provider Implementation Guide* for the testing requirements associated with participating in MDES as a Wallet Provider (rather than as an issuer onboarding to existing wallet programs participating in MDES).**

### Service Testing Overview—Parties Involved

- Mastercard—Provides MDES
- Issuer—Mastercard customer and Account PAN issuer
- Issuer/Issuer Processor—Processes the single messages and dual messages (authorization and clearing)

### Mastercard Simulators

Mastercard provides issuers with the ability to perform offline testing using the Mastercard Authorization Simulator, Mastercard Clearing Presentment Simulator, and the Mastercard Debit Financial Simulator. For more information, see the *Offline Validation Manual* and the *Testing and Validation Strategy Manual* on the Testing Reference Information Center on Publications.

### Network Interface Validation

Mastercard is responsible for the following:

- Configuring issuer parameters
- Delivering test environments as per MDES requirements
- Managing the testing process and providing a testing acknowledgment letter once complete

The issuer/issuer processor is responsible for implementing the required updates to the issuer's systems where required (refer to the Implementation chapter) to support the following:

- Pre-digitization messages (including Activation Code channel, if stipulated by the issuer)
- Single message and dual message interface updates to support the new fields required for contactless and DSRP
- Customer Service Testing requirements (Customer Service Application via Mastercard Connect™, or Customer Service API integration via the Mastercard Developers site)

## Mastercard Test Facility Functions

During issuer testing, the Mastercard Test Facility (MTF) acts as a counterpart acquirer, transmitting messages to the issuer's host and processing the network message responses.

When conducting integrated application testing and validation for dual message system operations, the MTF also ensures that all messages within a transaction lifecycle are compliant with the previous message in the lifecycle. This compliance monitoring is applied whether it is the issuer host or the MTF that initiates the transaction lifecycle.

In practice, this means that a message is not generated or accepted by the MTF if it is not in the correct sequence in the lifecycle. For example, a first chargeback may not precede a first presentment. Similarly, data and values in each message must be based on the contents of the preceding message.

An issuer's test systems are also expected to validate the consistency of messages and data in the transaction lifecycle. At the appropriate point, issuers must confirm to Mastercard that they successfully reconciled all transactions.

**NOTE: For pre-digitization message testing, the issuer/issuer processor must respond to either the Account Status Inquiry (ASI) for card eligibility or the Tokenization Authorization Request (TAR) within 1,200 milliseconds.**

## Test Scripts—Dual and Single Message

The testing scripts for dual and single message interface testing can be found in the Testing Reference Information Center on Mastercard Connect™.

The Testing Reference Information Center is located on Publications in Mastercard Connect™ ([www.mastercardconnect.com](http://www.mastercardconnect.com)). Testing issuers/processors should contact their Customer Implementation Services (CIS) representative for additional information.

Dual message and single message issuers/processors must successfully complete all test cases for magnetic stripe and chip products.

## Customer Service Tools Testing

Mastercard recommends that issuers perform testing using the issuer/processor-selected Customer Service Tools connectivity method (Customer Service API or Customer Service Application).

Although test cases are defined on a case-by-case basis with the issuer, emphasis should be placed on the following:

- Lifecycle management (resume, suspend, and delete token)
- Pre-digitization processes (including resuming provisioning)

---

For information on the Customer Service Tools, refer to Operational Management.

## Issuer Certification and Account PAN Whitelisting

Issuers should execute and pass Issuer Certification Testing for each and every account range/wallet combination.

The Issuer Certification Process applies when:

- New account ranges are added for wallets
- New wallets are added to existing account ranges

**NOTE: Issuer Certification and Testing must be passed before Account Range/Wallet combinations can be fully enabled for digitization requests.**

Issuer Account PAN Whitelisting requires the issuer to perform a set of tests in the production environment using a limited set of Account PANs (referred to as Whitelist Account PANs). Any digitization requests from other Account PANs outside of the Whitelist are blocked.

Issuers should provide Account PAN Whitelists for each new Account Range/Wallet combination intended for Issuer Certification Testing. Mastercard encourages issuers to do this as early as possible during the on-boarding process, ideally when initiating issuer enablement via Mastercard Connect™.

Once Account PAN Whitelists have been provided (and before Issuer Certification Testing completes), an issuer may use Mastercard Connect Issuer Maintenance to update the Account PAN Whitelists. Individual entries may be added, updated and deleted.

**NOTE: The removal of all Account PANs from an Account PAN Whitelist will not lead to a given Account Range/Wallet being enabled for full digitization. Mastercard must explicitly enable each Account Range/Wallet for full digitization, at which point the appropriate Account PAN Whitelist is automatically cleared and cannot be re-added.**

### Additional Resources

The following manuals can be accessed on Publications in Mastercard Connect™ ([www.mastercardconnect.com](http://www.mastercardconnect.com)):

- Testing and Validation Strategy (contains Network Interface Validation [NIV] testing information)
- Offline Validation Manual (contains NIV offline validation and tools information)
- Online Validation Manual (contains NIV online validation and tools information)

**NOTE: Support for this service may require the issuer/issuer processor to support MDES network messages. Issuers must ensure their processors are prepared to support the service profiles selected.**

## Chapter 18 Licensing

*This section describes the licensing and registration processes required for MDES.*

---

Licenses and Agreements.....	249
------------------------------	-----

## **Licenses and Agreements**

---

To use the services within MDES, issuers and issuer processors must agree to the MDES terms and conditions, as outlined in the article “Revised Standards for Tokenization and the Mastercard Digital Enablement Service,” *Global Operations Bulletin No. 8*, 1 August 2014.

### **Issuers Opting to Use MDES**

An issuer or issuer processor opting to use MDES has the opportunity during the issuer enablement process to accept the Rules and Standards relating to MDES. For more information, refer to the Issuer Enablement section.

## Appendix A Token Transaction Flows

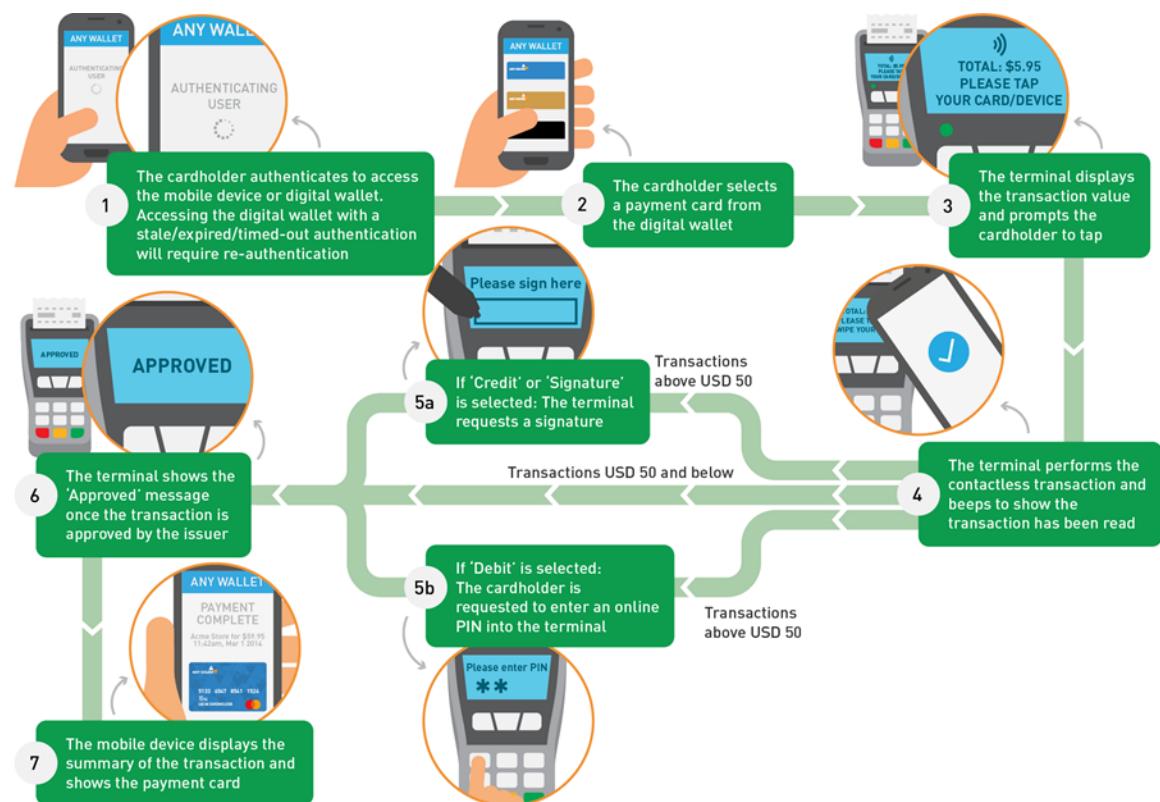
This appendix provides example token transaction flows with MDPS.

The following example transaction flows are shown:

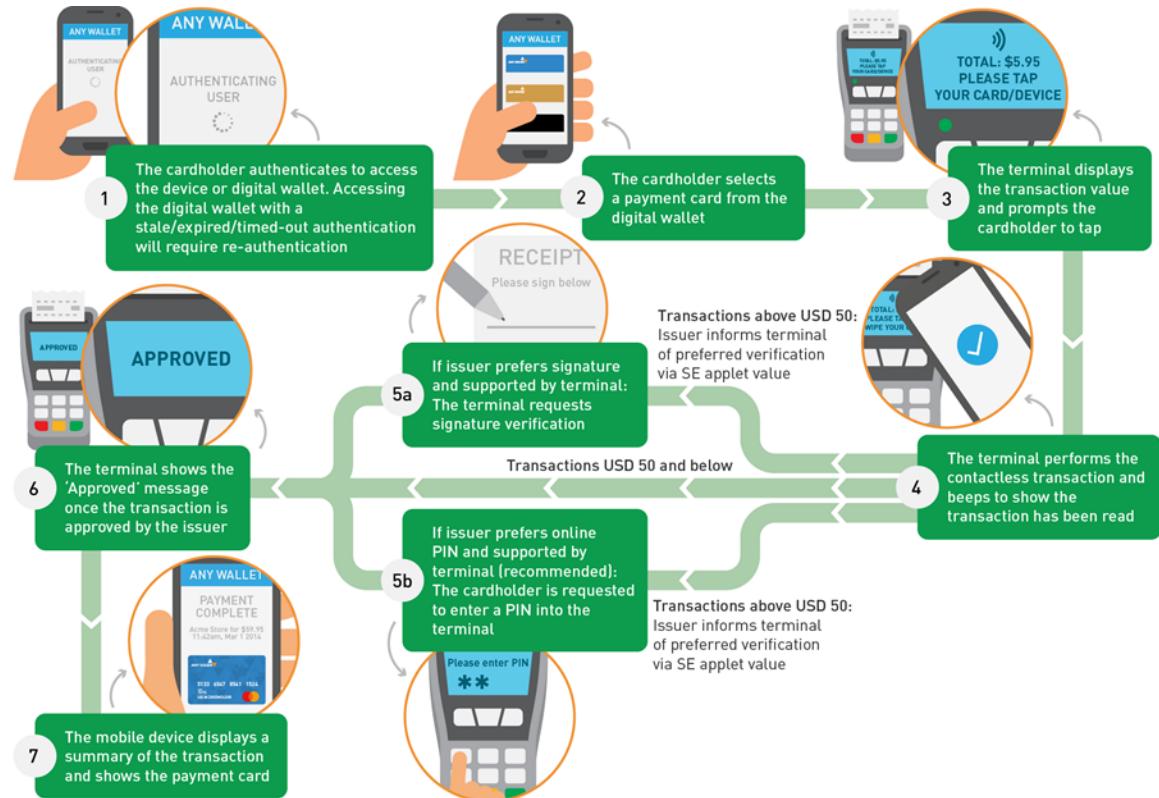
- U.S. Soft Limit Terminals
- EMV Soft Limit Terminals (Pre-V3 Terminal)
- V3 Terminals
- Hard Limit Terminals
- High-Value mPIN
- Mobile Debit Transaction—Mastercard Application Identifier (AID) selected by terminal (U.S. region-specific)

### U.S. Soft Limit Terminals

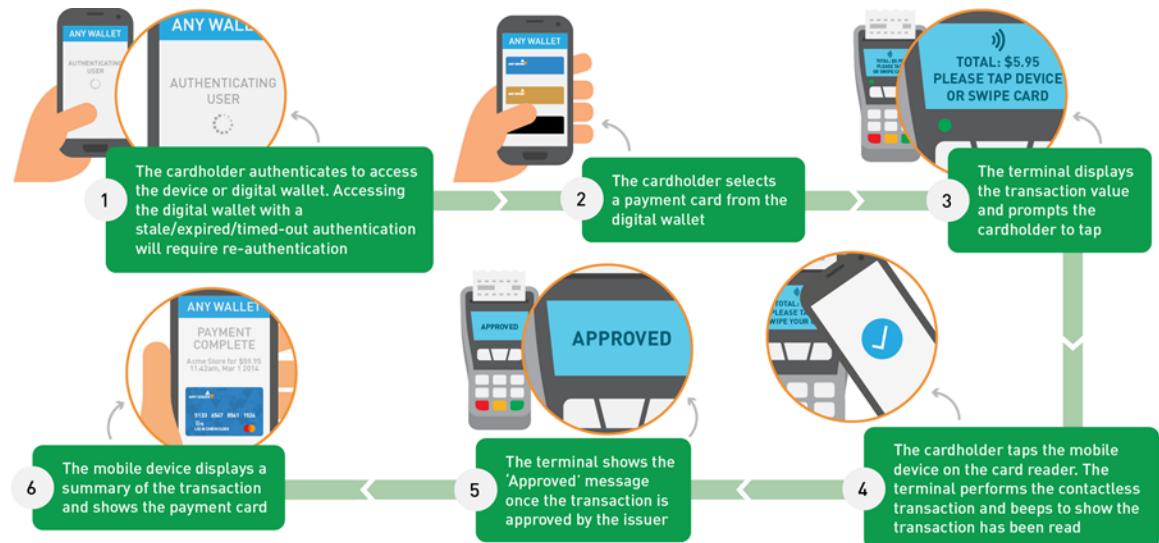
In ‘Soft Limit’ markets, the contactless-enabled terminal activates the contactless functionality for amounts both above and below the Terminal CVM Required limit, and the cardholder is asked to enter the mPIN, online PIN, or signature to complete the transaction. The majority of U.S. terminals are ‘soft limit’ terminals.



## EMV Soft Limit Terminals (Pre-V3 Terminal)



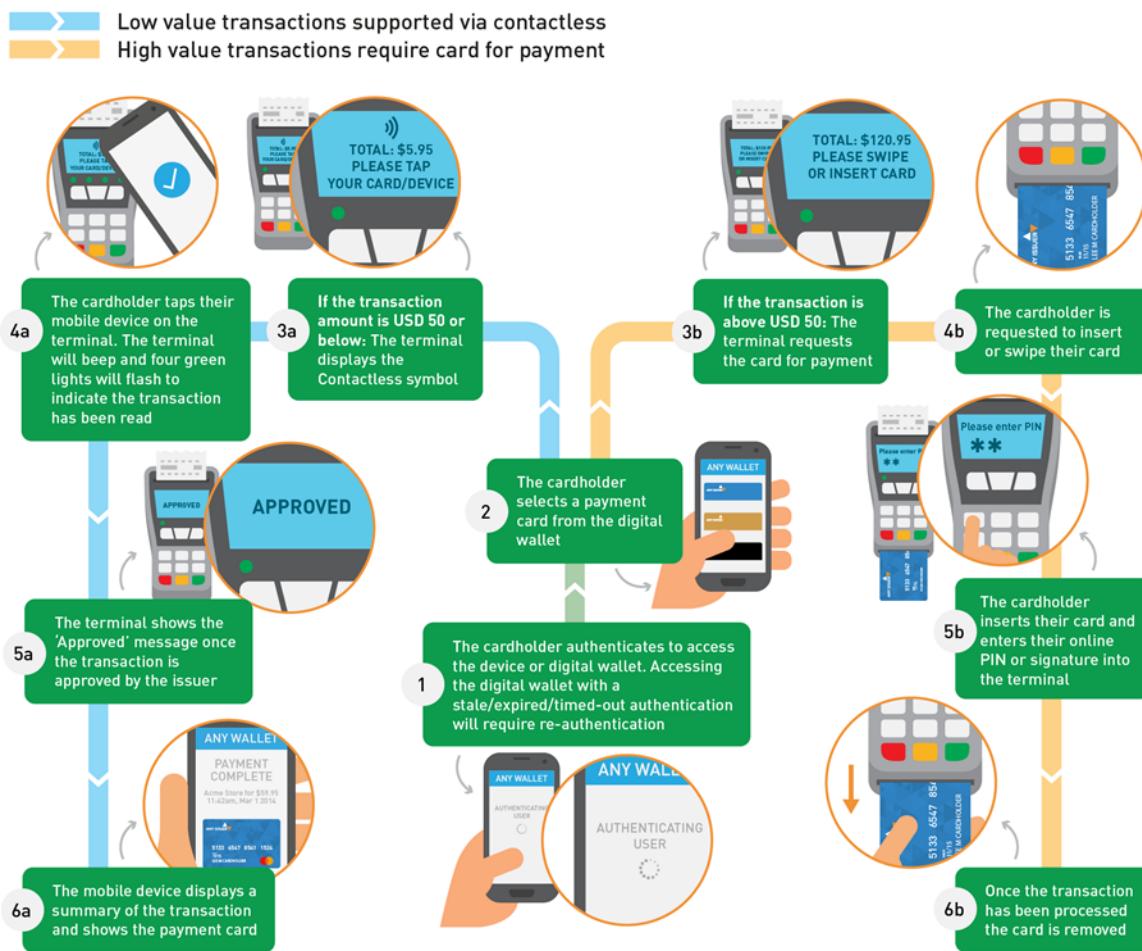
## V3 Terminals



## Hard Limit Terminals

'Hard Limit' markets are those in which the cardholder may be requested to insert the card into the reader and perform a contact transaction. In these instances, existing contactless-enabled terminals do not activate the contactless functionality above the Terminal CVM Required limit.

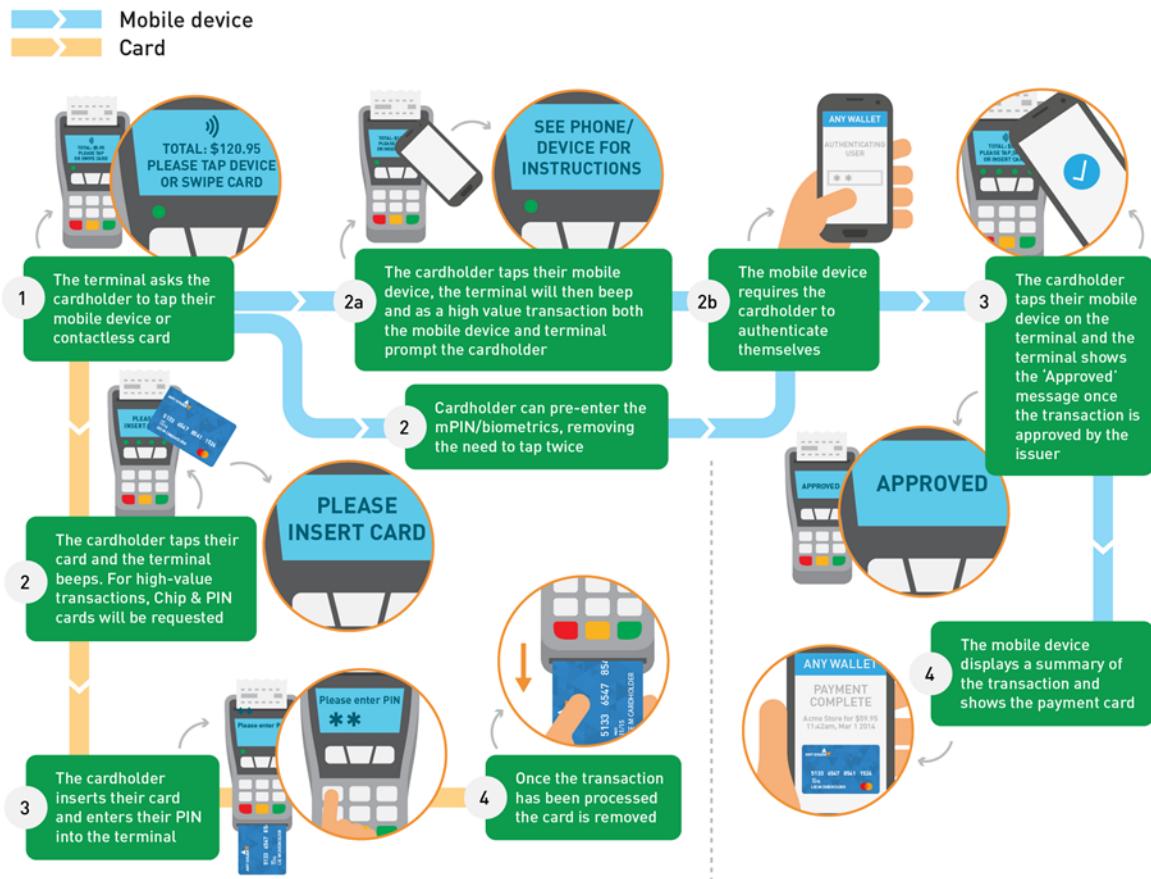
In this case, a mobile high-value transaction (HVT) is not possible, although transactions up to and including the CVM required limit are supported just as they are for contactless cards.



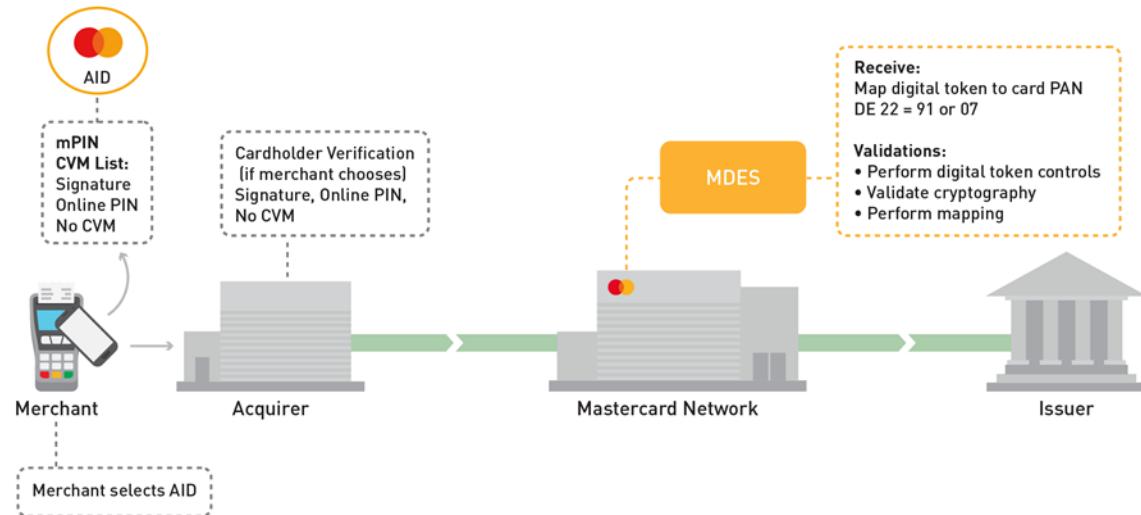
## High-Value mPIN

The following flow displays the sequence of events during a transaction that has an amount above the Cardholder Verification Method (CVM) limit.

**NOTE: This flow is only supported on terminals that support PayPass Version 3.0.**



### Mobile Debit Transaction—Mastercard Application Identifier (AID) selected by terminal (U.S. region-specific)



## Appendix B Transaction Analysis Technical Details

*This appendix provides detailed information about the new MDES Transaction Analysis service for tokenized transactions performed using MDES MCBP 2.0. For more general information, see the Transaction Analysis chapter.*

---

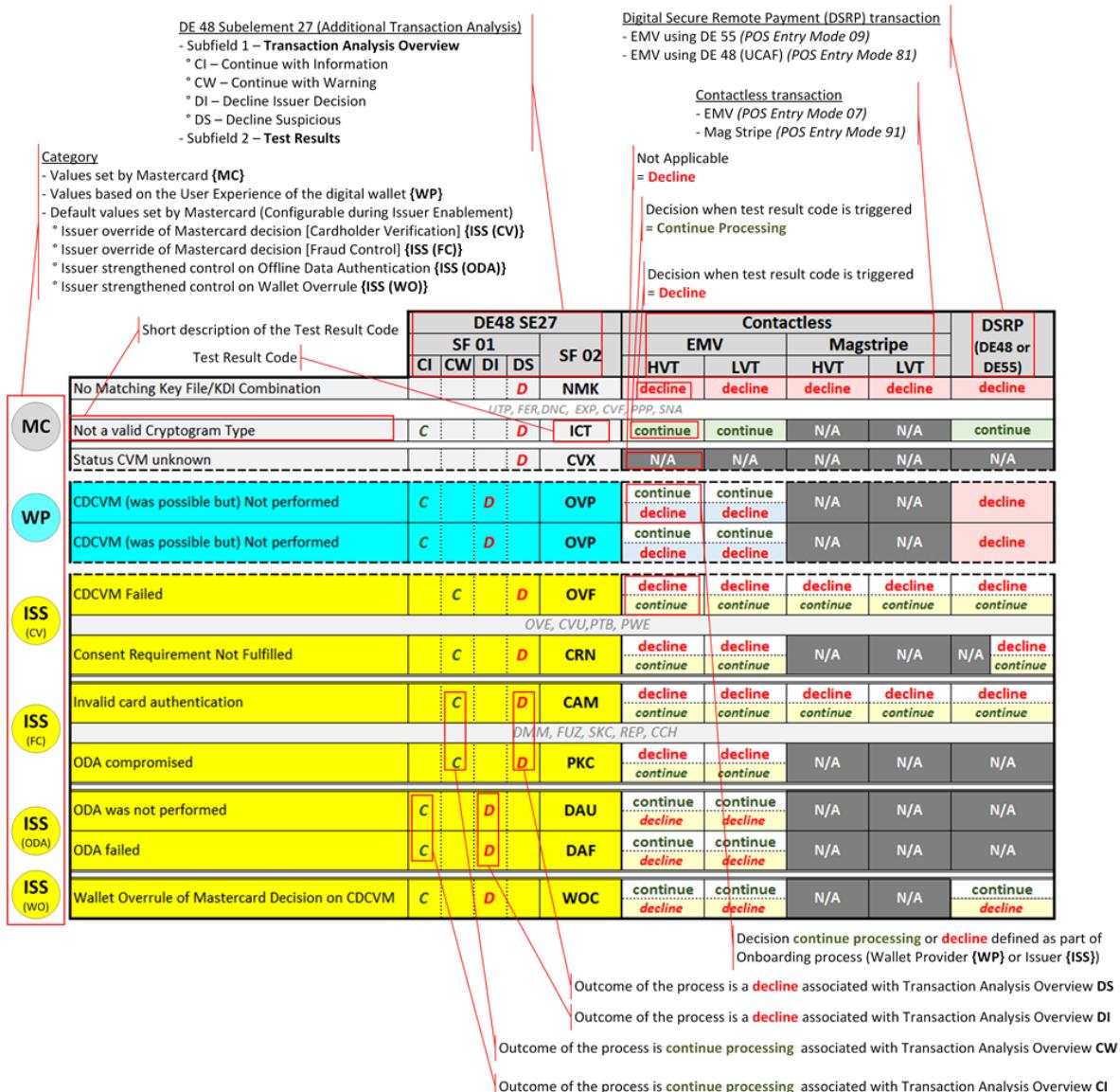
Overview.....	255
Decision Matrix Structure.....	256
Fixed Values Defined by Mastercard.....	259
Default Decision Matrix.....	259
Test Result Codes.....	259
Values Depending on the Wallet User Experience.....	262
Decision Matrix.....	262
Test Result Codes.....	262
Default Values Configurable by the Issuer.....	264
Issuer Override for Cardholder Verification.....	264
Issuer Override for Fraud Control.....	265
Issuer Strengthened Control on Token Authentication to Terminal.....	266
Issuer Strengthened Control on Wallet Overrule.....	267
Test Result Codes for Cardholder Verification.....	267
Test Result Codes for Fraud Control.....	272
Test Result Codes for Token Authentication to Terminal.....	276
Test Result Codes for Wallet Overrule.....	276

## Overview

Transaction Analysis is a process that combines a list of checks and a decision matrix used to determine the decision of the Mastercard Authorization System: whether the transaction must be declined or transaction processing should continue with the issuer or Stand-In processing.

The Transaction Analysis results are delivered to the issuer using DE 48 subelement 27.

The following diagram shows the decision matrix structure from a functional point of view.



**NOTE: For clarity, the diagram only shows a subset of the decision matrix; the entire content is provided in subsequent sections.**

## Decision Matrix Structure

The Decision Matrix contains multiple Test Result Codes, which can be grouped into six categories.

Category	Code	Name
<b>Fixed Values Defined by Mastercard</b>	NMK	No Matching Key File/KDI Combination
	UTP	Unable to process
	FER	Format error
	DNC	Data not consistent with application or product
	EXP	Token Expired
	CVF	Cardholder verification (on terminal) was not successful
	PPP	PIN Pad Problem
	SNA	Requested service not allowed for this product
	ICT	Not a valid Cryptogram Type
	CVX	Status CVM unknown
<b>Values Depending on the Wallet User Experience</b>	OVU	CDCVM Not Performed
	OVP	CDCVM (was possible but) not performed
<b>Default Values Configurable by the Issuer:</b> Issuer override of Mastercard default decision for Cardholder Verification	OVF	CDCVM Failed
	OVE	CDCVM retry exceeded – Token Suspended
	CVU	CVM Requirements not fulfilled
	PTB	PIN on Terminal Bypass
	PWE	Possible wedge attack
	CRN	Consent Requirement Not Fulfilled
<b>Default Values Configurable by the Issuer:</b> Issuer override of Mastercard default decision for Fraud Control	CAM	Invalid card authentication
	DMM	Data mismatch
	FUZ	Fuzzing
	SKC	Key Compromised
	REP	ATC Replay – Same UN
	CCH	Cross Channel
	PKC	ODA compromised

Category	Code	Name
<b>Default Values Configurable by the Issuer:</b> Issuer strengthened control on Token Authentication to Terminal	DAU	ODA was not performed
	DAF	ODA failed
<b>Default Values Configurable by the Issuer:</b> Issuer strengthened control on Wallet Overrule	WOC	Wallet Overrule of Mastercard Decision on CDCVM

A decision (**decline** or **continue processing**) is defined for each type of transaction that can be performed. The Transaction Analysis process uses the POS Entry Mode to determine the type of transaction:

- Contactless EMV (POS Entry Mode 07)
- Contactless Magnetic Stripe (POS Entry Mode 91)
- DSRP [using DE 55] (POS Entry Mode 09)
- DSRP [using DE 48 subelement 43 - UCAF] (POS Entry Mode 81)
- Credentials on File (POS Entry Mode 10)

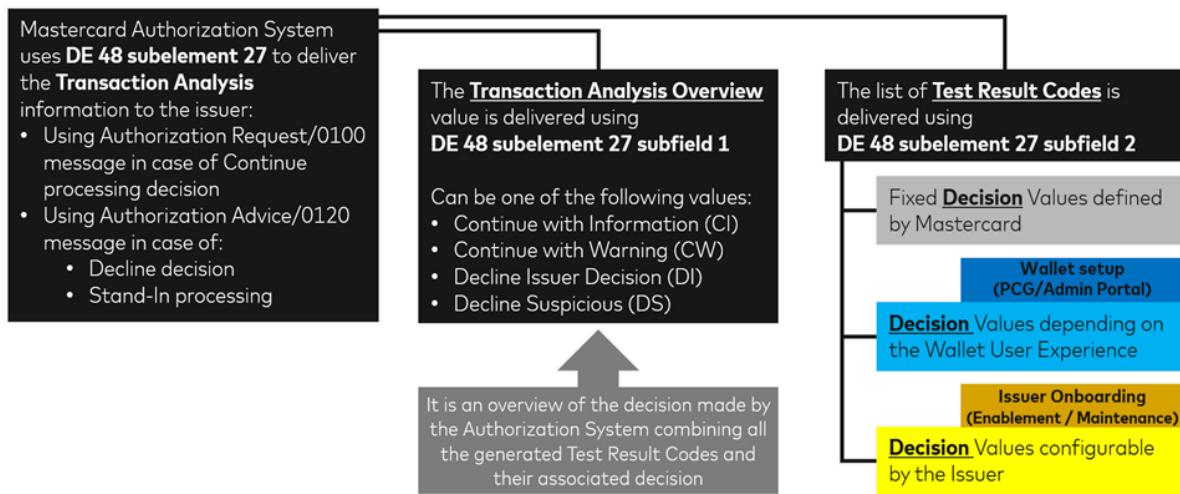
The granularity of the decision distinguishes low-value transaction (LVT) from high-value transaction (HVT).

**NOTE: When this information cannot be determined the Transaction Analysis process assumes it is an HVT.**

A value set to Not Applicable (**N/A**) means that the code is not expected to be triggered for this use case. In the situation it would be triggered anyway, the **N/A** value is associated with a **decline** in the decision matrix.

In addition to the associated decision of each code (**decline** or **continue processing**), the decision matrix also defines the value when the Transaction Analysis process must determine the outcome using the list of failed Test Result Codes. This information is delivered to the issuer using the Transaction Analysis Overview (DE 48 subelement 27 subfield 1) and can be one of the following:

- Continue with Information (**CI**)
- Continue with warning (**CW**)
- Decline Issuer Decision (**DI**)
- Decline Suspicious (**DS**)



A perfect transaction will not trigger a single Test Result Code and DE 48 subelement 27 will not be delivered to the issuer.

As soon as one Test Result Code is triggered, it is added to the list of Test Result Codes (delivered to the issuer using DE 48 subelement 27 subfield 2).

The decision process follows several rules:

- When a given Test Result Code is triggered more than once when analyzing a transaction, only one occurrence of the code will be present in the list of codes.
- As soon as one code associated with a **decline** is triggered, the final decision will be a **decline** regardless of the decisions associated with the other Test Result Codes.
- When setting the Transaction Analysis Overview value:
  - **CW** will prevail on any **CI** value
  - **DI** will prevail on any **CI** or **CW** values
  - **DS** will prevail on any **CI**, **CW** or **DI** values

## Fixed Values Defined by Mastercard

This section describes the default decision matrix and Test Result Codes for the values defined by Mastercard.

### Default Decision Matrix

The default decision matrix for **fixed** values defined by Mastercard is as follows.

	DE48 SE27				Contactless				DSRP (DE48 or DE55)	
	SF 01		SF 02		EMV		Magstripe			
	CI	CW	DI	DS	HVT	LVT	HVT	LVT		
No Matching Key File/KDI Combination				D	NMK	decline	decline	decline	decline	
Unable to process				D	UTP	decline	decline	decline	decline	
Format error				D	FER	decline	decline	decline	decline	
Data not consistent with application or product				D	DNC	decline	decline	N/A	N/A	
Token Expired	C			D	EXP	continue	continue	N/A	N/A	
Cardholder verification (on terminal) was not successful	C			D	CVF	continue	continue	N/A	N/A	
PIN Pad Problem	C			D	PPP	continue	continue	N/A	N/A	
Requested service not allowed for this product	C			D	SNA	continue	continue	N/A	N/A	
Not a valid Cryptogram Type	C			D	ICT	continue	continue	N/A	N/A	
Status CVM unknown				D	CVX	N/A	N/A	N/A	continue	

Those values cannot be configured and are used for the primary decision matrix but also for the alternative decision matrix that is used for Stand-In processing.

**NOTE: The CVX code is never triggered in the current implementation of MDES Transaction Analysis.**

### Test Result Codes

This section describes the Test Result Codes for the fixed values defined by Mastercard. The Test Result Codes are delivered to the issuer using DE 48 subelement 27 subfield 2.

#### NMK: No Matching Key File/KDI Combination

When using EMV-based transactions, the Key Derivation Index (KDI) is delivered as part of transaction data.

When using magnetic stripe transactions, the KDI value is stored on file.

There is a system-level check to validate that the value of the KDI in transaction data is known and matches the value defined in the configuration of the cryptographic material associated with the token. Any failure of this check adds the **NMK** code to the list of Test Result Codes.

Mastercard must have access to the cryptographic material to validate the transaction.

**NOTE: When there is no matching key file for the PAN, PAN expiry date and KDI combination, DE 48 subelement 71 subfield 2 is also set to value 'K'.**

### **UTP: Unable to Process**

The Mastercard Authorization System adds the **UTP** code to the list of Test Result Codes when the transaction cannot be processed as result of a fatal error detected in the transaction data.

### **FER: Format Error**

The Mastercard Authorization System checks the version of the UCAF format that is used when transacting with a token associated with the processing of MCBP 2.0 transactions.

Any failure to use UCAF format 0+ adds the **FER** code to the list of Test Result Codes. For information about UCAF formats, refer to *Digital Secure Remote Payments—UCAF Formats*, which is available from your Mastercard representative.

### **DNC: Data Not Consistent with Application or Product**

The Mastercard Authorization System checks if transaction data is consistent with the definition of the payment application or the product being used to perform a transaction.

When performing a contactless EMV transaction, the Terminal Verification Results (TVR) Byte 2 Bit 6 must be set (indicating Application not yet effective) by the payment terminal to report compliance with the MCBP product definition, using a specific setting of the Application Effective Date.

Any failure adds the **DNC** code to the list of Test Result Codes.

### **EXP: Token Expired**

The Mastercard Authorization System checks if the payment terminal has reported that the token is expired when performing a contactless EMV transaction.

If TVR Byte 2 Bit 7 is set (indicating Expired Application), the **EXP** code is added to the list of Test Result Codes.

### **CVF: Cardholder Verification (on Terminal) was Not Successful**

The Mastercard Authorization System checks if the payment terminal has reported that cardholder verification (on the terminal) was not successful when performing a contactless EMV transaction.

If TVR Byte 3 Bit 8 is set (indicating Cardholder verification was not successful), the **CVF** code is added to the list of Test Result Codes.

### **PPP: PIN Pad Problem**

The Mastercard Authorization System checks if the payment terminal has reported a problem with the PIN Pad when performing a contactless EMV transaction.

The **PPP** code is added to the list of Test Result Codes if all the following conditions are satisfied:

<b>Operator</b>	<b>Conditions</b>
AND	<b>None</b> of these are met: <ul style="list-style-type: none"> <li>• CDA was reported as performed and successful in transaction data (the check is done using TVR)</li> <li>• CDCVM was reported as successful (the check is done using Card Verification Results [CVR])</li> <li>• Online PIN block is present in the authorization request</li> </ul>
	Terminal Capabilities (EMV tag 9F33 in DE 55) is present and indicates that Online PIN is supported
	The CVM List associated with the Application Identifier (AID) used for the transaction indicates that Online PIN CVM rule precedes the Signature CVM Code
	TVR Byte 3 Bit 5 is set (indicating PIN entry required and PIN pad not present or not working)

### **SNA: Requested Service Not Allowed for this Product**

The Mastercard Authorization System checks if the payment terminal has reported that the requested service is not allowed for the given product when performing a contactless EMV transaction.

If TVR Byte 2 Bit 5 is set (indicating Requested service not allowed for card product), the **SNA** code is added to the list of Test Result Codes.

### **ICT: Not a Valid Cryptogram Type**

The Mastercard Authorization System checks if the EMV cryptogram type is an ARQC when performing an EMV-based transaction.

The validation is done using a control of the DE 48 subelement 71 subfield 2 (to check if value 'G' is reported) or checking the value of CVR Byte 1 Bit 6 and Bit 5 (indicating ARQC returned in the first generated AC).

Any failure to get an ARQC adds the **ICT** code to the list of Test Result Codes.

### **CVX: Status CVM Unknown**

The **CVX** code is defined to report that the status of the CVM cannot be determined.

**NOTE: This code is never triggered in the *current implementation of MDES Transaction Analysis.***

## Values Depending on the Wallet User Experience

This section describes the decision matrix and Test Result Codes for the values associated with user experience of the digital wallet.

### Decision Matrix

The default setting addresses the Card-Like and Flexible CDCVM user experiences. The decision matrix is as follows.

	DE48 SE27				Contactless				DSRP (DE48 or DE55)								
	SF 01				Magstripe												
	CI		CW		DI		DS			EMV		HVT		LVT			
	C		D				OVU			continue	continue	continue	continue	decline			
CDCVM Not Performed	C		D				OVU			continue	continue	N/A	N/A	decline			
CDCVM (was possible but) Not performed	C		D				OVP			continue	continue	N/A	N/A	decline			

When the wallet application is configured to support a CDCVM Always user experience for contactless transactions, the controls on CDCVM Not Performed are strengthened in the decision matrix at Mobile Wallet Application (MWA) account range level.

	DE48 SE27				Contactless				DSRP (DE48 or DE55)								
	SF 01				Magstripe												
	CI		CW		DI		DS			EMV		HVT		LVT			
	C		D				OVU			decline	decline	decline	decline	decline			
CDCVM Not Performed			D				OVU			decline	decline	N/A	N/A	decline			
CDCVM (was possible but) Not performed			D				OVP			decline	decline	N/A	N/A	decline			

### Test Result Codes

This section describes the Test Result Codes for the values that depend on the wallet user experience. The Test Result Codes are delivered to the issuer using DE 48 subelement 27 subfield 2.

#### OVU: CDCVM Not Performed

The Mastercard Authorization System checks if CDCVM was reported as not performed in transaction data.

The **OVU** code is added to the list of Test Result Codes if any of the following conditions are satisfied:

Operator	Conditions
OR	<p>For an EMV-based transaction (contactless or DSRP): CVR Byte 1 Bit 3 is not set (indicating that CDCVM was not performed)</p> <p>For a magnetic stripe transaction, <b>both</b> of these are met:</p> <ul style="list-style-type: none"><li>• nUN value is less or equal to 5 (no use of CDCVM reported by the POS device)</li><li>• Cryptographic validation reported an invalid UMD AC (DE 48 subelement 71 subfield 2 has value I, P or M):<ul style="list-style-type: none"><li>– I = Invalid MD AC and UMD AC</li><li>– P = Valid MD AC; Invalid UMD AC (Invalid Mobile PIN or failure of locally-verified CDCVM)</li><li>– M = Valid MD/Invalid UMD (PIN Try Count Reached)</li></ul></li></ul> <p>The logic deployed for magnetic stripe transactions integrates the lack of CDCVM-related information when using a POS device that is not compliant with Mastercard Contactless Reader Specification version 3. On a V3-compliant POS device, the nUN value less than or equal to 5 confirms that no CDCVM was performed on that device. There is an arbitrary decision by the Transaction Analysis engine to use the invalid UMD cryptogram as a sufficient condition to report that CDCVM was not performed when nUN is less than or equal to 5.</p>

### OVP: CDCVM (was possible but) Not Performed

The Mastercard Authorization System checks if CDCVM was reported as not performed in transaction data while the configuration of the token reports that CDCVM is supported for the type of transaction.

The **OVP** code is added to the list of Test Result Codes if both of the following conditions are satisfied for an EMV-based transaction:

- CVR Byte 1 Bit 3 is not set
- Application Interchange Profile (AIP) Byte 1 Bit 2 is set

## Default Values Configurable by the Issuer

This section describes the concept of issuer overrides and Test Result Codes for the values associated with Cardholder Verification, Fraud Control, Token Authentication to Terminal, and Wallet Overrule.

### Issuer Override for Cardholder Verification

The default setting of Mastercard controls on **Cardholder Verification** is as follows.

	DE48 SE27				Contactless				DSRP (DE48 or DE55)	
	SF 01		SF 02		EMV		Magstripe			
	CI	CW	DI	DS	HVT	LVT	HVT	LVT		
CDCVM Failed				D	OVF	decline	decline	decline	decline	decline
CDCVM retry exceeded - Token Suspended				D	OVE	decline	decline	decline	decline	decline
CVM Requirements not fulfilled		C		D	CVU	decline	continue	N/A	N/A	N/A
PIN on Terminal Bypass		C		D	PTB	decline	continue	N/A	N/A	N/A
Possible wedge		C		D	PWE	decline	continue	N/A	N/A	N/A
Consent Requirement Not Fulfilled				D	CRN	decline	decline	N/A	N/A	decline

The issuer has the option in the issuer enablement process to override this setting in order to avoid the transaction being declined by Mastercard when one or more Test Result Codes are triggered. That way the issuer can make its own decision with their risk management process using the list of Test Result Codes (delivered using DE 48 subelement 27 subfield 2) and the Transaction Analysis Overview (delivered using DE 48 subelement 27 subfield 1).

For example, under some conditions an issuer may want to approve a transaction using an invalid Mobile PIN or failure of locally-verified CDCVM (OVF will be raised) when the cardholder provided a valid Online PIN using the PIN Pad of the POS device while performing that transaction.

If the issuer uses the option to override the **Cardholder Verification** Mastercard setting, the decision matrix is set as follows at Mobile Wallet Application (MWA) account range level.

	DE48 SE27				Contactless				DSRP (DE48 or DE55)	
	SF 01		SF 02		EMV		Magstripe			
	CI	CW	DI	DS	HVT	LVT	HVT	LVT		
CDCVM Failed		C			OVF	continue	continue	continue	continue	continue
CDCVM retry exceeded - Token Suspended		C			OVE	continue	continue	continue	continue	continue
CVM Requirements not fulfilled		C		D	CVU	continue	continue	N/A	N/A	N/A
PIN on Terminal Bypass		C		D	PTB	continue	continue	N/A	N/A	N/A
Possible wedge		C		D	PTB	continue	continue	N/A	N/A	N/A
Consent Requirement Not Fulfilled		C		D	CRN	continue	continue	N/A	N/A	continue

Those changes (if any) apply to the primary decision matrix.

The alternative decision matrix that is used for Stand-In processing uses the default Mastercard setting in order to avoid approval of transactions that would most probably have been declined by the issuer as result of their risk analysis.

**NOTE: The issuer must be aware that this type of override has a direct impact on the security of the payment solution and it is assumed that the issuer will enable all the required controls on the transaction data and Transaction Analysis input when performing real-time approval of the transaction.**

When processing transactions from an alternative network, the Mastercard Authorization System will decline any transaction with the Transaction Analysis Overview set to Continue with Warning (CW).

It does mean that even if the issuer override is enabled, any trigger of the Test Result Codes (OVF, OVE, CVU, PTB or PWE) will lead to a declined transaction.

### Issuer Override for Fraud Control

The default setting of Mastercard controls on **Fraud Control** is as follows.

	DE48 SE27				Contactless				DSRP (DE48 or DE55)	
	SF 01		SF 02		EMV		Magstripe			
	CI	CW	DI	DS	HVT	LVT	HVT	LVT		
Invalid card authentication				D	CAM	decline	decline	decline	decline	
Data mismatch				D	DMM	decline	decline	decline	decline	
Fuzzing				D	FUZ	decline	decline	decline	decline	
Key Compromised				D	SKC	decline	decline	decline	decline	
ATC Replay - Same UN				D	REP	decline	decline	decline	decline	
Cross Channel				D	CCH	decline	decline	N/A	N/A	
ODA compromised				D	PKC	decline	decline	N/A	N/A	

The issuer has the option in the issuer enablement process to override this setting in order to avoid the transaction being declined by Mastercard when one or more Test Result Codes are triggered. That way the issuer can make its own decision with their risk management process using the list of Test Result Codes (delivered using DE 48 subelement 27 subfield 2) and the Transaction Analysis Overview (delivered using DE 48 subelement 27 subfield 1).

If the issuer uses the option to override the **Fraud Control** Mastercard setting, the decision matrix is set as follows at Mobile Wallet Application (MWA) account range level.

	DE48 SE27				Contactless				DSRP (DE48 or DE55)	
	SF 01		SF 02		EMV		Magstripe			
	CI	CW	DI	DS	HVT	LVT	HVT	LVT		
Invalid card authentication		C			CAM	continue	continue	continue	continue	continue
Data mismatch		C			DMM	continue	continue	continue	continue	continue
Fuzzing		C			FUZ	continue	continue	continue	continue	continue
Key Compromised		C			SKC	continue	continue	continue	continue	continue
ATC Replay - Same UN		C			REP	continue	continue	continue	continue	continue
Cross Channel		C	D		CCH	continue	continue	N/A	N/A	continue
ODA compromised		C	D		PKC	continue	continue	N/A	N/A	N/A

Those changes (if any) apply to the primary decision matrix.

The alternative decision matrix that is used for Stand-In processing uses the default Mastercard setting in order to avoid approval of transactions that would most probably have been declined by the issuer as result of their risk analysis.

**NOTE: The issuer must be aware that this type of override has a direct impact on the security of the payment solution and it is assumed that the issuer will enable all the required controls on the transaction data and Transaction Analysis input when performing real-time approval of the transaction.**

When processing transactions from an alternative network, the Mastercard Authorization System will decline any transaction with the Transaction Analysis Overview set to Continue with Warning (CW).

It does mean that even if the issuer override is enabled, any trigger of the Test Result Codes (CAM, DMM, FUZ, SKC, REP, CCH or PKC) will lead to a declined transaction.

### Issuer Strengthened Control on Token Authentication to Terminal

The default setting of Mastercard controls on **Token Authentication to Terminal** is as follows.

	DE48 SE27				Contactless				DSRP (DE48 or DE55)	
	SF 01		SF 02		EMV		Magstripe			
	CI	CW	DI	DS	HVT	LVT	HVT	LVT		
ODA was not performed	C		D		DAU	continue	continue	N/A	N/A	N/A
ODA failed	C		D		DAF	continue	continue	N/A	N/A	N/A

The issuer has the option in the issuer enablement process to strengthen the decision taken by Mastercard and decline transactions failing to perform a successful Offline Data Authentication (ODA).

If the issuer uses the option to strengthen the **Token Authentication to Terminal** Mastercard setting, the decision matrix is set as follows at Mobile Wallet Application (MWA) account range level.

	DE48 SE27				Contactless				DSRP (DE48 or DE55)	
	SF 01		SF 02		EMV		Magstripe			
	CI	CW	DI	DS	HVT	LVT	HVT	LVT		
ODA was not performed			D		DAU	decline	decline	N/A	N/A	N/A
ODA failed			D		DAF	decline	decline	N/A	N/A	N/A

Those changes (if any) apply to the primary decision matrix.

The alternative decision matrix that is used for Stand-In processing uses the default Mastercard setting, but any failure will regardless lead to a declined transaction when using the primary decision matrix. Stand-In processing will not apply in this situation.

## Issuer Strengthened Control on Wallet Overrule

The default setting of Mastercard controls on **Wallet Overrule** is as follows.

	DE48 SE27				Contactless				DSRP (DE48 or DE55)	
	SF 01		SF 02		EMV		Magstripe			
	CI	CW	DI	DS	HVT	LVT	HVT	LVT		
Wallet Overrule of Mastercard Decision on CDCVM	C		D		WOC	continue	continue	N/A	N/A	continue

The issuer has the option in the issuer enablement process to strengthen the decision taken by Mastercard regarding the overrule by the wallet and decline such transactions. A wallet overrule is defined as a decision by the mobile wallet to overrule the advice of the Mastercard process running on the mobile device to consider the CDCVM as unsuccessful, and to proceed with the transaction using that CDCVM.

If the issuer uses the option to strengthen the **Wallet Overrule** Mastercard setting, the decision matrix is set as follows at Mobile Wallet Application (MWA) account range level.

	DE48 SE27				Contactless				DSRP (DE48 or DE55)	
	SF 01		SF 02		EMV		Magstripe			
	CI	CW	DI	DS	HVT	LVT	HVT	LVT		
Wallet Overrule of Mastercard Decision on CDCVM			D		WOC	decline	decline	N/A	N/A	decline

Those changes (if any) apply to the primary decision matrix.

The alternative decision matrix that is used for Stand-In processing uses the default Mastercard setting, but any failure will regardless lead to a declined transaction when using the primary decision matrix. Stand-In processing will not apply in this situation.

## Test Result Codes for Cardholder Verification

This section describes the Test Result Codes for the default values defined by the issuer for Cardholder Verification. The Test Result Codes are delivered to the issuer using DE 48 subelement 27 subfield 2.

### OVF: CDCVM Failed

When using MCBP 2.0, the validity of the UMD cryptogram is conditional.

The Mastercard Authorization System checks if CDCVM was performed but the validation of the UMD cryptogram failed (CDCVM failed).

The **OVF** code is added to the list of Test Result Codes if both of the following conditions are satisfied:

Operator	Conditions
AND	<p><b>Either</b> of these are met:</p> <ul style="list-style-type: none"><li>• For an EMV-based transaction (contactless or DSRP) performed with CDCVM: CVR Byte 1 Bit 3 is set (indicating that CDCVM was performed)</li><li>• For a magnetic stripe transaction performed with CDCVM on a V3-compliant POS device: nUN value is greater than 5 (use of CDCVM reported by the POS device)</li></ul> <p>Cryptographic validation reported an invalid UMD AC (DE 48 subelement 71 subfield 2 has value I, P or M):</p> <ul style="list-style-type: none"><li>• I = Invalid MD AC and UMD AC</li><li>• P = Valid MD AC; Invalid UMD AC (Invalid Mobile PIN or failure of locally-verified CDCVM)</li><li>• M = Valid MD/Invalid UMD (PIN Try Count Reached)</li></ul>

The **OVF** (and **OVE**) code cannot be triggered for a magnetic stripe transaction performed on a non V3-compliant POS device, because there is no reliable information available in the transaction data to determine whether CDCVM was performed. On such a POS device, the invalid UMD cryptogram is not a sufficient condition to determine if CDCVM was performed.

### **OVE: CDCVM Retry Exceeded – Token Suspended**

The Mastercard Authorization System checks if CDCVM failed.

The **OVE** code is added to the list of Test Result Codes if all the following conditions are satisfied:

Operator	Conditions
AND	<p><b>Either</b> of these are met:</p> <ul style="list-style-type: none"><li>• For an EMV-based transaction (contactless or DSRP) performed with CDCVM: CVR Byte 1 Bit 3 is set (indicating that CDCVM was performed)</li><li>• For a magnetic stripe transaction performed with CDCVM on a V3-compliant POS device: nUN value is greater than 5 (use of CDCVM reported by the POS device)</li></ul> <p>Cryptographic validation generated the following value (also available in OBS Results delivered using DE 48 subelement 71 subfield 2), reporting that the UMD cryptogram validation failed: M = Valid MD/Invalid UMD (PIN Try Count Reached).</p> <p>The number of CDCVM failures has exceeded the threshold value defined in the Mastercard Authorization System for tokens associated with MCBP 2.0. The token has to be suspended when the PIN Try Counter (PTC) exceeds the PIN Try Limit (PTL).</p>

The **OVE** (and **OVF**) code cannot be triggered for a magnetic stripe transaction performed on a non V3-compliant POS device, because there is no reliable information available in the transaction data to determine whether CDCVM was performed. On such a POS device, the invalid UMD cryptogram is not a sufficient condition to determine if CDCVM was performed.

### **CVU: CVM Requirements Not Fulfilled**

The Mastercard Authorization System checks if CVM requirements were not fulfilled in the context of a contactless EMV transaction.

The **CVU** code is added to the list of Test Result Codes if all the following conditions are satisfied:

<b>Operator</b>	<b>Conditions</b>
AND	<p>Contactless EMV transaction: POS Entry Mode equal to 07</p> <p>Terminal Capabilities (EMV tag 9F33 in DE 55) and CVM Results (EMV tag 9F34 in DE 55) are present in transaction data</p> <p>Identify HVT using Terminal Capabilities and CVM Results—<b>either</b> of these are met:</p> <ul style="list-style-type: none"> <li>• Terminal Capabilities Byte 2 Bit 4 (No CVM Required) is not set</li> <li>• Check CVM Result (No report of 'No CVM'): CVM Results Byte 1 is not equal to 1F and CVM Results Byte 1 is not equal to 3F</li> </ul> <p>Check if CDCVM was not performed or failed, and no other CVM was done on the POS device—<b>both</b> of these are met:</p> <ul style="list-style-type: none"> <li>• One of the following codes is present in the list of Test Result Codes: <ul style="list-style-type: none"> <li>– OVU (CDCVM Not performed)</li> <li>– OVF (CDCVM Failed)</li> <li>– OVE (CDCVM retry exceeded – Token suspended)</li> </ul> </li> <li>• "No CVM" was used—CVM Results Byte 1 is equal to 1F or is equal to 3F</li> </ul>

### **PTB: PIN on Terminal Bypass**

The Mastercard Authorization System checks if the payment terminal has reported a PIN Bypass when performing a contactless EMV transaction.

The **PTB** code is added to the list of Test Result Codes if all the following conditions are satisfied:

<b>Operator</b>	<b>Conditions</b>
AND	<p><b>None</b> of these are met:</p> <ul style="list-style-type: none"> <li>• CDA was reported as performed and successful in transaction data (the check is done using TVR)</li> <li>• CDCVM was reported as successful (the check is done using CVR)</li> <li>• Online PIN block is present in authorization request</li> </ul> <p>Terminal Capabilities (EMV tag 9F33 in DE 55) is present and indicates that Online PIN is supported</p> <p>The CVM List associated with the AID used for the transaction indicates that the Online PIN CVM rule precedes the Signature CVM Code</p> <p>TVR Byte 3 Bit 4 is set (indicating PIN entry required, PIN pad present, but PIN was not entered)</p>

## PWE: Possible Wedge Attack

The Mastercard Authorization System checks conditions indicating a possible wedge attack.

The **PWE** code is added to the list of Test Result Codes if all the following conditions are satisfied:

Operator	Conditions
AND	<b>None</b> of these are met: <ul style="list-style-type: none"><li>• CDA was reported as performed and successful in transaction data. The check is done using:<ul style="list-style-type: none"><li>– CVR Byte 2 Bit 7 (indicating CDA was performed)</li><li>– TVR Byte 1 Bit 8 (indicating Cardholder verification was not successful)</li><li>– TVR Byte 1 Bit 3 (indicating Online PIN entered)</li></ul></li><li>• CDCVM was reported as successful (the check is done using CVR Byte 1 Bit 1)</li><li>• Online PIN block is present in authorization request</li></ul>
	CVM Results Byte 1 is equal to one of these values: 0x01, 0x03, 0x04, 0x05
	OVU (CDCVM Not Performed) is present in the list of Test Result Codes

## CRN: Consent Requirement Not Fulfilled

The Mastercard Authorization System checks if the wallet has reported that the consent requirement was not fulfilled during a Contactless EMV transaction or a DSRP transaction using DE 55.

Mastercard rules mandate consumer consent to any MCBP transaction. A consent can be explicit (such as press a button) or implicit (that is, derived from several parameters or automatically provided when using instant CDCVM). Any failure to receive consumer consent to a transaction is carried in transaction data.

If CVR Byte 6 Bit 4 is set, the **CRN** code is added to the list of Test Result Codes.

**NOTE: Mastercard has added the CRN code to the list of codes supported in the existing question about Cardholder Verification. On 12 June 2018, Mastercard will automatically update any existing issuer override (Cardholder Verification) defined for tokens already configured in the system (production environment) so that the issuer does not need to take any specific action to update their existing configuration.**

## Test Result Codes for Fraud Control

This section describes the Test Result Codes for the default values defined by the issuer for Fraud Control. The Test Result Codes are delivered to the issuer using DE 48 subelement 27 subfield 2.

### CAM: Invalid Card Authentication

The Mastercard Authorization System checks if the validation of the Mobile Device Authentication (MD) cryptogram failed.

The **CAM** code is added to the list of Test Result Codes if cryptographic validation reported an invalid MD cryptogram (DE 48 subelement 71 subfield 2 has value I or L):

- I = Invalid MD AC and UMD AC
- L = Invalid MD AC/Valid UMD AC

### DMM: Data Mismatch

The Mastercard Authorization System checks if there is any mismatch between values stored on file and values provided in transaction data.

The **DMM** code is added to the list of Test Result Codes if either of the following conditions are satisfied:

Operator	Conditions
OR	<p>For an EMV-based transaction, the following values <b>do not match</b>:</p> <ul style="list-style-type: none"><li>• Cryptogram Version Number (CVN) value provided in transaction data, <b>either</b> in:<ul style="list-style-type: none"><li>– Issuer Application Data (EMV tag 9F10) when using contactless EMV or DSRP (with DE 55)</li><li>– UCAF Format 0+ when using DSRP (with DE 48)</li></ul></li><li>• CVN value stored in the card profile of the token used to perform the EMV-based transaction</li></ul> <p>For a magnetic stripe transaction, the following values <b>do not match</b>:</p> <ul style="list-style-type: none"><li>• nUN value provided in transaction data <b>or</b> (nUN - 5) if nUN is greater than 5</li><li>• nUN value defined in the card profile of the token used to perform the magnetic stripe transaction</li></ul>

## FUZ: Fuzzing

The Mastercard Authorization System supports several methods to detect fuzzing.

A fuzzing attack occurs when invalid, unexpected, or random data is intentionally provided as input to a payment application. Attackers use this method in an attempt to better understand the capabilities of the application or to determine weaknesses of data input validations in order to alter the behavior of the system or choose a channel for attack.

The **FUZ** code is added to the list of Test Result Codes if any of the following conditions are satisfied:

<b>Operator</b>	<b>Conditions</b>
OR	<p>Suspicious behavior with validation of ODA:</p> <ul style="list-style-type: none"> <li>• Retrieve the following values from the transaction data (DE 55):           <ul style="list-style-type: none"> <li>– TVR using EMV tag 95</li> <li>– CVR included in Issuer Authentication data using EMV tag 9F10</li> <li>– AID using EMV tag 84</li> <li>– AIP using EMV tag 82</li> </ul> </li> <li>• ODA results are inconsistent—<b>both</b> of these are met:           <ul style="list-style-type: none"> <li>– TVR Byte 1 Bit 8 is set (indicating ODA was not performed)</li> <li>– CVR Byte 2 Bit 7 is not set (indicating CDA was not performed)</li> </ul> </li> <li>• Match found between AIP value on file for the token and the AIP in transaction data:           <ul style="list-style-type: none"> <li>– If AID value is present in DE 55, search for a matching record for the POS Entry Mode <b>and</b> AID values used in the transaction</li> <li>– If AID is not present, search for a matching record for the POS Entry Mode</li> </ul> <p>A matching record is defined as the AIP value found in the list of AIP values defined for the token used to perform the transaction.</p> </li> <li>• OBS Results delivered using DE 48 subelement 71 subfield 2 is <b>not</b> equal to value 'V' (Valid cryptogram)</li> </ul>
	<p>Invalid (Random) Application Transaction Counter (ATC) used for the transaction: OBS Results delivered using DE 48 subelement 71 subfield 2 is equal to value 'D' (Invalid ATC)</p>
	<p>ATC replay with different Unpredictable Number (UN) and not a valid cryptogram: OBS Results delivered using DE 48 subelement 71 subfield 2 is not equal to values 'E' and 'V'</p>
	<p>Non-matching AIP:</p> <ul style="list-style-type: none"> <li>• Retrieve the following values from transaction data (DE 55):           <ul style="list-style-type: none"> <li>– AIP using EMV tag 82</li> <li>– AID using EMV tag 84</li> </ul> </li> <li>• <b>No</b> match found between the AIP value on file for the token and the AIP in transaction data:           <ul style="list-style-type: none"> <li>– If AID value is present in DE 55, search for a matching record for the POS Entry Mode <b>and</b> AID values used in the transaction</li> <li>– If AID is not present, search for a matching record for the POS Entry Mode</li> </ul> <p>A matching record is defined as the AIP value found in the list of AIP values defined for the token used to perform the transaction.</p> </li> <li>• OBS Results delivered using DE 48 subelement 71 subfield 2 is equal to value 'I' (Invalid cryptogram)</li> </ul>

## **SKC: Key Compromised**

The Mastercard Authorization System supports several methods to detect that a payment key was compromised.

The **SKC** code is added to the list of Test Result Codes if either of the following conditions are satisfied:

<b>Operator</b>	<b>Conditions</b>
OR	<p>ATC replay with different Unpredictable Number (UN) and valid cryptogram—<b>both</b> of these are met:</p> <ul style="list-style-type: none"> <li>• ATC replay is detected (OBS Results delivered using DE 48 subelement 71 subfield 2 is equal to value 'E') with a different UN</li> <li>• Cryptographic validation was successful</li> </ul> <hr/> <p>Non-matching AIP but valid cryptogram—<b>any</b> of these are met:</p> <ul style="list-style-type: none"> <li>• Retrieve the following values from transaction data (DE 55): <ul style="list-style-type: none"> <li>– AIP using EMV tag 82</li> <li>– AID using EMV tag 84</li> </ul> </li> <li>• <b>No</b> match found between the AIP value on file for the token and the AIP in transaction data: <ul style="list-style-type: none"> <li>– If AID value is present in DE 55, search for a matching record for the POS Entry Mode <b>and</b> AID values used in the transaction</li> <li>– If AID is not present, search for a matching record for the POS Entry Mode</li> </ul> <p>A matching record is defined as the AIP value found in the list of AIP values defined for the token used to perform the transaction.</p> </li> <li>• OBS Results delivered using DE 48 subelement 71 subfield 2 is equal to value 'V' or 'T'</li> </ul>

## **REP: ATC Replay – Same Unpredictable Number (UN)**

The Mastercard Authorization System checks if ATC is replayed with a previously-recorded Unpredictable Number (UN) value.

The **REP** code is added to the list of Test Result Codes if ATC replay is detected (OBS Results delivered using DE 48 subelement 71 subfield 2 is equal to value 'E') using a known UN.

## **CCH: Cross Channel**

The Mastercard Authorization System checks if payment application credentials (such as AIP value) were detected as being used outside of their intended purpose, for example data defined for a contactless EMV transaction was used in a DSRP transaction.

The **CCH** code is added to the list of Test Result Codes if either of the following conditions are satisfied:

<b>Operator</b>	<b>Conditions</b>
OR	<p>Retrieve the following values from the transaction data (DE 55):</p> <ul style="list-style-type: none"> <li>• AIP using EMV tag 82</li> <li>• AID using EMV tag 84</li> </ul> <p>Any match found between the AIP value on file and the AIP in transaction data, but <b>not</b> for the POS Entry Mode used for the transaction:</p> <ul style="list-style-type: none"> <li>• If AID value is present in DE 55, search for a matching record for the AID value used in the transaction <b>and</b> any POS Entry Mode</li> <li>• If AID is not present, search for a matching record for the POS Entry Mode</li> </ul> <p>A matching record is defined as the AIP value found in the list of AIP values defined for the token used to perform the transaction.</p>

### **PKC: ODA Compromised**

The **PKC** code is added to the list of Test Result Codes if all the following conditions are satisfied:

<b>Operator</b>	<b>Conditions</b>
AND	<p>Retrieve the following values from the transaction data (DE 55):</p> <ul style="list-style-type: none"> <li>• TVR using EMV tag 95</li> <li>• CVR included in Issuer Authentication data using EMV tag 9F10</li> <li>• AID using EMV tag 84</li> <li>• AIP using EMV tag 82</li> </ul> <p>Inconsistency with ODA—<b>both</b> of these are met:</p> <ul style="list-style-type: none"> <li>• TVR Byte 1 Bit 8 is not set (indicating ODA was performed)</li> <li>• CVR Byte 2 Bit 7 is not set (indicating CDA was not performed)</li> </ul> <p>Match found between the AIP value on file and the AIP in transaction data:</p> <ul style="list-style-type: none"> <li>• If the AID value is present in DE 55, search for a matching record for the POS Entry Mode <b>and</b> AID values used in the transaction</li> <li>• If the AID is not present, search for a matching record for the POS Entry Mode</li> </ul> <p>A matching record is defined as the AIP value found in the list of AIP values defined for the token used to perform the transaction.</p> <p>OBS Results delivered using DE 48 subelement 71 subfield 2 is equal to value 'V' to report that the cryptogram is valid</p>

## Test Result Codes for Token Authentication to Terminal

This section describes the Test Result Codes for the default values defined by the issuer for Token Authentication to Terminal. The Test Result Codes are delivered to the issuer using DE 48 subelement 27 subfield 2.

### DAU: ODA was Not Performed

The Mastercard Authorization System checks if the payment terminal has reported that ODA was not performed during a contactless EMV transaction.

If TVR Byte 1 Bit 8 is set (indicating ODA was not performed), the **DAU** code is added to the list of Test Result Codes.

### DAF: ODA Failed

The Mastercard Authorization System checks if the payment terminal has reported that ODA failed during a contactless EMV transaction.

The **DAF** code is added to the list of Test Result Codes if one of the following is true:

- TVR Byte 1 Bit 3 is set (indicating CDA failed)
- TVR Byte 1 Bit 4 is set (indicating DDA failed)
- TVR Byte 1 Bit 7 is set (indicating SDA failed)

## Test Result Codes for Wallet Overrule

This section describes the Test Result Code for the default values defined by the issuer for Wallet Overrule. The Test Result Codes are delivered to the issuer using DE 48 subelement 27 subfield 2.

### WOC: Wallet Overrule of Mastercard decision on CDCVM

A wallet overrule is defined as a decision by the mobile wallet to overrule the advice of the Mastercard process running on the mobile device to consider the CDCVM as unsuccessful, and to proceed with the transaction using that CDCVM.

When a wallet performs an MCBP transaction, the process executed on the mobile device is as follows:

1. The payment engine specified by Mastercard asks the wallet for information about CDCVM, encompassing two questions:
  - Was CDCVM performed? (yes / no)
  - When was the last successful CDCVM? (timing in seconds)
2. The Mastercard process running on the mobile device formulates a decision (the Mastercard advice) about CDCVM based on:
  - CDCVM policy
  - CDCVM history
  - Information from the wallet

3. The Mastercard process running on the mobile device communicates this advice to the wallet.
4. The wallet responds with the final decision for the transaction.

Detailed information about the concept of the payment engine and Mastercard advice are available in the *MCBP 2.0 Mobile Payment Application Specification*.

The **WOC** code is added to the list of Test Result Codes if both of the following conditions are satisfied for an EMV-based transaction:

- CVR Byte 1 Bit 3 is set (indicating that CDCVM was performed)
- CVR Byte 1 Bit 1 is not set (indicating that CDCVM was not successful)

## Appendix C Mastercard Key Certification Process

This appendix describes the key certification process.

Issuers must obtain the *Public Key Infrastructure (PKI)—Exchange Procedures for Mastercard Business Partners* document, on Publications in Mastercard Connect™ ([www.mastercardconnect.com](http://www.mastercardconnect.com)).

This section provides the specific PKI requirements applicable to certify an issuer public key whose private key is used for creating Tokenization Authentication Value (TAV) signatures.

### Registration for Mastercard PKI Service

The issuer must use the procedures for initial registration of authorized certificate requestors and password (chapter 1 of *Public Key Infrastructure (PKI)—Exchange Procedures for Mastercard Business Partners*). The issuer must also complete Form 1075, *Mastercard X.509 Public Key Infrastructure (PKI) Enrollment—Business Partners* (available on Publications). The following information must be entered in the form:

- Mastercard CIS Project Number: contact Customer Implementation Services to initiate a project.
- Mastercard Service/Project Name: MDES—Issuer Application Activation Service
- Mastercard CIS Project Contact Person: contact Customer Implementation Services to initiate a project.
- CID: your Customer ID(s). There is no specific CID field contained within the form, but the issuer should indicate at least one CID next to the Mastercard Service/Project Number on the form.

If in the future an issuer needs to request a certificate for a CID that has not been communicated on the PKI Enrollment Form, authorized certificate requestors should send the CID in advance to [key\\_management@mastercard.com](mailto:key_management@mastercard.com). Include in the request a copy to the email address of a second registered authorized certificate requestor. On receipt of the email request, Mastercard validates that the authorized certificate requestors are registered, and that the CID belongs to the issuer. Requestors receive an email confirmation of acceptance of the CID.

### Requesting Certification

The issuer needs to first generate its own asymmetric key pair, either RSA (minimum 2048-bit key) (512-bit Public Key with curve P-256). The Private Key is called the issuer signing key and is used for creating TAV signatures. The Private Key must never leave the secure hardware security module used to generate the key pair. The Public Key needs to be certified by Mastercard. The certification enables Mastercard to validate TAV signatures generated by the issuer. The issuer identifies each of the key pair(s) they want to certify with a Key Unique Reference. Keys to validate TAV signatures can be different per account range. However, keys are certified per CID, which means that a key can potentially be associated to each account range of a CID.

**NOTE:**

- The same Key Unique Reference may be associated to account ranges from multiple CIDs, in which case a digital certificate per CID must be requested from Mastercard Key Management Services.**
- If an issuer sends several certificate requests with the same Key Unique Reference for a CID, the last generated certificate shall be used for TAV validation.**

The issuer must use the procedures for Certificate Exchange for requesting their certificate (chapter 2 of *Public Key Infrastructure (PKI)—Exchange Procedures for Mastercard Business Partners*).

The issuer sends their certification request in an email that contains the following table in the email body, and includes one or several Certificate Signing Request (CSR) file(s) as attachments.

Mastercard Project Number:	
Mastercard Project Name:	
Mastercard Project Contact Person:	
File Name:	
Environment:	MTF or Production
Certificate Usage:	Signing

The CSR must be in PKCS#10 format, base64 encoded.

Subject Distinguished Name (DN) of issued certificates is as follows:

- Common Name (CN) = Customer Identifier (CID), 6-digit identifier used internally by Mastercard to uniquely identify an institution
- Organization Unit (OU) = Key Unique Reference, UTF-8 encoded value restricted to alphanumeric upper case characters and '-' (U+002D); the value is a maximum of 24 characters determined by the issuer.
- Organization (O) = Free text determined by the issuer
- Country (C) = ISO 3166 2-character country code

Generated certificates are delivered to issuers in a PKCS#7 file format.

## Certification Authorities

Mastercard has two Certification Authorities (CA) for the specific purpose of MDES—Issuer Application Activation Service.

A separate CA called 'Mastercard MTF Token Validation CA G1' generates certificates to be used in the Mastercard Testing Facility (MTF) environment to perform end-to-end testing with issuer systems.

A separate CA called 'Mastercard PRD Token Validation CA G1' generates certificates to be used in the production environment including the primary, secondary live sites. There is no policy

preventing cryptographic keys being used for both in-field testing and actual production, as it is understood that such keys would be used on the same infrastructure/environment under strict production security procedures.

Each Mastercard CA uses a 4096-bit RSA key. Each CA signs RSA issuer keys directly without any intermediary CA.

### **Certificate Lifecycle Management**

Issued certificates are given a validity date of 4 years starting at the moment the certificate is generated. Tracking of certificate expiry date and ensuring that all systems are updated with the replacement certified key is the responsibility of the issuer.

If an issuer detects or suspects their key has been compromised, they must remove the association of the Key Unique Reference with their funding account range, using issuer enablement.

### **TAV Signature Validation**

Only signatures generated by keys certified by a dedicated Mastercard CA and where their Key Unique Reference has been associated to a funding account range, through the issuer enablement process, can be validated. MTF and production environments are strictly separated so that TAV signatures created with a key whose certificate is issued by the MTF CA cannot be validated in production (and vice versa).

MDES does not proceed to signature verification if the certificate associated to the Public Key is expired.

## Appendix D Card Art and Associated Data for MDES

*This appendix outlines the specific Mastercard requirements for issuers on card art and associated Product Configuration data used in the creation and proper display of an issuer's card art image in participating MDES programs. All card art and associated Product Configuration data are supplied as individual assets. Assets may be unique to a specific Product Configuration, or they may be re-used across multiple configurations.*

---

Card Art Image Assets.....	282
Visual Appearance Assets.....	285
Display Text Assets.....	286
Issuer Mobile Banking App Assets.....	289
Transaction Detail Service Direct (TDS Direct) Assets.....	290
Wireframe for Card Background (Non-Combined Only).....	290
Mastercard Card Image Standards.....	291
Card or Account Reference Icon Standards.....	293

## Related Concepts

- [Card Art Support and Associated Data](#)
- [Tokenization Eligibility Request \(TER\) Message](#)
- [Tokenization Authorization Request \(TAR\) or Authorize Service Message](#)

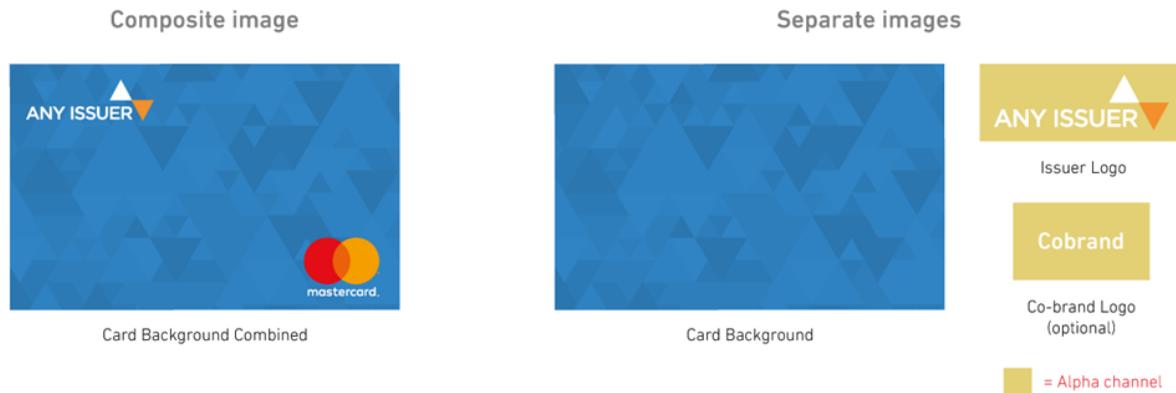
## Card Art Image Assets

All images must be provided with 1536px width by 969px height in either a vector resource or a raster image in RGB color format. MDES Manager supports vector images in SVG format and raster images in PNG format. PNG images are generally preferred. The maximum file size for SVG is up to 1MB and for PNG, up to 3MB.

MDES converts the supplied images as required, to meet the Wallet Provider's requirements such as converting a vector SVG image to a vector PDF.

**NOTE: Card art image files in PDF format are no longer supported, and hence, have been replaced with SVG file format.**

A card image is used in the wallet or user interface to represent the digitized card to the cardholder. Two options are available to configure this card image, as shown below.



Composite Image	Separate Images
<p>The issuer supplies a single Card Background Combined image that includes the Mastercard brand logo, the issuer logo, and any co-brand logo. For further details and examples of this option, refer to Mastercard Card Image Standards.</p> <p>The issuer must also supply the separate Issuer Logo and optional Co-brand Logo files so that Wallet Providers can render the card using the Background Color (see Visual Appearance Elements) if they are unable to use the Card Background Combined image.</p>	<p>The issuer supplies separate images of the Card Background, Issuer Logo, and Co-brand Logo.</p> <p>The separate images are automatically composited by the Wallet Provider, following a procedure set by Mastercard, to form the final card image. In accordance with Mastercard specifications and brand guidelines, the Mastercard brand logo shall be added to this composited final card image. For further details, refer to Wireframe for Card Background (Non-Combined Only).</p>

Submitted card art images should be rectangular in contour (with corners that are not rounded) and should not include the cardholder name, Account PAN, or expiry date. MDES-participating wallet programs are able to round the corners of submitted rectangular card art images on their user interfaces, with the radius of rounded corners no more than four percent of the card width.

Wallet programs are responsible for superimposing the consumer's Account PAN onto the submitted card art, with the digits of the Account PAN masked except for the last four digits. In accordance with Mastercard specifications and brand guidelines, the Mastercard brand logo shall be positioned on the lower right of the card art, with the superimposed masked Account PAN positioned on the lower left of the card art.

**NOTE: For the exact specification and positioning of the Mastercard brand logo, refer to Wireframe for Card Background (Non-Combined Only)**

Wallet programs must further present the token (masked except for the last four digits) in a manner readily-accessible, but not on the final card art image itself, to the consumer on the consumer device. Examples include consumer-initiated information settings associated with the specific card art image.

Image assets are primarily specified for specific purposes. However, unless otherwise stated, they are not limited to only those purposes. Flexibility is afforded to Wallet Providers to re-use image assets as they see fit to provide the best possible user experience within the scope of usage Terms and Conditions from the issuer.

Asset Name	Description
Card Background Combined	One or both must be provided:
Card Background	<ul style="list-style-type: none"> <li>• <b>Card Background Combined</b>—The composite (already combined) card image used to represent the digital card in the wallet or user interface. It should contain the Mastercard brand logo, issuer logo, and any co-brand logo. For Mastercard debit and prepaid accounts, the “Debit” identifier must be included. This image must conform to the Mastercard Card Image Standards; refer to Mastercard Card Image Standards.</li> <li>• <b>Card Background</b>—This image does not contain the Mastercard brand logo, issuer logo, or co-brand logo; those assets are supplied separately and are dynamically combined on the device to form the combined card image, refer to Wireframe for Card Background (Non-Combined Only). The standard Mastercard brand logo is assumed; for Debit Mastercard products, use Card Background Combined instead.</li> </ul> <p>The <i>Mobile PayPass—Card Layout Descriptor</i> (known as the ‘CLD’) requires the submitted image to be rectangular in contour, have a height-to-width ratio of sixty three percent (63%), and be supplied as a PNG image in RGB color format (preferred) or a SVG vector resource.</p> <p>The image must be 1536 x 969 pixels and not have rounded corners. The image must not include:</p> <ul style="list-style-type: none"> <li>• The cardholder name, Account PAN, or expiry date</li> <li>• Unnecessary physical card elements (for example embossed attributes, magstripe/personalization, EMV chip faceplate/contacts, hologram)</li> <li>• Any shading or three-dimensional elements attempting to look like a physical card</li> </ul> <p>Very light or very dark backgrounds should be avoided or otherwise checked to ensure that they remain clearly visible when displayed against the wallet program’s default white and black backgrounds.</p>
Issuer Logo	<p>Mandatory. The logo of the issuing bank. Up to 1372 x 283 pixels.</p> <p>Can be used as an overlay onto the Card Background if composite images are being used, or displayed in an appropriate area of the Digital Wallet UI separately.</p> <p>Supplied as a PNG image in RGB color format (preferred) or an SVG vector resource. The PNG image should contain an alpha channel for compositing onto the Card Background.</p>
Co-brand Logo	<p>Optional. The logo of the co-brand partner. Up to 1372 x 283 pixels.</p> <p>Supplied as a PNG image in RGB color format (preferred) or an SVG vector resource. The PNG image should contain an alpha channel for compositing onto the Card Background.</p>

Asset Name	Description
Icon	<p>Mandatory. The icon used for items such as notifications related to the card and/or account. It should be the primary brand(s) associated with the card. The icon must conform to Card or Account Reference Icon Standards (refer to Card or Account Reference Icon Standards found in this Appendix).</p> <p>Must be supplied as a PNG image.</p> <p>The image must be 100 x 100 pixels.</p>

**NOTE: Issuers must ensure that their digital card art includes the Program Identifier, if applicable, as per Mastercard Rules in [https://w201.mastercardconnect.com/hsm3ca267/homememb/library/shared/DE/suitehelp/r\\_Mastercard-ProgramIdentifiers.html](https://w201.mastercardconnect.com/hsm3ca267/homememb/library/shared/DE/suitehelp/r_Mastercard-ProgramIdentifiers.html):**

### Vertical Cards

Issuers who wish to use a vertical card should be aware that these cards:

- are supported only when using Card Background Combined
- must be rotated counter-clockwise, so that the Mastercard/Maestro logo is placed on the top-right of the rotated card
- must be used in such a way that there is a contrast between the four account PAN digits and the rotated card and the card background

## Visual Appearance Assets

Visual appearance assets provide extra properties for how the digital card is rendered within wallets and user interfaces.

Asset Name	Description
Background Color	<p>Mandatory.</p> <p>Background color for the digital card, specified in RGB format.</p> <p>This is used for the background of the digital card if the card image (Card Background Combined or Card Background) is not available for some unexpected reason.</p>
Foreground Color	<p>Mandatory.</p> <p>Foreground color for the digital card, specified in RGB format.</p> <p>This is used for the masked Account PAN digits that are overlaid on the bottom left of the card image.</p>

Asset Name	Description
Label Color	Mandatory. Label color for the digital card, specified in RGB format.  This is used for the short description text rendered on the card image if the card image (Card Background Combined or Card Background) is not available for some unexpected reason.

## Display Text Assets

Display text assets relate to the digital card and can be used to provide additional information within wallets and user interfaces.

Display text assets are primarily specified for specific purposes. However, unless otherwise stated, they are not limited to those purposes. Flexibility is afforded to Wallet Providers to re-use display text assets as they see fit to provide the best possible user experience.

Asset Name	Description
Issuer Name	Mandatory. Name of the issuing bank. It may be used to construct other strings (for example, if the name is 'Bank', it may be used to construct a string 'Contact Bank', or 'Bank Contact Information').  Up to 32 characters long.
Co-Brand Name	Conditional. Name of an issuer's co-brand partner. It may be used to construct other strings. It is required if the card is co-branded.  Up to 128 characters long.
Short Description	Mandatory. A short description of the card which, for example, could be used with lock screen notifications. This should include the word 'Mastercard'.  Up to 32 characters long.
Long Description	Optional. A long description of the card, which could appear on the user interface. This should include the word 'Mastercard'. If the Long Description is omitted, the Short Description is used instead.  Up to 64 characters long.

---

<b>Asset Name</b>	<b>Description</b>
Customer Service Website	Optional. Customer Service website of the issuing bank. It is recommended that this be a specific landing page URL for cards that are digitized for this wallet program. Must be a valid URL starting with 'http://' or 'https://'. Up to 128 characters long.
Customer Service Email	Optional. Customer Service email address of the issuing bank. Up to 32 characters long.
Customer Service Phone Number	Mandatory. Customer Service phone number of the issuing bank. Up to 20 characters long.

---

---

Asset Name	Description
Terms and Conditions File	Mandatory. Issuing bank's Terms and Conditions for the card, to be accepted by the cardholder when digitizing the card for a wallet program.  Provided as a plain text or HTML file, up to 3MB in size, with UTF-8 encoding. HTML files can only use basic block, formatting, and style tags. Issuers are recommended to avoid using CSS.
<b>NOTE:</b>	
<ul style="list-style-type: none"> <li><b>Cardholders might not be present during merchant or commerce platform tokenization, so those MDES program participants do not provide issuer Terms and Conditions to their cardholders during digitization.</b></li> <li><b>Only one Terms and Conditions File may be configured for each account range—the one that is part of the default Product Configuration for the account range. If an issuer wants to support Wallet Provider-specific Terms and Conditions in an account range, rather than generic ones, it must provide additional Wallet Provider-specific Terms and Conditions Files to Mastercard for manual configuration by Mastercard.</b></li> <li><b>MDES always uses the Terms and Conditions File from the default (or Wallet Provider-specific) account range-level Product Configuration. It is <i>not</i> overridden by a Product Configuration provided for a specific digitization via a Tokenization Eligibility Request (TER) or Tokenization Authorization Request (TAR) message response (if the issuer has chosen to use those network messages). This is because MDES sends the Terms and Conditions File to the Wallet Provider before receiving the TER or TAR message responses.</b></li> <li><b>There is currently no explicit mechanism to support separate Terms and Conditions Files for different languages. However, issuers may include Terms and Conditions repeated in multiple languages within a single file.</b></li> </ul>	
Terms and Conditions URL	Optional. URL pointing to issuing bank's Terms and Conditions for the card. Must be a valid URL starting with 'http://' or 'https://'.
Privacy Policy URL	Optional. URL pointing to issuing bank's privacy policy. Must be a valid URL starting with 'http://' or 'https://'.

---

## Issuer Mobile Banking App Assets

Issuer Mobile Banking App assets include parameters that allow a wallet application to communicate with an issuer's mobile banking application. The mechanisms for app-to-app communication vary by mobile device operating system.

### Apple iOS Apps

For details of the Apple iOS-specific Issuer Mobile Banking App assets, refer to the Apple Pay-specific documentation in the MDES Information Center, or contact your Mastercard representative for instructions on how to get access.

### Android OS Apps

MDES supports the Android OS Explicit Intent mechanism used by an Android app to invoke another app on the same device. Static parameters are used to define each Intent. These are provided by an issuer as part of Product Configuration data during the issuer enablement or maintenance processes, and subsequently provided to the Wallet Provider as part of the Product Configuration provisioned during digitization.

An Explicit Intent, made up of a Package Name and an Action, must be provided in the standard Android format. MDES supports the provision of multiple Android Intents if an issuer wants to configure different app-to-app Intents for different purposes. The issuer must declare a Purpose parameter for every Intent to specify how MDES is to use the Intent.

The required static parameters for each intent include:

Asset Name	Description
Purpose	Conditional—must be included when forming a complete Intent.  The Purpose of an Android OS Intent.  Allowed values: <ul style="list-style-type: none"><li>• Activate Token</li><li>• Open Issuer Mobile App</li></ul>
Package Name	Conditional—must be included when forming a complete Intent.  The package name of the issuer's mobile app. This identifies the app that the Intent will resolve to. If the app is not installed on the user's device, this package name will be used to open a link to the Android Play store for the user to download and install the app.  String, up to 128 characters long.  Example: com.mybank.bankingapp

Asset Name	Description
Action	<p>Conditional—must be included when forming a complete Intent.</p> <p>The name of the action to be performed. This must be a fully qualified name including the package name, to create an Explicit Intent. The action must be defined to be specific for the use expected for the given Purpose.</p> <p>String, up to 128 characters long.</p> <p>Example: com.mybank.bankingapp.action.MY_ACTION</p>

For more information on Android package names and Intents, see the [Android Developer documentation](#).

## Transaction Detail Service Direct (TDS Direct) Assets

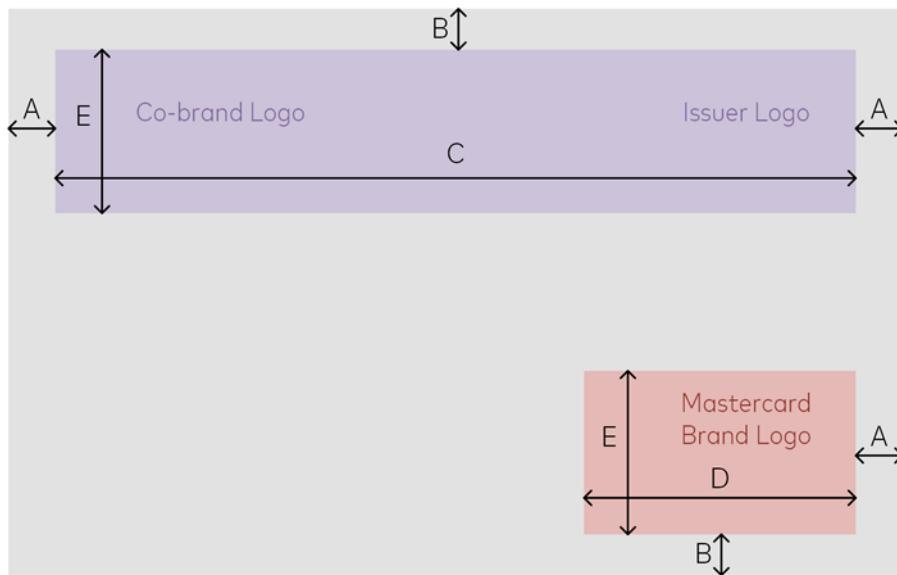
This section is only applicable if the issuer is providing its own Transaction Detail Service (TDS Direct). It may be omitted if the issuer is using the Mastercard Transaction Detail Service.

TDS Direct assets are described in wallet-specific documents on the MDES Information Center. Contact your Mastercard representative for instructions on how to request access from Mastercard Connect™.

## Wireframe for Card Background (Non-Combined Only)

When separate images are supplied, the following wireframe shows how the Card Background, Issuer Logo, Co-brand Logo (if supplied) and Mastercard Brand Logo must be composited to form the final card image, following the *Mobile PayPass—Card Layout Descriptor* (known as the 'CLD'), available on Publications in Mastercard Connect.

**NOTE: The Issuer Logo and the Co-brand Logo share the same area. If the logo files are smaller than the area, they are pinned (aligned) to the top corners of the area. If a logo file (with its alpha channel) matches the full size of the area, it can be positioned exactly; this can be used to center the logo.**



Height-to-Width Ratio	63%
Card Width	1536 pixels
Card Height	969 pixels
A—Side padding	82 pixels
B—Top/Bottom padding	57 pixels
C—Issuer Logo/Co-brand Logo area width	1372 pixels
D—Mastercard Brand Logo width	459 pixels
E—Logo height	283 pixels

## Mastercard Card Image Standards

Card images must conform to the standards as described in this section.

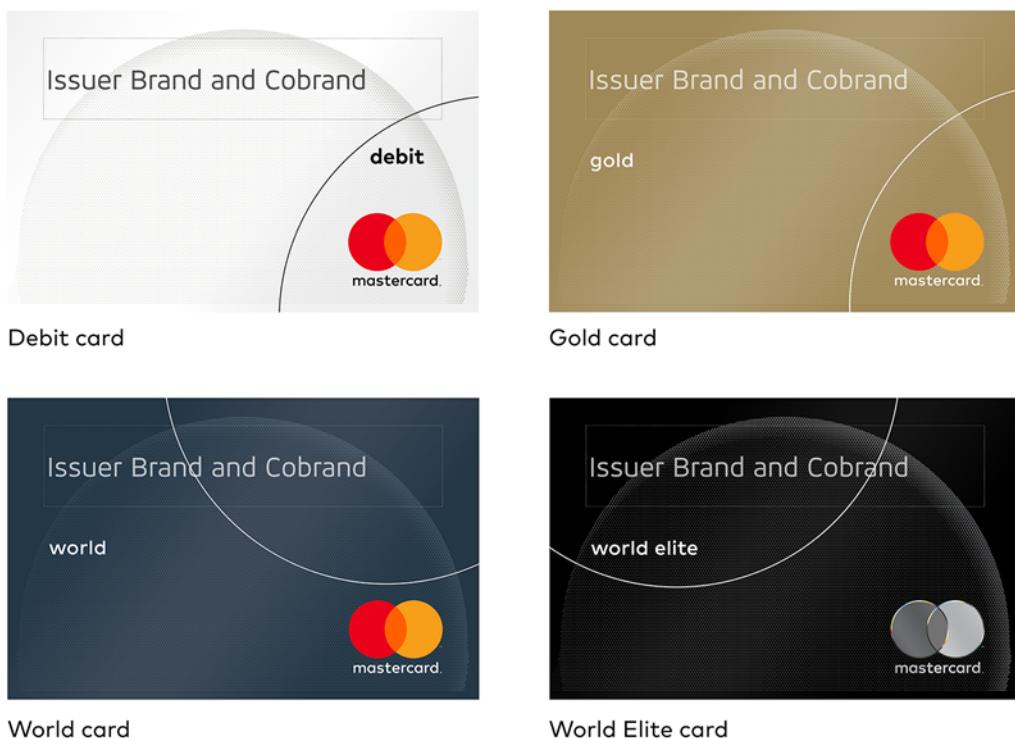
- A card image may be an exact replica of the corresponding physical card or a generic representation of a Mastercard card (not matching the exact design or background color of the physical card). However, chip face plate, account number, cardholder name, BIN, and other personalization elements must be removed.
- All Mastercard branding elements (Brand Mark, “Debit” Identifier, program identifiers) must be proportionally sized to match or exceed physical card design standards.
- Credit and Business cards must display the full-color Mastercard Brand Mark. For World Elite and Black Mastercard programs, the Premium Brand Mark should be used instead of the full-color Mark.

- Debit and Prepaid cards must display the full-color Mastercard Brand Mark with the “Debit” Identifier (use authorized Mastercard images).
- A card image may depart from conventional physical card layout and design. For example, placement of the Mastercard Brand Mark on the card image is flexible.
- The EMVCo Contactless Indicator may be displayed on the card image to reinforce NFC capability. Refer to brand usage standards for the Contactless Indicator at [www.emvco.com](http://www.emvco.com).
- All digital card images are subject to Mastercard review and approval.

**NOTE: The RGB version of the full-color Mastercard Brand Mark must be used in card images intended for on-screen applications. Authorized images can be downloaded from [brand.mastercard.com](http://brand.mastercard.com).**

**Card templates have been developed to assist issuers in the creation of Card Background Combined images. Contact Mastercard to obtain these templates (including Premium Brand Mark and the Mastercard logo with Debit identifier).**

**Figure 34: Sample Card Images**



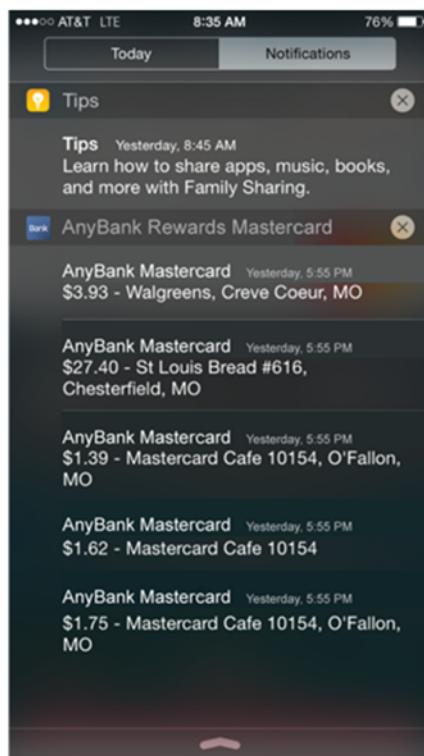
## Card or Account Reference Icon Standards

The icon must conform to the standards as described in this section.

- The icon should be based on the bank or co-brand name or logo, or the Mastercard Brand Mark. The overall design of the icon and placement of the brands and/or logos within is flexible. If the Mastercard Brand Mark is incorporated into the icon, the Brand Mark must be placed against a background color of sufficient contrast to ensure visibility of the Mark.
- The icon image must be 100 x 100 pixels and have square corners (the corners are automatically rounded in the application).
- All icon images incorporating the Mastercard Brand Mark are subject to Mastercard review and approval.

**NOTE: The design treatments shown here are illustrative. Contact Mastercard for turnkey icon images with the Mastercard brand displayed on 5 standard background colors.**

**Figure 35: Example Icons (left) and Use on Notification Screen (right)**



## Appendix E Commercial Cards

*This appendix describes MDES Commercial Card support.*

---

MDES and Commercial Enhanced Data.....	295
Processors.....	295
BIN Enablement.....	295

## MDES and Commercial Enhanced Data

---

The Mastercard Global Data Repository (GDR) supports data matching for real card transactions. At this time, Enhanced Data is not available for token transactions taking place on Corporate and Multi Cards.

Token transactions are available in Smart Data.

## Processors

---

Mastercard is working directly with processors on their readiness for commercial launch.

**NOTE: While issuers may have MDES-enabled consumer cards, commercial programs may sit on a separate platform that is not yet enabled.**

**NOTE: Issuers' processor(s) may be interacting with MDES on their behalf. It is important to review the MDES configurations with their processor(s) and confirm their selections based on what the processor(s) support/s. Specifically, they need to confirm support of the digital product they wish to enable, review the Product Configuration ID, message setup, and rule setup.**

**NOTE: If an issuer has a question about whether their processor is MDES-ready for commercial cards, they should contact their Mastercard Customer Service representative directly.**

## BIN Enablement

---

Issuers may have multiple corporate clients within a single BIN range.

If issuers only want to enable select corporate clients, they should contact their Mastercard Customer Service representative to determine the best execution strategy for their portfolio.

## Appendix F MDES Register for Issuer Pre-digitization Network Message Values

This appendix summarises pre-digitization network message values.

The following list of data elements provides the fixed values that pre-digitization network messages can contain. It is based on the message layouts and comprehensive lists of pre-digitization message fields provided in the *Customer Interface Specification* and *Single Message System Specifications*, available on Publications in Mastercard Connect™ ([www.mastercardconnect.com](http://www.mastercardconnect.com)).

The list here is provided for reference; issuers should check the latest version of the specifications for the most up-to-date information.

MDES Pre-Digitization API documentation that describes the API messages and parameters is available on the Mastercard Developers site.

In the table below:

- **Type of Presence** column: M = Mandatory, O = Optional, C = Conditional
- **Included in Request** and **Included in Response** columns:
  - ACN = Activation Code Notification
  - ASI = Account Status Inquiry
  - TAR = Tokenization Authorization Request
  - TCN = Tokenization Complete Notification
  - TER = Tokenization Eligibility Request
  - TVN = Tokenization Event Notification
  - AA = Administrative Advice/0620 message used to convey ACN, TCN, or TVN

ACN, ASI, TAR, TCN, TER, and TVN messages are sent as Authorization Request/0100 or Financial Transaction Request/0200 message types.

Data Element ID and Name	Values/Comments	Type of Presence	Included in Request	Included in Response
DE 3 (Processing Code)	00 = Purchase	M	ASI, TER, TAR, ACN, TCN, TVN	ASI, TER, TAR, ACN, TCN, TVN
DE 4 (Amount, Transaction)	Zero	M	ASI, TER, TAR, ACN, TCN, TVN	ASI, TER, TAR, ACN, TCN, TVN
DE 22 (POS Entry Mode)	Subfield 1 (POS Terminal PAN Entry Mode) = 01 (PAN manual entry) Subfield 2 (POS Terminal PIN Entry Mode) = 0 (Unspecified or unknown)	M	TER, TAR, ACN, TCN, TVN	

<b>Data Element ID and Name</b>	<b>Values/Comments</b>	<b>Type of Presence</b>	<b>Included in Request</b>	<b>Included in Response</b>
DE 22 (POS Entry Mode)	Subfield 1 (POS Terminal PAN Entry Mode) = 81 (PAN entry via e-commerce) Subfield 2 (POS Terminal PIN Entry Mode) = 0 (Unspecified or unknown)	M	ASI	
DE 35 (Track 2 Data)	Might be present	C	TER, TAR, ACN, TCN, TVN	
DE 39 (Response Code)	00 = Continue 05 = Decline, or any value other than 00 or 85 85 = Continue, but require additional authentication	M		TER
DE 39 (Response Code)	05 = Decline, or any value other than 00 or 85 If the 'USE RESPONSE CODE' option is chosen during issuer enablement: <ul style="list-style-type: none"><li>• 00 = Approve</li><li>• 85 = Approve, but require additional authentication</li></ul> If the 'USE RULES' option is chosen during issuer enablement: <ul style="list-style-type: none"><li>• 00 or 85 = Continue</li></ul>	M		TAR
DE 39 (Response Code)	00 = Approved	M		ACN, TCN, TVN
DE 39 (Response Code)	00 or 85 = Approve or continue 05 = Decline, or any value other than 00 or 85	M		ASI
DE 48 Transaction Category Code	T (Phone, Mail, or Electronic Commerce Order)	C	ASI, TER, TAR, ACN, TCN, TVN	
DE 48 (Additional Data—Private Use), subelement 26 (Wallet Program Data), subfield 1 (Wallet Identifier)	Depends on the wallet program or service	C	TER, TAR, ACN, TCN, TVN	

<b>Data Element ID and Name</b>	<b>Values/Comments</b>	<b>Type of Presence</b>	<b>Included in Request</b>	<b>Included in Response</b>
DE 48 (Additional Data—Private Use), subelement 33 (PAN Mapping File Information), subfield 1 (Account Number Indicator)	C = MDES Secure Element Device Token H = MDES Cloud-Based Payments Device Token F = MDES Card on File Token	C	TER, TAR, ACN, TCN, TVN	
DE 48 (Additional Data—Private Use), subelement 33 (PAN Mapping File Information), subfield 6 (Token Requestor ID)	Depends on the Token Requestor	C	TER, TAR, ACN, TCN, TVN	
DE 48 (Additional Data—Private Use), subelement 82 (Address Verification Service)	52 = Either: <ul style="list-style-type: none"><li>• AVS and Authorization Request/0100</li><li>• AVS and Financial Transaction Request/0200</li></ul>	C	ASI, TAR	ASI, TAR
DE 60 (Advice Reason Code), subfield 1 (Advice Reason Code)	141 = MDES Advice to Issuer	M	AA	
DE 60 (Advice Reason Code), subfield 2 (Advice Detail Code)	0250 = Activation Code Notification 0251 = Tokenization Complete Notification  0252 = Tokenization Event Notification	M	AA	
DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status)	9 = Tokenization Request/Notification	M	TER, TAR, ACN, TCN, TVN	
DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status)	8 = Account Status Inquiry Service	M	ASI	
DE 61 (Point-of-Service [POS] Data), subfield 13 (POS Country Code)	840 = USA Or appropriate country value, if digitizing Account PAN in Local Use Only account range	M	ASI, TER, TAR, ACN, TCN, TVN	
DE 61 (Point-of-Service [POS] Data), subfield 14 (POS Postal Code)	63368 = O'Fallon, MO	M	ASI, TER, TAR, ACN, TCN, TVN	
DE 124 (Member Defined Data), subfield 1 (Message Type)	TE = Tokenization Eligibility Request (TER)	M	TER	

<b>Data Element ID and Name</b>	<b>Values/Comments</b>	<b>Type of Presence</b>	<b>Included in Request</b>	<b>Included in Response</b>
DE 124 (Member Defined Data), subfield 1 (Message Type)	TA = Tokenization Authorization Request (TAR)	M	TAR	
DE 124 (Member Defined Data), subfield 1 (Message Type)	AC = Activation Code Notification (ACN)	M	ACN	
DE 124 (Member Defined Data), subfield 1 (Message Type)	TC = Tokenization Complete Notification (TCN)	M	TCN	
DE 124 (Member Defined Data), subfield 1 (Message Type)	TV = Tokenization Event Notification (TVN)	M	TVN	
DE 124 (Member Defined Data), subfield 3 (Primary Account Number Source)	1 = Card on file 2 = Card added manually 3 = Card added via application	M	TER	
DE 124 (Member Defined Data), subfield 3 (Primary Account Number Source)	1 = Card on file 2 = Card added manually 3 = Card added via application	C	TAR	
DE 124 (Member Defined Data), subfield 3 (Tokenization Event Indicator)	3 = Deactivate 4 = Deleted from consumer device 6 = Suspend 7 = Resume 8 = Tokenization Exception Event 9 = Replacement (token re-digitization)	M	TVN	

---

Data Element ID and Name	Values/Comments	Type of Presence	Included in Request	Included in Response
DE 124 (Member Defined Data), subfield 3 (Token Data and Activation Method[s])	<p>Two types of information can be supplied.</p> <p><b>Activation Methods:</b></p> <ul style="list-style-type: none"> <li>1 = Masked mobile phone number</li> <li>2 = Masked email address</li> <li>3 = Automated call center phone number</li> <li>4 = Call center phone number</li> <li>5 = Website</li> <li>6 = Mobile</li> <li>7 = Masked voice call phone number</li> </ul> <p><b>Token Data:</b></p> <ul style="list-style-type: none"> <li>a = Alternate Account Identifier</li> <li>t = One or multiple token personalization data items (TAR response only, see Providing Additional Personalization Data for a Token)</li> </ul> <p><b>NOTE: The methods and data are supplied using the ‘ ’ delimiter, which is the EBCDIC character for hex value 0x4F (and not the EBCDIC character ‘;’ that has hex value 0x6A). Mastercard advises issuers to verify that their systems do not unintentionally swap ‘ ’ for ‘;’ prior to integration testing with Mastercard.</b></p> <p>When masking data, use EBCDIC or ASCII display character representation. For more information, see Data Representation Notations in the <i>Customer Interface Specification</i>.</p>	O		TER, TAR

---

---

<b>Data Element ID and Name</b>	<b>Values/Comments</b>	<b>Type of Presence</b>	<b>Included in Request</b>	<b>Included in Response</b>
DE 124 (Member Defined Data), subfield 4 (Tokenization Event Reason Code)	<p>00 = Activation Code retries exceeded</p> <p>01 = Activation Code expired or invalidated</p> <p>02 = Activation Code entered incorrectly by cardholder</p>	C	TVN	
DE 124 (Member Defined Data), subfield 5 (Consumer's Activation Method Preference)	<p>The distribution method selected by the consumer, if only one method was offered by the issuer, then that distribution method. There is only one method contained in this field. This field is only present if the cardholder provides a choice. The method starts with a first numeric character (Activation Method Type) which can either be:</p> <ul style="list-style-type: none"> <li>1 = Masked mobile phone number</li> <li>2 = Masked email address</li> <li>3 = Automated call center phone number</li> <li>4 = Call center phone number</li> <li>5 = Website</li> <li>6 = Mobile</li> <li>7 = Masked voice call phone number</li> </ul>	C	ACN	

---

<b>Data Element ID and Name</b>	<b>Values/Comments</b>	<b>Type of Presence</b>	<b>Included in Request</b>	<b>Included in Response</b>
DE 124 (Member Defined Data), subfield 5 (Event Requestor)	0 = Wallet Provider or Token Requestor 1 = Funding Account issuer 2 = Cardholder 3 = The Tokenization Event was requested in relation to a systematic event triggered by Mobile PIN Validation security (applicable to Tokenization Event Indicator value of 6 [Suspend] or 7 [Resume] only) 4 = The Tokenization Event was requested in relation to a systematic event triggered by Mobile PIN Change Validation security (applicable to Tokenization Event Indicator value of 6 [Suspend] or 7 [Resume] only)	C	TVN	
DE 124 (Member Defined Data), subfield 7 (Final Tokenization Decision)	1 = Approve 2 = Approve, but require additional authentication	M	TCN	
DE 124 (Member Defined Data), subfield 8 (Final Tokenization Decision Indicator)	1 = Tokenization Eligibility Response 2 = Tokenization Authorization Response 3 = Issuer pre-defined tokenization rules 4 = Mobile Application	M	TCN	
DE 124 (Member Defined Data), subfield 8 (Wallet Service Provider Tokenization Recommendation)	0 = Decline 1 = Approve 2 = Require additional authentication	O	TAR	
DE 124 (Member Defined Data), subfield 8 (Token Type)	C = Mastercard Cloud-Based Payments (MCBP) F = Card on File S = Embedded Secure Element	M	TER	

Data Element ID and Name	Values/Comments	Type of Presence	Included in Request	Included in Response
DE 124 (Member Defined Data), subfield 14 (Token Type)	C = Mastercard Cloud-Based Payments (MCBP) F = Card on File S = Embedded Secure Element	M	TCN	
DE 124 (Member Defined Data), subfield 16 (Token Type)	C = Mastercard Cloud-Based Payments (MCBP) F = Card on File S = Embedded Secure Element	M	TAR	

## Appendix G Wallet Provider Tokenization Recommendations, Reasons, and Interpretation

This appendix relates to the Wallet Provider Tokenization Recommendation.

The following tables list the valid Recommendation Reasons and associated conditions that must be met when a Wallet Provider indicates a Tokenization Recommendation in DE 124, subfield 8 (Wallet Provider Tokenization Recommendation).

### Approve

The following reasons relate to an 'Approve' recommendation.

Bit No.	Reason	Description (Conditions)
1	Long Account Tenure	The Wallet Provider consumer account has existed for an extended period prior to the request for digitization. The Wallet Provider may define its own extended period, but it should be at least one year.
2	Good Activity History	The card to which the digitization applies has been financially active with no suspicious or fraudulent activity for an extended period. The Wallet Provider can define its own criteria for the extended period appropriate to its service. A card with normal activity within a period of at least one year would have good activity history.
3	Additional Device	The device to which the digitization applies is for the same Account PAN and Wallet Provider consumer account as a linked device where an active token present.
4	Software Update	The digitization has been requested due to an authenticated operating system or other software update being installed on the device, causing the token data to be wiped or otherwise unable to be restored. This digitization must be for the same device to which a token was previously digitized and activated for the same Account PAN and consumer account.

### Require Additional Authentication or Decline

The following reasons relate to 'Require additional authentication' and 'Decline' recommendations.

Bit No.	Reason	Description (Conditions)
1	Account Too New Since Launch	The Wallet Provider consumer account was created after the Wallet Provider's service launch and is still considered too recently opened to qualify for a recommendation of Approve. The Wallet Provider can define its own 'too new' period, but it should be a period measured in days or a low number of weeks. An account tenure of more than a month prior to service launch should not be considered too new.

<b>Bit No.</b>	<b>Reason</b>	<b>Description (Conditions)</b>
2	Account Too New	The Wallet Provider consumer account was recently opened and does not qualify for a recommendation of Approve. The Wallet Provider can define its own 'too new' period, but it should be a period measured in days or a low number of weeks. An account tenure of more than a month prior to digitization should not be considered too new.
3	Account Card Too New	The card being digitized was recently linked to the Wallet Provider consumer account and does not qualify for a recommendation of Approve. The Wallet Provider can define its own 'too new' period, but it should be a period measured in days or a low number of weeks. A link created more than a few weeks prior to digitization should not be considered too new.
4	Account Recently Changed	Changes have recently been made to Wallet Provider consumer account data. Examples are where personal details have been updated, address information changed, or a password reset. The Wallet Provider can define its own recent period, but it should be a period greater than a week measured in days or a low number of weeks. Account updates older than a month should not be considered recent.
5	Suspicious Activity	There is identified suspicious activity linked to this Wallet Provider consumer account. The nature of the activity may not necessarily be financial, for example multiple password resets may be considered suspicious.
6	Inactive Account	The Wallet Provider consumer account has been inactive for an extended period prior to the request for digitization. When financial activity normally or regularly occurs in the service, this should be the activity considered rather than other consumer activity. The Wallet Provider can define its own inactivity period, but it should be between three months and one year. An account with no activity for more than a year must always be considered inactive.
7	Has Suspended Tokens	The device to which the digitization applies contains other suspended tokens. These tokens may relate to cards digitized from other issuers.
8	Device Recently Lost	The device to which the digitization applies was recently reported lost. The Wallet Provider can define its own recent period, but it should be a period greater than a week measured in days or a maximum of a week. This reason also applies for devices currently considered lost. Devices reported lost more than a week prior to the digitization request and currently considered found should not be considered recently lost.
9	Too Many Recent Attempts	The number of recent digitization attempts to this device or for this card has breached the Wallet Provider's threshold. The Wallet Provider can define its recent period, but it should be measured in days and the threshold for 'too many' should be a mid-range single-digit value. The Wallet Provider may record attempts at device level and card level and trigger this reason for either threshold being exceeded.

<b>Bit No.</b>	<b>Reason</b>	<b>Description (Conditions)</b>
10	Too Many Recent Tokens	<p>The rate of digitizations to this device or for this card has breached the Wallet Provider's threshold. The Wallet Provider can define its own criteria for too frequent, but it should be measured as:</p> <ul style="list-style-type: none"> <li>• A mid-range single-digit value over a period of hours or one day</li> <li>• A low-range two-digit value over a period of a low number of days up to a week</li> </ul> <p>The Wallet Provider may measure the digitizations at a device level and a card level and trigger this reason for either velocity threshold being exceeded. Successful and unsuccessful digitizations should be included.</p>
11	Too Many Different Cardholders	<p>The number of cardholder names entered during digitization with this device has breached the Wallet Provider's own threshold. The Wallet Provider can define its own threshold, but it should be a low-range single-digit value. When multiple users exist for a device, the device threshold should apply for all users, not for each individual user.</p>
12	Low Device Score	<p>If the Wallet Provider performs an algorithmic risk analysis of a device prior or during digitization and the result is low, this reason shall be set. The Wallet Provider may devise its own proprietary algorithm to determine the device score, but it should take into account and be weighted towards identifying devices linked to suspicious or fraudulent consumer activity.</p>
13	Low Account Score	<p>If the Wallet Provider performs an algorithmic risk analysis of a consumer account prior or during digitization and the result is low, this reason shall be set. The Wallet Provider may devise its own proprietary algorithm to determine the consumer account score, but it should take into account and be weighted towards identifying accounts linked to suspicious or fraudulent consumer activity.</p>
14	Outside Home Territory	<p>The digitization attempt is occurring in a geographic region outside the consumer's home region. The Wallet Provider may determine the level of geographic granularity used to assess this reason. If the Wallet Provider has home address information for a consumer, this reason may be present when the digitization occurs within a different geographic region or administrative region, for example outside of a consumer's home state or county. The Wallet Provider shall set this reason when digitization is occurring outside the country associated with the consumer account, if applicable.</p>
15	Unable to Assess	<p>When the Wallet Provider is unable to provide an Approve recommendation due to temporary technical reasons, insufficient consumer or device-related data or business reasons they should provide this reason.</p>
16	High Risk Digitization	<p>The Wallet Provider has determined that this digitization exhibits an abnormally high risk. The Wallet Provider may determine its definition of high risk. When applicable, the Wallet Provider must use this reason to identify digitizations to devices that are currently identified by a consumer as lost or stolen.</p>

## Appendix H Terminology

*This section explains key terms and concepts used in this document.*

---

Activation Code.....	308
Mobile Device.....	308
mobile device manufacturer.....	308
M/Chip Mobile Application.....	308
Over the Air.....	308
Over the Air Personalization.....	308
Payment Credentials.....	308
Proximity Payment System Environment.....	309
Secure Element.....	309
Secure Element Provider.....	309
Token Connect.....	309
Token Requestor.....	309
Wallet Provider.....	309

## **Activation Code**

---

A series of digits or letters that are provided to a consumer for authentication during the digitization process.

## **Mobile Device**

---

Any mobile phone, smartphone, handheld PDA, or other communications device. The device may include Near Field Communication (NFC) functionality.

## **mobile device manufacturer**

---

The manufacturer of the mobile device. The scope of the role of this entity can range from simply manufacturing the hardware, managing the payment application, providing the User Interface Application, or a combination of these roles.

## **M/Chip Mobile Application**

---

A payment application that conforms to the M/Chip Mobile Requirements and M/Chip Mobile technical specifications. The M/Chip Mobile application supports contactless and Digital Secure Remote Payment.

## **Over the Air**

---

Refers to any process that involves the transfer of data (including applications) to the mobile device or any component within the mobile device using wireless data transfer, such as the mobile network.

## **Over the Air Personalization**

---

Over the Air Personalization of a payment application within a mobile device.

## **Payment Credentials**

---

The payment details used to create the data necessary to perform a transaction. This data typically includes the account number, cryptographic keys and other configuration data, used by the payment application to generate the data presented for a transaction.

## Proximity Payment System Environment

---

An application that points to a default, or other selectable, payment application within the Secure Element. *Proximity Payment System Environment (PPSE)* provides a directory of the payment Application Identifiers (AIDs), and, where applicable, the associated priority order. A contactless terminal is required to select the highest priority application it finds within the *PPSE* that it supports.

**Surface Form:** Proximity Payment System Environment (PPSE)

**Abbreviated Form:** PPSE

## Secure Element

---

A secure, tamper-resistant storage and execution environment holding payment applications and payment assets such as keys.

## Secure Element Provider

---

An entity that controls access to space within a Secure Element for use in a mobile device.

## Token Connect

---

An optional MDES framework for issuers and Token Requestors, to support issuer-initiated digitization

## Token Requestor

---

An entity, such as a Wallet Provider, that uses MDES for token requests and token transactions. Each Token Requestor is registered and identified uniquely by MDES.

## Wallet Provider

---

Provides the wallet application (app) on the mobile device, and is responsible for managing the wallet account and integrating to the Account Enablement System (AES) to digitize cards into the wallet.

# Notices

Following are policies pertaining to proprietary rights, trademarks, translations, and details about the availability of additional information online.

## Proprietary Rights

The information contained in this document is proprietary and confidential to Mastercard International Incorporated, one or more of its affiliated entities (collectively "Mastercard"), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of Mastercard.

## Trademarks

Trademark notices and symbols used in this document reflect the registration status of Mastercard trademarks in the United States. Please consult with the Global Customer Service team or the Mastercard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

## Disclaimer

Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, Mastercard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not Mastercard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, Mastercard specifically disclaims all representations and warranties that any practice or implementation of this document will not infringe any third party patents, copyrights, trade secrets or other rights.

## Translation

A translation of any Mastercard manual, bulletin, release, or other Mastercard document into a language other than English is intended solely as a convenience to Mastercard customers. Mastercard provides any translated document to its customers "AS IS" and makes no representations or warranties of any kind with respect to the translated document, including, but not limited to, its accuracy or reliability. In no event shall Mastercard be liable for any damages resulting from reliance on any translated document. The English version of any Mastercard document will take precedence over any translated version in any legal proceeding.

## Information Available Online

Mastercard provides details about the standards used for this document—including times expressed, language use, and contact information—on the Publications Support page available on Mastercard Connect™. Go to Publications [Support](#) for centralized information.