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 manual reflect the registration status of MasterCard trademarks in the United States. Please consult with the Customer Operations Services 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

Access to this document is subject to a separate Non-Disclosure Agreement with MasterCard.

If you are not certain that you are disclosed, or that you should have access to this document, please stop reading now, and consult the appropriate legal resource within your company before proceeding.

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 the 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 the Specification will not infringe any third party patents, copyrights, trade secrets or other rights.
## Contents

1    Introduction .................................................................................................................. 6
1.1  What is the MasterCard Digital Enablement Service? ......................................................... 6
1.2  Document Scope ........................................................................................................... 6
1.3  Using This Document .................................................................................................. 6

2    MDES Issuer API ........................................................................................................... 7
2.1  Overview ........................................................................................................................ 7
2.1.1 Flow Diagram ............................................................................................................. 7
2.1.2 API Design Principles ............................................................................................... 8
2.1.3 URL Scheme ............................................................................................................... 8
2.1.4 Security Overview and Encryption ............................................................................. 9
2.1.5 API Request / Response Common Elements and Headers .............................................10
2.1.6 Retry Strategy ...........................................................................................................11
2.2  RequestActivationMethods .............................................................................................12
2.2.1 URL Endpoint ............................................................................................................12
2.2.2 HTTP Method ............................................................................................................12
2.2.3 Request Parameters ....................................................................................................12
2.2.4 Response Values ........................................................................................................14
2.2.5 Example Request Body ..............................................................................................15
2.2.6 Example Response Body ............................................................................................15
2.3  DeliverActivationCode .....................................................................................................16
2.3.1 URL Endpoint ............................................................................................................16
2.3.2 HTTP Method ............................................................................................................16
2.3.3 Request Parameters ....................................................................................................16
2.3.4 Response Values ........................................................................................................17
2.3.5 Example Request Body ..............................................................................................17
2.3.6 Example Response Body ............................................................................................18
2.4  NotifyServiceActivated ...................................................................................................18
2.4.1 URL Endpoint ............................................................................................................18
2.4.2 HTTP Method ............................................................................................................18
2.4.3 Request Parameters ....................................................................................................18
C.2 Require Additional Authentication or Declined Reason Codes ........................................50
1 Introduction

1.1 What is the MasterCard Digital Enablement Service?

The MasterCard Digital Enablement Service (MDES) is a suite of on-behalf-of (OBO) services that supports the management and generation of digital payment tokens to enable simpler, more secure digital payment experiences.

MDES was developed to facilitate the financial industry transition from consumer account credentials stored on payment cards to digital credentials. Digital credentials may be provisioned into mobile devices, enabling consumers to perform payments via existing contactless point-of-sale (POS) systems, or via remote payment use cases such as in-app payments. Digital credentials may also be stored on file by merchants and digital Wallet Providers (WP), allowing them to exchange payment cards on file with digital payment tokens.

1.2 Document Scope

This document is the controlling specification of the Application Programming Interface (API) for the MDES Issuer API.

The MDES Issuer API supports the pre-digitization web services provided by the Digitization Service, which must be implemented by Issuers participating in MDES.

The following diagram illustrates integration of the MDES Issuer API with an Issuer web service complying with the API described in this document:

1.3 Using This Document

The document is a technical specification of the MDES Issuer API. It is assumed that the reader is familiar with high-level MDES use cases and MDES pre-digitization messages in ISO format.
2 MDES Issuer API

2.1 Overview

The MDES Issuer API provides a set of outbound web requests to inform Issuers of MDES services being requested by, or on-behalf of, their Cardholders. Issuers may provide information in their responses to guide or inform the Cardholder’s experience through the Wallet Provider.

2.1.1 Flow Diagram

The first diagram illustrates a web service managed by the Issuer or Service Provider that implements pre-digitization services using the MDES Issuer API. This includes:

- Authorizing the creation of a token (digitization) or activation of a service.
- Authenticating the Cardholder, managing the Activation Methods list and the Activation Code Distribution Methods.

The second diagram shows a hybrid implementation of the pre-digitization services where:

- The Issuer uses the Tokenization Authorization pre-digitization message for authorizing the creation of a token (digitization).
- The Issuer designates a Web Service (e.g. managed by a Service Provider) implementing the MDES Issuer API for authentication of the Cardholder, managing both the Activation Methods list and the Activation Code Distribution Methods.
2.1.2 API Design Principles

The MDES Issuer API is designed as a set of RPC style stateless web services where each API endpoint represents an operation to be performed. All request and response payloads are sent in the JSON (JavaScript Object Notation) data-interchange format. Each endpoint in the API specifies the HTTP Method used to access it. All strings in request and response objects are UTF-8 encoded. Each API URI includes the major and minor version of API that it conforms to. This allows multiple concurrent versions of the API to be deployed simultaneously.

All APIs return an HTTP response code of 200 if the call was successfully received and accepted for processing. To ensure forward-compatibility, all API client implementations must be resilient to new elements being added to requests. Any errors that subsequently occur during processing are returned in the response payload.

2.1.3 URL Scheme

All API URLs follow the format:
scheme://host[:port]/contextRoot/api/majorVer/minorVer/apiName

<table>
<thead>
<tr>
<th>URL Element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheme</td>
<td>https</td>
</tr>
</tbody>
</table>
host[:port] Hostname (and port number if required) for the environment.
  e.g. www.issuersite.com

contextRoot Context root for the services. The rest of the URL must
  conform to the URL Scheme exactly. e.g.
  /root/directory1/directory2/

mdes

api issuerServices

majorVer The major version of the APIs. This is not related to the
  version of this document. This version of the document
  corresponds to a major version of:
  1

minorVer The minor version of the APIs. This version of the document
  corresponds to a minor version of:
  0

apiName The URL endpoint as defined in the respective section for the
  API operation.

2.1.4 Security Overview and Encryption

All communication between the Issuer’s Server(s) and the MDES Issuer APIs are secured
using mutually authenticated TLS. In addition, all PCI sensitive data (such as a PAN) and all
Cardholder personally identifiable information (PII) are encrypted for transport using a
separate key. In some cases, the encrypted data may contain an additional timestamp to
specify the encrypted data validity period. This prevents the same encrypted data from
being replayed after the validity period expires.

All keys exchanges shall comply with the MasterCard Public Key Infrastructure policy.

Two security layers are used for the protection of sensitive PCI/PII information, as follows:

- Communication between MDES Issuer API and Issuer web service are secured
  using mutually authenticated TLS.
- Both CardInfoData (illustrated in the figure below) and CardAndTokenData are
  encrypted using a single use encryption key (SK), and are exposed by, respectively,
  the RequestActivationMethods API and NotifyServiceActivated API as
encryptedData within the TLS tunnel. SK is wrapped with the Issuer Encryption Public Key, in an RSA digital envelope, exposed by the API in encryptedKey.

The Optimal Asymmetric Encryption Padding (OAEP) scheme is used together with the RSA encryption. The MDES Issuer API exposes the hashing algorithm used by the OAEP scheme - oaepHashingAlgorithm.

The MDES Issuer API also exposes:

- The public key fingerprint - publicKeyFingerprint - of the Issuer Encryption Public Key used by the RSA-OAEP encryption scheme.
- The initialization vector - iv - for the bulk encryption with AES in CBC block cipher mode.

2.1.5 API Request / Response Common Elements and Headers

Every inbound and outbound request contains an element requestId which uniquely identifies the request. Every response contains an element responseld which uniquely identifies the response. The responseld may optionally use the corresponding requestId. Note that the format and uniqueness of the requestId and responseld are not validated.

In the case of an operation reporting an error, the response (or an object within the response) contains the element 'errorCode' and optionally the element 'errorDescription', as defined in Appendix B -- Error Codes. Unless explicitly stated otherwise, no other element (including 'Required' fields) is present if an error is reported.
The error elements can be returned in the response for any of the API calls.

### 2.1.5.1 Common Request Elements

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Data Type</th>
<th>Max Length</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>requestId</td>
<td>Unique identifier for the request.</td>
<td>String</td>
<td>64</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### 2.1.5.2 Common Response Elements

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Data Type</th>
<th>Max Length</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>responseId</td>
<td>Unique identifier for the response.</td>
<td>String</td>
<td>64</td>
<td>Yes</td>
</tr>
<tr>
<td>errorCode</td>
<td>Error code for the reason the operation failed.</td>
<td>String</td>
<td>32</td>
<td>Conditional – required if an error occurred performing the operation</td>
</tr>
<tr>
<td>errorDescription</td>
<td>Error description of the reason the operation failed.</td>
<td>String</td>
<td>256</td>
<td>No</td>
</tr>
</tbody>
</table>

### 2.1.6 Retry Strategy

MDES will automatically retry 3 times with up to a 5-second wait between each attempt of the DeliverActivationCode and NotifyServiceActivated API calls that fail with a:

- Timeout
- Connection failure
- HTTP response code of 302, 500 or 503
If the call has not succeeded after the initial retries, MDES will attempt a second round of 3 retries with increasing time intervals between each retry. Between attempts the system will wait 15 minutes, 30 minutes and then 2 hours. In the case of a 503, the Retry-After header will be respected if present and will count as a retry.

2.2 Request Activation Methods

Request Activation Methods advises an Issuer that a service activation has been requested and that an Issuer should provide Activation Methods for the Cardholder. The Activation Methods will be presented to the Cardholder so they may select their preferred delivery channel to receive an Activation Code only when the card eligibility decision is “Require Authentication.” If there are no methods to return then an empty Activation Methods array is returned. This call is made as part of the service activation flow and may be subject to strict time constraints based on the service.

If applicable to the service, when no methods are returned or in case of service failure the MDES system will use the methods returned by the pre-digitization network messages or the default methods for the account range. The methods returned from this API will be combined with the activation methods returned from the pre-digitization network messages and any methods configured as forced.

2.2.1 URL Endpoint

/requestActivationMethods

2.2.2 HTTP Method

POST

2.2.3 Request Parameters

<table>
<thead>
<tr>
<th>services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description: Array of services that are being requested for the account.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Value</th>
<th>Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIGITIZATION</td>
<td>Provision the card to a device.</td>
</tr>
</tbody>
</table>

Data Type: Array[String]
Max Length: N/A
Required: Yes
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Data Type</th>
<th>Max Length</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>cardInfo</td>
<td>Contains card information of the card to be digitized.</td>
<td>CardInfo object</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>correlationId</td>
<td>Value linking pre-digitization messages generated during provisioning.</td>
<td>String</td>
<td>14</td>
<td>Yes</td>
</tr>
<tr>
<td>tokenRequestorId</td>
<td>The party that requested the digitization.</td>
<td>String</td>
<td>11</td>
<td>Yes</td>
</tr>
<tr>
<td>walletId</td>
<td>The identifier of the Wallet Provider who requested the digitization. Only present when the token is provided to a Wallet Provider.</td>
<td>String</td>
<td>3</td>
<td>No</td>
</tr>
<tr>
<td>paymentAppInstanceId</td>
<td>The identifier of the Payment App instance within a device that will be provisioned with a token. Only present when supplied by a Wallet Provider. Note: This may contain the identifier of the Secure Element or a mobile device for some programs.</td>
<td>String</td>
<td>48</td>
<td>No</td>
</tr>
</tbody>
</table>
accountIDHash
Description: SHA-256 hash of the Cardholder’s account ID with the Payment App Provider. Typically expected to be an email address.
Data Type: String (Alpha-Numeric). Hex-encoded data (case-insensitive).
Max Length: 64
Required: No

mobileNumberSuffix
Description: The last few digits (typically four) of the device’s mobile phone number.
Data Type: String (Numeric)
Max Length: 32
Required: No

tokenType
Description: The type of token requested for this digitization.
Valid values are:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMBEDDED_SE</td>
<td>Embedded Secure Element</td>
</tr>
<tr>
<td>CLOUD</td>
<td>MasterCard Cloud-Based Payments</td>
</tr>
<tr>
<td>STATIC</td>
<td>Static token</td>
</tr>
</tbody>
</table>

Data Type: String
Max Length: 16
Required: Yes

2.2.4 Response Values

activationMethods
Description: The activation methods to be used for this digitization. Return empty array if no methods are to be returned.
Data Type: Array[ActivationMethod]
Required: Yes
2.2.5 Example Request Body
{
    "requestId": "123456",
    "services": [
        "DIGITIZATION"
    ],
    "cardInfo": {
        "encryptedData": "45454330443232363739304532433610DE1D1461475EB6D815F31764DDC20298BD779FBE37EE5AB3CBDA9F9825E1DDE321469537FE461E824AA55BA67BF6A",
        "publicKeyFingerprint": "4c4ead5927f0df8117f178eea9308daa58e27c2b",
        "encryptedKey": "A1B2C3D4E5F6112233445566",
        "oaepHashingAlgorithm": "SHA512",
        "iv": "31323334353637383930313233343536",
        "panUniqueReference": "FWSPMC000000000159f71f703d2141efaf04dd26803f922b",
        "correlationId": "D98765432104",
        "tokenRequestorId": "123456",
        "walletId": "123",
        "paymentAppInstanceId": "1b24f24a24ba98e27d43e345b532a245e4723d7a9c4f624e93452c",
        "accountIdHash": "5ae9c9890b326bd23bfa9db9672298ae3b10a9388e56ec17a001e191f24572aa",
        "mobileNumberSuffix": "1234",
        "tokenType": "CLOUD"
    }
}

2.2.6 Example Response Body
{
    "responseld": "123456",
    "activationMethods": [
        {
            "type": "TEXT_TO_CARDHOLDER_NUMBER",
            "value": "12X-XXX-XX32"
        },
        {
            "type": "CARDHOLDER_TO_CALL_AUTOMATED_NUMBER",
            "value": "1-800-BANK-NUMBER"
        }
    ]
}

© 2016 MasterCard. Proprietary and Confidential. All rights reserved.
MasterCard Digital Enablement Service - Issuer API Specification • Version 1.1 (Release 3.2)
2.3 DeliverActivationCode

DeliverActivationCode is used to request an Activation Code be sent to authenticate the Cardholder.

MDES generates an Activation Code and delivers it, along with the chosen Activation Code Distribution Method, to the Issuer for transmission to the Cardholder. The Cardholder will then enter the Activation Code into the Mobile Payment App.

Once an Activation Code has been generated, it will be valid for a limited activation period, after which the code will expire. Once a code expires, the Issuer can request a new Activation Code via the Customer Service Portal/API, or remotely activate the token via the Customer Service Portal/API.

The Cardholder may request the Activation Code again with the same or a different Activation Code Distribution Method. This will trigger another request as long as the activation period has not expired. It will not cause the Activation Code to be regenerated nor extend the validity period of the Activation Code.

2.3.1 URL Endpoint

/deliverActivationCode

2.3.2 HTTP Method

POST

2.3.3 Request Parameters

<table>
<thead>
<tr>
<th>tokenUniqueReference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description:</td>
</tr>
<tr>
<td>Data Type:</td>
</tr>
<tr>
<td>Max Length:</td>
</tr>
<tr>
<td>Required:</td>
</tr>
</tbody>
</table>
2.3.4 Response Values
Only common response elements

2.3.5 Example Request Body
{
    "requestId" : "123456",
    "tokenUniqueReference" : "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
}
"correlationId" : "D98765432104",
"activationCode" : "A1B2C3D4",
"expirationDateTime" : "2016-07-04T12:08:56.123-07:00",
"activationMethod" : {
    "type" : "CARDHOLDER_TO_CALL_AUTOMATED_NUMBER",
    "value" : "1-800-BANK-NUMBER"
}
}

2.3.6 Example Response Body
{
    "responseId" : "123456"
}

2.4 NotifyServiceActivated

NotifyServiceActivated is used to receive notifications that the provisioning and activation of a token for a Primary Account Number has been completed by the digitization service.

2.4.1 URL Endpoint

/notifyServiceActivated

2.4.2 HTTP Method

POST

2.4.3 Request Parameters
<table>
<thead>
<tr>
<th><strong>services</strong></th>
<th>Description: Array of services that are being requested for the account.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Value</strong></td>
<td><strong>Request</strong></td>
</tr>
<tr>
<td>DIGITIZATION</td>
<td>Provision the card to a device.</td>
</tr>
<tr>
<td>Data Type:</td>
<td>Array[String]</td>
</tr>
<tr>
<td>Max Length:</td>
<td>N/A</td>
</tr>
<tr>
<td>Required:</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>cardAndToken</strong></th>
<th>Description: Contains card and token information of the card to be digitized.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Type:</strong></td>
<td>CardAndTokenInfo object.</td>
</tr>
<tr>
<td><strong>Max Length:</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Required:</strong></td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>deviceInfo</strong></th>
<th>Description: Contains information about the target device to be provisioned.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Type:</strong></td>
<td>Map (DeviceInfo).</td>
</tr>
<tr>
<td><strong>Max Length:</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Required:</strong></td>
<td>No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>correlationId</strong></th>
<th>Description: Value linking pre-digitization messages generated during provisioning.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Type:</strong></td>
<td>String</td>
</tr>
<tr>
<td><strong>Max Length:</strong></td>
<td>14</td>
</tr>
<tr>
<td><strong>Required:</strong></td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>tokenRequestorId</strong></th>
<th>Description: The party that requested the digitization.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Type:</strong></td>
<td>String</td>
</tr>
<tr>
<td><strong>Max Length:</strong></td>
<td>11</td>
</tr>
<tr>
<td><strong>Required:</strong></td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>walletId</strong></th>
<th>Description: The identifier of the Wallet Provider who requested the digitization. Only present when the token is provided to a Wallet Provider.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Type:</strong></td>
<td>String</td>
</tr>
<tr>
<td><strong>Max Length:</strong></td>
<td>3</td>
</tr>
<tr>
<td><strong>Required:</strong></td>
<td>No</td>
</tr>
</tbody>
</table>
### paymentAppInstanceId
**Description:** The identifier of the Payment App instance within a device that will be provisioned with a token. Only present when supplied by a Wallet Provider.

*Note: This may contain the identifier of the Secure Element or a mobile device for some programs.*

**Data Type:** String  
**Max Length:** 48  
**Required:** No

### tokenType
**Description:** The type of token requested for this digitization.  
**Valid values are:**

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMBEDDED_SE</td>
<td>Embedded Secure Element</td>
</tr>
<tr>
<td>CLOUD</td>
<td>MasterCard Cloud-Based Payments</td>
</tr>
<tr>
<td>STATIC</td>
<td>Static token</td>
</tr>
</tbody>
</table>

**Data Type:** String  
**Max Length:** 16  
**Required:** Yes

### secureElementId
**Description:** The identifier of the Secure Element to be provisioned with the token. Present only when the token is provisioned to a Secure Element and when provided by the Wallet Provider.

**Data Type:** String  
**Max Length:** 48  
**Required:** No

### accountPanSuffix
**Description:** The last few digits (typically four) of the Account PAN being digitized.

**Data Type:** String  
**Max Length:** 8  
**Required:** Yes
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Data Type</th>
<th>Max Length</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>serviceRequestDateTime</td>
<td>The date and time the service for the PAN was requested. Expressed in ISO 8601 extended format as one of the following: YYYY-MM-DD Thh:mm:ss[.sss]Z YYYY-MM-DD Thh:mm:ss[.sss]±hh:mm Where [.sss] is optional and can be 1 to 3 digits.</td>
<td>String</td>
<td>29</td>
<td>Yes</td>
</tr>
<tr>
<td>termsAndConditionsAssetId</td>
<td>The Terms and Conditions as presented to and accepted by the Cardholder.</td>
<td>String</td>
<td>64</td>
<td>No</td>
</tr>
<tr>
<td>termsAndConditionsAcceptedTimestamp</td>
<td>The date and time the Terms and Conditions were accepted by the Cardholder. Expressed in ISO 8601 extended format as one of the following: YYYY-MM-DD Thh:mm:ss[.sss]Z YYYY-MM-DD Thh:mm:ss[.sss]±hh:mm Where [.sss] is optional and can be 1 to 3 digits.</td>
<td>String</td>
<td>29</td>
<td>No</td>
</tr>
<tr>
<td>productConfigurationId</td>
<td>Freeform identifier for the product configuration as assigned by the Issuer.</td>
<td>String</td>
<td>64</td>
<td>No</td>
</tr>
</tbody>
</table>
consumerLanguage

Description: Language preference selected by the consumer. Formatted as an ISO-639-1 two-letter language code.
Data Type: String
Max Length: 2
Required: No

decision

Description: The authorization decision for the service request. Must be one of:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPROVED</td>
<td>Service request was approved.</td>
</tr>
<tr>
<td>REQUIRE_ADDITIONAL_AUTHENTICATION</td>
<td>Service request requires additional authentication to be approved.</td>
</tr>
<tr>
<td></td>
<td>One or more Activation Methods will be provided.</td>
</tr>
</tbody>
</table>

Data Type: String
Max Length: 64
Required: Yes

decisionMadeBy

Description: The process that determined the final authorization decision for the request. Must be one of:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>ELIGIBILITY_REQUEST</td>
<td>The decision was made by the eligibility request to the Issuer.</td>
</tr>
<tr>
<td>AUTHORIZATION_REQUEST</td>
<td>The decision was made by the authorization request to the Issuer.</td>
</tr>
<tr>
<td>RULES</td>
<td>The decision was made by the rule engine.</td>
</tr>
</tbody>
</table>

Data Type: String
Max Length: 32
Required: Yes
**tokenActivatedDateTime**
Description: Expressed in ISO 8601 extended format as one of the following:
- YYYY-MM-DDThh:mm:ss[.sss]Z
- YYYY-MM-DDThh:mm:ss[.sss]±hh:mm
Where [.sss] is optional and can be 1 to 3 digits.
Data Type: String
Max Length: 29
Required: Yes

**numberOfActivationAttempts**
Description: The number of times an Activation Code was received to activate the token.
Data Type: Number
Max Length: 1
Required: No

**numberOfActiveTokens**
Description: The number of active tokens for the Primary Account Number.
Data Type: Number
Max Length: 2
Required: No

**tokenAssuranceLevel**
Description: The assurance level assigned to the token.
Data Type: Number
Max Length: 2
Required: No

### 2.4.4 Response Values
Only common response elements

### 2.4.5 Example Request Body
```json
{
  "requestId" : "123456",
  "services" : [
    "DIGITIZATION"
  ],
  "cardAndToken" : {
```
"encryptedData": "45454330443232363739304532433610DE1D461475BEB6D815F31764DCC20298BD779FBE37EE5AB3CBDA9F9825E1DDE321469537FE461E824AA55BA678F6A",
"publicKeyFingerprint": "4c4ead5927f0df8117f178eea9308daa58e27c2b",
"encryptedKey": "A1B2C3D4E5F6112233445566",
"oaepHashingAlgorithm": "SHA512",
"iv": "31323334353637383930313233343536",
"tokenUniqueReference": "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
"panUniqueReference": "FWSPMC000000000159f71f703d2141efaf04dd26803f922",

deviceInfo": {
  "deviceName": "My Phone",
  "serialNumber": "2F6D63",
  "formFactor": "PHONE",
  "isoDeviceType": "09",
  "osName": "ANDROID",
  "osVersion": "4.4",
  "imei": "352099001761481",
  "msisdn": "7307406945",
  "paymentTypes": ["NFC"],
  "storageTechnology": "SE"
},
correlationId": "D98765432104",
"tokenRequestorId": "123456",
"walletId": "123",
"paymentApplInstanceId": "1b24f24a24ba98e27d43e345b532a245e4723d7a9c4f624e93452c",
"tokenType": "CLOUD",
"secureElementId": "1b24f24a24ba98e27d43e345b532a245e4723d7a9c4f624e93452c",
"accountPanSuffix": "1234",
"serviceRequestDateTime": "2015-07-04T12:08:56.123-07:00",
"termsAndConditionsAssetId": "a9f027e5-629d-11e3-949a-0800200c9a66",
"termsAndConditionsAcceptedTimestamp": "2015-07-04T12:09:56.123-07:00",
"productConfigurationId": "1234",
"consumerLanguage": "en",
"decision": "REQUIRE_ADDITIONAL_AUTHENTICATION",
"decisionMadeBy": "RULES",
"tokenActivatedDateTime": "2015-07-04T12:09:57.123-07:00"
"numberOfActivationAttempts": 1,
"numberOfActiveTokens": 2,
"tokenAssuranceLevel": 1
}

2.4.6 Example Response Body
{
   "responseId": "123456"
}

2.5 AuthorizeService

AuthorizeService requests an Issuer to authorize a Primary Account Number for a MasterCard service or set of services. Information about the service request will be provided to assist with authorization of the account.

If additional authentication is required the Issuer may return a list of Activation Methods. The Activation Methods will be presented to the Cardholder so they may select their preferred delivery channel to receive an Activation Code. If there are no methods to return the field may be omitted. This call is made as part of the service activation flow and may be subject to strict time constraints based on the service.

2.5.1 URL Endpoint
/authorizeService

2.5.2 HTTP Method
POST

2.5.3 Request Parameters

<table>
<thead>
<tr>
<th>services</th>
<th>Description: Array of services that are being requested for the account.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>Request</td>
</tr>
<tr>
<td>DIGITIZATION</td>
<td>Provision the card to a device.</td>
</tr>
</tbody>
</table>

| Data Type:        | Array[String]                                                               |
| Max Length:       | N/A                                                                        |
| Required:         | Yes                                                                         |
### cardInfo
- **Description:** Contains card information of the card to be digitized.
- **Data Type:** CardInfo object.
- **Max Length:** N/A
- **Required:** Yes

### correlationId
- **Description:** Value linking pre-digitization messages generated during provisioning.
- **Data Type:** String
- **Max Length:** 14
- **Required:** Yes

### tokenRequestorId
- **Description:** The party that requested the digitization.
- **Data Type:** String
- **Max Length:** 11
- **Required:** Yes

### walletId
- **Description:** The identifier of the Wallet Provider who requested the digitization. Only present when the token is provided to a Wallet Provider.
- **Data Type:** String
- **Max Length:** 3
- **Required:** No

### paymentAppInstanceId
- **Description:** The identifier of the Payment App instance within a device that will be provisioned with a token. Only present when supplied by a Wallet Provider.
  - Note: This may contain the identifier of the Secure Element or a mobile device for some programs.
- **Data Type:** String
- **Max Length:** 48
- **Required:** No
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Data Type</th>
<th>Max Length</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>accountIdHash</td>
<td>SHA-256 hash of the Cardholder’s account ID with the Payment App Provider. Typically expected to be an email address.</td>
<td>String (Alpha-Numeric). Hex-encoded data (case-insensitive).</td>
<td>64</td>
<td>No</td>
</tr>
<tr>
<td>mobileNumberSuffix</td>
<td>The last few digits (typically four) of the device’s mobile phone number.</td>
<td>String (Numeric)</td>
<td>32</td>
<td>No</td>
</tr>
<tr>
<td>deviceInfo</td>
<td>Contains information about the target device to be provisioned.</td>
<td>Map (DeviceInfo)</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td>walletProviderDecisioningInfo</td>
<td>Contains information about the decision recommended by the Wallet Provider.</td>
<td>Map (DecisioningInfo).</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td>activeTokenCount</td>
<td>The number of active tokens that already exist for the PAN based on the token type. Secure Element and Cloud tokens are counted together.</td>
<td>String (Numeric).</td>
<td>N/A</td>
<td>No</td>
</tr>
</tbody>
</table>
**tokenType**

Description: The type of token requested for this digitization. Valid values are:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMBEDDED_SE</td>
<td>Embedded Secure Element</td>
</tr>
<tr>
<td>CLOUD</td>
<td>MasterCard Cloud-Based Payments</td>
</tr>
<tr>
<td>STATIC</td>
<td>Static token</td>
</tr>
</tbody>
</table>

Data Type: String  
Max Length: 16  
Required: Yes

### 2.5.4 Response Values

**services**

Description: Array of services for the account that the authorization decision applies to. Must be a subset of the services in the request object. Services that are not approved for the account will be omitted.

<table>
<thead>
<tr>
<th>Value</th>
<th>Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIGITIZATION</td>
<td>Provision the card to a device.</td>
</tr>
</tbody>
</table>

Data Type: Array[String]  
Max Length: N/A  
Required: Yes
**decision**

**Description:** The authorization decision for the authorization of the requested services.

Must be one of:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPROVED</td>
<td>Services request was approved.</td>
</tr>
<tr>
<td>DECLINED</td>
<td>Services request was declined.</td>
</tr>
<tr>
<td>REQUIRE_ADDITIONAL_AUTHENTICATION</td>
<td>Services request requires additional authentication to be approved. One or more Activation Methods may be provided.</td>
</tr>
</tbody>
</table>

**Data Type:** String

**Max Length:** 64

**Required:** Yes

**activationMethods**

**Description:** The activation methods to be used for this digitization. Return empty array if no methods are to be returned.

**Data Type:** Array[ActivationMethod]

**Required:** No

**panSequenceNumber**

**Description:** The pan sequence number for the card.

**Data Type:** String(numeric)

**Max Length:** 3

**Required:** No

**issuerProductConfigId**

**Description:** The unique Issuer identifier assigned to the product configuration in BPMS. It is provided for the Digitization service only.

**Data Type:** String

**Max Length:** 10

**Required:** No

### 2.5.5 Example Request Body

```
{
    "requestId" : "123456",
    "services" : [
        "DIGITIZATION"
    ]
}```

{
    "cardInfo": {
        "encryptedData": "4545433044322323267379304532433610DE1D1461475BEB6D815F31764DCC20298BD779FBE37EE5AB3CB8A9F9825E1DE321469537F461E824AA55BA6786A",
        "publicKeyFingerprint": "4c4ead5927f0df8117f178eea9308daa58e27c2b",
        "encryptedKey": "A1B2C3D4E5F6112233445566",
        "oaepHashingAlgorithm": "SHA512",
        "iv": "31323334353637383930313233343536",
        "panUniqueReference": "FWSPMC000000000159f71f703d2141efaf04dd26803f922b"
    },
    "correlationId": "D98765432104",
    "tokenRequestorId": "123456",
    "walletId": "123",
    "paymentAppInstanceId": "1b24f24a24ba98e27d43e345b532a245e4723d7a9c4f624e93452c",
    "accountIdHash": "5ae9c9890b326bd23bfa9db9672298ae3b10a9388e56ec17a001e191f24572aa",
    "mobileNumberSuffix": "1234",
    "activeTokenCount": "3",
    "deviceInfo": {
        "deviceName": "My Phone",
        "serialNumber": "2F6D63",
        "formFactor": "PHONE",
        "isoDeviceType": "09",
        "osName": "ANDROID",
        "osVersion": "4.4",
        "imei": "352099001761481",
        "msisdn": "7307406945",
        "paymentTypes": ["NFC"],
        "storageTechnology": "SE"
    },
    "walletProviderDecisioningInfo": {
        "recommendedDecision": "REQUIRE_ADDITIONAL_AUTHENTICATION",
        "recommendationStandardVersion": "1.0.0",
        "deviceScore": "3",
        "accountScore": "4",
        "recommendationReasons": ["ACCOUNT_TOO_NEW", "DEVICE_RECENTLY_LOST", "OUTSIDE_HOME_TERRITORY"]
    }
},
"tokenType": "CLOUD"

© 2016 MasterCard. Proprietary and Confidential. All rights reserved.
MasterCard Digital Enablement Service - Issuer API Specification • Version 1.1 (Release 3.2)
2.5.6 Example Response Body

{
"responseId" : "123456",
"services" : ["DIGITIZATION"],
"decision" : "REQUIRE_ADDITIONAL_AUTHENTICATION",
"activationMethods" : [
{
"type" : "TEXT_TO_CARDHOLDER_NUMBER",
"value" : "12X-XXX-XX32"
},
{
"type" : "CARDHOLDER_TO_CALL_AUTOMATED_NUMBER",
"value" : "1-800-BANK-NUMBER"
},
{
"type" : "CARDHOLDER_TO_USE_MOBILE_APP",
"value" : "App Name"
}
],
"panSequenceNumber" : "001",
"issuerProductConfigId" : "I1234D7890"
}

2.6 NotifyTokenUpdated

NotifyTokenUpdated is used by MDES to notify the Issuer of significant token updates, such as when the token is activated, suspended, unsuspended or deleted; or when information about the token or its product configuration has changed.

It may be triggered as a result of Service Provider update (for example, the provider suspends or deletes the token), or if MDES changes the state of a token (for example, when Cardholder activates the token using an Activation Code).

2.6.1 URL Endpoint

/notifyTokenUpdated
2.6.2 HTTP Method

POST

2.6.3 Request Parameters

Tokens
- Description: Contains the Tokens which were updated.
- Data Type: Array[Token object]
- Max Length: N/A
- Required: Yes

2.6.4 Response Parameters

Only common response elements

2.6.5 Example Request Body

```json
{
    "requestId" : "123456",
    "tokens" : [
        {
            "tokenUniqueReference" : "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
            "status" : "ACTIVE"
        },
        {
            "tokenUniqueReference" : "DWSPMC00000000032d72d4fcb2f4136a0532d32d72d4fcb",
            "status" : "ACTIVE"
        },
        {
            "tokenUniqueReference" : "DWSPMC000000000fcb2f4136b2f4136a0532d2f4136a0532",
            "status" : "SUSPENDED",
            "suspendedBy" : ["PAYMENT_APP_PROVIDER"]
        }
    ]
}
```

2.6.6 Example Response Body

```json
{
    "responseId" : "123456"
}
```
### A. Appendix A – Request and Response Member Objects

#### A.1 ActivationMethod

**Type**

Description: Specifies the activation method type.

Must be one of:

<table>
<thead>
<tr>
<th>Type</th>
<th>Meaning</th>
<th>Value Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>TEXT_TO_CARDHOLDER_NUMBER</td>
<td>Text message to Cardholder’s mobile phone number. Value will be the Cardholder’s masked mobile phone number.</td>
<td>Yes</td>
</tr>
<tr>
<td>EMAIL_TO_CARDHOLDER_ADDRESS</td>
<td>Email to Cardholder’s email address. Value will be the Cardholder’s masked email address.</td>
<td>Yes</td>
</tr>
<tr>
<td>CARDHOLDER_TO_CALL_AUTOMATED_NUMBER</td>
<td>Cardholder-initiated call to automated call center phone number. Value will be the phone number for the Cardholder to call.</td>
<td>Yes</td>
</tr>
<tr>
<td>CARDHOLDER_TO_CALL_MANNED_NUMBER</td>
<td>Cardholder-initiated call to manned call center phone number. Value will be the phone number for the Cardholder to call.</td>
<td>Yes</td>
</tr>
<tr>
<td>CARDHOLDER_TO_VISIT_WEBSITE</td>
<td>Cardholder to visit a website. Value will be the website URL.</td>
<td>Yes</td>
</tr>
<tr>
<td>CARDHOLDER_TO_USE_MOBILE_APP</td>
<td>Cardholder to use a specific mobile app to activate token. Value will be replaced by a formatted string.</td>
<td>Yes</td>
</tr>
<tr>
<td>ISSUER_TO_CALL_CARDHOLDER_NUMBER</td>
<td>Issuer-initiated voice call to Cardholder’s phone. Value will be the Cardholder’s masked voice call phone number.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Data Type:** String

**Max Length:** 64

**Required:** Yes
<table>
<thead>
<tr>
<th>value</th>
<th>Description: Specifies the activation method value (meaning varies depending on the activation method type).</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data Type: String</td>
</tr>
<tr>
<td></td>
<td>Max Length: 64</td>
</tr>
<tr>
<td></td>
<td>Required: Yes</td>
</tr>
</tbody>
</table>

### A.2 BillingAddress

<table>
<thead>
<tr>
<th>line1</th>
<th>Description: First line of the billing address.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data Type: String</td>
</tr>
<tr>
<td></td>
<td>Max Length: 64</td>
</tr>
<tr>
<td></td>
<td>Required: No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>line2</th>
<th>Description: Second line of the billing address.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data Type: String</td>
</tr>
<tr>
<td></td>
<td>Max Length: 64</td>
</tr>
<tr>
<td></td>
<td>Required: No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>city</th>
<th>Description: The city of the billing address.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data Type: String</td>
</tr>
<tr>
<td></td>
<td>Max Length: 32</td>
</tr>
<tr>
<td></td>
<td>Required: No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>countrySubdivision</th>
<th>Description: The country subdivision (for example, the state in the U.S.) of the billing address.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data Type: String</td>
</tr>
<tr>
<td></td>
<td>Max Length: 12</td>
</tr>
<tr>
<td></td>
<td>Required: No</td>
</tr>
<tr>
<td>postalCode</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td></td>
</tr>
<tr>
<td>Description: The postal code (for example, zipcode in the U.S.) of the billing address.</td>
<td></td>
</tr>
<tr>
<td>Data Type: String</td>
<td></td>
</tr>
<tr>
<td>Max Length: 16</td>
<td></td>
</tr>
<tr>
<td>Required: No</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description: The country of the billing address. Expressed as a 3-letter (alpha-3) country code as defined in ISO 3166-1.</td>
</tr>
<tr>
<td>Data Type: String</td>
</tr>
<tr>
<td>Max Length: 3 (Exact)</td>
</tr>
<tr>
<td>Required: No</td>
</tr>
</tbody>
</table>

### A.3 CardAndTokenData

<table>
<thead>
<tr>
<th>card</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description: The account PAN information</td>
</tr>
<tr>
<td>Data Type: CardInfoData</td>
</tr>
<tr>
<td>Max Length: NA</td>
</tr>
<tr>
<td>Required: Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>token</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description: The token information</td>
</tr>
<tr>
<td>Data Type: TokenData</td>
</tr>
<tr>
<td>Max Length: NA</td>
</tr>
<tr>
<td>Required: Yes</td>
</tr>
</tbody>
</table>

### A.4 CardAndTokenInfo

<table>
<thead>
<tr>
<th>panUniqueReference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description: Reference to the PAN that is unique per Wallet Provider.</td>
</tr>
<tr>
<td>Data Type: String</td>
</tr>
<tr>
<td>Max Length: 64</td>
</tr>
<tr>
<td>Required: Yes</td>
</tr>
</tbody>
</table>
**tokenUniqueReference**
Description: Globally unique identifier for the token, as assigned by MDES.
Data Type: String
Max Length: 64
Required: Yes

**publicKeyFingerprint**
Description: The fingerprint of the public key used to encrypt the ephemeral AES key.
Data Type: String. Hex-encoded data (case-insensitive).
Max Length: 64
Required: Yes

**encryptedKey**
Description: One-time use AES key encrypted by the Issuer's public key (as identified by 'publicKeyFingerprint') using the OAEP scheme. Requirement is for a 128-bit key (with 256-bit key supported as an option).
Data Type: String. Hex-encoded data (case-insensitive).
Max Length: 512
Required: Yes

**oaepHashingAlgorithm**
Description: Hashing algorithm used with the OAEP scheme. Must be one of:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA256</td>
<td>Use the SHA-256 algorithm</td>
</tr>
<tr>
<td>SHA512</td>
<td>Use the SHA-512 algorithm</td>
</tr>
</tbody>
</table>

Data Type: String
Max Length: 6
Required: Yes
**iv**

Description: 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.

Data Type: String. Hex-encoded data (case-insensitive).

Max Length: 32 (Exact)

Required: No

**encryptedData**

Description: Contains the encrypted CardAndTokenData object containing the Account PAN and token information. Encrypted by the ephemeral AES key using CBC mode (IV as provided in 'iv', or zero if none provided) and PKCS#7 padding.

Sample unencrypted object:

```
{
  "card": {
    "accountNumber": "5123456789012345",
    "expiryMonth": "12",
    "expiryYear": "15",
    "source": "CARD_ON_FILE",
    "cardholderName": "John Doe",
    "securityCode": "123",
    "cardholderData": {
      "sourceIp": "127.0.0.1",
      "deviceLocation": "38.63, -90.2"
    }
  },
  "token": {
    "token": "5345678901234521",
    "expiryMonth": "10",
    "expiryYear": "17"
  }
}  
```

Data Type: String. Hex-encoded data (case-insensitive).

Max Length: 256K

Required: Yes
A.5 CardholderData

sourceIp
Description: The IP of the device initiating the request.
Data Type: String
Max Length: 64
Required: No

deviceLocation
Description: Latitude and longitude where the device the consumer is attempting to authorize is located. In the format "(sign) latitude, (sign) longitude" with a precision of 2 decimal places. Ex: "38.63, -90.2" Latitude is between -90 and 90. Longitude between -180 and 180.
Data Type: String
Max Length: 64
Required: No

A.6 CardInfo

panUniqueReference
Description: Reference to the PAN that is unique per Wallet Provider.
Data Type: String
Max Length: 64
Required: No

publicKeyFingerprint
Description: The fingerprint of the public key used to encrypt the ephemeral AES key.
Data Type: String. Hex-encoded data (case-insensitive).
Max Length: 64
Required: Yes
encryptedKey
Description: One-time use AES key encrypted by the Issuer's public key (as identified by 'publicKeyFingerprint') using the OAEP scheme.
   Requirement is for a 128-bit key (with 256-bit key supported as an option).
Data Type: String. Hex-encoded data (case-insensitive).
Max Length: 512
Required: Yes

oaepHashingAlgorithm
Description: Hashing algorithm used with the OAEP scheme.
   Must be one of:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA256</td>
<td>Use the SHA-256 algorithm</td>
</tr>
<tr>
<td>SHA512</td>
<td>Use the SHA-512 algorithm</td>
</tr>
</tbody>
</table>

Data Type: String
Max Length: 6
Required: Yes

iv
Description: 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.
Data Type: String. Hex-encoded data (case-insensitive).
Max Length: 32 (Exact)
Required: No
encryptedData
Description: Contains the encrypted CardInfoData object containing the Account PAN information. Encrypted by the ephemeral AES key using CBC mode (IV as provided in 'iv', or zero if none provided) and PKCS#7 padding.
Sample unencrypted object:
{
    "accountNumber": "5123456789012345",
    "expiryMonth": "12",
    "expiryYear": "15",
    "source": "CARD_ON_FILE",
    "cardholderName": "John Doe",
    "securityCode": "123",
    "cardholderData": {
        "sourceIp": "127.0.0.1",
        "deviceLocation": "38.63, -90.2"
    }
}
Data Type: String. Hex-encoded data (case-insensitive).
Max Length: 256 K
Required: Yes

A.7 CardInfoData

accountNumber
Description: The Account PAN of the card associated with the service or the token PAN.
Data Type: String (Numeric)
Max Length: 19 (min length 12)
Required: Yes
**expiryMonth**

Description: 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.

Data Type: String (Numeric)
Max Length: 2 (Exact)
Required: No

**expiryYear**

Description: 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.

Data Type: String (Numeric)
Max Length: 2 (Exact)
Required: No

**source**

Description: The source of this card information. Must be one of:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>CARD_ON_FILE</td>
<td>Source was an existing card on file.</td>
</tr>
<tr>
<td>CARD_ADDED_MANUALLY</td>
<td>Source was a new card entered manually by the Cardholder.</td>
</tr>
<tr>
<td>CARD_ADDED_VIA_APPLICATION</td>
<td>Source was a new card added by another application (for example, Issuer banking app).</td>
</tr>
</tbody>
</table>

Data Type: String
Max Length: 32
Required: No – Optionally present for Account PAN.
### cardholderName
**Description:** The name of the Cardholder in the format LASTNAME/FIRSTNAME or FIRSTNAME LASTNAME.
**Data Type:** String
**Max Length:** 27
**Required:** No – Optionally present for Account PAN.

### securityCode
**Description:** The CVC2 for the card to be digitized, as entered by the Cardholder. Verified as part of reaching the digitization decision.
**Data Type:** String(Numeric)
**Max Length:** 3 (Exact)
**Required:** No

### dataValidUntilTimestamp
**Description:** The date/time after which this CardInfoData object is considered invalid. If present, all systems should 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:
- YYYY-MM-DDTH:mm:ss[.sss]Z
- YYYY-MM-DDTH:mm:ss[.sss]±hh:mm

Where [.sss] is optional and can be 1 to 3 digits.

Must be a value no more than 30 days in the future. MasterCard recommends using a value of (Current Time + 30 minutes).

**Data Type:** String
**Max Length:** 29
**Required:** No

### billingAddress
**Description:** Cardholder billing address information.
**Data Type:** BillingAddress
**Required:** No
cardholderData
Description: Cardholder information used for authorizing the account.
Data Type: CardHolderData
Required: No

A.8 DecisioningInfo – MAP<String, Object>

recommendedDecision
Description: The decision recommended by the Wallet Provider.
Must be one of:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPROVED</td>
<td>Services request was approved.</td>
</tr>
<tr>
<td>DECLINED</td>
<td>Services request was declined.</td>
</tr>
<tr>
<td>REQUIRE_ADDITIONAL_AUTHENTICATION</td>
<td>Services request requires additional authentication to be approved.</td>
</tr>
</tbody>
</table>

Data Type: String
Max Length: 64
Required: No

recommendationStandardVersion
Description: The standards version used by the Wallet Provider to determine the recommended decision.

Data Type: String
Max Length: 64
Required: No

deviceScore
Description: Score given to the device by the Wallet Provider. Value between 1 and 5

Data Type: String(Numeric)
Max Length: 64
Required: No
accountScore
Description: Score given to the account by the Wallet Provider. Value between 1 and 5
Data Type: String
Max Length: 64
Required: No

recommendationReasons
Description: Reasons provided to the Wallet Provider on how the recommended decision was reached. Values for reason codes are defined in Appendix C.
Data Type: Array[String]
Max Length: NA
Required: No

A.9 DeviceInfo – MAP<String, Object>

deviceName
Description: The name that the Cardholder has associated to the device with the Payment App Provider.
Data Type: String
Max Length: 64
Required: No

serialNumber
Description: The serial number of the device. May be masked.
Data Type: String
Max Length: 64
Required: No

isoDeviceType
Description: The 2 digit device type provided on the iso messages that the token is being provisioned to. Only present when provided by a Wallet Provider. See Global Communication bulletins for values.
Data Type: String
Max Length: 2
Required: No
**formFactor**

Description: The form factor of the device to be provisioned. Must be one of:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHONE</td>
<td>Mobile phone.</td>
</tr>
<tr>
<td>TABLET</td>
<td>Tablet computer.</td>
</tr>
<tr>
<td>WATCH</td>
<td>Watch.</td>
</tr>
</tbody>
</table>

Data Type: String  
Max Length: 64  
Required: No

**storageTechnology**

Description: The architecture or technology used for token storage. Must be one of:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEVICE_MEMORY</td>
<td>Device memory.</td>
</tr>
<tr>
<td>DEVICE_MEMORY_PROTECTED_TPM</td>
<td>Device memory using a protected trust platform module.</td>
</tr>
<tr>
<td>TEE</td>
<td>Trusted execution environment.</td>
</tr>
<tr>
<td>SE</td>
<td>Secure element.</td>
</tr>
<tr>
<td>SERVER</td>
<td>Server host.</td>
</tr>
<tr>
<td>VEE</td>
<td>Virtual Execution Environment</td>
</tr>
</tbody>
</table>

Data Type: String  
Max Length: 32  
Required: No

**osName**

Description: The name of the device operating system. Must be one of:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANDROID</td>
<td>Google Android operating system.</td>
</tr>
<tr>
<td>WINDOWS</td>
<td>Microsoft Windows operating system.</td>
</tr>
<tr>
<td>TIZEN</td>
<td>Tizen operating system.</td>
</tr>
<tr>
<td>IOS</td>
<td>Apple iOS operation system.</td>
</tr>
</tbody>
</table>

Data Type: String  
Max Length: 32  
Required: No
### osVersion
**Description:** The version of the device operating system.
**Data Type:** String (supports numbers and decimals).
**Max Length:** 32
**Required:** No

### paymentTypes
**Description:** Different types of Payments supported for the token.
Must be one of:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFC</td>
<td>The token is NFC capable</td>
</tr>
<tr>
<td>DSRP</td>
<td>The token is DSRP capable</td>
</tr>
<tr>
<td>ECOMMERCE</td>
<td>The token can be used for e-commerce transactions.</td>
</tr>
</tbody>
</table>

**Data Type:** Array[String]
**Max Length:** N/A
**Required:** No

### imei
**Description:** The IMEI number of the device being provisioned.
**Data Type:** String
**Max Length:** 15 (exact)
**Required:** No

### msisdn
**Description:** The MSISDN of the device being provisioned.
**Data Type:** String
**Max Length:** 15
**Required:** No

### A.10 Token

#### tokenUniqueReference
**Description:** The unique reference allocated to the token in the Digitize response.
**Data Type:** String
**Max Length:** 64
**Required:** Yes – always present even when an error occurs.
status
Description: The current status of token. Must be one of:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>INACTIVE</td>
<td>Token has not yet been activated</td>
</tr>
<tr>
<td>ACTIVE</td>
<td>Token is active and ready to transact</td>
</tr>
<tr>
<td>SUSPENDED</td>
<td>Token is suspended and unable to transact</td>
</tr>
<tr>
<td>DEACTIVATED</td>
<td>Token has been permanently deactivated</td>
</tr>
</tbody>
</table>

Data Type: String
Max Length: 32
Required: Yes

suspendedBy
Description: Who or what caused the token to be suspended.
One or more values of:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISSUER</td>
<td>Suspended by the Issuer. Payment App Provider unable to unsuspend this Token.</td>
</tr>
<tr>
<td>PAYMENT_APP_PROVIDER</td>
<td>Suspended by the Payment App Provider.</td>
</tr>
<tr>
<td>MOBILE_PIN_LOCKED</td>
<td>Suspended due to the Mobile PIN being locked.</td>
</tr>
<tr>
<td>CARDHOLDER</td>
<td>Suspended by the Cardholder</td>
</tr>
</tbody>
</table>

Data Type: Array[String]
Max Length: N/A
Required: Conditional – required if status = SUSPENDED.

A.11 TokenData

token
Description: The token issued for this service request.
Data Type: String (Numeric)
Max Length: 19 (min length 12)
Required: Yes

expiryMonth
Description: The month of the expiration date.
Data Type: String (Numeric)
Max Length: 2 (Exact)
Required: Yes

expiryYear
Description: The year of the expiration date.
Data Type: String (Numeric)
Max Length: 2 (Exact)
Required: Yes
## B. Appendix B – Error Codes

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Error Description</th>
<th>Error Circumstances</th>
</tr>
</thead>
<tbody>
<tr>
<td>INVALID_JSON</td>
<td>Invalid JSON</td>
<td>The JSON could not be parsed.</td>
</tr>
<tr>
<td>MISSING_REQUIRED_FIELD</td>
<td>Missing Required Field - {fieldName}</td>
<td>A required field is missing.</td>
</tr>
<tr>
<td>INVALID_FIELD_FORMAT</td>
<td>Invalid Field Format - {fieldName}</td>
<td>The field is not in the correct format. For instance, it should be a number but is a string.</td>
</tr>
<tr>
<td>INVALID_FIELD_LENGTH</td>
<td>Invalid Field Length - {fieldName}</td>
<td>The value does not fall between the minimum and maximum length for the field.</td>
</tr>
<tr>
<td>INVALID_FIELD_VALUE</td>
<td>Invalid Field Value - {fieldName}</td>
<td>The value is not allowed for the field.</td>
</tr>
<tr>
<td>CRYPTOGRAPHY_ERROR</td>
<td>Cryptography Error</td>
<td>There was an error decrypting the encrypted payload.</td>
</tr>
<tr>
<td>INTERNAL_SERVICE_FAILURE</td>
<td>The system had an internal exception</td>
<td>System had an internal exception.</td>
</tr>
<tr>
<td>MISSING_EXPIRY_DATE</td>
<td>Missing Expiry Date</td>
<td>The expiry date is required for this product but was missing. Retry the request supplying the expiry date for this card.</td>
</tr>
</tbody>
</table>
### Appendix C – Reason Codes

#### C.1 Approved Reason Codes

Recommendation reasons for an ‘APPROVED’ recommendation must be one of:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>LONG_ACCOUNT_TENURE</td>
<td>Account has existed for an extended period of not less than one year. A Payment App Provider may determine a longer account tenure to qualify for this reason.</td>
</tr>
<tr>
<td>GOOD_ACTIVITY_HISTORY</td>
<td>There has been financial activity linked to the account for at least and within a period of not less than six months; no suspicious activity is linked to the account within a period of at least one year.</td>
</tr>
<tr>
<td>ADDITIONAL_DEVICE</td>
<td>The digitization is for an additional device for the same Account PAN and consumer account. There must be a currently active (not suspended) Token that was previously digitized and activated on an existing device for the same Account PAN and consumer account.</td>
</tr>
<tr>
<td>SOFTWARE_UPDATE</td>
<td>The digitization has been requested due to an authenticated operating system or other software update being installed on the device, causing mobile payment data to be wiped and unable to be restored. This digitization must be for the same paymentAppinstanceld to which a Token was previously digitzed and activated for the same Account PAN and consumer account.</td>
</tr>
</tbody>
</table>

#### C.2 Require Additional Authentication or Declined Reason Codes

Recommendation reasons for a 'REQUIRE_ADDITIONAL_AUTHENTICATION' or 'DECLINED' recommendation must be one of:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCOUNT_TOO_NEW_SINCE_LAUNCH</td>
<td>Account is considered new relative to Payment App Provider service launch</td>
</tr>
<tr>
<td>ACCOUNT_TOO_NEW</td>
<td>Account is considered new relative to provisioning request</td>
</tr>
<tr>
<td>ACCOUNT_CARD_TOO_NEW</td>
<td>Account/card is considered new relative to provisioning request</td>
</tr>
<tr>
<td>ACCOUNT_RECENTLY_CHANGED</td>
<td>Changes have recently been made to account data</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>SUSPICIOUS_ACTIVITY</td>
<td>Suspicious activity has been linked to this account</td>
</tr>
<tr>
<td>INACTIVE_ACCOUNT</td>
<td>Inactive account</td>
</tr>
<tr>
<td>HAS_SUSPENDED_TOKENS</td>
<td>Device contains suspended tokens</td>
</tr>
<tr>
<td>DEVICE_RECENTLY_LOST</td>
<td>Device has recently been reported lost</td>
</tr>
<tr>
<td>TOO_MANY_RECENT_ATTEMPTS</td>
<td>Excessive recent tokenization attempts to this device</td>
</tr>
<tr>
<td>TOO_MANY_RECENT_TOKENS</td>
<td>Excessive recent tokenization to this device</td>
</tr>
<tr>
<td>TOO_MANY_DIFFERENT_CARDHOLDERS</td>
<td>Excessive non-matching Cardholder names within the device</td>
</tr>
<tr>
<td>LOW_DEVICE_SCORE</td>
<td>Low device score</td>
</tr>
<tr>
<td>LOW_ACCOUNT_SCORE</td>
<td>Low account score</td>
</tr>
<tr>
<td>OUTSIDE_HOME_TERRITORY</td>
<td>Non-domestic tokenization attempt</td>
</tr>
<tr>
<td>UNABLE_TO_ASSESS</td>
<td>Unable to provide recommendation due to system issues.</td>
</tr>
<tr>
<td>HIGH_RISK</td>
<td>High fraud risk identified. Enhanced verification recommended.</td>
</tr>
</tbody>
</table>