Mastercard Digital Enablement Service

Application Programming Interface

Version 1.2.0

14 December 2017

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.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

Summary of Changes

Description of Change	Where to Look
Recent regulations in certain regions are requiring digital payment devices to provide a unique identifier for each consumer, which financial institutions will then need to verify before a consumer can add their credentials to the payment-enabled devices. The first implementation of this feature will be in support of the Korean market. Wallet Providers will provide a value (up to 88 bytes) that represents the consumer as part of the information supplied during Digitization. This information is then passed to the Issuer for validation. A new field, 'consumerIdentifier', is available within the cardInfo object.	A.10 CardInfoData

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

Abbreviations and Acronyms

The following abbreviations and acronyms are used in this document:

Abbreviation	Description
AC	Application Cryptogram
AID	Application Identifier
API	Application Programming Interface
ARQC	Authorization Request Cryptogram
ATC	Application Transaction Counter
CAM	Card Authentication Method
CSR	Customer Service Representative
CVC	Card Verification Code
CVM	Cardholder Verification Method
DPAN	Device Primary Account Number
DSRP	Digital Secure Remote Payment
EMV	Europay, Mastercard and Visa
eSE	Embedded Secure Element
GCM	Google Cloud Messaging
HCE	Host Card Emulation
ID&V	Identification and Verification
IDN	ICC Dynamic Number
MD	Mobile Device Authentication
MNO	Mobile Network Operator
NFC	Near Field Communication
PAN	Primary Account Number
RNS	Remote Notification Service
SD	Security Domain
SE	Secure Element
SEI TSM	Secure Element Issuer Trusted Service Manager
PTC	PIN Try Counter
TAV	Tokenization Authentication Value
DTVC	Dynamic token verification code. (Dynamic one time CVC2 generated for a token).
UMD	User and Mobile Device Authentication

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

Contents

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

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 support the management, generation, and provisioning of digital payment credentials into mobile devices, to enable simpler, more secure digital payment experiences.

MDES was developed to facilitate the financial industry transition from consumer account credentials stored on traditional payment cards, to digital credentials provisioned into mobile devices. These digitized credentials enable the consumer's mobile device to perform payments via existing contactless point-of-sale systems and via new remote payment use cases, such as in-app payments. These MDES-enhanced, device-based payment methods offer simpler checkout and payment experiences, and greater payment security.

1.2 Document Scope

This document is the controlling specification of the Application Programming Interfaces (APIs) for MDES. The use of each API is determined by the MDES deployment model (See Section 2.1)

It includes:

- The Digitization API
- The Credentials Management API
- The Mobile Payment API
- The MPA Management API
- The Transaction Details API
- The Remote Transaction API

It does not include:

- The Customer Service API (refer to the Mastercard Developer's Zone for the Customer Service API).
- Any other internal interfaces to Mastercard systems

The APIs currently support Embedded Secure Element and Mastercard Cloud-Based Payments tokens. UICC support is currently out of scope of this document.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

1.3 Related Documents

- Mastercard Digital Enablement Service – Embedded Secure Element Use Cases Description
- Mastercard Digital Enablement Service – Mastercard Cloud-Based Payments Use Cases Description
- Mastercard Digital Enablement Service – Embedded Secure Elements Mobile PayPass Payments Configuration Description
- Mastercard Digital Enablement Service – Mastercard Cloud-Based Payments Card Profile Specification (Note: document version depends on MCBP version supported by the mobile wallet app)
- Mastercard Cloud-Based Payments – Issuer Cryptographic Algorithms

1.4 Using This Document

The document is a technical specification of the APIs. It is assumed that the reader is familiar with the high-level use cases supported by MDES. Refer to the Use Cases Description documents for more information.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

2 General

2.1 Deployment Models

The MDES Service supports two deployment models. The main difference between each model revolves around the hosting of the Credentials Management (dedicated) function also referred to as CMS-D. The CMS-D manages token credentials and is an integral part of the digitization process.

2.1.1 CMS-D supplied by Mastercard.

In this deployment model the CMS-D is hosted by Mastercard therefore the Credentials Management API is not used by the Token Requestor but by MDES itself.

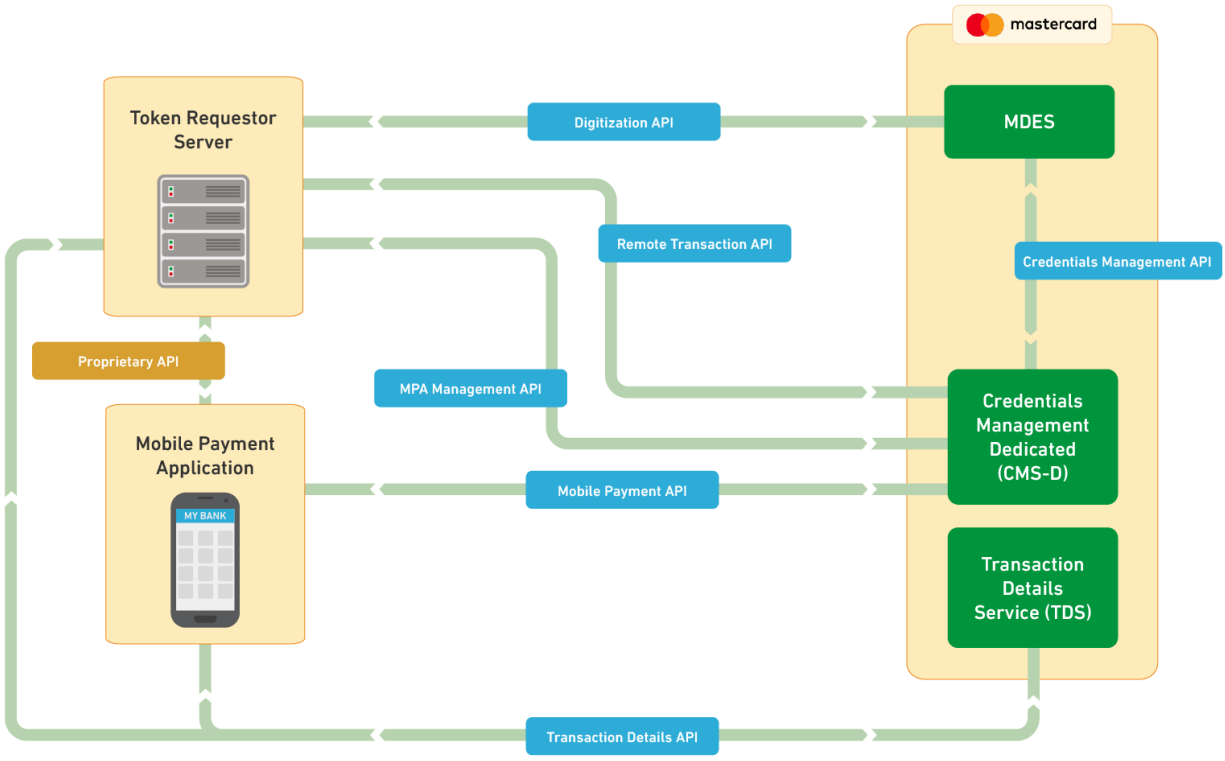


Figure 1 - Diagram showing interaction of MDES API's (using Mastercard CMS-D)

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

2.1.2 CMS-D supplied by Token Requestor Server

In this deployment model the Token Requestor Server hosts a CMS-D which interacts with MDES using the Credentials Management API.

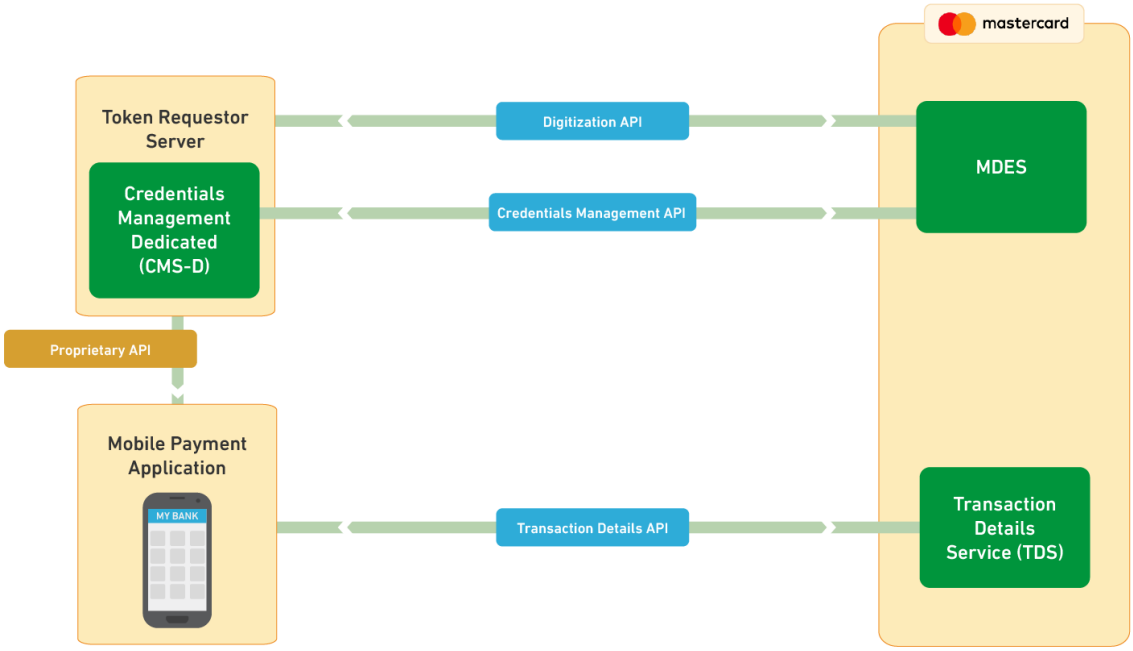


Figure 2 - Diagram showing interaction of MDES API's (using Token Requestor hosted CMS-D)

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3 Digitization API

3.1 General

The Digitization API encompasses a set of APIs that are either initiated by the Token Requestor or asynchronous API (outbound) calls made from MDES.

3.1.1 API Design Principles

The Digitization APIs are designed as 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 to be UTF-8 encoded. Each API URI includes the major and minor version of API that it conforms to. This will allow multiple concurrent versions of the API to be deployed simultaneously.

The client must handle any standard HTTP response code that could result from a web service call including but not limited to 302, 401, 404, or 500.

All APIs return an HTTP response code of 200 if the call was successfully received and accepted for processing, with the exception of certain scenarios where a 503 HTTP response code will be returned. Any errors that subsequently occur during processing are returned in the response payload.

All asynchronous API calls must include a task identifier, allowing the caller to subsequently check the task status, if required. The task identifier should be persisted for at least 30 days (or until the Token is deleted, whichever is sooner) during which time the task status may be checked.

In order to make the API implementation more fault tolerant, the Check Eligibility and Digitize APIs return a cached response if they receive a duplicate request as long as the 'eligibilityReceipt' has not expired. The lifecycle management APIs (Suspend, Unsuspend, and Delete) do not return an error code if the Token is already in the desired end state. For example, if Unsuspend is called and the Token is already in an Active state, no error is returned and the call returns successfully. Additionally the Check Eligibility and Digitize APIs return a 503 with a Retry-After header in the case of a duplicate concurrent request being detected.

Assets retrieved through the Get Asset API may be cached in perpetuity. Any future updates to an Asset will always result in a new AssetId being issued.

To ensure forward-compatibility, all API client implementations must be resilient to new elements being added to outbound requests and responses from MDES.

3.1.2 URL Scheme

All API URLs follow the format:

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

scheme://host[:port]/contextRoot/api/majorVer/minorVer/[paymentAppInstanceId/]apiName

URL Element	Definition
scheme	https
host[:port]	Hostname (and port number if required) for the environment. services.Mastercard.com ~~ws.Mastercard.com~~ **(deprecated)**
contextRoot	mdes
api	digitization (for all APIs except Get Assets) assets (for Get Assets API)
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 ~~Not present for the Get System Health API~~ **(deprecated)**
minorVer	The minor version of the APIs. This version of the document corresponds to a minor version of: 0 ~~Not present for the Get System Health API~~ **(deprecated)**
~~paymentAppInstanceId~~	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization. This field is alphanumeric and additionally web-safe base64 characters per RFC 4648 (minus "-", underscore "_" and URL-encoded equals sign "%3D") up to a maximum length of 48 (after URL-decoding). Not present for the Get Assets API or the Get System Health API. **Deprecated –** use paymentAppInstanceId in request body instead.
apiName	The URL endpoint as defined in the respective section for the API operation.

3.1.3 Security Overview and Encryption

All communication between the client and the Digitization 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

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

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.

3.1.4 API Request / Response Common Elements and Headers

All requests and responses from MDES contain an element 'responseHost'. This identifies the specific MDES host that originated a request or response. It should be used by the client in the URL for future calls in order to direct the call to a specific host. As MDES is deployed in a dual active environment, this ensures that when a client makes a series of API calls, they must direct all calls within the same conversation to the same host. This minimizes the risk of some calls being routed to a different site, where data from a previous call may not yet have been replicated. When a conversation is complete, the client should revert back to the default host (provided during onboarding) to ensure that it is not locked permanently to one host.

The client may also provide its 'responseHost' in requests and responses originating from the client, and MDES will honor the responseHost per the above. Note that all valid client hosts must be pre-configured in MDES. Should a 'responseHost' value be submitted that is not yet configured, MDES will respond with an error.

In addition, every inbound and outbound request contains an element 'requestId' which uniquely identifies the request. Every response contains an element 'responseId' which uniquely identifies the response. The responseId may optionally use the corresponding requestId. Note that the format and uniqueness of the requestId and responseId are not necessarily validated on the Digitization API.

In the case of an operation reporting an error, the response (or an object within the response) contains the elements 'errorCode' and 'errorDescription' as defined in Section 3.1.5. Unless explicitly stated otherwise, other elements (including 'Required' fields) are not present if an error is reported.

3.1.4.1 Common Request Elements

responseHost	
Description:	The host that originated the request. Future calls in the same conversation may be routed to this host. Must be provided as: host[:port][/contextRoot] Where port and contextRoot are optional. If contextRoot is not provided, the default (per the URL Scheme) is assumed and must be used.
Data Type:	String
Max Length:	64
Required:	No

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

requestId	
Description:	Unique identifier for the request.
Data Type:	String
Max Length:	64
Required:	Yes

3.1.4.2 Common Response Elements

responseHost	
Description:	The host that originated the response. Future calls in the same conversation must be routed to this host. Must be provided as: host[:port][/contextRoot] Where port and contextRoot are optional. If contextRoot is not provided, the default (per the URL Scheme) is assumed and must be used.
Data Type:	String
Max Length:	64
Required:	Conditional – see section 3.1.4. In Production, the responseHost supplied by MDES must be used by the client for future API calls within a conversation. When the conversation is complete, the client will revert back to the default host supplied during onboarding.

responseId	
Description:	Unique identifier for the response.
Data Type:	String
Max Length:	64
Required:	Yes

~~**errorCode**~~	
Description:	Error code for the reason the operation failed.
Data Type:	String
Max Length:	32
Required:	**Deprecated** – use errors instead.

~~**errorDescription**~~	
Description:	Error description of the reason the operation failed.
Data Type:	String
Max Length:	256
Required:	**Deprecated** – use errors instead.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

errors	
Description:	An element used to encapsulate a collection of errors that occurred during a single request.
Data Type:	Array[Error object]
Max Length:	N/A
Required:	Conditional – required if one or more errors occurred performing the operation. Not present if the operation was successful.

3.1.5 Error Reason Codes

Reason Code	Reason Description	Detail
INVALID_JSON	Invalid JSON	The JSON could not be parsed.
UNRECOGNIZED_FIELD	Unrecognized Field - {fieldName}	The field name is not valid for the object.
AUTHORIZATION_FAILED	Authorization failed.	The request failed to present a valid cert to access the API.
INVALID_FIELD_FORMAT	Invalid Field Format - {fieldName}	The field is not in the correct format. For instance, it should be a number but is a string.
INVALID_FIELD_LENGTH	Invalid Field Length - {fieldName}	The value does not fall between the minimum and maximum length for the field.
INVALID_FIELD_VALUE	Invalid Field Value - {fieldName}	The value is not allowed for the field.
INVALID_RESPONSE_HOST	Invalid Response Host	The requested response host is invalid.
NO_RESPONSE_FROM_ISSUER	Issuer did not respond in time. Retry the request.	The issuer did not respond to the network message in the allotted time. An asynchronous message will be sent. The Token Requestor should retry after the time specified in the retry-after header.
MISSING_REQUIRED_FIELD	Missing Required Field - {fieldName}	A required field is missing.
CRYPTOGRAPHY_ERROR	Cryptography Error	There was an error decrypting the encrypted payload.
INTERNAL_SERVICE_FAILURE	The system had an internal exception	MDES had an internal exception.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

Reason Code	Reason Description	Detail
INVALID_PAN	Invalid PAN	The PAN format is not valid, or other data associated with the PAN was incorrect or entered incorrectly. The request may be retried if the data is re-entered correctly.
MISSING_EXPIRY_DATE	Missing Expiry Date	The expiry date is required for this product but was missing. Retry the request supplying the expiry date for this card.
DUPLICATE_REQUEST	Duplicate Request	The PAN has already been provisioned to the device or the same request is currently being processed.
PROVISION_FAILED	Provisioning Failed	The provisioning of PAN to the device has failed.
PAN_INELIGIBLE	PAN Ineligible	The PAN is not in an approved account range for MDES.
DEVICE_INELIGIBLE	Device Ineligible	The device is not supported for use with MDES.
PAN_INELIGIBLE_FOR_DEVICE	PAN Ineligible for the device	The PAN is not allowed to be provisioned to the device because of Issuer rules.
PAN_PROVISIONING_COUNT_EXCEEDED	PAN provisioning count exceeded	The PAN has already been provisioned to the maximum number of devices.
INVALID_ELIGIBILITY_RECEIPT	Invalid Eligibility Receipt	The eligibility receipt is expired or the value cannot be found.
INVALID_TASK_ID	Invalid Task Id	The taskId could not be found or, for inbound calls, the taskId was not unique.
INVALID_TERMS_AND_CONDITIONS	Invalid Terms and Conditions	The terms and conditions id accepted by the cardholder does not match what was sent on the CheckEligibility response.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

Reason Code	Reason Description	Detail
~~INVALID_ACTIVATION_METHOD~~ **Deprecated** – use INVALID_AUTHENTICATION_METHOD instead.	Invalid Activation Method	The activation method could not be found.
INVALID_AUTHENTICATION_METHOD	Invalid Authentication Method	The authentication method could not be found.
INVALID_TOKEN_UNIQUE_REFERENCE	Invalid Token Unique Reference	The token unique reference could not be found or does not match the paymentAppInstanceId provided.
INVALID_PAN_UNIQUE_REFERENCE	Invalid PAN Unique Reference	The PAN unique reference could not be found.
INVALID_TOKEN_STATUS	Invalid Token status.	The token is in an invalid status for the requested operation. For instance, trying to unsuspend a deleted token.
INVALID_WORKFLOW	Invalid Workflow	The operation requested is invalid for the token. For instance, calling Activate for an Approved mapping, or supplying rnsInfo when it is not the first card being digitized.
INVALID_AID_CARD_TYPE	AID PIX value was not correct for the account	The PIX value in the aid was not correct for the account range brand product.
INVALID_AID_RID	AID RID value was not correct.	The RID value in the aid was not correct for Mastercard
INVALID_CARDLET_ID	The cardlet ID could not be found.	The cardlet ID could not be mapped to a cardlet.
INVALID_METHOD	Call failed – unrecognized URI or required parameters not present	The URI for the call was not able to be mapped to an API endpoint.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

Reason Code	Reason Description	Detail
INCORRECT_TAV	Incorrect Tokenization Authentication Value	The Tokenization Authentication Value provided in the call was incorrect and rejected.
EXPIRED_CODE	Expired Authentication Code	Authentication Code has expired or was invalidated.
INVALID_DATA	Invalid Data	The data supplied for the request was invalid. No further detail is provided.
NO_ACTIVE_TOKENS	No Active Tokens	There are no active (not suspended) Tokens for the given Account PAN and consumer account.
ALT_CREDENTIALS_COUNT_EXCEEDED	The count of alternate payment credentials permitted at a time for the token has exceeded the limit.	The maximum number of alternate payment credentials for the token is reached. Additional credentials cannot be generated until an already returned alternate payment credential not used in a transaction expires or is used for the first time in a transaction.
INVALID_CRYPTOGRAPHIC_DATA	Cryptographic data has already been exchanged	The cryptographic data has already been exchanged for alternate payment account credentials. The credentials have already been used in a transaction or the validity period of the alternate payment account credentials has already expired. This error will also be returned if the cryptogram has already been exchanged but the value for merchantSupportsDtvc or the walletMerchantIdentifier does not match the original request.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

Reason Code	Reason Description	Detail
TOKEN_PAN_NOT_FOUND	The token pan in the request could not be found or the token is expired.	The token pan that was supplied in the request could not be found. This could be an invalid token or a token number, token expiration mismatch, or the token is expired.

3.1.6 Retry Strategy

For outbound calls (except Notify Transaction Details) that fail with a timeout, connection failure, or an HTTP response code of 302, 500, or 503 MDES will automatically retry 3 times with up to a 5-second wait between each try. 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.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2 Inbound APIs (to MDES)

3.2.1 Check Eligibility

3.2.1.1 Overview

This API is used to check card availability and device eligibility before making a Digitize request. It is used to check issuer participation for this card and this wallet, and to check device eligibility including whether or not the device is a Mastercard type-approved device, hardware and software compatibility and any applicable Issuer policies related to the device.

If successful, MDES provides associated data to the Token Requestor including Issuer Terms and Conditions to allow the Mobile Payment App to present them to the Cardholder before they proceed with digitization. MDES also provides an Eligibility Receipt which must be presented when calling the Digitize API (see Section 3.2.2).

Note that an Account PAN may only be provisioned once to a given Mobile Payment App unless it has previously been removed. If a Token (active, suspended, or inactive pending activation) for that Account PAN is found for the given Mobile Payment App, the digitization will be declined by this API.

This API can also be used without device parameters to only perform card availability checks; or without card parameters in order to only perform device eligibility checks. This provides flexibility to the Token Requestor in designing the optimal user experience for the Cardholder (for example, if the device is not eligible for digitization, this can be presented to the Cardholder before they start entering their card details). However, note that both card and device eligibility checks must be performed to receive an Eligibility Receipt.

If eligibility checks fail, reasons are provided in the response to potentially allow certain failed checks to be resolved (for example, if the OS on the target device is not the latest version, the Cardholder can be prompted to upgrade in order to proceed).

MDES may pass on data in a Tokenization Eligibility message to the Issuer as part of this request to allow the Issuer an opportunity to perform any specific eligibility checks. Note that as the Issuer checks take time, this Check Eligibility response will not yet factor in any Issuer token eligibility checks. At this stage, MDES will only perform basic card *availability* checks to ensure that the card is within a valid range that is available for digitization. The card *eligibility* checks to check that this specific card is eligible for digitization will only be factored into the final decision in the Digitize response (see Section 3.2.2.5).

3.2.1.2 URL Endpoint

/checkEligibility

3.2.1.3 HTTP Method

POST

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.1.4 Request Parameters

tokenType

Description: The type of Token requested.

Must be one of:

Value	Meaning
EMBEDDED_SE	Embedded Secure Element
CLOUD	Mastercard Cloud-Based Payments

Data Type: String

Max Length: 32

Required: Yes

paymentAppInstanceId

Description: Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization.

This field is alphanumeric and additionally web-safe base64 characters per RFC 4648 (minus "-", underscore "_") up to a maximum length of 48, = should not be URL encoded.

Data Type: String

Max Length: 48

Required: Conditional – not applicable for server-based tokens. Required otherwise.

paymentAppId

Description: Identifier for the Payment App, unique per app as assigned by Mastercard for this Payment App.

Data Type: String

Max Length: 30

Required: Yes

deviceInfo

Description: Contains information about the target device to be provisioned.

Data Type: Map.

Max Length: N/A

Required: Conditional – may be omitted if performing card availability checks. Otherwise required. (See B.1).

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

seInfo	
Description:	Contains information about the target Secure Element to be provisioned.
Data Type:	SeInfo Object
Max Length:	N/A
Required:	Conditional – required if tokenType = EMBEDDED_SE in order to check device eligibility, may be omitted if only performing card availability checks.
cardInfo	
Description:	Contains card information of the card to be digitized.
Data Type:	CardInfo object.
Max Length:	N/A
Required:	Conditional – required in order to check card availability, may be omitted if only performing device eligibility checks.
cardletId	
Description:	An identifier representing the cardlet being used (as assigned during onboarding).
Data Type:	String
Max Length:	10
Required:	Yes
spsdInfo	
Description:	Contains information about the Service Provider Security Domain.
Data Type:	Spsd object.
Max Length:	N/A
Required:	Conditional – required if tokenType = EMBEDDED_SE.
consumerLanguage	
Description:	Language preference selected by the consumer. Formatted as an ISO-639-1 two-letter language code.
Data Type:	String
Max Length:	2 (exact)
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.1.5 Response Values

eligibilityReceipt

Description:	Contains the Eligibility Receipt, provided by MDES if both card availability and device eligibility checks were successful. The client must provide the Eligibility Receipt value back to MDES in the Digitize API (see Section 3.2.2) to proceed with digitization.
Data Type:	EligibilityReceipt object.
Max Length:	N/A
Required:	Conditional – required if eligibility checks were successful.

deviceNotEligibleReasons

Description: The reasons why the device was deemed not eligible for the service.

Reason strings must be one of:

Value	Meaning
OS_NOT_SUPPORTED	The Operating System is not supported by the service.
OS_VERSION_NOT_SUPPORTED	The Operating System version is not supported by the service.
DEVICE_TYPE_NOT_SUPPORTED	The technology types specified do not represent a supported Mastercard Device Type for digitization.

Data Type:	Array[String]
Max Length:	N/A
Required:	Conditional – required if device eligibility checks failed.

termsAndConditionsAssetId

Description:	The Terms and Conditions to be presented to the Cardholder. Provided as an Asset ID – use the Get Asset API (See Section 3.2.5) to retrieve the actual asset.
Data Type:	String
Max Length:	64
Required:	Conditional – required if eligibility checks were successful.

applicableCardInfo

Description:	Contains flags to indicate what additional card information is applicable for this product and may be provided in the Digitize request.
Data Type:	ApplicableCardInfo object
Max Length:	N/A
Required:	Conditional – required if eligibility checks were successful.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.1.6 Examples

3.2.1.6.1 Sample Request for "CLOUD" Token Type

```
{
   "responseHost":"site1.your-server.com",
   "requestId":"123456",
   "paymentAppInstanceId":"123456789",
   "tokenType":"CLOUD",
   "paymentAppId":"WalletApp1",
   "deviceInfo":{
      "deviceName":"My Phone",
      "serialNumber":"2F6D63",
      "formFactor":"PHONE",
      "storageTechnology":"SERVER"      "osName":"ANDROID",
      "osVersion":"4.4",
      "imei":"352099001761481",
      "msisdn":"7307406945",
      "nfcCapable":true
   },
   "cardInfo":{

"encryptedData":"4545433044323232363739304532433610DE1D1461475BEB6D815F31764DDC20298B
D779FBE37EE5AB3CBDA9F9825E1DDE321469537FE461E824AA55BA67BF6A",
      "publicKeyFingerprint":"4c4ead5927f0df8117f178eea9308daa58e27c2b",
      "encryptedKey":"A1B2C3D4E5F6112233445566",
      "oaepHashingAlgorithm":"SHA512"
   },
   "cardletId":"1.0",
   "consumerLanguage":"en"
}
```

3.2.1.6.2 Sample Request for "EMBEDDED_SE" Token Type

```
{
      "responseHost" : "site1.your-server.com",
      "requestId" : "123456",
      "paymentAppInstanceId" : "123456789",
"tokenType": "EMBEDDED_SE",
      "paymentAppId" : "WalletApp1",
      "deviceInfo" : {
"deviceName" : "My Phone",
"serialNumber" : "2F6D63",
"formFactor" : "PHONE",
"storageTechnology : "SE"
"osName" : "ANDROID",
"osVersion" : "4.4",
"imei" : "352099001761481",
"msisdn" : "7307406945",
"nfcCapable" : true
      },
      "seInfo" : {
            "seId": "824bb0419714df99bc5095dd",
            "seCapabilities": {
            }
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
      },
      "cardInfo" : {
"encryptedData" :
"4545433044323232363739304532433610DE1D1461475BEB6D815F31764DDC20298BD779FBE37EE5AB3C
BDA9F9825E1DDE321469537FE461E824AA55BA67BF6A",
"publicKeyFingerprint" :  "4c4ead5927f0df8117f178eea9308daa58e27c2b",
"encryptedKey" : "A1B2C3D4E5F6112233445566",
"oaepHashingAlgorithm" : "SHA512"
      },
      "cardletId" : "1.0",
      "spsdInfo" : {
            "aid" : "A0000000045353440000001",
            "appletInstanceAid" : "A000000004101011",
            "spsdSequenceCounter" : "01",
            "rgk" :
"80AEB98CB02C99294E696ADCC3C3CE1B70CD89493B6E95238487D2570FBF3FED0878B5B9F2EA943CEB80
ADB35BC49CFF2EDA015BE0AE5E84166F992ACD44FEA750B9E61BCAAEBC2D26D55879FD46C72615FAF88E8
8BB6434F6059608FF3DBB649887297C21FEF0598F7683ECD965F4234B22116FE748028860365239267 7BB
32FF3442D5F897ECFD5A681BF90AFE06E369B2469D8CA8CBF186E2FD6DF53F58D54E695E5875BD31AAB15
A0AE795A8DDE635A38F1E73AB",
            "casdPkCertificate" :
"7F2181DE9310000000000000000000000000000000001420200025F200D4A3547314D335F4D3031503030
9501825F25005F2404201604304502000 45F3781800A25E500241D95F73E6B39BED97D358622F358ACA02
D5EEFEED9782D0CB2024981495FA8811B9C0E82C09F110CADB031083EFAE04D39F42243F683EAD8E39782
824256C06EADCD2AC924D41682B55CA38D72AF6291CEF602130E5C2F85924E3BE27BE1B52BBD5DB8D1EFD
48E29218E0D5D347185C61D9DB322E803B5DEE7C2EF5F3820EDB7FED76B485DE45BEB829A3D4730848A36
6D3324C3027032FF8D16A1E44D8D"
},
      "consumerLanguage" : "en"
}
```


3.2.1.6.3 Sample contents of encryptedData in cardInfo


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


3.2.1.6.4 Sample Response


```
{
      "responseHost" : "site1.Mastercard.com",
"responseId" : "123456",
      "eligibilityReceipt" : {
            "value" : "f9f027e5-629d-11e3-949a-0800200c9a66",
            "validForMinutes" : 30
      },
      "termsAndConditionsAssetId" : "a9f027e5-629d-11e3-949a-0800200c9a66",
      "applicableCardInfo" : {
            "isSecurityCodeApplicable" : true
      }
}
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.2 Digitize

3.2.2.1 Overview

This API is used to proceed with digitization.

Prior to calling this API, the Token Requestor must have previously called the Check Eligibility API (see Section 3.2.1) and received an Eligibility Receipt, which must be supplied.

The Token Requestor must supply any applicable Cardholder authentication data (such as a CVC2).

MDES may pass on any data in a Tokenization Authorization message to the Issuer as part of this request to authorize the digitization. The Issuer may bypass this step by providing a cryptographically-signed Tokenization Authentication Value (TAV) to the Token Requestor prior to calling this API to indicate that this digitization request has already been approved.

The digitization decision will be one of:

- Approved
- Declined
- Require Additional Authentication

For 'Approved' digitization requests, MDES will manage the creation of the Token and the provisioning of data to the target SEI TSM or Credentials Management System.

For any digitization requests that 'Require Additional Authentication', MDES will provision the Token in an 'Inactive' state, and will return a list of available Authentication Methods. For any Authentication Method involving a user-entered Authentication Code, the Token Requestor should call the Request Activation Code API (see Section 3.2.4).

Once the Cardholder has been authenticated, the Token Requestor should call the Activate API (see Section 3.2.6) to activate the Token.

Once digitization is complete and the Token has been provisioned and activated, MDES will notify the Token Requestor of the result using the Notify Token Updated API (see Section 3.3.1). The Token Requestor may also use the Get Task Status API (see Section 3.2.11) to query the status of the digitization task.

If the Digitize Service does not receive a response from the issuer in the allotted amount of time it will return a 503 with a Retry-After header indicating how many seconds the client should allow to elapse before retrying the API call. The client should call back after the allotted amount of time to retrieve the decision.

3.2.2.2 URL Endpoint

/digitize

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.2.3 HTTP Method

POST

3.2.2.4 Request Parameters

paymentAppInstanceId	
Description:	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization. This field is alphanumeric and additionally web-safe base64 characters per RFC 4648 (minus "-", underscore "_" and URL-encoded equals sign "%3D") up to a maximum length of 48 (after URL-decoding), = should not be URL encoded.
Data Type:	String
Max Length:	48
Required:	Conditional – not applicable for server-based tokens. Required otherwise.

eligibilityReceipt	
Description:	The Eligibility Receipt value as provided by MDES in the Check Eligibility response (see Section 3.2.1.5).
Data Type:	EligibilityReceipt object.
Max Length:	N/A
Required:	Yes

taskId	
Description:	Identifier for this task as assigned by the Wallet Provider, unique across a given Wallet Identifier. May be used in the Get Task Status API (see Section 3.2.11) to query the status of this task.
Data Type:	String
Max Length:	64
Required:	Yes

termsAndConditionsAssetId	
Description:	The Terms and Conditions as presented to and accepted by the Cardholder. Must be a valid Asset ID.
Data Type:	String
Max Length:	64
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

termsAndConditionsAcceptedTimestamp	
Description:	The date/time stamp when the Cardholder accepted the Terms and Conditions. Must be 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
~~rnsInfo~~	
Description:	Contains information about the Remote Notification Service to be used by the Credentials Management (Dedicated) to register the Mobile Payment App, and subsequently to deliver credentials to the target application instance. Must only be present for a new Mobile Payment App instance performing registration. Must not be present for existing registered Mobile Payment App instances with one or more Tokens (unless they are deactivated). May not be applicable to all deployment models – may be omitted if RNS is not the registration mechanism.
Data Type:	RnsInfo object.
Max Length:	N/A
Required:	**Deprecated** – use rnsInfo in the Register request in the MPA Management API instead.
cardInfo	
Description:	Contains card information of the card to be digitized.
Data Type:	CardInfo object.
Max Length:	N/A
Required:	No
tokenizationAuthenticationValue	
Description:	The Tokenization Authentication Value (TAV) as cryptographically signed by the Issuer to authorize this digitization request.
Data Type:	String
Max Length:	2048
Required:	No

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

decisioningData

Description:	Contains data relevant to the digitization decision process.
Data Type:	Map.
Max Length:	N/A
Required:	No

3.2.2.5 Response Values

decision

Description: The tokenization decision for this digitization request.

Must be one of:

Value	Meaning
APPROVED	Digitization request was approved.
DECLINED	Digitization request was declined.
REQUIRE_ADDITIONAL_AUTHENTICATION	Digitization request requires additional authentication to be approved. One or more Activation Methods will be provided.

Data Type:	String
Max Length:	64
Required:	Yes

~~activationMethods~~

Description:	When additional authentication is required, this is the list of supported activation methods.
Data Type:	Array[ActivationMethod object]
Max Length:	N/A
Required:	**Deprecated** – use authenticationMethods instead.

authenticationMethods

Description:	When additional authentication is required, this is the list of supported authentication methods.
Data Type:	Array[AuthenticationMethod object]
Max Length:	N/A
Required:	Conditional – required if decision = REQUIRE_ADDITIONAL_AUTHENTICATION.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

tokenUniqueReference	
Description:	The unique reference allocated to the new Token. Serves as a unique identifier for all subsequent queries or management functions relating to this Token.
Data Type:	String
Max Length:	64
Required:	Conditional – required if the decision was APPROVED or REQUIRE_ADDITIONAL_AUTHENTICATION.
panUniqueReference	
Description:	The unique reference allocated to the Account Primary Account Number.
Data Type:	String
Max Length:	64
Required:	Conditional – required if the decision was APPROVED or REQUIRE_ADDITIONAL_AUTHENTICATION.
productConfig	
Description:	Contains all Product Configuration data for this card.
Data Type:	ProductConfig object
Max Length:	N/A
Required:	Conditional – required if the decision was APPROVED or REQUIRE_ADDITIONAL_AUTHENTICATION.
tokenInfo	
Description:	Contains all the token specific data for this card.
Data Type:	TokenInfo object
Max Length:	N/A
Required:	Conditional – required if the decision was APPROVED or REQUIRE_ADDITIONAL_AUTHENTICATION.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

tdsRegistrationUrl

Description:	The URL endpoint for the Transaction Details Service. Must be provided as: host[:port][/contextRoot] Where port and contextRoot are optional. If contextRoot is not provided, the default (per the URL Scheme) is assumed and must be used.
Data Type:	String
Max Length:	128
Required:	Conditional – required if TDS is supported. Not present if TDS is not supported or if the Token is not eligible for transaction details.

encryptedPayload

Description:	Contains an encrypted object. Conditionally returned if the Token Requestor has opted to receive PAR, is using "External Customer Wrapping Key" to decrypt information from MDES and providing PAR is assigned by Mastercard or the Issuer provides PAR in the authorization message response.
Data Type:	EncryptedPayload object containing a DigitizeResponsePayload object.
Max Length:	N/A
Required:	No

3.2.2.6 Examples

3.2.2.6.1 Sample Request


```
{
      "responseHost" : "site1.your-server.com",
"requestId" : "123456",
"paymentAppInstanceId" : "123456789",
      "eligibilityReceipt" : {
            "value" : "f9f027e5-629d-11e3-949a-0800200c9a66"
      },
      "termsAndConditionsAssetId" : "81d9f8e0-6292-11e3-949a-0800200c9a66",
      "termsAndConditionsAcceptedTimestamp" : "2014-07-04T12:08:56.123-07:00",
      "cardInfo" : {
"encryptedData" :
"4545433044323232363739304532433610DE1D1461475BEB6D815F31764DDC20298BD779FBE37EE5AB3C
BDA9F9825E1DDE321469537FE461E824AA55BA67BF6A",
"publicKeyFingerprint" : "4c4ead5927f0df8117f178eea9308daa58e27c2b",
"encryptedKey" : "A1B2C3D4E5F6112233445566",
"oaepHashingAlgorithm" : "SHA512"
      },
      "tokenizationAuthenticationValue" :
"RHVtbXkgYmFzZSA2NCBkYXRhIC0gdGhpcyBpcyBub3QgYSByZWFsIFRBViBleGFtcGxl",
,
      "decisioningData" : {
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
            "recommendation" : "REQUIRE_ADDITIONAL_AUTHENTICATION",
            "recommendationAlgorithmVersion" : "01",
            "deviceScore" : "1",
            "accountScore" : "1",
            "recommendationReasons" : [
                  "ACCOUNT_TOO_NEW",
                  "TOO_MANY_RECENT_ATTEMPTS",
                  "OUTSIDE_HOME_TERRITORY"
            ]
      }
}
```

3.2.2.6.2 Sample contents of encryptedData in cardInfo

```
{
      "securityCode" : "123",
      "billingAddress" : {
            "line1" : "100 1st Street",
            "line2" : "Apt. 4B",
            "city" : "St. Louis",
            "countrySubdivision" : "MO",
            "postalCode" : "61000",
            "country" : "USA"
      }
}
```

3.2.2.6.3 Sample Response

```
{
  "responseHost" : "site1.Mastercard.com",
  "responseId" : "123456",
  "decision" : "REQUIRE_ADDITIONAL_AUTHENTICATION",
  "authenticationMethods" : [
{
        "id" : 12344,
        "type" : "MASKED_MOBILE_PHONE_NUMBER",
        "value" : "12X-XXX-XX32"
      },
      {
        "id" : 12345,
        "type" : "AUTOMATED_CALL_CENTER_PHONE_NUMBER",
        "value" : "1-800-BANK-NUMBER"
      },
{
        "id" : 12346,
        "type" : "CARDHOLDER_TO_USE_ISSUER_MOBILE_APP",
  "value":"{\"activateWithIssuerMobileAppAndroidIntent\": \"{\"action\" :
\"com.mybank.bankingapp.action.ACTIVATE_TOKEN\",\"packageName\" :
\"com.mybank.bankingapp\",\"extraTextValue\" :
\"ew0KICAgICJwYXltZW50QXBwUHJvdmlkZXJJZCI6ICIxMjM0NTY3ODkiLA0KICAgICJwYXltZW50QXBwSW5
zdGFuY2VJZCI6ICIxMjM0NTY3ODkiLA0KICAgICJ0b2tlblVuaXF1ZVJlZmVyZW5jZSI6ICJEV1NQTUMwMDAw
MDAwMDBmY2IyZjQxMzZiMmY0MTM2YTA1MzJkMmY0MTM2YTA1MzIiLA0KICAgICJhY2NvdW50UGFuU3VmZml4I
jogIjY3ODkiLA0KICAgICJhY2NvdW50RXhwaXJ5IjogIjEwMTgiDQp9\"}\"}"
      }
  ],
  "tokenUniqueReference" : "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
  "panUniqueReference" : "FWSPMC000000000159f71f703d2141efaf04dd26803f922b",
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
  "productConfig" : {
       "brandLogoAssetId" : "800200c9-629d-11e3-949a-0739d27e5a66",
"isCoBranded" : "true",
"coBrandName" : "Co brand partner",
"coBrandLogoAssetId" : "dbc55444-496a-4896-b41c-5d5e2dd431e2",
"cardBackgroundCombinedAssetId" : "739d27e5-629d-11e3-949a-0800200c9a66",
"foregroundColor" : "000000",
"issuerName" : "Issuing Bank",
"shortDescription" : "Bank Rewards Mastercard",
"longDescription" : "Bank Rewards Mastercard with rewards program",
"issuerLogoAssetId" : "BED1503C-0D6D-40A7-AE8A-749DB4A05D86",
"iconAssetId" : "C307F0AE-298E-48EB-AA43-A7C40B32DDDE",
"customerServiceUrl" : "https://bank.com/customerservice",
"issuerMobileApp" : {
  "openIssuerMobileAppAndroidIntent": {
"action": "com.mybank.bankingapp.action.OPEN_ISSUER_MOBILE_APP",
"packageName": "com.mybank.bankingapp",
"extraTextValue":"ew0KICAgICJwYXltZW50QXBwUHJvdmlkZXJJZCI6ICIxMjM0NTY3ODkiLA0KICAgICJ
wYXltZW50QXBwSWQiOiAiV2FsbGV0QXBwMSIsDQogICAgInBheW1lbnRBcHBJbnN0YW5jZUlkIjogIjEyMzQ1
Njc4OSIsDQogICAgInRva2VuVW5pcXVlUmVmZXJlbmNlIjogIkRXU1BNQzAwMDAwMDAwMGZjYjJmNDEzNmIyZ
jQxMzZhMDUzMmQyZjQxMzZhMDUzMiINCn0="
        }
       },
"termsAndConditionsUrl" : "https://bank.com/termsAndConditions",
"privacyPolicyUrl" : "https://bank.com/privacy",
"issuerProductConfigCode" : "123456"
  },
  "tokenInfo" : {
"tokenPanSuffix": "1234",
       "accountPanSuffix": "6789",
"alternateAccountIdentifierSuffix": "4567",
       "tokenExpiry" : "1018",
       "dsrpCapable" : true
  },
  "tdsRegistrationUrl" : "tds.Mastercard.com",
  "encryptedPayload" : {
"encryptedData":"4545433044323232363739304532433610DE1D1461475BEB6D815F31764DDC20298B
D779FBE37EE5AB3CBDA9F9825E1DDE321469537FE461E824AA55BA67BF6A",
"publicKeyFingerprint" :  "4c4ead5927f0df8117f178eea9308daa58e27c2b",
"encryptedKey" : "A1B2C3D4E5F6112233445566",
"oaepHashingAlgorithm" : "SHA512"
  }
}
```


3.2.2.6.4 Sample contents of encryptedData in encryptedPayload


```
{
  "paymentAccountReference" : "500181d9f8e0629211e3949a08002"
}
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.3 Tokenize

3.2.3.1 Overview

This API is used to digitize a card to create a server-based Token.

MDES will perform both card availability and eligibility checks to check that this specific card is eligible for digitization. As both steps are combined, only a Tokenization Authorization message is sent to the issuer as part of this request to authorize the digitization. No Tokenization Eligibility message is sent.

The digitization decision will be one of:

- Approved
- Declined
- Require Additional Authentication

Unlike the Check Eligibility and Digitize API where additional cardholder authentication is a mandatory requirement in order to activate a Token, when using the Tokenize API, additional cardholder authentication is an optional requirement for Token Requestors. Token Requestors may not provide any mechanism to facilitate cardholder authentication, and the cardholder may not be involved in or necessarily be aware of the digitization process taking. Token Requestor's authentication capabilities and the cardholder's availability at the time of digitization should be indicated in the recommendation reason codes as appropriate.

Decisions of 'Require Additional Authentication' are considered approved with the option of performing cardholder authentication after the token is created and activated.

In both cases of 'Approved' or 'Require Additional Authentication', MDES will manage the creation of the Token and the provisioning of data to the target Credentials Management System, and upon successful provisioning, the token will be immediately activated. MDES will notify the Token Requestor of the successful activation using the Notify Token Updated API (see Section 3.3.1). The Token Requestor may also use the Get Task Status API (see Section 3.2.11) to query the status of the digitization task.

3.2.3.2 URL Endpoint

/tokenize

3.2.3.3 HTTP Method

POST

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.3.4 Request Parameters

tokenRequestorId

Description:	Identifies the Token Requestor.
Data Type:	String
Max Length:	11 (Exact)
Required:	Yes

tokenType

Description: The type of Token requested.

Must be one of:

Value	Meaning
CLOUD	Mastercard Cloud-Based Payments
STATIC	Static Token

Data Type:	String
Max Length:	32
Required:	Yes

cardInfo

Description:	Contains card information of the card to be tokenized.
Data Type:	CardInfo object
Max Length:	N/A
Required:	Yes

consumerLanguage

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

taskId

Description:	Identifier for this task as assigned by the Token Requestor, unique across a given Token Requestor Identifier. May be used in the Get Task Status API (see Section 3.2.11) to query the status of this task.
Data Type:	String
Max Length:	64
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

tokenizationAuthenticationValue

Description:	The Tokenization Authentication Value (TAV) as cryptographically signed by the Issuer to authorize this digitization request.
Data Type:	String
Max Length:	2048
Required:	No

decisioningData

Description:	Contains data relevant to the decisioning process.
Data Type:	Map
Max Length:	N/A
Required:	No

paymentAppId

Description:	Identifier for the Payment App, unique per app as assigned by Mastercard for this Payment App.
Data Type:	String
Max Length:	30
Required:	Conditional – required if there are multiple payment applications that share the same tokenRequestorId.

3.2.3.5 Response Values

decision

Description: The tokenization decision for this digitization request.

Must be one of:

Value	Meaning
APPROVED	Digitization request was approved.
DECLINED	Digitization request was declined.
REQUIRE_ADDITIONAL_AUTHENTICATION	Digitization request was approved but optionally requires additional authentication. One or more Authentication Methods may be provided.

Data Type:	String
Max Length:	64
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

authenticationMethods

Description:	When additional authentication is required, this is the list of supported authentication methods. Note that this list may be empty if authentication cannot be initiated by the Token Requestor. The issuer may support other out-of-band methods to authenticate the cardholder.
Data Type:	Array[AuthenticationMethod object]
Max Length:	N/A
Required:	Conditional – required if decision = REQUIRE_ADDITIONAL_AUTHENTICATION and tokenType is not STATIC.

tokenUniqueReference

Description:	The unique reference allocated to the new Token. Serves as a unique identifier for all subsequent queries or management functions relating to this Token.
Data Type:	String
Max Length:	64
Required:	Conditional – required if the decision was APPROVED or REQUIRE_ADDITIONAL_AUTHENTICATION.

panUniqueReference

Description:	The unique reference allocated to the Account Primary Account Number.
Data Type:	String
Max Length:	64
Required:	Conditional – required if the decision was APPROVED or REQUIRE_ADDITIONAL_AUTHENTICATION.

productConfig

Description:	Contains all Product Configuration data for this card.
Data Type:	ProductConfig object
Max Length:	N/A
Required:	Conditional – required if the decision was APPROVED or REQUIRE_ADDITIONAL_AUTHENTICATION.

tokenInfo

Description:	Contains all the token specific data for this card.
Data Type:	TokenInfo object
Max Length:	N/A
Required:	Conditional – required if the decision was APPROVED or REQUIRE_ADDITIONAL_AUTHENTICATION.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

tokenDetail	
Description:	Contains token information of the card tokenized.
Data Type:	TokenDetail Object
Max Length:	N/A
Required:	Conditional – required if tokenType = STATIC and decision is not DECLINED. Token Pan and expiration date will only be populated if tokenType= "STATIC".

3.2.3.6 Examples

3.2.3.6.1 Sample Request for CLOUD Token Type

```
{
      "responseHost" : "site1.your-server.com",
      "requestId" : "123456",

"tokenType": "CLOUD",
"tokenRequestorId": "98765432101",
"taskId": "123456",

      "cardInfo" : {
"encryptedData" :
"4545433044323232363739304532433610DE1D1461475BEB6D815F31764DDC20298BD779FBE37EE5AB3C
BDA9F9825E1DDE321469537FE461E824AA55BA67BF6A",
"publicKeyFingerprint" :  "4c4ead5927f0df8117f178eea9308daa58e27c2b",
"encryptedKey" : "A1B2C3D4E5F6112233445566",
"oaepHashingAlgorithm" : "SHA512"
      },
"tokenizationAuthenticationValue" :
"RHVtbXkgYmFzZSA2NCBkYXRhIC0gdGhpcyBpcyBub3QgYSByZWFsIFRBViBleGFtcGxl",
      "decisioningData" : {
            "recommendation" : "REQUIRE_ADDITIONAL_AUTHENTICATION",
            "recommendationAlgorithmVersion" : "01",
            "deviceScore" : "1",
            "accountScore" : "1",
            "recommendationReasons" : [
                  "ACCOUNT_TOO_NEW",
                  "TOO_MANY_RECENT_ATTEMPTS",
                  "OUTSIDE_HOME_TERRITORY",
                  "USER_NOT_AVAILABLE",
                  "AUTHENTICATION_NOT_SUPPORTED"
            ]
      },

      "consumerLanguage" : "en",
"paymentAppId" : "WalletApp1"
}
```

3.2.3.6.2 Sample contents of encryptedData in cardInfo

```
{
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
      "accountNumber" : "5123456789012345",
"expiryMonth" : "12" ,
      "expiryYear" : "18" ,
      "source" : "CARD_ON_FILE" ,
      "cardholderName" : "John Doe" ,
"securityCode" : "123",
      "billingAddress" : {
            "line1" : "100 1st Street",
            "line2" : "Apt. 4B",
            "city" : "St. Louis",
            "countrySubdivision" : "MO",
            "postalCode" : "61000",
            "country" : "USA"
      }
}
```

3.2.3.6.3 Sample Request for STATIC Token Type

```
{
      "responseHost" : "site1.your-server.com",
      "requestId" : "123456",
"tokenType": "STATIC",
"tokenRequestorId": "98765432101",

      "cardInfo" : {
            "tokenUniqueReferenceForPanInfo":
"DWSPMC000000000132d72d4fcb2f4136a0532d3093ffffff"
},
"tokenizationAuthenticationValue" :
"RHVtbXkgYmFzZSA2NCBkYXRhIC0gdGhpcyBpcyBub3QgYSByZWFsIFRBViBleGFtcGxl",
      "decisioningData" : {
            "recommendation" : "REQUIRE_ADDITIONAL_AUTHENTICATION",
            "recommendationAlgorithmVersion" : "01",
            "deviceScore" : "1",
            "accountScore" : "1",
            "recommendationReasons" : [
                  "ACCOUNT_TOO_NEW",
                  "TOO_MANY_RECENT_ATTEMPTS",
                  "OUTSIDE_HOME_TERRITORY",
                  "USER_NOT_AVAIALABLE",
                  "AUTHENTICATION_NOT_SUPPORTED"
            ]
      }

      "consumerLanguage" : "en"
}
```

3.2.3.6.4 Sample Response for Static Token Type

```
{
      "responseHost" : "site1.Mastercard.com",
"responseId" : "123456",
      "decision" : "REQUIRE_ADDITIONAL_AUTHENTICATION",

      "tokenUniqueReference" : "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
      "panUniqueReference" : "FWSPMC000000000159f71f703d2141efaf04dd26803f922b",
      "productConfig" : {
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
            "brandLogoAssetId" : "800200c9-629d-11e3-949a-0739d27e5a66",
            "isCoBranded" : "true",
            "coBrandName" : "Co brand partner",
            "coBrandLogoAssetId" : "dbc55444-496a-4896-b41c-5d5e2dd431e2",
"cardBackgroundCombinedAssetId" : "739d27e5-629d-11e3-949a-0800200c9a66",
"foregroundColor" : "000000",
"issuerName" : "Issuing Bank",
"shortDescription" : "Bank Rewards Mastercard",
"longDescription" : "Bank Rewards Mastercard with rewards program",
"issuerLogoAssetId" : "BED1503C-0D6D-40A7-AE8A-749DB4A05D86",
"iconAssetId" : "C307F0AE-298E-48EB-AA43-A7C40B32DDDE",
"customerServiceUrl" : "https://bank.com/customerservice",
"issuerMobileApp" : {
    "openIssuerMobileAppAndroidIntent": {
        "action": "com.mybank.bankingapp.action.OPEN_ISSUER_MOBILE_APP",
        "packageName": "com.mybank.bankingapp",
        "extraTextValue":
"ew0KICAgICJwYXltZW50QXBwUHJvdmlkZXJJZCI6ICIxMjM0NTY3ODkiLA0KICAgICJwYXltZW50QXBwSWQi
OiAiV2FsbGV0QXBwMSIsDQogICAgInBheW1lbnRBcHBJbnN0YW5jZUlkIjogIjEyMzQ1Njc4OSIsDQogICAgI
nRva2VuVW5pcXVlUmVmZXJlbmNlIjogIkRXU1BNQzAwMDAwMDAwMGZjYjJmNDEzNmIyZjQxMzZhMDUzMmQyZj
QxMzZhMDUzMiINCn0="
    }
},
"termsAndConditionsUrl" : "https://bank.com/termsAndConditions",
"privacyPolicyUrl" : "https://bank.com/privacy",
"issuerProductConfigCode" : "123456"
      },
      "tokenInfo" : {
            "tokenPanSuffix": "1234",
            "accountPanSuffix": "6789",
            "alternateAccountIdentifierSuffix": "4567",
            "tokenExpiry" : "1018",
            "dsrpCapable" : true,
            "tokenAssuranceLevel" : 0
      },
      "tokenDetail" : {
            "tokenUniqueReference" :
"DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
            "encryptedData" :
"4545433044323232363739304532433610DE1D1461475BEB6D815F31764DDC20298BD779FBE37EE5AB3C
BDA9F9825E1DDE321469537FE461E824AA55BA67BF6A",
            "publickKeyFingerprint" :  "4c4ead5927f0df8117f178eea9308daa58e27c2b",
            "encryptedKey" : "A1B2C3D4E5F6112233445566",
            "oaepHashingAlgorithm" : "SHA512"
      }
}
```


3.2.3.6.5 Sample contents of encryptedData in tokenDetail for Static Token Type


```
{
      "token" : "5123456789012345",
      "expiryMonth" : "12",
      "expiryYear" : "18",
"paymentAccountReference" : "5001a9f027e5629d11e3949a0800a"
}
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.3.6.6 Sample Response for Cloud Token Type


```
{
       "responseHost" : "site1.Mastercard.com",
"responseId" : "123456",
       "decision" : "REQUIRE_ADDITIONAL_AUTHENTICATION",
       "authenticationMethods" : [
              {
                     "id" : 12344,
                     "type" : "MASKED_MOBILE_PHONE_NUMBER",
                     "value" : "12X-XXX-XX32"
              },
              {
                     "id" : 12345,
                     "type" : "AUTOMATED_CALL_CENTER_PHONE_NUMBER",
                     "value" : "1-800-BANK-NUMBER"
              },
{
                     "id" : 12346,
                     "type" : "CARDHOLDER_TO_USE_ISSUER_MOBILE_APP",
                     "value": "value": "{\"activateWithIssuerMobileAppAndroidIntent\":
\"{\"action\" : \"com.mybank.bankingapp.action.ACTIVATE_TOKEN\",\"packageName\" :
\"com.mybank.bankingapp\",\"extraTextValue\" :
\"ew0KICAgICJwYXltZW50QXBwUHJvdmlkZXJJZCI6ICIxMjM0NTY3ODkiLA0KICAgICJwYXltZW50QXBwSW5
zdGFuY2VJZCI6ICIxMjM0NTY3ODkiLA0KICAgICJ0b2tlblVuaXF1ZVJlZmVyZW5jZSI6ICJEV1NQTUMwMDAw
MDAwMDBmY2IyZjQxMzZiMmY0MTM2YTA1MzJkMmY0MTM2YTA1MzIiLA0KICAgICJhY2NvdW50UGFuU3VmZml4I
jogIjY3ODkiLA0KICAgICJhY2NvdW50RXhwaXJ5IjogIjEwMTgiDQp9\"}\"}"          }
       ],
       "tokenUniqueReference" : "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
       "panUniqueReference" : "FWSPMC000000000159f71f703d2141efaf04dd26803f922b",
       "productConfig" : {
              "brandLogoAssetId" : "800200c9-629d-11e3-949a-0739d27e5a66",
              "isCoBranded" : "true",
              "coBrandName" : "Co brand partner",
              "coBrandLogoAssetId" : "dbc55444-496a-4896-b41c-5d5e2dd431e2",
"cardBackgroundCombinedAssetId" : "739d27e5-629d-11e3-949a-0800200c9a66",
"foregroundColor" : "000000",
"issuerName" : "Issuing Bank",
"shortDescription" : "Bank Rewards Mastercard",
"longDescription" : "Bank Rewards Mastercard with rewards program",
"issuerLogoAssetId" : "BED1503C-0D6D-40A7-AE8A-749DB4A05D86",
"iconAssetId" : "C307F0AE-298E-48EB-AA43-A7C40B32DDDE",
"customerServiceUrl" : "https://bank.com/customerservice",
"issuerMobileApp" : {
    "openIssuerMobileAppAndroidIntent": {
        "action": "com.mybank.bankingapp.action.OPEN_ISSUER_MOBILE_APP",
        "packageName": "com.mybank.bankingapp",
        "extraTextValue":
"ew0KICAgICJwYXltZW50QXBwUHJvdmlkZXJJZCI6ICIxMjM0NTY3ODkiLA0KICAgICJwYXltZW50QXBwSWQi
OiAiV2FsbGV0QXBwMSIsDQogICAgInBheW1lbnRBcHBJbnN0YW5jZUlkIjogIjEyMzQ1Njc4OSIsDQogICAgI
nRva2VuVW5pcXVlUmVmZXJlbmNlIjogIkRXU1BNQzAwMDAwMDAwMGZjYjJmNDEzNmIyZjQxMzZhMDUzMmQyZj
QxMzZhMDUzMiINCn0="
    }
},
"termsAndConditionsUrl" : "https://bank.com/termsAndConditions",
"privacyPolicyUrl" : "https://bank.com/privacy",
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
"issuerProductConfigCode" : "123456"
	},
	"tokenInfo" : {
		"tokenPanSuffix": "1234",
		"accountPanSuffix": "6789",
		"alternateAccountIdentifierSuffix": "4567",
		"tokenExpiry" : "1018",
		"dsrpCapable" : true,
		"tokenAssuranceLevel" : 0
	},
	"tokenDetail" : {
		"tokenUniqueReference" :
"DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
		"encryptedData" :
"4545433044323232363739304532433610DE1D1461475BEB6D815F31764DDC20298BD779FBE37EE5AB3C
BDA9F9825E1DDE321469537FE461E824AA55BA67BF6A",
		"publickKeyFingerprint" :  "4c4ead5927f0df8117f178eea9308daa58e27c2b",
		"encryptedKey" : "A1B2C3D4E5F6112233445566",
		"oaepHashingAlgorithm" : "SHA512"
	}
}
```


3.2.3.6.7 Sample contents of encryptedData in tokenDetail for Cloud Token Type


```
{
	"paymentAccountReference" : "5001a9f027e5629d11e3949a0800a"
}
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.4 Request Activation Code

3.2.4.1 Overview

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

MDES generates an Activation Code and facilitates its delivery via the chosen Activation Code Distribution Method 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 Token Requestor may call this API again in order to trigger a re-send, or to select a different Activation Code Distribution Method, as long as the activation period has not expired. Calling this API again will not cause the Activation Code to be regenerated nor extend the validity period of the Activation Code.

The Token Requestor can complete activation of the Token by supplying the Activation Code via the Activate API (see Section 3.2.6) to activate the Token.

3.2.4.2 URL Endpoint

/requestActivationCode

3.2.4.3 HTTP Method

POST

3.2.4.4 Request Parameters

paymentAppInstanceId	
Description:	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization. This field is alphanumeric and additionally web-safe base64 characters per RFC 4648 (minus "-", underscore "_") up to a maximum length of 48, = should not be URL encoded.
Data Type:	String
Max Length:	48
Required:	Conditional – not applicable for server-based tokens. Required otherwise.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

tokenUniqueReference	
Description:	The Token for which to send an Activation Code. This is the unique reference allocated to the Token. Must be a valid reference as assigned by MDES.
Data Type:	String
Max Length:	64
Required:	Yes
~~**activationMethod**~~	
Description:	Identifies the Activation Method chosen by (or on behalf of) the Cardholder from the list of Activation Methods returned by MDES in the Digitize response (see Section 3.2.2.5) for this Token.
Data Type:	AuthenticationMethod object
Max Length:	N/A
Required:	**Deprecated** – use authenticationMethod instead.
authenticationMethod	
Description:	Identifies the AuthenticationMethod chosen by (or on behalf of) the Cardholder from the list of AuthenticationMethods returned by MDES in the Digitize response (see Section 3.2.2.5) for this Token.
Data Type:	AuthenticationMethod object
Max Length:	N/A
Required:	Yes

3.2.4.5 Response Values

Only common response elements.

3.2.4.6 Examples

3.2.4.6.1 Sample Request

```
{
	"responseHost" : "site1.your-server.com",
"requestId" : "123456",
"paymentAppInstanceId" : "123456789",
	"tokenUniqueReference" : "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
	"authenticationMethod" : {
		"id" : 12344
	}
}
```

3.2.4.6.2 Sample Response

```
{
	"responseHost" : "site1.Mastercard.com",
	"responseId" : "123456"
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.5 Get Asset

3.2.5.1 Overview

This API is used to retrieve static Assets from MDES's repository, such as:

- Card art
- Mastercard brand logos
- Issuers' logos
- Terms and Conditions

Every Asset in the repository is referenced using an Asset ID. Once an Asset has been assigned to an Asset ID, the contents of the Asset will not change. If contents do need to change (for example, Issuer has supplied new artwork for a product), they will be updated in the repository and be assigned a new Asset ID.

Different types of Assets are supported in the repository, such as images and text files; and for each type of Asset, multiple formats may be supported. For example, a single image Asset may be supported in various file formats; or variant sizes, allowing the Token Requestor to select the most appropriate format to use for a particular target device.

3.2.5.2 URL Endpoint

/asset/<AssetId>

Where <AssetId> is the Asset ID value used to reference an Asset.

3.2.5.3 HTTP Method

GET

3.2.5.4 Response Values

mediaContents	
Description:	Contains all contents of the Asset, including all variations (if any).
Data Type:	Array[MediaContent object]
Max Length:	N/A
Required:	Yes

3.2.5.5 Sample Response


```
{
	"mediaContents" : [
		{
			"type" : "image/png",
			"height":"375",
"width":"375",
"data":"iVBORw0KGgoAAAANSUhEUgAAAXcAAAF3CAIAAADRopypAAAABGdBTUEAANbY1E9YMgAAAAlwSFlzA
AAASAAAAEgARslrPgAAGtNJREFUeNrt3W9oW+e9wPFTkx5MpIlItJKppVJHI7Ea1yY0ieskkKbM8VizS0lvy2
CXezvaN3uxQTNYX\/RCU7h90TcpdC"
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
            },
            {
                  "type" : "image/png",
                  "height":"575",
"width":"575",
"data":"Ppefulr4Ydre1RYhpmkWCtOFwnRHIt7b28NSMbASV1RmplzJT1117eBlzYOfGTlNa4CVKK7MTLkyM
XHZB9Pg+dbsHuhnDgUspKwyvunLohd1
e9wPFTkx5MpIlItJKppVJHI7Ea1yY0ieskkKbM8VizS0lvy2CXezvaN3uxQTNYX\/RCU7h90TcpdC "
            }
      ]
}
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.6 Activate

3.2.6.1 Overview

This API is used to activate a Token for first-time use if the digitization decision was to 'Require Additional Authentication' in the Digitize response (see Section 3.2.2.5).

A Token may be activated via this API using either:

- An Authentication Code – a code generated by MDES and delivered via a secure channel to the Cardholder, typically keyed in by the user.
- A Tokenization Authentication Value – a cryptographically signed value that is generated by the Issuer to authorize the request.

A Token may also be activated by Issuer via customer service or otherwise outside this API.

If activation is successful, MDES will complete the provisioning process and will notify the Token Requestor when the Token is ready to transact, using the Notify Token Updated API (see Section 3.3.1).

Note that the user is only given a limited number of attempts to enter a correct Authentication Code (typically 3 attempts), after which the Authentication Code becomes invalid. In this event, it may be possible to request a new Authentication Code directly from the Issuer via customer service or otherwise. This is dependent on individual Issuer implementation and out of scope of this API.

3.2.6.2 URL Endpoint

/activate

3.2.6.3 HTTP Method

POST

3.2.6.4 Request Parameters

paymentAppInstanceId	
Description:	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization. This field is alphanumeric and additionally web-safe base64 characters per RFC 4648 (minus "-", underscore "_") up to a maximum length of 48, = should not be URL encoded.
Data Type:	String
Max Length:	48
Required:	Conditional – not applicable for server-based tokens. Required otherwise.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

tokenUniqueReference	
Description:	The Token to be activated. This is the unique reference allocated to the Token. Must be a valid reference as assigned by MDES.
Data Type:	String
Max Length:	64
Required:	Yes.
~~**activationCode**~~	
Description:	The Authentication Code as entered by the Cardholder (or entered by other means) to activate the Token.
Data Type:	String
Max Length:	32
Required:	**Deprecated** – use authenticationCode instead.
authenticationCode	
Description:	The Authentication Code as entered by the Cardholder (or entered by other means) to activate the Token.
Data Type:	String
Max Length:	32
Required:	Conditional – one of either the 'authenticationCode' or the 'tokenizationAuthenticationValue' is required.
tokenizationAuthenticationValue	
Description:	The Tokenization Authentication Value (TAV) as cryptographically signed by the Issuer to activate this Token.
Data Type:	String
Max Length:	2048
Required:	Conditional – one of either the 'authenticationCode' or the 'tokenizationAuthenticationValue' is required.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.6.5 Response Values

result

Description: Whether the activation request was successful.

Success will result in MDES attempting to complete the provisioning process. MDES will notify the Token Requestor when the Token is ready to transact using the Notify Token Updated API (see Section 3.3.1).

Must be one of:

Value	Meaning
SUCCESS	Activation was successful
INCORRECT_CODE	Authentication Code was incorrect and rejected. Retries permitted.
INCORRECT_CODE_RETRIES_EXCEEDED	Authentication Code was incorrect and the maximum number of retries now exceeded.
EXPIRED_CODE	Authentication Code has expired or was invalidated.
INCORRECT_TAV	Tokenization Authentication Value was incorrect and rejected.
EXPIRED_SESSION	The Token cannot be activated because the digitization session has expired. The caller must delete any artifacts relating to the Token and restart the process from the beginning.

Data Type: String

Max Length: 64

Required: Yes

3.2.6.6 Examples

3.2.6.6.1 Sample Request

```
{
      "responseHost" : "site2.your-server.com",
      "requestId" : "123456",
      "paymentAppInstanceId" : "123456789",
      "tokenUniqueReference" : "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
      "authenticationCode" : "A1B2C3D4"
}
```

3.2.6.6.2 Sample Response

```
{
      "responseHost" : "site1.Mastercard.com",
      "responseId" : "123456",
      "result" : "SUCCESS"
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.7 Suspend

3.2.7.1 Overview

This API is used to temporarily suspend one or more Tokens (for example, suspending all Tokens on a device in response to the device being lost). The API is limited to 10 Tokens per request.

MDES will coordinate the suspension of the Tokens and notify any relevant parties that the Tokens have been suspended.

A suspended Token can be unsuspended using the Unsuspend API (see Section 3.2.8).

3.2.7.2 URL Endpoint

/suspend

3.2.7.3 HTTP Method

POST

3.2.7.4 Request Parameters

paymentAppInstanceId	
Description:	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization. This field is alphanumeric and additionally web-safe base64 characters per RFC 4648 (minus "-", underscore "_") up to a maximum length of 48, = should not be URL encoded.
Data Type:	String
Max Length:	48
Required:	Conditional – not applicable for server-based tokens. Required otherwise.

tokenUniqueReferences	
Description:	The Tokens to be suspended. Array of one or more valid references as assigned by MDES.
Data Type:	Array[String]
Max Length:	N/A
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

causedBy

Description: Who or what caused the Token to be suspended.

Must be one of:

Value	Meaning
CARDHOLDER	Operation requested by the Cardholder. Not valid for STATIC tokens.
~~PAYMENT_APP_PROVIDER~~	Operation requested by the Payment App provider for a systematic reason. **Deprecated** – use TOKEN_REQUESTOR instead.
TOKEN_REQUESTOR	Operation requested by the Token Requestor.

Data Type: String

Max Length: 64

Required: Yes

reason

Description: Free form reason why the Tokens are being suspended.

Data Type: String

Max Length: 256

Required: No

reasonCode

Description: The reason for the action to be suspended

Must be one of:

Value	Meaning
DEVICE_LOST	Token device lost. Not valid for STATIC tokens.
DEVICE_STOLEN	Token device stolen. Not valid for STATIC tokens.
SUSPECTED_FRAUD	Suspected fraudulent token transactions.
OTHER	Other – default, used if value not provided.

Data Type: String

Max Length: 64

Required: Yes – but may be omitted in some existing implementations for backwards-compatibility.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.7.5 Response Values

tokens

Description:	State of each Token following this operation.
Data Type:	Array[Token object]
Max Length:	N/A
Required:	Yes.

3.2.7.6 Examples

3.2.7.6.1 Sample Request

```
{
"responseHost" : "site2.your-server.com",
"requestId" : "123456",
"paymentAppInstanceId" : "123456789",
      "tokenUniqueReferences" : [
            "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
            "DWSPMC00000000032d72d4ffcb2f4136a0532d32d72d4fcb",
            "DWSPMC000000000fcb2f4136b2f4136a0532d2f4136a0532"
      ],
      "reason" : "Lost/stolen device",
      "reasonCode" : "DEVICE_LOST",
"causedBy" : "CARDHOLDER"
}
```

3.2.7.6.2 Sample Response

```
{
      "responseHost" : "site1.Mastercard.com",
      "responseId" : "123456",
      "tokens" : [
            {
                  "tokenUniqueReference" :
"DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
                  "status" : "SUSPENDED",
                  "statusTimestamp" : "2017-07-20T04:56:23.345-07:00",
                  "suspendedBy" : [
"CARDHOLDER",
"TOKEN_REQUESTOR"
]
            },
            {
                  "tokenUniqueReference" :
"DWSPMC00000000032d72d4ffcb2f4136a0532d32d72d4fcb",
            "status" : "SUSPENDED",
"statusTimestamp" : "2017-07-20T04:56:23.345-07:00",
                  "suspendedBy" :  ["CARDHOLDER"]
            },
            {
                  "tokenUniqueReference" :
"DWSPMC000000000fcb2f4136b2f4136a0532d2f4136a0532",
                  "errorCode" : "INVALID_TOKEN_UNIQUE_REFERENCE",
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
                    "errorDescription": " Invalid Token Unique Reference",
                    "errors" : [
                      {
                           "source" : "INPUT",
                           "reasonCode" : "INVALID_TOKEN_UNIQUE_REFERENCE",
                    "description" : " Invalid Token Unique Reference"
                       }
                    ]
               }
        ]
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.8 Unsuspend

3.2.8.1 Overview

This API is used to unsuspend one or more previously suspended Tokens (see Section 3.2.7 – Suspend). The API is limited to 10 Tokens per request.

MDES will coordinate the unsuspension of the Tokens and notify any relevant parties that the Tokens have now been unsuspended.

3.2.8.2 URL Endpoint

/unsuspend

3.2.8.3 HTTP Method

POST

3.2.8.4 Request Parameters

paymentAppInstanceId	
Description:	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization. This field is alphanumeric and additionally web-safe base64 characters per RFC 4648 (minus "-", underscore "_") up to a maximum length of 48, = should not be URL encoded.
Data Type:	String
Max Length:	48
Required:	Conditional – not applicable for server-based tokens. Required otherwise.

tokenUniqueReferences	
Description:	The Tokens to be unsuspended. Array of one or more valid references as assigned by MDES.
Data Type:	Array[String]
Max Length:	N/A
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

causedBy

Description: Who or what caused the Token to be unsuspended.

Must be one of

Value	Meaning
CARDHOLDER	Operation requested by the Cardholder. Not valid for STATIC tokens.
~~PAYMENT_APP_PROVIDER~~	Operation requested by the Payment App provider for a systematic reason. **Deprecated** – use TOKEN_REQUESTOR instead.
TOKEN_REQUESTOR	Operation requested by the Token Requestor.

Data Type: String

Max Length: 64

Required: Yes

reason

Description: Freeform reason why the Tokens are being unsuspended.

Data Type: String

Max Length: 256

Required: No

reasonCode

Description: The reason for the action to be unsuspended

Must be one of:

Value	Meaning
DEVICE_FOUND	Token device found or not stolen. Not valid for STATIC tokens.
NOT_FRAUD	Confirmed no fraudulent token transactions.
OTHER	Other – default, used if value not provided.

Data Type: String

Max Length: 64

Required: Yes – but may be omitted in some existing implementations for backwards-compatibility.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.8.5 Response Values

tokens	
Description:	State of each Token following this operation.
Data Type:	Array[Token object]
Max Length:	N/A
Required:	Yes.

3.2.8.6 Examples

3.2.8.6.1 Sample Request

```
{
      "responseHost" : "site2.your-server.com",
      "requestId" : "123456",
      "tokenUniqueReferences" : [
            "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
            "DWSPMC00000000032d72d4ffcb2f4136a0532d32d72d4fcb",
            "DWSPMC000000000fcb2f4136b2f4136a0532d2f4136a0532"
      ],
      "reason" : " LOST_STOLEN_DEVICE_FOUND ",
      "reasonCode" : "DEVICE_FOUND",
"causedBy" : "CARDHOLDER"
}
```

3.2.8.6.2 Sample Response

```
{
      "responseHost" : "site1.Mastercard.com",
      "responseId" : "123456",
      "paymentAppInstanceId" : "123456789",
      "tokens" : [
{
                  "tokenUniqueReference" :
"DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
                  "status" : "SUSPENDED",
"statusTimestamp" : "2017-07-20T04:56:23.345-07:00",
                  "suspendedBy" : [
"TOKEN_REQUESTOR"
]
            },
            {
                  "tokenUniqueReference" :
"DWSPMC00000000032d72d4ffcb2f4136a0532d32d72d4fcb",
                  "status" : "ACTIVE",
"statusTimestamp" : "2017-07-20T04:56:23.345-07:00"
            },
            {
                  "tokenUniqueReference" :
"DWSPMC000000000fcb2f4136b2f4136a0532d2f4136a0532",
                  "errorCode" : "INVALID_TOKEN_UNIQUE_REFERENCE",
                  "errorDescription": " Invalid Token Unique Reference",
                  "errors" : [
                     {
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
                        "source" : "INPUT",
                        "reasonCode" : "INVALID_TOKEN_UNIQUE_REFERENCE",
                        "description" : " Invalid Token Unique Reference"
                    }
                ]
            }
        ]
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.9 Delete

3.2.9.1 Overview

This API is used to delete one or more Tokens. The API is limited to 10 Tokens per request.

MDES will coordinate the deactivation of the Tokens and notify any relevant parties that the Tokens have now been deactivated.

3.2.9.2 URL Endpoint

/delete

3.2.9.3 HTTP Method

POST

3.2.9.4 Request Parameters

paymentAppInstanceId	
Description:	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization. This field is alphanumeric and additionally web-safe base64 characters per RFC 4648 (minus "-", underscore "_") up to a maximum length of 48, = should not be URL encoded.
Data Type:	String
Max Length:	48
Required:	Conditional – not applicable for server-based tokens. Required otherwise.

tokenUniqueReferences	
Description:	The Tokens to be deleted. Array of valid references as assigned by MDES.
Data Type:	Array[String]
Max Length:	N/A
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

causedBy

Description: Who or what caused the Token to be deleted.

Must be one of

Value	Meaning
CARDHOLDER	Operation requested by the Cardholder
~~PAYMENT_APP_PROVIDER~~	Operation requested by the Payment App provider for a systematic reason. **Deprecated** – use TOKEN_REQUESTOR instead.
TOKEN_REQUESTOR	Operation requested by the Token Requestor.

Data Type: String

Max Length: 64

Required: Yes

reason

Description: Freeform reason why the Tokens are being deleted.

Data Type: String

Max Length: 256

Required: No

reasonCode

Description: The reason for the action to be suspended

Must be one of:

Value	Meaning
DEVICE_LOST	Token device lost. Not valid for STATIC tokens.
DEVICE_STOLEN	Token device stolen. Not valid for STATIC tokens.
ACCOUNT_CLOSED	Account closed
SUSPECTED_FRAUD	Suspected fraudulent token transactions.
OTHER	Other – default, used if value not provided.

Data Type: String

Max Length: 64

Required: Yes – but may be omitted in some existing implementations for backwards-compatibility.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.9.5 Response Values

tokens	
Description:	State of each Token following this operation.
Data Type:	Array[Token object]
Max Length:	N/A
Required:	Yes.

3.2.9.6 Examples

3.2.9.6.1 Sample Request

```
{
"responseHost" : "site2.your-server.com",
"requestId" : "123456",
"paymentAppInstanceId" : "123456789",
      "tokenUniqueReferences" : [
            "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
            "DWSPMC00000000032d72d4ffcb2f4136a0532d32d72d4fcb",
            "DWSPMC000000000fcb2f4136b2f4136a0532d2f4136a0532"
      ],
      "causedBy" : "CARDHOLDER",
      "reasonCode" : "DEVICE_LOST",
"reason" : "LOST_STOLEN_DEVICE"
}
```

3.2.9.6.2 Sample Response

```
{
"responseHost" : "site1.Mastercard.com",
      "responseId" : "123456",
      "tokens" : [
            {
                  "tokenUniqueReference" :
"DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
                  "status" : "DEACTIVATED",
"statusTimestamp" : "2017-07-20T04:56:23.345-07:00"
},
            {
                  "tokenUniqueReference" :
"DWSPMC00000000032d72d4ffcb2f4136a0532d32d72d4fcb",
                  "status" : "DEACTIVATED",
"statusTimestamp" : "2017-07-20T04:56:23.345-07:00"
            },
            {
                  "tokenUniqueReference" :
"DWSPMC000000000fcb2f4136b2f4136a0532d2f4136a0532",
                  "errorCode" : "INVALID_TOKEN_UNIQUE_REFERENCE",
                  "errorDescription": " Invalid Token Unique Reference",
                  "errors" : [
                     {
                         "source" : "INPUT",
                         "reasonCode" : "INVALID_TOKEN_UNIQUE_REFERENCE",
                         "description" : " Invalid Token Unique Reference"
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
                    }
                ]
            }
        ]
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.10 Get Device Status (deprecated – use Search Tokens)

3.2.10.1 Overview

This API is used to get the status of all Tokens on a specified device, or the status of a specified Token on a device.

When used to query all Tokens on a specified device, only Token statuses are provided in the response. To retrieve full details about a Token including its product configuration and Token information, the Token Unique Reference must be given identifying the specific Token to be queried. Deactivated tokens may be queried only by specifying the Token to be queried – deactivated tokens are not shown when querying all Tokens.

It may be used to check current Token(s) state or in exception scenarios (such as network time out) to ensure that external systems remain in sync with the Token state as maintained by MDES.

The caller will only receive information for Tokens relating to them. It cannot be used to perform a general query on other Tokens in the system.

3.2.10.2 URL Endpoint

/getDeviceStatus

3.2.10.3 HTTP Method

POST

3.2.10.4 Request Parameters

tokenUniqueReference	
Description:	The specific Token to be queried. This is the unique reference allocated to the Token.
Data Type:	String
Max Length:	64
Required:	No

paymentAppInstanceId	
Description:	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization. This field is alphanumeric and additionally web-safe base64 characters per RFC 4648 (minus "-", underscore "_") up to a maximum length of 48, = should not be URL encoded.
Data Type:	String
Max Length:	48
Required:	Required

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.10.5 Response Values

tokens	
Description:	Status of specified Tokens on the specified device.
Data Type:	Array[Token object]
Max Length:	N/A
Required:	Yes

3.2.10.6 Examples

3.2.10.6.1 Sample Request (querying all Tokens)

```
{
"responseHost" : "site2.your-server.com",
	"requestId" : "123456",
	"paymentAppInstanceId" : "123456789"
}
```

3.2.10.6.2 Sample Response (querying all Tokens)

```
{
"responseHost" : "site1.Mastercard.com",
	"responseId" : "123456",
	"tokens" : [
 {
			"tokenUniqueReference" :
"DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
			"status" : "ACTIVE"
		},
		{
			"tokenUniqueReference" :
"DWSPMC00000000032d72d4ffcb2f4136a0532d32d72d4fcb",
			"status" : "ACTIVE"
		},
		{
			"tokenUniqueReference" :
"DWSPMC000000000fcb2f4136b2f4136a0532d2f4136a0532",
			"status" : "SUSPENDED",
			"suspendedBy" : ["TOKEN_REQUESTOR"]
		}
	]
}
```

3.2.10.6.3 Sample Request (querying a specified Token)

```
{
"responseHost" : "site2.your-server.com",
	"requestId" : "123456",
	"paymentAppInstanceId" : "123456789",
"tokenUniqueReference" : "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45"
}
```

3.2.10.6.4 Sample Response (querying a specified Token)

```
{
"responseHost" : "site1.Mastercard.com",
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
      "responseId" : "123456",
      "tokens" : [
 {
                    "tokenUniqueReference" :
"DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
                    "status" : "ACTIVE",
"productConfig" : {
                           "brandLogoAssetId" : "800200c9-629d-11e3-949a-
0739d27e5a66",
                           "isCoBranded" : "true",
                           "coBrandName" : "Co brand partner",
                           "coBrandLogoAssetId" : "dbc55444-496a-4896-b41c-
5d5e2dd431e2",

                           "cardBackgroundCombinedAssetId" : "739d27e5-629d-11e3-
949a0800200c9a66",
                           "foregroundColor" : "000000",
                           "issuerName" : "Issuing Bank",
                           "shortDescription" : "Bank Rewards Mastercard",
                           "longDescription" : "Bank Rewards Mastercard with the
super duper rewards program",
                           "customerServiceUrl" : "https://bank.com/customerservice",
                           "termsAndConditionsUrl" :
"https://bank.com/termsAndConditions",
                           "privacyPolicyUrl" : "https://bank.com/privacy",
                           "issuerProductConfigCode" : "123456"
                    },
                    "tokenInfo" : {
                           "tokenPanSuffix": "1234",
                           "accountPanSuffix": "6789",
                           "tokenExpiry" : "1018",
                           "dsrpCapable" : true
                    }
             }
      ]
}
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.11 Get Task Status

3.2.11.1 Overview

This API is used to check the status of any asynchronous task that was previously requested.

3.2.11.2 URL Endpoint

/getTaskStatus

3.2.11.3 HTTP Method

POST

3.2.11.4 Request Parameters

paymentAppInstanceId	
Description:	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization. This field is alphanumeric and additionally web-safe base64 characters per RFC 4648 (minus "-", underscore "_") up to a maximum length of 48, = should not be URL encoded.
Data Type:	String
Max Length:	48
Required:	Conditional – not applicable for server-based tokens. Required otherwise.

tokenRequestorId	
Description:	Identifies the Token Requestor.
Data Type:	String
Max Length:	11 (Exact)
Required:	Conditional – required when paymentAppInstanceId not present. Not applicable otherwise.

taskId	
Description:	Unique identifier for this task. Must be an identifier previously used when requesting a task.
Data Type:	String
Max Length:	64
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.11.5 Response Values

status

Description: The status of the specified task. Must be one of:

Value	Meaning
PENDING	The task has been received and is pending processing.
IN_PROGRESS	The task is currently in progress
COMPLETED	The task was completed successfully
FAILED	The task was processed but failed to complete successfully.
~~UNKNOWN_TASK~~	The taskId given was not recognized. **Deprecated –** use an error of INVALID_TASK_ID instead.

Data Type: String

Max Length: 64

Required: Yes

3.2.11.6 Examples

3.2.11.6.1 Sample Request

```
{
      "requestId": "123456",
      "paymentAppInstanceId" : "123456789",
      "taskId": "123456"
}
```

3.2.11.6.2 Sample Response

```
{
      "responseId": "123456",
      "status": "PENDING"
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.12 Get System Health

3.2.12.1 Overview

This API is used to check the general status of a Digitization API host.

A successful response contains an HTTP response code of 200 with an empty body, and indicates that the service is running and accepting requests.

3.2.12.2 URL Endpoint

/health

3.2.12.3 HTTP Method

GET

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.13 Search Tokens

3.2.13.1 Overview

This API is used to get basic token information for all tokens on a specified device, or all tokens mapped to the given Account PAN.

It may be used to check current Token(s) state or, in exception scenarios (such as network time out), to ensure that external systems remain in sync with the Token state as maintained by MDES.

Deactivated tokens are not returned.

3.2.13.2 URL Endpoint

/searchTokens

3.2.13.3 HTTP Method

POST

3.2.13.4 Request Parameters

paymentAppInstanceId	
Description:	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization. This field is alphanumeric and additionally web-safe base64 characters per RFC 4648 (minus "-", underscore "_") up to a maximum length of 48, = should not be URL encoded.
Data Type:	String
Max Length:	48
Required:	Conditional – not applicable for server-based tokens. Required otherwise.
cardInfo	
Description:	Contains card information of the card being queried. Only pan and expiry date fields are supported.
Data Type:	CardInfo object.
Max Length:	N/A
Required:	Conditional – required if paymentAppInstanceId is not provided. Not applicable otherwise.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

tokenRequestorId	
Description:	Identifies the Token Requestor. Only tokens associated with the Token Requestor will be returned.
Data Type:	String
Max Length:	11 (Exact)
Required:	Conditional – required if cardInfo is provided.

3.2.13.5 Response Values

tokens	
Description:	State of each Token assigned to the PAN related to the requestor.
Data Type:	Array[Token object]
Max Length:	N/A
Required:	Yes.

3.2.13.6 Examples

3.2.13.6.1 Sample Request by Card Number

```
{
      "requestId": "123456",
      "cardInfo" : {
"encryptedData" :
"4545433044323232363739304532433610DE1D1461475BEB6D815F31764DDC20298BD779FBE37EE5AB3C
BDA9F9825E1DDE321469537FE461E824AA55BA67BF6A",
            "publicKeyFingerprint" :  "4c4ead5927f0df8117f178eea9308daa58e27c2b",
            "encryptedKey" : "A1B2C3D4E5F6112233445566",
            "oaepHashingAlgorithm" : "SHA512"
      },
      "tokenRequestorId": "98765432101"
}
```

3.2.13.6.2 Sample contents of encryptedData in cardInfo

```
{
"accountNumber" : "5123456789012345",
"expiryMonth" : "12",
      "expiryYear" : "18"
}
```

3.2.13.6.3 Sample Request by Payment App Instance Id

```
{
      "requestId": "123456",
      "paymentAppInstanceId" : "123456789"
}
```

3.2.13.6.4 Sample Response

```
{
  "responseHost" : "site1.Mastercard.com",
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
  "responseId" : "123456",
  "tokens" : [
{
        "tokenUniqueReference" : "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
        "status" : "SUSPENDED",
        "statusTimestamp" : "2017-07-20T04:56:23.345-07:00",
        "suspendedBy" : [ "TOKEN_REQUESTOR"]
      },
      {
        "tokenUniqueReference" : "DWSPMC00000000032d72d4ffcb2f4136a0532d32d72d4fcb",
  "status" : "ACTIVE","
  "statusTimestamp" : "2017-07-20T04:56:23.345-07:00"
      }
  ]
}
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.14 Get Token

3.2.14.1 Overview

This API is used to get the status and details of a single given Token.

It may be used to check current Token state or in exception scenarios (such as network time out) to ensure that external systems remain in sync with the Token state as maintained by MDES.

Optionally, if requested, the token number can also be provided in the response (in encrypted form).

3.2.14.2 URL Endpoint

/getToken

3.2.14.3 HTTP Method

POST

3.2.14.4 Request Parameters

paymentAppInstanceId	
Description:	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization. This field is alphanumeric and additionally web-safe base64 characters per RFC 4648 (minus "-", underscore "_") up to a maximum length of 48, = should not be URL encoded.
Data Type:	String
Max Length:	48
Required:	Conditional – not applicable for server-based tokens. Required otherwise.

tokenUniqueReference	
Description:	The specific Token to be queried.
Data Type:	String
Max Length:	64
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

includeTokenDetail

Description: Flag to indicate if the encrypted token should be returned.
Must be one of:

Value	Meaning
true	Token Detail object should be returned
false	Token Detail object should not be returned.

Data Type: Boolean

Max Length: 5

Required: No

3.2.14.5 Response Values

token

Description: Status of the specified Token.

Data Type: Token

Max Length: N/A

Required: Yes

tokenDetail

Description: The encrypted Token information. Only provided in Get Token Status if includeTokenDetail flag is true.

Data Type: TokenDetail Object

Max Length: N/A

Required: No

3.2.14.6 Examples

3.2.14.6.1 Sample Request

```
{
	"requestId": "123456",
	"paymentAppInstanceId" : "123456789",
	"tokenUniqueReference" : "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
	"includeTokenDetail" : true
}
```

3.2.14.6.2 Sample Response

```
{
	"responseId": "123456",
	"token" : {
		"tokenUniqueReference" :
"DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
		"status" : "ACTIVE",
		"statusTimestamp" : "2017-07-20T04:56:23.345-07:00",

		"productConfig" : {
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
                    "brandLogoAssetId" : "800200c9-629d-11e3-949a-0739d27e5a66",
                   "isCoBranded" : "true",
                    "coBrandName" : "Co brand partner",
                    "coBrandLogoAssetId" : "dbc55444-496a-4896-b41c-5d5e2dd431e2",
                    "cardBackgroundCombinedAssetId" : "739d27e5-629d-11e3-
949a0800200c9a66",
                    "foregroundColor" : "000000",
                    "issuerName" : "Issuing Bank",
                    "shortDescription" : "Bank Rewards Mastercard",
                    "longDescription" : "Bank Rewards Mastercard with the super duper
rewards program",
                    "customerServiceUrl" : "https://bank.com/customerservice",
                    "termsAndConditionsUrl" : "https://bank.com/termsAndConditions",
                    "privacyPolicyUrl" : "https://bank.com/privacy",
                    "issuerProductConfigCode" : "123456"
             },
             "tokenInfo" : {
                    "tokenPanSuffix": "1234",
                    "accountPanSuffix": "6789",
"alternateAccountIdentifierSuffix": "4567",
                    "tokenExpiry" : "1018",
                    "dsrpCapable" : true,
                    "tokenAssuranceLevel" : 0
             }
      },
      "tokenDetail" : {
             "tokenUniqueReference" :
"DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
             "encryptedData" :
"4545433044323232363739304532433610DE1D1461475BEB6D815F31764DDC20298BD779FBE37EE5AB3C
BDA9F9825E1DDE321469537FE461E824AA55BA67BF6A",
             "publicKeyFingerprint" :  "4c4ead5927f0df8117f178eea9308daa58e27c2b",
             "encryptedKey" : "A1B2C3D4E5F6112233445566",
             "oaepHashingAlgorithm" : "SHA512"
      }
}
```


3.2.14.6.3 Sample contents of encryptedData in tokenDetail


```
{
      "token" : "5123456789012345",
      "expiryMonth" : "12",
      "expiryYear" : "18",
"paymentAccountReference" : "500181d9f8e0629211e3949a08002"
}
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.15 Get Transaction History

3.2.15.1 Overview

This API is used by the Token Requestor to get recent transactions for one or more Tokens. This API may be called in response to a notification from the Transaction Details Service, or it may be called independently (for example, in response to the Cardholder manually refreshing the transaction history from the user interface).

An error will be returned if the client is not configured to use the server to server TDS model (as configured during onboarding), or if the token is not eligible for the service.

3.2.15.2 URL Endpoint

/getTransactionHistory

3.2.15.3 HTTP Method

POST

3.2.15.4 Request Parameters

tokenUniqueReferences	
Description:	The Tokens for which to get transaction details. Array of one or more valid references as assigned by MDES.
Data Type:	Array[String]
Max Length:	10
Required:	Yes

transactionsFromTimestamp	
Description:	This can optionally be used to filter the list of records to be returned – when supplied, the transaction details returned shall be filtered to include only those transactions which are new or have been updated since the timestamp provided. Note that the 'transactionsFromTimestamp' is not bound to a specific 'tokenUniqueReference'. The 'transactionsFromTimestamp' also has no time limit. Must be 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:	No

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.15.5 Response Values

tokenTransactions

Description:	All the transactions for the requested Tokens, filtered by the 'transactionsFromTimestamp' if one was provided in the request.
Data Type:	Array[TokenTransaction object]
Max Length:	N/A
Required:	Yes

3.2.15.6 Examples

3.2.15.6.1 Sample Request

```
{
      "requestId" : "123456",
"tokenUniqueReferences" : [
"DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
"DWSPMC000000000538d7244ffb2341a7cc29bd3135a822b4",
"DWSPMC0000000002083cc44f09aaa21b0139cb11773e00e0"
],

      "transactionsFromTimestamp" : "2016-05-04T12:08:56.123-07:00"
}
```

3.2.15.6.2 Sample Successful Response

```
{
"responseId" : "123456",
"responseHost" : "site2.Mastercard.com",
       "tokenTransactions" : [
             {
                    "tokenUniqueReference" :
"DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
                    "transactions": [
                          {
                              "tokenUniqueReference" :
"DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
                               "recordId" : "123456",
            "transactionIdentifier" :
"6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b",
            "transactionType" : "PURCHASE",
            "amount" : 123.45,
            "currencyCode" : "USD",
            "authorizationStatus" : "CLEARED",
            "transactionTimestamp" : "2016-05-05T08:23:05.000-07:00",
            "merchantName" : "Bob's Burgers",
            "merchantType" : "5812",
            "merchantPostalCode" : "61000"

                           },
                           {
                               "recordId" : "123457",
            "transactionIdentifier" :
"d4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35",
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
            "transactionType" : "REFUND",
            "amount" : -54.23,
            "currencyCode" : "USD",
            "authorizationStatus" : "CLEARED",
            "transactionTimestamp" : "2016-05-06T09:33:05.000-07:00",
            "merchantName" : "Bob's Burgers",
            "merchantType" : "5812",
            "merchantPostalCode" : "61000"
                           }

                     ]
              },
              {
                     "tokenUniqueReference" : "
DWSPMC000000000538d7244ffb2341a7cc29bd3135a822b4",
                     "transactions": []
              },
              {
                     "tokenUniqueReference" : "
DWSPMC0000000002083cc44f09aaa21b0139cb11773e00e0",
                     "transactions": []
              }

       ]
}
```

3.2.15.6.3 Sample Error Response

```
{
"responseId" : "123456",
"responseHost" : "site2.Mastercard.com",
       "tokenTransactions" : [
              {
                     "tokenUniqueReference" :
"DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
 "errorCode" : "INVALID_TOKEN_UNIQUE_REFERENCE",
                     "errorDescription": " Invalid Token Unique Reference",
                     "errors" : [
                        {
                           "source" : "INPUT",
                           "reasonCode" : "INVALID_TOKEN_UNIQUE_REFERENCE",
                           "description" : " Invalid Token Unique Reference "
                        }
                     ]
              }
       ]
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.16 Get Alternate Payment Credentials

3.2.16.1 Overview

Note: This API is not applicable to device or server based digital wallets.

Get Alternate Payment Credentials API is used to obtain payment credentials usable with merchants who have not yet been upgraded to support DSRP with Full EMV data or UCAF to be able to process Secure Element or Cloud-based MDES token transactions.

This API is only exposed to Masterpass when the partner wallet provides a token and a cryptogram for use in a DSRP transaction but the merchant cannot use the cryptogram.

The API swaps a cryptogram with a Dynamic Expiration Date and optionally a Dynamic Token Verification Code to use alongside with the token in a payment transaction. When the transaction is processed the Mastercard network uses the Dynamic Expiration Date to look up the cryptogram and re-inject it into the transaction so that the MDES on-behalf crypto service can run. To merchants located in US and for a Durbin eligible BIN the API returns an Account PAN and an Account PAN expiration date unless the US merchant explicitly chooses to process the debit transaction using the Mastercard network.

An error will be returned if the mobile wallet application is not configured to use getAlternatePaymentCredentials or if the token in the request does not belong to the wallet.

3.2.16.2 URL Endpoint

/getAlternatePaymentCredentials

3.2.16.3 HTTP Method

POST

3.2.16.4 Request Parameters

encryptedPayload	
Description:	Contains an encrypted object.
Data Type:	EncryptedPayload object containing a AlternatePaymentCredentialsRequest object.
Max Length:	N/A
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

minutesValid

Description:	The number of minutes the exchanged cryptogram should be valid. After the validity period expires a transaction submitted with the dynamic data will be declined. The maximum validity period is 30 days or 43,200 minutes. If not supplied a default validity period will be applied.
Data Type:	String(Numeric)
Max Length:	5
Required:	No

merchantSupportsDtvc

Description: Flag to indicate if the merchant supports receiving a Dynamic Token Verification Code (DTVC) value. If true then a DTVC will be returned and should be submitted by the merchant in the DE 48, subelement 92 (CVC2) field of the authorization or financial transaction message.

Must be one of:

Value	Meaning
true	Merchant supports receiving the DTVC and submitting an authorization or financial transaction message with the DTVC in the CVC2 field.
false	Merchant does not support receiving the DTVC and submitting an authorization or financial transaction message with the DTVC in the CVC2 field.

Data Type:	Boolean
Max Length:	5
Required:	Yes

walletMerchantIdentifier

Description:	Unique identifier assigned by the wallet used to identify the merchant. Only alpha-numeric characters are accepted.
Data Type:	String (Alpha-Numeric)
Max Length:	36
Required:	No

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

durbinRightsRequested

Description: Flag to indicate if the US merchant chooses to process the transactions for a Durbin eligible BIN through any network. If true then the merchant is located in US and requested their Durbin rights. If false then either the merchant is not in US or the merchant explicitly chooses to process Durbin eligible BIN transactions using the Mastercard network (by opting out of their Durbin rights).

Must be one of:

Value	Meaning
true	US merchant chooses to keep their rights to process the transactions for a Durbin eligible BIN through any network
false	US merchant has opted out of Durbin rights or is not a US merchant

Data Type: Boolean

Max Length: 5

Required: Yes

3.2.16.5 Response Values

dynamicExpirationDate

Description: The dynamically generated expiration date to be used in place of the cryptographic data in the authorization request. Expressed as YYMM.

Data Type: String(Numeric)

Max Length: 4

Required: Conditional – required if the encryptedPayload is not returned. Not present otherwise.

dynamicTokenVerificationCode

Description: The dynamicTokenVerificationCode to be submitted by the merchant in the CVC2 field of the authorization request. The dynamicTokenVerificationCode will only be returned if merchantSupportsDtvc is True in the request.

Data Type: String(Numeric)

Max Length: 3

Required: No

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

minutesValid	
Description:	The number of minutes the exchanged cryptogram is valid. After the validity period expires a transaction submitted with the dynamic data will be declined.
Data Type:	String(Numeric)
Max Length:	5
Required:	Conditional – required if dynamicExpirationDate is not null. Not present otherwise.
encryptedPayload	
Description:	Contains an encrypted object only returned if durbinRightsRequested is true and for the token in the request is associated to a Durbin eligible BIN (i.e. a debit account range with country of issuance in US capable of being processed by an alternate network).
Data Type:	EncryptedPayload object containing a CardInfoData object.
Max Length:	N/A
Required:	Conditional – required if all of the conditions in the description are met. Not present otherwise.

3.2.16.6 Examples

3.2.16.6.1 Sample Request

```
{
  "responseHost" : "site1.mastercard.com ",
  "requestId" : "123456",
  "encryptedPayload" : {
"encryptedData" :
"4545433044323232363739304532433610DE1D1461475BEB6D815F31764DDC20298BD779FBE37EE5AB3C
BDA9F9825E1DDE321469537FE461E824AA55BA67BF6A",
"publicKeyFingerprint" :  "4c4ead5927f0df8117f178eea9308daa58e27c2b",
"encryptedKey" : "A1B2C3D4E5F6112233445566",
"oaepHashingAlgorithm" : "SHA512"
  },
  "minutesValid" : "15",
  "merchantSupportsDtvc" : true,
  "walletMerchantIdentifier" : "fadf46a54fhjuk4yukjd44gewrw44f4gsd42",
  "durbinRightsRequested" : true
}
```

3.2.16.6.2 Sample contents of encryptedData in the request encryptedPayload

```
{
       "tokenNumber" :"5480981500100002",
       "tokenExpiry" : "1809",
       "cryptographicData" : "112233445566778899001122334 4"
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.16.6.3 Sample Successful Response – not Durbin eligible


```
{
"responseId" : "123456",
"responseHost" : "site2.mastercard.com",
       "dynamicExpirationDate" : "1912",
       "dynamicTokenVerificationCode" : "123",
       "minutesValid" : "15"
}
```


3.2.16.6.4 Sample Successful Response – Durbin eligible


```
{
"responseId" : "123456",
"responseHost" : "site2.mastercard.com",
       "minutesValid" : "15",
       "encryptedPayload" : {
  "encryptedData" :
"4545433044323232363739304532433610DE1D1461475BEB6D815F31764DDC20298BD779FBE37EE5AB3C
BDA9F9825E1DDE321469537FE461E824AA55BA67BF6A",
  "publicKeyFingerprint" :  "4c4ead5927f0df8117f178eea9308daa58e27c2b",
  "encryptedKey" : "A1B2C3D4E5F6112233445566",
  "oaepHashingAlgorithm" : "SHA512"
      }
}
```


3.2.16.6.5 Sample contents of encryptedData in the response encryptedPayload


```
{
       "accountNumber" : "5123456789012345",
"expiryMonth" : "12" ,
       "expiryYear" : "18"
}
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.2.17 Get Digital Assets

3.2.17.1 Overview

NOTE: This API is not applicable to device based digital wallets. Only applicable to server based implementations with explicit approval.

Get Digital Asset API is used to obtain to retrieve digital assets for a funding pan for use cases in which the token requestor does not wish to tokenize the funding pan. The issuer will need to approve each token requestor that wishes to access the issuer's digital assets

An error will be returned if the token requestor is not approved by the issuer to use getDigitalAssets.

3.2.17.2 URL Endpoint

/getDigitalAssets

3.2.17.3 HTTP Method

POST

3.2.17.4 Request Parameters

encryptedPayload

Description:	Contains an encrypted CardInfoData object.
Data Type:	EncryptedPayload object containing a CardInfoData object.
Max Length:	N/A
Required:	Yes

3.2.17.5 Response Values

brandLogoAssetId

Description:	The MasterCard or Maestro brand logo associated with this card. Provided as an Asset ID – use the Get Asset API (See Section 3.2.5) to retrieve the actual asset.
Data Type:	String
Max Length:	64
Required:	Yes

issuerLogoAssetId

Description:	The logo of the issuing bank. Provided as an Asset ID – use the Get Asset API (See Section 3.2.5) to retrieve the actual asset.
Data Type:	String
Max Length:	64
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

coBrandLogoAssetId

Description:	The co-brand logo (if any) for this product. Provided as an Asset ID – use the Get Asset API (See Section 3.2.5) to retrieve the actual asset.
Data Type:	String
Max Length:	64
Required:	No

cardBackgroundCombinedAssetId

Description:	The card image used to represent the digital card in the wallet. This 'combined' option contains the MasterCard, bank and any co-brand logos. Provided as an Asset ID – use the Get Asset API (See Section 3.2.5) to retrieve the actual asset.
Data Type:	String
Max Length:	64
Required:	Conditional – either CardBackgroundCombined or CardBackground will be provided.

cardBackgroundAssetId

Description:	The card image used to represent the digital card in the wallet. This 'non-combined' option does not contain the MasterCard, bank, or co-brand logos. Provided as an Asset ID – use the Get Asset API (See Section 3.2.5) to retrieve the actual asset.
Data Type:	String
Max Length:	64
Required:	Conditional – either CardBackgroundCombined or CardBackground will be provided.

iconAssetId

Description:	The icon representing the primary brand(s) associated with this product. Provided as an Asset ID – use the Get Asset API (See Section 3.2.5) to retrieve the actual asset.
Data Type:	String
Max Length:	64
Required:	Yes

foregroundColor

Description:	Foreground color, used to overlay text on top of the card image.
Data Type:	String - Hexadecimal RGB color format (case-insensitive).
Max Length:	6
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

issuerName	
Description:	Name of the issuing bank.
Data Type:	String
Max Length:	64
Required:	Yes
shortDescription	
Description:	A short description for this product.
Data Type:	String
Max Length:	128
Required:	Yes
longDescription	
Description:	A long description for this product.
Data Type:	String
Max Length:	256
Required:	No

3.2.17.6 Examples

3.2.17.6.1 Sample Request

```
{
  "responseHost" : "site1.mastercard.com ",
  "requestId" : "123456",
  "encryptedPayload" : {
"encryptedData" :
"4545433044323232363739304532433610DE1D1461475BEB6D815F31764DDC20298BD779FBE37EE5AB3C
BDA9F9825E1DDE321469537FE461E824AA55BA67BF6A",
"publicKeyFingerprint" :  "4c4ead5927f0df8117f178eea9308daa58e27c2b",
"encryptedKey" : "A1B2C3D4E5F6112233445566",
"oaepHashingAlgorithm" : "SHA512"
  }
}
```

3.2.17.6.2 Sample contents of encryptedData in the request encryptedPayload

```
{
      "accountNumber" : "5123456789012345"
}
```

3.2.17.6.3 Sample Successful Response

```
{
"responseId" : "123456",
"responseHost" : "site2.mastercard.com",
"brandLogoAssetId" : "800200c9-629d-11e3-949a-0739d27e5a66",
"coBrandLogoAssetId" : "dbc55444-496a-4896-b41c-5d5e2dd431e2",
"cardBackgroundCombinedAssetId" : "739d27e5-629d-11e3-949a-0800200c9a66",
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
"foregroundColor" : "000000",
"issuerName" : "Issuing Bank",
"shortDescription" : "Bank Rewards MasterCard",
"longDescription" : "Bank Rewards MasterCard with the rewards program",
"issuerLogoAssetId" : "BED1503C-0D6D-40A7-AE8A-749DB4A05D86",
"iconAssetId" : "C307F0AE-298E-48EB-AA43-A7C40B32DDDE"
}
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.3 Outbound APIs (from MDES)

3.3.1 Notify Token Updated

3.3.1.1 Overview

This API is used by MDES to notify the Token Requestor 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 Issuer update (for example, the Issuer suspends or deletes the Token), or in response to a previous Token Requestor request (for example, when the Token Requestor activates the Token using an Authentication Code). When static tokens are used No notifyTokenUpdated is sent as part of the provisioning.

For CLOUD tokens, if the DSRP capability of the Token has been updated, any existing Transaction Credentials on the Mobile Payment App must be deleted.

3.3.1.2 URL Endpoint

/notifyTokenUpdated

3.3.1.3 HTTP Method

POST

3.3.1.4 Request Parameters

encryptedPayload	
Description:	Contains an encrypted NotifyTokenUpdatedRequest object.
Data Type:	EncryptedPayload object containing a NotifyTokenUpdatedRequest object
Max Length:	N/A
Required:	Yes
~~tokens~~	
Description:	Contains the Tokens which were updated.
Data Type:	Array[Token object]
Max Length:	N/A
Required:	**Deprecated** – use encryptedPayload instead.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

~~paymentAppInstanceId~~	
Description:	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization. This field is alphanumeric and additionally web-safe base64 characters per RFC 4648 (minus "-", underscore "_") up to a maximum length of 48, = should not be URL encoded.
Data Type:	String
Max Length:	48
Required:	**Deprecated** – use encryptedPayload instead.

3.3.1.5 Response Values

Only common response elements.

3.3.1.6 Examples

3.3.1.6.1 Sample Request

```
{
  "responseHost" : "site1.Mastercard.com ",
  "requestId" : "123456",
  "encryptedPayload" : {
"encryptedData" :
"4545433044323232363739304532433610DE1D1461475BEB6D815F31764DDC20298BD779FBE37EE5AB3C
BDA9F9825E1DDE321469537FE461E824AA55BA67BF6A",
"publicKeyFingerprint" :  "4c4ead5927f0df8117f178eea9308daa58e27c2b",
"encryptedKey" : "A1B2C3D4E5F6112233445566",
"oaepHashingAlgorithm" : "SHA512"
  }
}
```

3.3.1.6.2 Sample contents of encryptedData in encryptedPayload

```
{
"paymentAppInstanceId" : "123456789",
    "tokens" : [
{
        "tokenUniqueReference" : "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
        "status" : "ACTIVE",
  "statusTimestamp" : "2017-07-20T04:56:23.345-07:00",
        "tdsRegistrationUrl" : "tds.Mastercard.com"
      },
      {
        "tokenUniqueReference" : "DWSPMC00000000032d72d4ffcb2f4136a0532d32d72d4fcb",
        "status" : "ACTIVE",
  "statusTimestamp" : "2017-07-20T04:56:23.345-07:00",
        "productConfig" : {
    "brandLogoAssetId" : "800200c9-629d-11e3-949a-0739d27e5a66",
          "isCoBranded" : "true",
          "coBrandName" : "Co brand partner",
          "coBrandLogoAssetId" : "dbc55444-496a-4896-b41c-5d5e2dd431e2",
    "cardBackgroundCombinedAssetId" : "739d27e5-629d-11e3-949a-0800200c9a66",
    "foregroundColor" : "000000",
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
    "issuerName" : "Issuing Bank",
    "shortDescription" : "Bank Rewards Mastercard",
    "longDescription" : "Bank Rewards Mastercard with the super duper rewards
program",
    "customerServiceUrl" : "https://bank.com/customerservice",
    "termsAndConditionsUrl" : "https://bank.com/termsAndConditions",
    "privacyPolicyUrl" : "https://bank.com/privacy",
    "issuerProductConfigCode" : "123456"
        },
        "tokenInfo" : {
          "tokenPanSuffix": "1234",
          "accountPanSuffix": "6789",
          "alternateAccountIdentifierSuffix": "4567",
          "tokenExpiry" : "1018",
          "dsrpCapable" : true,
          "tokenAssuranceLevel" : 0
        }
},
      {
        "tokenUniqueReference" : "DWSPMC000000000fcb2f4136b2f4136a0532d2f4136a0532",
        "status" : "SUSPENDED",
  "statusTimestamp" : "2017-07-20T04:56:23.345-07:00",
        "suspendedBy" : ["TOKEN_REQUESTOR"]
      }
    ]
}
```


3.3.1.6.3 Sample Response


```
{
"responseHost" : "site1.your-server.com",
      "responseId" : "123456"
}
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.3.2 Notify Transaction Details

3.3.2.1 Overview

This API is used by MDES to send a transaction details notification to the Mobile Payment App (via the Token Requestor).

It is used by the Transaction Details Service to deliver a second registration code to the Mobile Payment App during the registration process. For more information, see the TDS Register API (see Section 7.2.2).

Once the Mobile Payment App is registered for the service, this API is subsequently used to notify the Mobile Payment App that new transaction details are available. No actual transaction data is included in the notification payload – this is only a notification that there is new transaction data to be collected. The Mobile Payment App must use the Get Transactions API (see Section 7.2.3) to get transaction data directly from the service.

The Token Requestor must deliver this notification to the Mobile Payment App in real-time, or at the earliest opportunity.

Note that Notify Transaction Details does not follow the general retry strategy and will not be retried in the case of timeout or other failure.

3.3.2.2 URL Endpoint

/notifyTransactionDetails

3.3.2.3 HTTP Method

POST

3.3.2.4 Request Parameters

tokenUniqueReference	
Description:	The Token to which the new transaction details relate
Data Type:	String
Max Length:	64
Required:	Yes

registrationCode2	
Description:	Second part of the registration code required to register for transaction details. Used during the registration process; not applicable otherwise.
Data Type:	String
Max Length:	32
Required:	No

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

tdsUrl	
Description:	The URL used to get transaction details. If supplied, the Mobile Payment App should connect to this specific URL to get the most recent transactions relating to this notification. Must be provided as: host[:port][/contextRoot] Where port and contextRoot are optional. If contextRoot is not provided, the default (per the URL Scheme) is assumed and must be used.
Data Type:	String
Max Length:	128
Required:	No

paymentAppInstanceId	
Description:	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization. This field is alphanumeric and additionally web-safe base64 characters per RFC 4648 (minus "-", underscore "_") up to a maximum length of 48, = should not be URL encoded.
Data Type:	String
Max Length:	48
Required:	Conditional – not applicable for server-based tokens. Required otherwise.

3.3.2.5 Response Values

Only common response elements.

3.3.2.6 Examples

3.3.2.6.1 Sample Request

```
{
      "requestId" : "123456",
      "tokenUniqueReference" : "DWSPMC000000000fcb2f4136b2f4136a0532d2f4136a0532",
      "tdsUrl" : "site2.Mastercard.com",
      "paymentAppInstanceId" : "123456789"
}
```

3.3.2.6.2 Sample Response

```
{
      "responseId" : "123456"
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.3.3 Push Transaction Details

3.3.3.1 Overview

This API is used by MDES to send a list of transaction details to the Token Requestor.

In the server to server TDS model, it is used to send a list of transaction details to the Token Requestor. Actual transaction data will be included in the notification payload.

The Token Requestor must deliver the transaction details to Payment App in real-time, or at the earliest opportunity.

3.3.3.2 URL Endpoint

/pushTransactionDetails

3.3.3.3 HTTP Method

POST

3.3.3.4 Request Parameters

transactions	
Description:	New transaction details for Tokens.
Data Type:	Array[TransactionDetails object]
Max Length:	N/A
Required:	Yes

3.3.3.5 Response Values

Only common response elements.

3.3.3.6 Examples

3.3.3.6.1 Sample Request

```
{
      "requestId" : "123456",
"transactions" : [
      {
            "tokenUniqueReference" : "
DWSPMC000000000fcb2f4136b2f4136a0532d2f4136a0532",
            "recordId" : "123456",
"transactionIdentifier" :
"6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b",
"transactionType" : "PURCHASE",
"amount" : 123.45,
"currencyCode" : "USD",
"authorizationStatus" : "CLEARED",
"transactionTimestamp" : "2016-04-25T12:00:00.000-07:00",
"merchantName" : "Bob's Burgers",
"merchantType" : "5812",
"merchantPostalCode" : "61000"
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
        }
        ]
}
```

3.3.3.6.2 Sample Response

```
{
        "responseId" : "123456"
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.3.4 Get Device Info

3.3.4.1 Overview

This API is used by MDES to retrieve information relating to the device.

In particular, it may be used during customer service inquiries to retrieve a device name that is familiar to the user.

3.3.4.2 URL Endpoint

/getDeviceInfo

3.3.4.3 HTTP Method

POST

3.3.4.4 Request Parameters

tokenUniqueReference	
Description:	The Token provisioned to the device.
Data Type:	String
Max Length:	64
Required:	Yes

paymentAppInstanceId	
Description:	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization. This field is alphanumeric and additionally web-safe base64 characters per RFC 4648 (minus "-", underscore "_") up to a maximum length of 48, = should not be URL encoded.
Data Type:	String
Max Length:	48
Required:	Conditional – not applicable for server-based tokens. Required otherwise.

3.3.4.5 Response Values

deviceInfo	
Description:	Contains device information of the device provisioned with this Token. Must include at least the 'deviceName'.
Data Type:	Map
Max Length:	N/A
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

3.3.4.6 Examples

3.3.4.6.1 Sample Request

```
{
"responseHost" : "site1.Mastercard.com",
	"requestId" : "123456",
	"tokenUniqueReference" : "DWSPMC000000000fcb2f4136b2f4136a0532d2f4136a0532",
	"paymentAppInstanceId" : "123456789"
}
```

3.3.4.6.2 Sample Response

```
{
"responseHost" : "site1.your-server.com",
	"responseId" : "123456",
	"deviceInfo" : {
		"deviceName" : "My Phone",
		"serialNumber" : "123456789"
	}
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

4 Credentials Management API

4.1 General

The MDES Credentials Management API encompasses a set of inbound and outbound APIs between MDES and either of the following:

- The Credentials Management System (Dedicated) – CMS-D (for MCBP implementations). MDES Credentials Management API supports MCBP implementations from 1.0 to 2.0.
- The Secure Element Issuer Trusted Service Manager - SEI TSM (for device-based Secure Element implementations).

4.1.1 API Design Principles

The Credentials Management APIs are designed as 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 will specify the HTTP Method used to access it. All strings in request and response objects are to be UTF-8 encoded. Each API URI includes the major and minor version of API that it conforms to. This will allow multiple concurrent versions of the API to be deployed simultaneously.

The client must handle any standard HTTP response code that could result from a web service call including but not limited to 302, 401, 404, or 500.

All APIs return an HTTP response code of 200 if the call was successfully received and accepted for processing. Any errors that subsequently occur during processing are returned in the response payload (see Sections 4.1.4 and 4.1.5 and for more information on error code elements and error handling).

All asynchronous API calls must include a task identifier, allowing the caller to subsequently check the task status, if required. The task identifier should be persisted for at least 30 days (or until the Token is deleted, whichever is sooner) during which time the task status may be checked.

To ensure forward-compatibility, all API client implementations must be resilient to new elements being added to outbound requests and responses from MDES.

4.1.2 URL Scheme

All API URLs follow the format:

scheme://host[:port]/contextRoot/api/majorVer/minorVer/apiName

URL Element	Definition
scheme	https

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

host[:port]	Hostname (and port number if required) for the environment. services.Mastercard.com ~~ws.Mastercard.com~~ **(deprecated)**
contextRoot	mdes
api	credentials
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 ~~Not present for the Get System Health API~~ **(deprecated)**
minorVer	The minor version of the APIs. This version of the document corresponds to a minor version of: 0 ~~Not present for the Get System Health API~~ **(deprecated)**
apiName	The URL endpoint as defined in the respective section for the API operation.

4.1.3 Security Overview and Encryption

All communication between the client and the Credentials Management Dedicated will be secured using mutually authenticated TLS.

Counter with CBC-MAC (CCM) encryption is used for authentication and confidentiality of card data and transaction credentials within applicable requests.

4.1.4 API Request / Response Common Elements and Headers

All requests and responses from MDES contain an element 'responseHost'. This identifies the specific MDES host that originated a request or response. It should be used by the client in the URL for future calls in order to direct the call to a specific host. As MDES is deployed in a dual active environment, this ensures that when a client makes a series of API calls, they must direct all calls within the same conversation to the same host. This minimizes the risk of some calls being routed to a different site, where data from a previous call may not yet have been replicated. When a conversation is complete, the client should revert back to the default host (provided during onboarding) to ensure that it is not locked permanently to one host.

The client may also provide its 'responseHost' in requests and responses originating from the client, and MDES will honor the responseHost per the above. Note that all valid client hosts must be pre-configured in MDES. Should a 'responseHost' value be submitted that is not yet configured, MDES will respond with an error.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

In addition every inbound and outbound request contains an element ‘requestId’ which uniquely identifies the request. Every response contains an element ‘responseId’ which uniquely identifies the response. The responseId may optionally use the corresponding requestId. Note that the format and uniqueness of the requestId and responseId are not necessarily validated on the Credentials Management API.

In the case of an operation reporting an error, a response contains one or more errors with the elements ‘reasonCode’ and ‘description’ as defined in Section 4.1.5. Unless explicitly stated otherwise, other elements (including 'Required' fields) are not present if an error is reported.

4.1.4.1 Common Request Elements

responseHost	
Description:	The host that originated the request. Future calls in the same conversation must be routed to this host. Must be provided as: host[:port][/contextRoot] Where port and contextRoot are optional. If contextRoot is not provided, the default (per the URL Scheme) is assumed and must be used.
Data Type:	String
Max Length:	64
Required:	No

requestId	
Description:	Unique identifier for the request.
Data Type:	String
Max Length:	64
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

4.1.4.2 Common Response Elements

responseHost	
Description:	The host that originated the response. Future calls in the same conversation must be routed to this host. Must be provided as: host[:port][/contextRoot] Where port and contextRoot are optional. If contextRoot is not provided, the default (per the URL Scheme) is assumed and must be used.
Data Type:	String
Max Length:	64
Required:	Conditional – See Section 4.1.4. In Production, the responseHost supplied by MDES must be used by the client for future API calls within a conversation. When the conversation is complete, the client will revert back to the default host supplied during onboarding.

responseId	
Description:	Unique identifier for the response.
Data Type:	String
Max Length:	64
Required:	Yes

errors	
Description:	One or more errors for the reasons the operation failed.
Data Type:	Array[Error object]
Max Length:	N/A
Required:	Conditional – required if one or more errors occurred performing the operation.

4.1.5 Error Reason Codes

Reason Code	Reason Description	Detail
INVALID_JSON	Invalid JSON	The JSON could not be parsed.
INVALID_FIELD_FORMAT	Invalid Field Format - {fieldName}	The field is not in the correct format. For instance, it should be a number but is a string.
INVALID_FIELD_LENGTH	Invalid Field Length - {fieldName}	The value does not fall between the minimum and maximum length for the field.
INVALID_FIELD_VALUE	Invalid Field Value - {fieldName}	The value is not allowed for the field.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

Reason Code	Reason Description	Detail
INVALID_RESPONSE_HOST	Invalid Response Host	The requested response host is invalid.
INVALID_OPERATION	Invalid Operation	The requested operation is invalid. For example, if a token-level PIN management operation is invoked on a token using a wallet-level PIN.
MISSING_REQUIRED_FIELD	Missing Required Field - {fieldName}	A required field is missing.
CRYPTOGRAPHY_ERROR	Cryptography Error	There was an error decrypting the encrypted payload.
INTERNAL_SERVICE_FAILURE	Internal Service Failure	MDES had an internal exception.
DUPLICATE_REQUEST	Duplicate Request	The same request is currently being processed.
INVALID_TASK_ID	Invalid Task Id	The taskId could not be found or, for inbound calls, the taskId was not unique.
INVALID_TOKEN_UNIQUE_REFERENCE	Invalid Token Unique Reference	The token unique reference could not be found.
INVALID_TOKEN_STATUS	Invalid Token status.	The token is in an invalid status for the requested operation.
MAX_NUM_TRANSACTION_CREDENTIALS_REACHED	Max number of Transaction Credentials reached	Replenishment request was rejected because the maximum number of Transaction Credentials permitted by the Issuer for this Token has been reached.
RNS_UNAVAILABLE	RNS Unavailable	The Remote Notification Service was unavailable
DEVICE_UNREACHABLE	Device Unreachable	The device could not be contacted or did not respond to complete the provisioning.
DEVICE_SUSPICIOUS	Device Suspicious	Payment app instance was not registered because suspicious behavior was detected from the device.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

Reason Code	Reason Description	Detail
INVALID_PAYMENT_APP_PROVIDER_ID	Invalid Payment App Provider Id	The Payment App Provider Id (Wallet Identifier) could not be found.
INVALID_PAYMENT_APP_INSTANCE_ID	Invalid Payment App Instance Id	The Payment App Instance Id could not be found.
PAYMENT_APP_INSTANCE_NOT_REGISTERED	Payment App Instance Not Registered	Payment app instance has not yet been registered and the provisioning request did not include RNS data needed for registration
INVALID_RNS_INFO	Invalid RNS Info	The RNS info provided was not valid for use with the Remote Notification Service.

4.1.6 Retry Strategy

For outbound calls that fail with a timeout, connection failure, or an HTTP response code of 302, 500, or 503 MDES will automatically retry 3 times with up to a 5-second wait between each try. 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.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

4.2 Outbound APIs (from MDES)

4.2.1 Provision

4.2.1.1 Overview

This API is used by MDES to provision a new Token Credential to the Credentials Management (Dedicated), as part of processing a digitization request.

The Provision request includes the provisioning data such as the Card Profile. For Embedded SE, the data is provisioned into the target SE. For Mastercard Cloud-Based Payments, this is delivered to the Mobile Payment App.

MDES guarantees that a Provision is only requested once it has completed any card and device eligibility checks. Note that the Cardholder authentication may not yet be complete when MDES requests provisioning.

Once provisioning is complete, the Credentials Management System must notify MDES of the provisioning result using the Notify Provisioning Result API (see Section 4.3.1). MDES may also use the Get Task Status API (see Section 4.2.3) to query the status of the provisioning task.

4.2.1.2 URL Endpoint

/provision

4.2.1.3 HTTP Method

POST

4.2.1.4 Request Parameters

paymentAppProviderId	
Description:	Globally unique identifier for the Wallet Provider, as assigned by MDES. Commonly known as the Wallet Identifier.
Data Type:	String
Max Length:	64
Required:	Yes

paymentAppId	
Description:	Identifier for the Payment App, unique per app as assigned by Mastercard for this Payment App.
Data Type:	String
Max Length:	30
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

paymentAppInstanceId

Description: Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization.

Data Type: String

Max Length: 48

Required: Conditional – not applicable for server-based tokens. Required otherwise.

tokenUniqueReference

Description: Globally unique identifier for the Token, as assigned by MDES. Serves as a unique identifier for all subsequent queries or management functions relating to this Token.

Data Type: String

Max Length: 64

Required: Yes

tokenType

Description: The type of Token requested. Must be one of:

Value	Meaning
EMBEDDED_SE	Embedded Secure Element
CLOUD	Mastercard Cloud-Based Payments

Data Type: String

Max Length: 32

Required: Yes

taskId

Description: Unique identifier for this task as assigned by MDES. May be used in the Get Task Status API (see Section 4.2.3) to query the status of this task.

Data Type: String

Max Length: 64

Required: Yes

apduCommands

Description: Contains an array of APDUCommand objects to be sent to the Secure Element to provision the Token. Each APDU is secured by the Global Platform session key.

Data Type: Array[APDUCommand object]

Max Length: N/A

Required: Conditional – required if tokenType = EMBEDDED_SE.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

tokenCredential		
Description:	Contains the card profile representing the Token Credential to be provisioned to the Mobile Payment App.	
Data Type:	TokenCredential object	
Max Length:	N/A	
Required:	Conditional – required if TokenType = CLOUD.	
seId		
Description:	Identifier of the target SE to be provisioned.	
Data Type:	String	
Max Length:	128	
Required:	Conditional – required if tokenType = EMBEDDED_SE.	
~~**rnsInfo**~~		
Description:	Contains information about the Remote Notification Service to be used by the Credentials Management (Dedicated) to deliver credentials to the target application instance.	
Data Type:	RnsInfo object.	
Max Length:	N/A	
Required:	**Deprecated** – use rnsInfo in the Register request in the MPA Management API instead.	

4.2.1.5 Response Values

Only common response elements.

4.2.1.6 Examples

4.2.1.6.1 Sample CLOUD Request


```
{
"responseHost" : "site1.Mastercard.com",
       "requestId" : "123456",
       "paymentAppProviderId" : "123456789",
       "paymentAppInstanceId" : "123456789",
       "tokenUniqueReference" : "DWSPMC000000000fcb2f4136b2f4136a0532d2f4136a0532",
       "tokenType" : "CLOUD",
       "taskId" : "3dacc64b-9703-4201-af40-02e636e3ff3b",
       "tokenCredential" : {
              "encryptedData" :
"546869732073686F756C6420626520612043434D20656E637279707465642043726564656E7469616C2050726F66696C65
20747970652E",
              "ccmKeyId": "123456",
              "ccmNonce":
"b0e6c22b59ea0e5b934efe1c47a090bda7a40e03f552aa5cda3fa5df6755f0a4",
              "ccmMac" : "123456789012345678901234"
       }
}
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

4.2.1.6.2 Sample EMBEDDED_SE Request


```
{
	"responseHost" : "site1.Mastercard.com",
	"requestId" : "123456",
	"paymentAppProviderId" : "123456789",
	"paymentAppInstanceId" : "123456789",
	"tokenUniqueReference" : "DWSPMC000000000fcb2f4136b2f4136a0532d2f4136a0532",
	"tokenType" : "EMBEDDED_SE",
	"taskId" : "3dacc64b-9703-4201-af40-02e636e3ff3b",
	"apduCommands" : [
		{
			"messageId": "00000000000000000000000000000001",
			"apduCommand": "00A4040008A00000000410101100"
		},
		{
			"messageId": "00000000000000000000000000000002",
			"apduCommand": "8050220008112233445566778800"
		},
		{
			"messageId": "00000000000000000000000000000003",
			"apduCommand": "848203001001E48FEB145FD5F946A5E497F1200042"
		},
		{
			"messageId": "00000000000000000000000000000004",
			"apduCommand":
"84E20000987B3DA45991129260B28F9E8C434AB18151776A28B783CCE658653957759F70A982CEC5B77A
C39F0D762F0E9A56CFD8DA6462BEDB879A1A3A2BF606AF1EDCB0BB8367FF01710D5B0A2136F1A64604A96
05AD9341F63D634B673002B0126D0393370EB851B5FE8DE50311C2B421ADE1F3BD8FC434DDAB6E71604A2
F8789B930438A3E69D88EEEF970EEEFDF4B686D912C72225025AA990DEDF"
		}
	],
	"seId": "824bb0419714df99bc5095dd"
}
```


4.2.1.6.3 Sample Response


```
{
"responseId" : "123456",
"responseHost" : "site1.your-server.com"
}
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

4.2.2 Change Mobile PIN

4.2.2.1 Overview

This API is used to trigger a Mobile PIN change. Only applicable to Mastercard Cloud-Based Payments.

Currently, a Mobile PIN change may only be requested by MDES as part of a Mobile PIN reset, where the Cardholder forgets their Mobile PIN and contacts Issuer customer service to reset their PIN.

The Credentials Management (Dedicated) must notify MDES of the outcome of the Mobile PIN change using the Notify Mobile PIN Change Result API (see Section 4.3.3). In response to Notify Mobile PIN Change Result, MDES will replenish the Credentials Management (Dedicated) with new Session Keys using the Replenish API (see Section 4.3.2) so that the Credentials Management (Dedicated) can replace any Transaction Credentials on the Mobile Payment App with new Transaction Credentials generated using the new Mobile PIN.

For Mobile Payment Applications that support a Locally-verified Consumer Device CVM (CDCVM) instead of Mobile PIN, this API is also used to trigger a reset of the Locally-verified CDCVM on the device.

4.2.2.2 URL Endpoint

/changeMobilePin

4.2.2.3 HTTP Method

POST

4.2.2.4 Request Parameters

paymentAppProviderId	
Description:	Globally unique identifier for the Wallet Provider, as assigned by MDES. Commonly known as the Wallet Identifier.
Data Type:	String
Max Length:	64
Required:	Conditional – required if the Mobile PIN relates to the whole payment app instance. Not present otherwise.

paymentAppInstanceId	
Description:	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization.
Data Type:	String
Max Length:	48
Required:	Conditional – required if the Mobile PIN relates to the whole payment app instance. Not present otherwise.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

tokenUniqueReference

Description:	The Token Credential for which to trigger a Mobile PIN change. Must be a valid reference as assigned by MDES.
Data Type:	String
Max Length:	64
Required:	Conditional – required if the Mobile PIN relates to a specific Token. Not present otherwise.

type

Description: The type of Mobile PIN change being requested. Must be one of:

Value	Meaning
FORCE_RESET	Reset the Mobile PIN – request a new Mobile PIN value from the Cardholder.

Data Type:	String
Max Length:	64
Required:	Yes

4.2.2.5 Response Values

Only common response elements.

4.2.2.6 Examples

4.2.2.6.1 Sample Request

```
{
      "responseHost" : "site1.Mastercard.com",
      "requestId" : "123456",
      "tokenUniqueReference" : "123456",
      "type" : "FORCE_RESET"
}
```

4.2.2.6.2 Sample Response

```
{
"responseId" : "123456",
"responseHost" : "site1.your-server.com"
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

4.2.3 Get Task Status

4.2.3.1 Overview

This API is used to check the status of any asynchronous task that was previously requested.

4.2.3.2 URL Endpoint

/getTaskStatus

4.2.3.3 HTTP Method

POST

4.2.3.4 Request Parameters

taskId

Description:	Unique identifier for this task as assigned by MDES. Must be an identifier previously used when requesting a task.
Data Type:	String
Max Length:	64
Required:	Yes

4.2.3.5 Response Values

status

Description: The status of the specified task. Must be one of:

Value	Meaning
PENDING	The task has been received and is pending processing.
IN_PROGRESS	The task is currently in progress
COMPLETED	The task was completed successfully
FAILED	The task was processed but failed to complete successfully.
~~UNKNOWN_TASK~~	The taskId given was not recognized. **Deprecated –** use an error of INVALID_TASK_ID instead.

Data Type:	String
Max Length:	64
Required:	Yes

4.2.3.6 Examples

4.2.3.6.1 Sample Request

```
{
      "responseHost" : "site1.Mastercard.com",
      "requestId": "123456",
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
        "taskId": "123456"
}
```

4.2.3.6.2 Sample Response

```
{
        "responseHost" : "site1.your-server.com",
        "responseId": "123456",
        "status": "PENDING"
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

4.3 Inbound APIs (to MDES)

4.3.1 Notify Provisioning Result

4.3.1.1 Overview

This API is used by the SEI TSM / Credentials Management (Dedicated) to notify MDES of the outcome of a previous Provision request (see Section 4.2.1).

4.3.1.2 URL Endpoint

/notifyProvisioningResult

4.3.1.3 HTTP Method

POST

4.3.1.4 Request Parameters

tokenUniqueReference

Description:	The Token Credential being provisioned. Must be a valid reference as assigned by MDES, on which MDES requested provisioning.
Data Type:	String
Max Length:	64
Required:	Yes

result

Description: Whether the provisioning was successful. Must be one of:

Value	Meaning
SUCCESS	Provisioning completed successfully and the target device/application is ready.
ERROR	An error occurred during provisioning

Data Type:	String
Max Length:	64
Required:	Yes

errorCode

Description:	Error code for the reason the provisioning failed.
Data Type:	String
Max Length:	32
Required:	Conditional – required if result = ERROR.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

errorDescription	
Description:	Error description of the reason the provisioning failed.
Data Type:	String
Max Length:	256
Required:	No

apduResponses	
Description:	Contains an array of APDUResponse objects with the responses from the Secure Element from executing the APDU commands.
Data Type:	Array[APDUResponse object]
Max Length:	N/A
Required:	Conditional – required if tokenType = EMBEDDED_SE.

4.3.1.5 Response Values

Only common response elements.

4.3.1.6 Examples

4.3.1.6.1 Sample CLOUD Request

```
{
      "requestId": "123456",
"responseHost": "site2.your-server.com",
      "tokenUniqueReference": "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
      "result": "SUCCESS"
}
```

4.3.1.6.2 Sample EMBEDDED_SE Request

```
{
      "requestId": "123456",
"responseHost": "site2.your-server.com",
      "tokenUniqueReference": "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
      "apduResponses": [
            {
                  "messageId": "00000000000000000000000000000001",
                  "apduResponse": "9000"
            },
            {
                  "messageId": "00000000000000000000000000000002",
                  "apduResponse": "9000"
            },
            {
                  "messageId": "00000000000000000000000000000003",
                  "apduResponse": "9000"
            },
            {
                  "messageId": "00000000000000000000000000000004",
                  "apduResponse": "9000"
            }
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
],
      "result": "SUCCESS"
}
```

4.3.1.6.3 Sample Response

```
{
      "responseId" : "123456",
      "responseHost" : "site2.Mastercard.com"
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

4.3.2 Replenish

4.3.2.1 Overview

This API is used by the Credentials Management (Dedicated) to request replenishment of Session Keys from MDES. Only applicable to Mastercard Cloud-Based Payments.

To request replenishment, the Credentials Management (Dedicated) must supply accurate status information (from the Mobile Payment App) for every Transaction Credential in the Mobile Payment App after the last successful replenishment. This is defined as:

- All active/unused Transaction Credentials remaining on the Mobile Payment App.
- All Transaction Credentials used or discarded since the last replenishment.

Once a Transaction Credential has been successfully reported as used or discarded, it does not need to be reported on again. Note that Transaction Credentials that are never reported on are assumed to be lost and count as discarded. If replenishment is unsuccessful, Transaction Credential status information should be retained and submitted again until replenishment succeeds.

Replenishment may be rejected by MDES if the Token is not currently in a state that permits replenishment (for example, if it is currently suspended).

Successful replenishment will top up the number of Transaction Credentials up to the maximum permitted by the Issuer for this Token.

4.3.2.2 URL Endpoint

/replenish

4.3.2.3 HTTP Method

POST

4.3.2.4 Request Parameters

tokenUniqueReference	
Description:	The Token Credential to be replenished. Must be a valid reference as assigned by MDES.
Data Type:	String
Max Length:	64
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

transactionCredentialsStatus	
Description:	The status of all active/unused Transaction Credentials on the Mobile Payment App and all Transaction Credentials used since the last replenishment.
Data Type:	Array[TransactionCredentialStatus object]
Max Length:	N/A
Required:	Conditional – required unless this is the first replenishment

4.3.2.5 Response Values

maxNumTransactionCredentials	
Description:	The maximum number of Transaction Credentials permitted.
Data Type:	Number
Max Length:	2
Required:	Conditional – required if replenishment failed with an reasonCode = MAX_NUM_TRANSACTION_CREDENTIALS_REACHED

rawTransactionCredentials	
Description:	Contains the raw transaction credentials to be transformed by the Credentials Management (Dedicated) prior to being replenished to the Mobile Payment App.
Data Type:	RawTransactionCredentials object
Max Length:	N/A
Required:	Conditional – required if replenishment succeeded

4.3.2.6 Examples

4.3.2.6.1 Sample Request

```
{
	"responseHost" : "site1.your-server.com",
	"requestId": "123456",
	"tokenUniqueReference": "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
	"transactionCredentialsStatus":[
		{
			"atc" : 100,
			"status" : "UNUSED_DISCARDED",
			"timestamp" : "2015-03-10T12:10:14.123-06:00"
		},
		{
			"atc" : 101,
			"status" : "USED_FOR_CONTACTLESS",
			"timestamp" : "2015-03-10T12:10:39.482-06:00"
		},
		{
			"atc" : 102,
			"status" : "UNUSED_ACTIVE",
			"timestamp" : "2015-03-18T09:16:11.698-06:00"
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
            }
      ]
}
```

4.3.2.6.2 Sample Response

```
{
      "responseHost" : "site1.Mastercard.com",
      "responseId" : "123456",
      "rawTransactionCredentials" : {
            "encryptedData" :
"546869732073686F756C64206265206120434D20656E63727970746564206172726179206F66206372
6564656E7469616C2074797065732E",
            "ccmNonce" :
"b0e6c22b59ea0e5b934efe1c47a090bda7a40e03f552aa5cda3fa5df6755f0a4",
            "ccmKeyId" : "123456",
"ccmMac" : "12345678901234567890123 4"
      }
}
```

4.3.2.6.3 Sample Error Response

```
{
      "responseHost" : "site1.Mastercard.com",
      "responseId" : "123456",
      "errors" : [
{
      "source" : "MDES",
      "errorCode" : "MAX_NUM_TRANSACTION_CREDENTIALS_REACHED",
      "errorDescription" : "Maximum number of Transaction Credentials reached",
                  "reasonCode" : "MAX_NUM_TRANSACTION_CREDENTIALS_REACHED",
                  "description" : "Maximum number of Transaction Credentials
reached"
            }
      ]
      "maxNumTransactionCredentials" : 1
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

4.3.3 Notify Mobile PIN Change Result

4.3.3.1 Overview

This API is used by the Credentials Management (Dedicated) to notify MDES about the result of an attempt to change the Mobile PIN. Only applicable to Mastercard Cloud-Based Payments.

For a successful Mobile PIN Change, the Credentials Management (Dedicated) should request new Session Keys from MDES using the Replenish API (see Section 4.3.2), replacing any Transaction Credentials on the Mobile Payment App with new Transaction Credentials generated using the new Mobile PIN.

In the case of a token-level Mobile PIN, MDES will reset the Mobile PIN try counter and unsuspend the Token as necessary. Note that in cases where the Token was suspended as a result of the Mobile PIN being locked, a Token will only be unsuspended by this operation if it is done in response to a previous Change Mobile PIN request that triggered the Mobile PIN reset for this Token. The notification must occur within 10 minutes after the Change Mobile PIN request.

In the case of a wallet-level Mobile PIN, MDES will reset the Mobile PIN try counters and unsuspend the Tokens as necessary, regardless whether this operation is done in response to a previous Change Mobile PIN request.

The Credentials Management (Dedicated) must also use this API to notify MDES of when the Mobile PIN try limit has been exceeded, so that MDES can block the Mobile PIN at the Transaction Management System.

For Mobile Payment Applications that support a Locally-verified Consumer Device CVM (CDCVM) instead of Mobile PIN, this API is also used to notify a successful reset of the Locally-verified CDCVM on the device. MDES will reset the Mobile PIN try counters and unsuspend the Tokens as necessary.

4.3.3.2 URL Endpoint

/notifyMobilePinChangeResult

4.3.3.3 HTTP Method

POST

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

4.3.3.4 Request Parameters

paymentAppProviderId

Description: Globally unique identifier for the Wallet Provider, as assigned by MDES. Commonly known as the Wallet Identifier.

Data Type: String

Max Length: 64

Required: Conditional – required if the Mobile PIN relates to the whole payment app instance. Not present otherwise.

paymentAppInstanceId

Description: Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization.

Data Type: String

Max Length: 48

Required: Conditional – required if the Mobile PIN relates to the whole payment app instance. Not present otherwise.

tokenUniqueReference

Description: The Token Credential for which a Mobile PIN change was triggered. Must be a valid reference as assigned by MDES.

Data Type: String

Max Length: 64

Required: Conditional – required if the Mobile PIN relates to a specific Token. Not present otherwise.

result

Description: Whether the Mobile PIN change was successful. Must be one of:

Value	Meaning
SUCCESS	Mobile PIN change completed successfully.
MOBILE_PIN_TRIES_EXCEEDED	Mobile PIN change failed due to the user being unable to enter the correct existing PIN value, exceeding their maximum number of allowed Mobile PIN tries.

Data Type: String

Max Length:

Required: Yes

4.3.3.5 Response Values

Only common response elements.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

4.3.3.6 Examples

4.3.3.6.1 Sample Request

```
{
	"responseHost" : "site1.your-server.com",
	"requestId": "123456",
	"tokenUniqueReference": "DWSPMC000000000fcb2f4136b2f4136a0532d2f4136a0532",
	"result": "SUCCESS"
}
```

4.3.3.6.2 Sample Response

```
{
	"responseId" : "123456",
	"responseHost" : "site1.Mastercard.com"
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

4.3.4 Get System Health

4.3.4.1 Overview

This API is used to check the general status of a Credentials Management API host.

A successful response contains an HTTP response code of 200 with an empty body, and indicates that the service is running and accepting requests.

4.3.4.2 URL Endpoint

/health

4.3.4.3 HTTP Method

GET

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

5 Mobile Payment API

5.1 General

The MDES Mobile Payment API encompasses a set of inbound and outbound APIs between the MCBP Mobile Payment Application and Mastercard Credentials Management System (Dedicated) – CMS-D.

MDES Mobile Payment API supports MCBP implementations from 1.0 to 2.0.

5.1.1 API Design Principles

The Mobile Payment APIs are designed as RPC style stateless web services where each API endpoint represents an operation to be performed. All request and response payloads are sent in 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 to be UTF-8 encoded. Each API URI includes the major and minor version of API that it conforms to. This will allow multiple concurrent versions of the API to be deployed simultaneously.

The client must handle any standard HTTP response code that could result from a web service call including but not limited to 302, 401, 404 or 500.

All APIs return an HTTP response code of 200 if the call was successfully received and accepted for processing. Any errors that subsequently occur during processing are returned in the response payload (see Sections 5.1.5 and 5.1.6 on error code elements and error handling).

To ensure forward-compatibility, all API client implementations must be resilient to new elements being added to outbound requests and responses from MDES.

5.1.2 URL Scheme

All API URLs follow the format:

scheme://host[:port]/contextRoot/api/majorVer/minorVer/apiName

URL Element	Definition
scheme	https
host[:port]	Hostname (and port number if required) for the environment. services.Mastercard.com ~~ws.Mastercard.com~~ **(deprecated)**
contextRoot	mdes
api	paymentapp

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

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.

5.1.3 Security Overview and Encryption

5.1.3.1 Overview

All communications between the client and the Mobile Payment APIs are secured using an HTTPS connection. During digitization of the first card, MDES sends a one-time registration code to the Mobile Payment App using a remote notification. The Mobile Payment App must supply this to MDES to register for the service. Upon successful registration, MDES generates and returns a set of Mobile Keys to the Mobile Payment App.

To securely transport the Mobile Keys, MDES includes a public key (alongside the one-time registration code) in the initial remote notification payload. To perform registration, the Mobile Payment App generates a random key, encrypts it using MDES's public key, and supplies it in the registration request. MDES returns the Mobile Keys encrypted using this random key in the registration response.

The Mobile Payment App also provides its Device Fingerprint to MDES in this initial registration request. This is stored by MDES and used later.

Once the Mobile Keys have been established, all subsequent communications are secured using the Mobile Keys. The Mobile Payment App starts by requesting a new remote management session. MDES acknowledges the request. It separately sends a unique Session Code to the Mobile Payment App via a remote notification. The Session Code and any other payload data in the remote notification are encrypted using the Mobile Keys. The Mobile Payment App decrypts the payload and uses the Session Code in two ways:

1. To compute an Authentication Code – this is a hash of the Mobile Keyset Identifier, the Session Code, and the Device Fingerprint.
2. To derive the Mobile Session Keys from the Mobile Keys using the Session Code as a diversifier. The Mobile Session Keys are then used to encrypt any request payload sent to MDES. They are also used to decrypt any response payload sent by MDES.

The Authentication Code and any encrypted payload data are sent by the Mobile Payment App in the request. MDES can verify the Authentication Code to check that the request is received from the genuine registered Mobile Payment App with a valid and active remote

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

management session. The Mobile Session Keys provides additional protection over and above HTTPS to ensure message privacy and integrity, as well as to prevent replay of messages in both directions.

Any sensitive data (such as the Mobile PIN value) are further encrypted at a field level before they are formatted into a message and encrypted using the Mobile Session Keys.

5.1.3.2 Mobile PIN Encipherment Algorithm

The Mobile Payment App supplies a Mobile PIN value to MDES in order to set the Mobile PIN for the first time, or to subsequently change the value of the Mobile PIN upon user request.

Whenever the Mobile PIN value is transported, it must be enciphered as a Format 4 PIN block according to ISO 9564-1 as amended in 2015, using a substitute value for the PAN. The Token PAN value is not itself used in the PIN block.

The substitute value for the PAN is calculated as follows:

1. Take the entire 'paymentAppInstanceId' as input (without any additional padding or truncation), in UTF-8 encoding, outputting a max length 48-byte value (as the 'paymentAppInstanceId' is a max length 48-char string).
2. Hash this value using SHA-1 to output a 20-byte value.
3. Convert the 20-byte value into a base-10 numeric value.
4. Take the least significant 16 digits including any zeroes and use this instead of the PAN in the Format 4 PIN Block. If there are less than 16 digits available, the value should be front-padded with zeroes to make up 16 digits.
    a. Construct a 16-byte container for the PIN using the Mobile PIN value prefaced with 1-byte hex value “4”n (where n is the number of PIN digits) and appended with padding nibbles set to hex “A” and a fresh random 8-byte value
    b. Construct a 16-byte container for the PAN using the generated PAN value prefaced with the nibble “4”
    c. Encrypt (in ECB mode) the container (PIN) and XOR the result with the container (PAN)
    d. Encrypt (in ECB mode) the value resulting from step c to generate the 16-byte Format 4 PIN block

For example:

1. Given a 'paymentAppInstanceId' value: "myPaymentAppInstanceId123"
2. Hashed using SHA-1 to output (shown in hex):
   8df0c57980d7fa44e3a7286cfd9a4589c5eb1eb0
3. Converted to base-10 numeric value:
   810337079999566280018410685437385308775358602928

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

4. Truncated to the least significant 16 digits: 5308775358602928
5. Given a Mobile PIN value: "1234" and a random value "d382ae19c3ae790b", construct the container for the PIN (shown in hex): 441234aaaaaaaaaad382ae19c3ae790b
6. Note for a Mobile PIN value: "24680", the container for the PIN (shown in hex): 4524680aaaaaaaaad382ae19c3ae790b
7. Given the generated PAN value "5308775358602928", construct the container for the PAN (shown in hex): 45308775358602928000000000000000

5.1.4 API Request / Response Common Elements and Headers

All requests and responses, except the ~~Register~~ and Request Session APIs, contain the same three common request elements: the Mobile Keyset Identifier, the Authentication Code and an Encrypted Data request payload; and the same common response element: an Encrypted Data response payload. The encrypted request and response payloads are encrypted using the Mobile Session Keys as discussed above (see Section 5.1.3). This ensures that only the minimal information is provided in plaintext; any meaningful payload data is always protected in both directions.

Within the encrypted payloads, every request contains an element 'requestId' which uniquely identifies the request. Every response contains an element 'responseId' which uniquely identifies the response. The responseId may optionally use the corresponding requestId.

In the case of an operation reporting an error, the elements 'errorCode' and 'errorDescription' is included in the encrypted response. For any errors that occur before the authentication / encryption protocol is established, the elements 'errorCode' and 'errorDescription' is included in the plaintext response. See Section 5.1.5 for more information. Unless explicitly stated otherwise, other elements (including 'Required' fields) are not present if an error is reported.

5.1.4.1 Common Request Elements

mobileKeysetId	
Description:	Identifies the Mobile Keys used for this remote management session.
Data Type:	String
Max Length:	64
Required:	Conditional – required except in a ~~Register~~ or Request Session API request.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

authenticationCode

Description:	The authentication code, computed as a SHA-256 hash over the mobileKeysetId (encoded as UTF-8, up to 64 bytes), the remote management session code (binary, up to 29 bytes) and the device fingerprint (binary, up to 32 bytes) as supplied during registration.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	64 (Exact)
Required:	Conditional – required except in a ~~Register~~ or Request Session API request.

encryptedData

Description:	An encrypted object containing the request parameters for the API being called. Encryption and MAC using the Mobile Session Keys according to the Algorithm Used When Receiving Data From The Mobile Payment Application as described in Mastercard Cloud-Based Payments – Issuer Cryptogram Algorithms.
Data Type:	String. Base64-encoded data.
Max Length:	256 K
Required:	Conditional – required except in a ~~Register~~ or Request Session API request.

5.1.4.2 Common Response Elements

encryptedData

Description:	An encrypted object containing the response values for the API being called. Encryption and MAC using the Mobile Session Keys according to the Algorithm For Protecting Data Sent to Mobile Payment Application as described in Mastercard Cloud-Based Payments – Issuer Cryptogram Algorithms.
Data Type:	String. Base64-encoded data.
Max Length:	256 K
Required:	Conditional – optional except in a ~~Register~~ or Request Session API response where it is never present.

errorCode

Description:	Error code for the reason the operation failed.
Data Type:	String
Max Length:	32
Required:	Conditional – required if an error occurred performing the operation when encryptedData is not present.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

errorDescription

Description:	Error description of the reason the operation failed.
Data Type:	String
Max Length:	256
Required:	No

5.1.4.3 Common Encrypted Request Elements

requestId

Description:	Unique identifier for the request.
Data Type:	String
Max Length:	64
Required:	Yes

5.1.4.4 Common Encrypted Response Elements

responseHost

Description:	The host that the Mobile Payment App should route any subsequent requests to. This allows MDES to control requests related to a specific conversation to the desired location. If omitted, then the default host (provided during registration) should be assumed. Must be provided as: host[:port][/contextRoot] Where port and contextRoot are optional. If contextRoot is not provided, the default (per the URL Scheme) is assumed and must be used.
Data Type:	String
Max Length:	64
Required:	No

responseId

Description:	Unique identifier for the response.
Data Type:	String
Max Length:	64
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

errorCode	
Description:	Error code for the reason the operation failed.
Data Type:	String
Max Length:	32
Required:	Conditional – required if an error occurred performing the operation.
errorDescription	
Description:	Error description of the reason the operation failed.
Data Type:	String
Max Length:	256
Required:	No

5.1.5 Error Codes

Only a limited subset of error codes may be used in plaintext responses. In general, any error requiring knowledge of any data or other internal state held by MDES is returned only in an encrypted response.

Error Code	Error Description	Detail	Encrypted Response Only
INVALID_JSON	Invalid JSON	The JSON could not be parsed.	No
UNRECOGNIZED_FIELD	Unrecognized Field - {fieldName}	The field name is not valid for the object.	No
INVALID_FIELD_FORMAT	Invalid Field Format - {fieldName}	The field is not in the correct format. For instance, it should be a number but is a string.	No
INVALID_FIELD_LENGTH	Invalid Field Length - {fieldName}	The value does not fall between the minimum and maximum length for the field.	No
INVALID_FIELD_VALUE	Invalid Field Value - {fieldName}	The value is not allowed for the field.	No
MISSING_REQUIRED_FIELD	Missing Required Field - {fieldName}	A required field is missing.	No
INTERNAL_SERVICE_FAILURE	Internal Service Failure	MDES had an internal exception.	No

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

Error Code	Error Description	Detail	Encrypted Response Only
INVALID_TOKEN_UNIQUE_REFERENCE	Invalid Token Unique Reference	The token unique reference could not be found or does not match the identifiers provided.	Yes
INVALID_TOKEN_STATUS	Invalid Token Status	The token is in an invalid status for the requested operation.	Yes
INVALID_OPERATION	Invalid Operation	The requested operation is invalid. For example, if a token-level PIN management operation is invoked on a token using a wallet-level PIN.	Yes
CRYPTOGRAPHY_ERROR	Cryptography Error	There was an error decrypting the encrypted field.	Yes
INVALID_TASK_ID	Invalid Task Id	The taskId could not be found or, for inbound calls, the taskId was not unique.	Yes

5.1.6 Retry Strategy

For calls that fail with a timeout, connection failure, or an HTTP response code of 302, 500 or 503, the Mobile Payment App may retry the request as needed to fulfil the request. In the case of a 503, the Retry-After header must be respected if present.

Except for Register and Request Session, when attempting a retry, the Mobile Payment App must use the same 'requestId' from the original request. This will be used by MDES to detect duplicate requests. However, the payload must be freshly encrypted using the Mobile Session Keys, incrementing the counter, otherwise MDES may consider it a replay attack and reject the request.

When attempting a retry of a Register request, the same exact payload (including the encrypted RGK) from the original request must be resent. Retries shall only be honored until the Mobile Keys are first used. Attempts to reuse a registration code with different payload data will be treated as suspicious and may result in provisioning failure.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

5.2 Outbound APIs (from MDES)

5.2.1 Send Remote Notification

5.2.1.1 Overview

Remote notifications are used by MDES to send messages to the Mobile Payment App. This is used in response to the Request Session API (see Section 5.3.2). It may also be initiated by MDES to notify the Mobile Payment App that it should register itself (using the ~~Register~~ API 5.3.1) or that provisioning data is ready and the Mobile Payment App should call the Provision API (see Section 5.3.3) to be provisioned with a new Token Credential.

MDES uses third-party Remote Notification Services (such as Google Cloud Messaging) to send notifications to a Mobile Payment App. For the exact format of all the parameters in a Remote Notification Service message, refer to the third-party documentation for the specific Remote Notification Service being used.

For Google Cloud Messaging, all notification message data is wrapped in a JSON parent object with the key "payload" before it is supplied as a parameter in the "data" field of a downstream GCM message.

5.2.1.2 Notification Message Data

responseHost	
Description:	The host that the Mobile Payment App should route requests to. This allows MDES to control requests related to a specific conversation to the desired location. If omitted, then the default host (provided during registration) should be assumed. Must be provided as: host[:port][/contextRoot] Where port and contextRoot are optional. If contextRoot is not provided, the default (per the URL Scheme) is assumed and must be used.
Data Type:	String
Max Length:	64
Required:	Conditional – required for initial registration, optional otherwise.

~~registrationData~~	
Description:	Contains the data necessary for the Mobile Payment App to complete registration with MDES.
Data Type:	PaymentAppRegistrationData object.
Max Length:	N/A
Required:	**Deprecated** – perform registration using the MPA Management API instead.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

mobileKeysetId	
Description:	Identifies the Mobile Keys used for this remote management session.
Data Type:	String
Max Length:	64
Required:	Yes

encryptedData	
Description:	Contains the encrypted RemoteManagementSessionData object. The plaintext data is prepended with a random 16-byte value before it is encrypted by the Mobile Transport Key using CBC mode padded with '80' followed by '00' bytes until the end of the block. The MAC is then computed over the output, which is appended to the end.
Data Type:	String. Base64-encoded data.
Max Length:	256 K
Required:	Yes

5.2.1.3 Examples

5.2.1.3.1 Sample Notification Message Data to trigger Registration

```
{
	"responseHost" : "site1.Mastercard.com",
	"registrationData" : {
		"registrationCode" : "6cc063fb-766d-4849-930d-eb0fdf4e15a5",
		"publicKey" :
"4E4F54205245414C2044415441202D2074686973207769 6C6C20626520612075626C6963206B657920
70726F766964656420627920746865204372656 4656E7469616C73204D616E6167656D656E74202844656
469636174656429",
		 "pkCertificateUrl" :
"https://services.Mastercard.com/mdes/paymentapp/1/0/pkCertificate"
	},
	"mobileKeysetId" : "e279760f-f4cd-4683-ba42-4d8053817a69",
	"encryptedData" :
"Tk9UIFJFQUwgREFUQSAtIHRoaXMgd2lsbCBiZSB0aGUgYWN0dWFsIGRhdGEgZW5jcnlwdGVkIHVzaW5nIHRo
ZSBNb2JpbGUgS2V5cyA="
}
```

Where the "encryptedData" would decrypt to:

```
{
	"version" : "1.0",
	"sessionCode" : "92d60ba5-dd1f-4bb8-b08e-0648b3098d1e",
	"expiryTimeStamp" : "2015-03-06T03:23:26Z",
	"validForSeconds" : "3600",
	"pendingAction" : "PROVISION",
	"tokenUniqueReference" : "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45"
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

5.2.1.3.2 Sample Notification Message Data in response to a Request Session


```
{
	"responseHost" : "site1.Mastercard.com",
	"mobileKeysetId" : "e279760f-f4cd-4683-ba42-4d8053817a69",
	"encryptedData" :
"Tk9UIFJFQUwgREFUQSAtIHRoaXMgd2lsbCBiZSB0aGUgYWN0dWFsIGRhdGEgZW5jcnlwdGVkIHVzaW5nIHRo
ZSBNb2JpbGUgS2V5cyA="
}
```


Where the "encryptedData" would decrypt to:


```
{
	"version" : "1.0",
	"sessionCode" : "92d60ba5-dd1f-4bb8-b08e-0648b3098d1e",
	"expiryTimeStamp" : "2015-03-06T03:23:26Z",
	"validForSeconds" : "3600"
}
```


5.2.1.3.3 Sample Notification Message Data to force reset of a Token-specific Mobile PIN


```
{
	"responseHost" : "site1.Mastercard.com",
	"mobileKeysetId" : "e279760f-f4cd-4683-ba42-4d8053817a69",
	"encryptedData" :
"Tk9UIFJFQUwgREFUQSAtIHRoaXMgd2lsbCBiZSB0aGUgYWN0dWFsIGRhdGEgZW5jcnlwdGVkIHVzaW5nIHRo
ZSBNb2JpbGUgS2V5cyA="
}
```


Where the "encryptedData" would decrypt to:


```
{
	"version" : "1.0",
	"sessionCode" : "92d60ba5-dd1f-4bb8-b08e-0648b3098d1e",
	"expiryTimeStamp" : "2015-03-06T03:23:26Z",
	"validForSeconds" : "3600",
	"pendingAction" : "RESET_MOBILE_PIN",
	"tokenUniqueReference" : "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45"
}
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

5.3 Inbound APIs (to MDES)

5.3.1 ~~Register~~ (deprecated – use MPA Management API)

5.3.1.1 Overview

This API is used by the Mobile Payment App in response to a remote notification, in order to register itself with MDES for use. The registration code from the remote notification must be supplied by the Mobile Payment App to complete the registration process.

MDES supports two methods for registering a Mobile Payment App, either it is performed by a server on behalf of the Mobile Payment App (see Section 6.2.1 for more information on the Register API on the MPA Management API); or it is performed directly by the Mobile Payment App in response to a remote notification using this API.

5.3.1.2 URL Endpoint

/register

5.3.1.3 HTTP Method

POST

5.3.1.4 Request Parameters

paymentAppProviderId	
Description:	Globally unique identifier for the Wallet Provider, as assigned by MDES. Commonly known as the Wallet Identifier.
Data Type:	String
Max Length:	64
Required:	Yes

paymentAppInstanceId	
Description:	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization.
Data Type:	String
Max Length:	48
Required:	Yes

registrationCode	
Description:	The registration code as supplied by MDES in the remote notification.
Data Type:	String
Max Length:	64
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

rgk	
Description:	The randomly-generated 128-bit AES key, encrypted by the Mastercard public key (as provided in the remote notification) using OAEP with SHA-256 hashing algorithm.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	512
Required:	Yes
deviceFingerprint	
Description:	The unique device fingerprint, which is a SHA-256 hash computed over a list of data elements retrieved from the Mobile Payment App and the Mobile Device.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	64 (Exact)
Required:	Yes

5.3.1.5 Response Values

mobileKeysetId	
Description:	The identifier for the Mobile Keys used to manage the CLOUD credentials, as assigned by MDES upon successful registration.
Data Type:	String
Max Length:	64
Required:	Yes
mobileKeys	
Description:	Contains the mobile keys used to secure the communication during subsequent remote management sessions.
Data Type:	MobileKeys object.
Max Length:	N/A
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

remoteManagementUrl	
Description:	The URL endpoint for subsequent remote management sessions. The Mobile Payment App must store this URL for future use in order to be able to request new remote management sessions. Must be provided as: host[:port][/contextRoot] Where port and contextRoot are optional. If contextRoot is not provided, the default (per the URL Scheme) is assumed and must be used.
Data Type:	String
Max Length:	128
Required:	Yes

5.3.1.6 Examples

5.3.1.6.1 Sample Request

```
{
	"paymentAppProviderId" : "123456789",
	"paymentAppInstanceId" : "123456789",
	"registrationCode" : "6cc063fb-766d-4849-930d-eb0fdf4e15a5",
	"rgk" :
"4E4F54205245414C2044415441202D20746869732077696C6C2062652072616E646F6D206B6579206765
6E6572617465642062792074686520D504120616E6420656E63727970746564207573696E67207468652
04D617374657243617264207075626C6963206B6579",
	"deviceFingerprint" :
"1bbefaa95b26b9e82e3fdd37b20050fc782b2f229a8f8bcbbcb6aa6abe4c851e"
}
```

5.3.1.6.2 Sample Response

```
{
	"mobileKeysetId" : "e279760f-f4cd-4683-ba42-4d8053817a69",
	"mobileKeys" : {
		"transportKey" :
"4E4F54205245414C2044415441202D20746869732077696C6C206265207468",
		"macKey" :
"4E4F54205245414C2044415441202D20746869732077696C6C206265207468",
		"dataEncryptionKey" :
"4E4F54205245414C2044415441202D20746869732077696C6C206265207468"

	},
	"remoteManagementUrl" : "loadbalanced.Mastercard.com"
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

5.3.2 Request Session

5.3.2.1 Overview

This API is used by the Mobile Payment App to request that MDES initiate a new remote management session.

This can be used by the Mobile Payment App to initiate specific actions (such as changing the Mobile PIN) or to inform MDES that it is low on Transaction Credentials and needs to be replenished.

MDES responds by sending a remote notification to the registered Mobile Payment App using the Send Remote Notification API (see Section 5.2.1).

5.3.2.2 URL Endpoint

/requestSession

5.3.2.3 HTTP Method

POST

5.3.2.4 Request Parameters

paymentAppProviderId	
Description:	Globally unique identifier for the Wallet Provider, as assigned by MDES. Commonly known as the Wallet Identifier.
Data Type:	String
Max Length:	64
Required:	Yes

paymentAppInstanceId	
Description:	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization.
Data Type:	String
Max Length:	48
Required:	Yes

mobileKeysetId	
Description:	The identifier for the Mobile Keys used to manage the CLOUD credentials, as assigned by MDES upon successful registration.
Data Type:	String
Max Length:	64
Required:	Yes

5.3.2.5 Response Values

No response values.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

5.3.2.6 Examples

5.3.2.6.1 Sample Request

```
{
       "paymentAppProviderId" : "123456789",
       "paymentAppInstanceId" : "123456789",
       "mobileKeysetId" : "e279760f-f4cd-4683-ba42-4d8053817a69"
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

5.3.3 Provision

5.3.3.1 Overview

This API is used to provision a new Token Credential to the Mobile Payment App, or to update an existing Token Credential.

The response does not include any single-use Transaction Credentials. Transaction Credentials are supplied using the Replenish API (see Section 5.3.5).

Once provisioning is complete, the Mobile Payment App must notify MDES of the provisioning result using the Notify Provisioning Result (see Section 5.3.4).

5.3.3.2 URL Endpoint

/provision

5.3.3.3 HTTP Method

POST

5.3.3.4 Encrypted Request Parameters

tokenUniqueReference

Description:	Globally unique identifier for the Token, as assigned by MDES.
Data Type:	String
Max Length:	64
Required:	Yes

5.3.3.5 Encrypted Response Values

cardProfile

Description:	The card profile data payload.
Data Type:	See Mastercard Digital Enablement Service Mastercard Cloud-Based Payments – Card Profile Specification. Please use the document version that corresponds to the MCBP version supported by the mobile wallet app.
Max Length:	N/A
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

iccKek	
Description:	The 128-bit AES key used to encrypt the ICC private keys in the 'cardProfile'. Provided as a 32-byte field, encrypted by the Mobile Data Encryption Key using ECB mode padded with '80' followed by '00' bytes until the end of the block.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	64
Required:	Conditional. Not present when the profile does not contain contactless data

5.3.3.6 Examples

5.3.3.6.1 Sample Request

```
{
       "mobileKeysetId" : "e279760f-f4cd-4683-ba42-4d8053817a69",
       "authenticationCode" :
"94c46d98ecdeed2957e45c576bc2e0e97ce326e9715d2b99832608472950b7f3"
       "encryptedData" :
"Tk9UIFJFQUwgREFUQSAtIHRoaXMgd2lsbCBiZSB0aGUgYWN0dWFsIGRhdGEgZW5jcnlwdGVkIHVzaW5nIHRo
ZSBNb2JpbGUgS2V5cw=="
}
```

Where the "encryptedData" would decrypt to:

```
{
       "requestId" : "3000000001",
       "tokenUniqueReference" : "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45"
}
```

5.3.3.6.2 Sample Response

```
{
       "encryptedData" :
"Tk9UIFJFQUwgREFUQSAtIHRoaXMgd2lsbCBiZSB0aGUgYWN0dWFsIGRhdGEgZW5jcnlwdGVkIHVzaW5nIHRo
ZSBNb2JpbGUgS2V5cw=="
}
```

Where the "encryptedData" would decrypt to:

```
{
  "cardProfile": {
    "version": "2.0",
    "walletRelatedData": {
      "cardholderValidator": "MOBILE_PIN"
    },
    "mchipCardProfile": {
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
      "commonData": {
        "digitizedCardId": "5480982300100009FFFF01170504175615",
        "cardCountryCode": "0826",
        "pan": "5480982300100009",
        "accountType": "CREDIT",
        "productType": "CREDIT",
        "isTransactionIdRequired": true
      },
      "contactlessPaymentData": {
        "aid": "A0000000041010",
        "ppseFci":
"6F2A840E325041592E5359532E4444463031A518BF0C1561134F07A0000000410108701019F0A0400010102",
        "paymentFci":
"6F3C8407A0000000041010A531500A4D4153544552434152448701015F2D02656E9F38069F1D089F1A02BF0C119F6E070826000031340009F0A0400010102",
        "gpoResponse": "770E82021B8094080801010010010301",
        "cdol1RelatedDataLength": 57,
        "umdGeneration": "GENERATE_VALID_UMD_ON_CDCVM",
        "alternateContactlessPaymentData": null,
        "cvmModel": "CDCVM_ALWAYS",
        "issuerApplicationData": "03140001000000000000000000000000FF",
        "isUsAipMaskingSupported": true,
        "isTransitSupported": true,
        "pinIvCvc3Track2": "9440",
        "track1ConstructionData": {
          "nAtc": "04",
          "pUnAtc": "000000000F0E",
          "pCvc3": "0000000000F0",
          "trackData":
"42353438303938323330303130303030395E202F5E3232313232303131303030303030303030303030303030"
        },
        "track2ConstructionData": {
          "nAtc": "04",
          "pUnAtc": "0F0E",
          "pCvc3": "00F0",
          "trackData": "5480982300100009D22122011000000000000F"
        },
        "protectedIccPrivateKeyCrtComponents": {
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
          "p":
"D1845E788E06F9E4E4A8A1E719677F0191FF23595F46AA9864FB4D863E587E262B94A54DB276B3679D23
974B56F8739527EFCC7FD837AEFEA678789F3C1437B725E883ECBBC83F152218EAC057FB1476",
          "q":
"AD4CFA5F0A7616C3AE01F528DCEED9A87B8E77A433116F572FEDAC0A7A5E2C1ABFAA5939E0EDE5337170
0371F730AC912A88CBD15B0BE46457FBA2AF776ADF9425E883ECBBC83F152218EAC057FB1476",
          "u":
"46AB24E672310973A368E9BB1775D8C9238A576D22E34DACB3616BAF467BD5E9B5D0ACC090EAC9520AD9
0A865392F5AE717D24209458E4087E269E20F794081225E883ECBBC83F152218EAC057FB1476",
          "dp":
"7C5E6F0DB44A96241DEF4CD17599C9CB9E5C3A1A0EB661ED6EE6C710DEDF874D4BA3A641A3DFE6E191B0
35E14B035AC962DECBE66406ED17D50D6DAB748BF00B25E883ECBBC83F152218EAC057FB1476",
          "dq":
"DBF38FB23303966D7755952D0FC7826A23A969F82FEA78D5C34233279A004E1B79EA85A0C335DC4F5C27
D2AFAEE96DA097354D2281C210C289B1F91C8E34D77B25E883ECBBC83F152218EAC057FB1476"
        },
        "records": [
          {
            "recordNumber": 1,
            "sfi": "0C",
            "recordValue":
"70818C9F6C0200019F6206000000000F09F6306000000000F0E5629423534383039383233303031303
03030395E202F5E3232313232303131303030303030303030303030309F6401049F650200F09F66020F0E9F6
B13548098230010000 9D2212201100000000000F9F6701049F691F9F6A049F7E019F02065F2A029C019A
039F15029F35019F4E149F03069F3303"
          },
          {
            "recordNumber": 1,
            "sfi": "14",
            "recordValue":
"7081BF5713548098230010000 9D2212201100000000000F5A0854809823001000099F241D353030314
14A534347394B5A4B4F3451584C585A56375657455932334B5F24032212315F25034912315F280208265F3
401018C249F02069F030695055F2A029A039C019F37049F35019F34039F15029F7E019F33039F4E148D0C
910A8A0295059F37049F4C088E0A0000000000000001F039F0702FFC09F080200029F0D0500600000009
F0E0500000000009F0F0500600000009F420208269F4A0182"
          },
          {
            "recordNumber": 2,
            "sfi": "14",
            "recordValue":
"7081E08F01F19F32010392240590DE0D2933F6FC8E725FDBC51D19E4FA7B530B717082ACAD76B58ECDBD
C9C0F5E1263B9081B088D2455DB0992C45FAB57C10495F591D8B84C1BDBF9D36C8EEB835045D37071D6EF
2D76DB71248FAD3639B794E52DECBE60C8E46467817070C3EF94774A9FFFA12DD66E6CD32812FDCAE52B5
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
89C9BB4A64E5F73FE4C01FBFCC78DC64530B3391668085EDAB2E621ADA47C03830DDBBCF731C58BBA7B00
B74DEA85307A54E08020BA71AA76650059A89F1E5803E1B2CCC2DB0211A43AC0AA922CCD023AAD956450D
8BB9A5CC739A9537ADCB22E437E13F"
          },
          {
            "recordNumber": 3,
            "sfi": "14",
            "recordValue":
"7081BB9F4701039F48009F4681B03B055D468B503DC8B54FF1CF1B2171D952B5054032D6D2555EA1D0CC
4A18F5C498816FFF1832B90ED88C8C5E2F66220C49C0329440F7E1A79D5F6E99F2157E9CC5BC8A3434A6C
CE23232218BCCC2816094B090CFAB7D6FBE59767F11480837F969EEDE487FBB9784E9DDA5A59AB63432A3
47EAE855841C76C96246142C6ED5CA8B3E396EB3D534BE5585256AC3629151BF16BD61C73B10BEF0D468D
3CBE89FB74D92F8915CFBB2AB7358ED9B02533D63"
          }
        ]
      },
      "dsrpData": {
        "par": "35303031414A534347394B5A4B4F3451584C585A56375657455932334B",
        "umdGeneration": "GENERATE_VALID_UMD_ON_CDCVM",
        "issuerApplicationData": "0314000000000000000000000000000000FF",
        "track2EquivalentData": "5480982300100009D2212201100000000000F",
        "ucafVersion": "V0_PLUS",
        "panSequenceNumber": "01",
        "aip": "1A00",
        "cvmModel": "CDCVM_ALWAYS",
        "expirationDate": "221231"
      }
    }
  },
  "iccKek": "4E4F54205245414C2044415441",
}
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

5.3.4 Notify Provisioning Result

5.3.4.1 Overview

This API is used by the Mobile Payment App to notify MDES of the outcome of a previous Provision request (see Section 5.3.3).

5.3.4.2 URL Endpoint

/notifyProvisioningResult

5.3.4.3 HTTP Method

POST

5.3.4.4 Encrypted Request Parameters

tokenUniqueReference

Description:	The Token Credential provisioned. Must be a valid reference as assigned by MDES.
Data Type:	String
Max Length:	64
Required:	Yes

result

Description: Whether the provisioning was successful. Must be one of:

Value	Meaning
SUCCESS	Provisioning completed successfully and the target device/application is ready.
ERROR	An error occurred during provisioning

Data Type:	String
Max Length:	64
Required:	Yes

errorCode

Description:	Error code for the reason the provisioning failed.
Data Type:	String
Max Length:	32
Required:	Conditional – required if result = ERROR.

errorDescription

Description:	Error description of the reason the provisioning failed.
Data Type:	String
Max Length:	256
Required:	No

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

5.3.4.5 Encrypted Response Values

Only common response elements.

5.3.4.6 Examples

5.3.4.6.1 Sample Request


```
{
      "mobileKeysetId" : "e279760f-f4cd-4683-ba42-4d8053817a69",
      "authenticationCode" :
"94c46d98ecdeed2957e45c576bc2e0e97ce326e9715d2b99832608472950b7f3"
      "encryptedData" :
"Tk9UIFJFQUwgREFUQSAtIHRoaXMgd2lsbCBiZSB0aGUgYWN0dWFsIGRhdGEgZW5jcnlwdGVkIHVzaW5nIHRo
ZSBNb2JpbGUgS2V5cw=="
}
```


Where the "encryptedData" would decrypt to:


```
{
      "requestId" : "4000000001",
      "tokenUniqueReference" : "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
      "result": "SUCCESS"
}
```


5.3.4.6.2 Sample Response


```
{
      "encryptedData" :
"Tk9UIFJFQUwgREFUQSAtIHRoaXMgd2lsbCBiZSB0aGUgYWN0dWFsIGRhdGEgZW5jcnlwdGVkIHVzaW5nIHRo
ZSBNb2JpbGUgS2V5cw=="
}
```


Where the "encryptedData" would decrypt to:


```
{
      "responseId" : "4000000001",
      "responseHost" : "site2.Mastercard.com"
}
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

5.3.5 Replenish

5.3.5.1 Overview

This API is used to replenish the Mobile Payment App with new Transaction Credentials.

To request replenishment, the Mobile Payment App must supply accurate status information for every Transaction Credential in the Mobile Payment App after the last successful replenishment. This is defined as:

- All active/unused Transaction Credentials remaining on the Mobile Payment App.
- All Transaction Credentials used or discarded since the last replenishment.

Once a Transaction Credential has been successfully reported as used or discarded, it does not need to be reported on again. Note that Transaction Credentials that are never reported on are assumed to be lost and count as discarded. If replenishment is unsuccessful, Transaction Credential status information should be retained and submitted again until replenishment succeeds.

Replenishment may be rejected if the Token is not currently in a state that permits replenishment (for example, if it is currently suspended).

Successful replenishment will top up the number of Transaction Credentials up to the maximum permitted by the Issuer for this Token.

5.3.5.2 URL Endpoint

/replenish

5.3.5.3 HTTP Method

POST

5.3.5.4 Encrypted Request Parameters

tokenUniqueReference	
Description:	The Token to be replenished
Data Type:	String
Max Length:	64
Required:	Yes

transactionCredentialsStatus	
Description:	The status of all active/unused Transaction Credentials on the Mobile Payment App and all Transaction Credentials used since the last replenishment.
Data Type:	Array[TransactionCredentialStatus object]
Max Length:	N/A
Required:	Conditional – required unless this is the first replenishment

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

5.3.5.5 Encrypted Response Values

transactionCredentials

Description:	One or more Transaction Credentials replenished.
Data Type:	Array[TransactionCredential object]
Max Length:	N/A
Required:	Yes

5.3.5.6 Examples

5.3.5.6.1 Sample Request

```
{
	"mobileKeysetId" : "e279760f-f4cd-4683-ba42-4d8053817a69",
	"authenticationCode" :
"94c46d98ecdeed2957e45c576bc2e0e97ce326e9715d2b99832608472950b7f3"
	"encryptedData" :
"Tk9UIFJFQUwgREFUQSAtIHRoaXMgd2lsbCBiZSB0aGUgYWN0dWFsIGRhdGEgZW5jcnlwdGVkIHVzaW5nIHRo
ZSBNb2JpbGUgS2V5cw=="
}
```

Where the "encryptedData" would decrypt to:

```
{
	"requestId" : "500000000001",
	"tokenUniqueReference" : "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
	"transactionCredentialsStatus" : [
		{
			"atc" : 1,
			"status" : "UNUSED_DISCARDED",
			"timestamp" : "2015-03-02T09:00:00Z"
		},
		{
			"atc" : 2,
			"status" : "USED_FOR_CONTACTLESS",
			"timestamp" : "2015-03-05T11:45:04Z"
		},
		{
			"atc" : 3,
			"status" : "USED_FOR_DSRP",
			"timestamp" : "2015-03-05T11:50:55Z"
		},
		{
			"atc" : 4,
			"status" : "UNUSED_ACTIVE",
			"timestamp" : "2015-03-06T03:30:15Z"
		}
	]
}
```

5.3.5.6.2 Sample Response

```
{
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
      "encryptedData" :
"Tk9UIFJFQUwgREFUQSAtIHRoaXMgd2lsbCBiZSB0aGUgYWN0dWFsIGRhdGEgZW5jcnlwdGVkIHVzaW5nIHRo
ZSBNb2JpbGUgS2V5cw=="
}
```


Where the "encryptedData" would decrypt to:


```
{
      "responseId" : "500000000001",
      "responseHost" : "site2.Mastercard.com",
      "transactionCredentials" : [
            {
                  "atc" : 5,
                  "idn" : "4E4F54205245414C2049444E",
                  "contactlessMdSessionKey":
"4E4F54205245414C204E4643204D4420534B",
                  "contactlessUmdSingleUseKey" :
"4E4F54205245414C204E464320554D442053554B",
                  "dsrpMdSessionKey" :  "4E4F54205245414C2044535250204D4420534B",
                  "dsrpUmdSingleUseKey" :
"4E4F54205245414C204453525020554D442053554B"
            },
            {
                  "atc" : 6,
                  "idn" : "4E4F54205245414C2049444E",
                  "contactlessMdSessionKey":
"4E4F54205245414C204E4643204D4420534B",
                  "contactlessUmdSingleUseKey" :
"4E4F54205245414C204E464320554D442053554B",
                  "dsrpMdSessionKey" :  "4E4F54205245414C2044535250204D4420534B",
                  "dsrpUmdSingleUseKey" :
"4E4F54205245414C204453525020554D442053554B"
            },
            {
                  "atc" : 7,
                  "idn" : "4E4F54205245414C2049444E",
                  "contactlessMdSessionKey":
"4E4F54205245414C204E4643204D4420534B",
                  "contactlessUmdSingleUseKey" :
"4E4F54205245414C204E464320554D442053554B",
                  "dsrpMdSessionKey" :  "4E4F54205245414C2044535250204D4420534B",
                  "dsrpUmdSingleUseKey" :
"4E4F54205245414C204453525020554D442053554B"
            }
      ]
}
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

5.3.6 Change Mobile PIN

5.3.6.1 Overview

This API is used to trigger a Mobile PIN change, or to set up a new Mobile PIN (during initial provisioning, or subsequently if the Mobile PIN was reset by the Issuer).

The Mobile Payment App prompts the user to enter their current PIN and to choose a new PIN. Both values are returned to MDES, which will verify that the current PIN is correct, and will change the Mobile PIN to the new value.

Note that if the Mobile Payment App does not receive a response to the Change Mobile PIN request (due to timeout or otherwise), it should attempt to retry the request until it is successful. If the Mobile Payment App persistently fails in the retry, it must use the Get Task Status API (see Section 5.3.8) to determine the outcome of the Change Mobile PIN request, so that the Mobile PIN is not left in an unknown state. MDES shall respond to a Change Mobile PIN request within at most five seconds.

Upon a successful Mobile PIN change, the Mobile Payment App must delete all existing Transaction Credentials and call the Replenish API (see Section 5.3.5) to replenish its Transaction Credentials.

Applicable only if the Mobile PIN is supplied directly by the Mobile Payment App. Not applicable if the Mobile PIN is supplied by a server using the MPA Management API (see Section 6.2.3 – Set Mobile PIN).

For Mobile Payment Applications that support a Locally-verified Consumer Device CVM (CDCVM) instead of Mobile PIN, this API may also be used to notify a successful reset of the Locally-verified CDCVM on the device. In this case, the Mobile PIN value embedded in parameter newMobilePin is a dummy value, and currentMobilePin is built with the last (dummy) value provided to the CMS-D, if any. MDES will reset the Mobile PIN try counters and unsuspend the Tokens as necessary.

5.3.6.2 URL Endpoint

/changeMobilePin

5.3.6.3 HTTP Method

POST

5.3.6.4 Encrypted Request Parameters

tokenUniqueReference	
Description:	The Token for which the Mobile PIN is to be changed
Data Type:	String
Max Length:	64
Required:	Conditional – required if the Mobile PIN relates to a specific Token. Not present otherwise.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

taskId

Description:	Unique identifier for this Change Mobile PIN task as assigned by the Mobile Payment App. May be used in the Get Task Status API (see Section 5.3.8) to query the status of this task.
Data Type:	String
Max Length:	64
Required:	Yes

currentMobilePin

Description:	The current Mobile PIN value as entered by the user, to be verified by MDES. The Mobile PIN value is supplied as a Format 4 PIN Block using a substitute value for the PAN as specified in Section 5.1.3.2, encrypted using the Mobile Data Encryption Key.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	64
Required:	Conditional – required when changing the Mobile PIN, not required when setting a new Mobile PIN.

newMobilePin

Description:	The new Mobile PIN value as chosen by the user, to be updated in MDES. The Mobile PIN value is supplied as a Format 4 PIN Block using a substitute value for the PAN as specified in Section 5.1.3.2, encrypted using the Mobile Data Encryption Key.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	64
Required:	Yes

5.3.6.5 Encrypted Response Values

result

Description: Whether the Mobile PIN change was successful. Must be one of:

Value	Meaning
SUCCESS	The Mobile PIN was successfully changed. The Mobile Payment App should proceed to delete any existing Transaction Credentials.
INCORRECT_PIN	The current PIN was entered incorrectly.

Data Type:	String
Max Length:	32
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

mobilePinTriesRemaining	
Description:	The current Mobile PIN tries remaining. If the PIN was entered incorrectly, the number of tries remaining may have been decremented. If the Mobile PIN change was successful, this value would have been reset. Note that this PIN tries remaining count reflects the number of PIN tries remaining for changing the Mobile PIN. It does not necessarily reflect the number of PIN tries remaining when transacting.
Data Type:	Number
Max Length:	2
Required:	Yes

5.3.6.6 Examples

5.3.6.6.1 Sample Request to set a new Token-specific Mobile PIN

```
{
	"mobileKeysetId" : "e279760f-f4cd-4683-ba42-4d8053817a69",
	"authenticationCode" :
"94c46d98ecdeed2957e45c576bc2e0e97ce326e9715d2b99832608472950b7f3"
	"encryptedData" :
"Tk9UIFJFQUwgREFUQSAtIHRoaXMgd2lsbCBiZSB0aGUgYWN0dWFsIGRhdGEgZW5jcnlwdGVkIHVzaW5nIHRo
ZSBNb2JpbGUgS2V5cw=="
}
```

Where the "encryptedData" would decrypt to:

```
{
	"requestId" : "6000000001",
	"taskId" : "123456",
	"tokenUniqueReference" :  "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
	"newMobilePin" : "4E4F54205245414C2050494E20424C4F434B"
}
```

5.3.6.6.2 Sample Request to change the Token-specific Mobile PIN

```
{
	"mobileKeysetId" : "e279760f-f4cd-4683-ba42-4d8053817a69",
	"authenticationCode" :
"94c46d98ecdeed2957e45c576bc2e0e97ce326e9715d2b99832608472950b7f3"
	"encryptedData" :
"Tk9UIFJFQUwgREFUQSAtIHRoaXMgd2lsbCBiZSB0aGUgYWN0dWFsIGRhdGEgZW5jcnlwdGVkIHVzaW5nIHRo
ZSBNb2JpbGUgS2V5cw=="
}
```

Where the "encryptedData" would decrypt to:

```
{
	"requestId" : "6000000001",
	"taskId" : "123456",
	"tokenUniqueReference" :  "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
	"currentMobilePin" : "4E4F54205245414C2050494E20424C4F434B",
	"newMobilePin" : "4E4F54205245414C2050494E20424C4F434B"
}
```

5.3.6.6.3 Sample Response for a successful call

```
{
	"encryptedData" :
"Tk9UIFJFQUwgREFUQSAtIHRoaXMgd2lsbCBiZSB0aGUgYWN0dWFsIGRhdGEgZW5jcnlwdGVkIHVzaW5nIHRo
ZSBNb2JpbGUgS2V5cw=="
}
```

Where the "encryptedData" would decrypt to:

```
{
	"responseId" : "6000000001",
	"responseHost" : "site2.Mastercard.com",
	"result" : "SUCCESS",
	"mobilePinTriesRemaining" : 3
}
```

5.3.6.6.4 Sample Response for a failed call due to an incorrect current PIN

```
{
	"encryptedData" :
"Tk9UIFJFQUwgREFUQSAtIHRoaXMgd2lsbCBiZSB0aGUgYWN0dWFsIGRhdGEgZW5jcnlwdGVkIHVzaW5nIHRo
ZSBNb2JpbGUgS2V5cw=="
}
```

Where the "encryptedData" would decrypt to:

```
{
	"responseId" : "6000000001",
	"responseHost" : "site2.Mastercard.com",
	"result" : "INCORRECT_PIN",
	"mobilePinTriesRemaining" : 2
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

5.3.7 Delete

5.3.7.1 Overview

This API is used by the Mobile Payment App to delete a Token Credential.

5.3.7.2 URL Endpoint

/delete

5.3.7.3 HTTP Method

POST

5.3.7.4 Encrypted Request Parameters

tokenUniqueReference

Description:	The Token to be deleted.
Data Type:	String
Max Length:	64
Required:	Yes

transactionCredentialsStatus

Description:	The current status of the Mobile Payment App's Transaction Credentials at the time of deletion.
Data Type:	Array[TransactionCredentialStatus object]
Max Length:	N/A
Required:	Yes

5.3.7.5 Encrypted Response Values

Only common response elements.

5.3.7.6 Examples

5.3.7.6.1 Sample Request

```
{
      "mobileKeysetId" : "e279760f-f4cd-4683-ba42-4d8053817a69",
      "authenticationCode" :
"94c46d98ecdeed2957e45c576bc2e0e97ce326e9715d2b99832608472950b7f3"
      "encryptedData" :
"Tk9UIFJFQUwgREFUQSAtIHRoaXMgd2lsbCBiZSB0aGUgYWN0dWFsIGRhdGEgZW5jcnlwdGVkIHVzaW5nIHRo
ZSBNb2JpbGUgS2V5cw=="
}
```

Where the "encryptedData" would decrypt to:

```
{
      "requestId" : "700000000001",
      "tokenUniqueReference" : "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
	"transactionCredentialsStatus" : [
		{
			"atc" : 1,
			"status" : "UNUSED_DISCARDED",
			"timestamp" : "2015-03-02T09:00:00Z"
		},
		{
			"atc" : 2,
			"status" : "USED_FOR_CONTACTLESS",
			"timestamp" : "2015-03-05T11:45:04Z"
		},
		{
			"atc" : 3,
			"status" : "USED_FOR_DSRP",
			"timestamp" : "2015-03-05T11:50:55Z"
		},
		{
			"atc" : 4,
			"status" : "UNUSED_ACTIVE",
			"timestamp" : "2015-03-06T03:30:15Z"
		}
	]
}
```


5.3.7.6.2 Sample Request (for a new Token that was never replenished)


```
{
	"mobileKeysetId" : "e279760f-f4cd-4683-ba42-4d8053817a69",
	"authenticationCode" :
"94c46d98ecdeed2957e45c576bc2e0e97ce326e9715d2b99832608472950b7f3"
	"encryptedData" :
"Tk9UIFJFQUwgREFUQSAtIHRoaXMgd2lsbCBiZSB0aGUgYWN0dWFsIGRhdGEgZW5jcnlwdGVkIHVzaW5nIHRoZSBNb2JpbGUgS2V5cw=="
}
```


Where the "encryptedData" would decrypt to:


```
{
	"requestId" : "700000000001",
	"tokenUniqueReference" : "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
	"transactionCredentialsStatus" : []
}
```


5.3.7.6.3 Sample Response


```
{
	"encryptedData" :
"Tk9UIFJFQUwgREFUQSAtIHRoaXMgd2lsbCBiZSB0aGUgYWN0dWFsIGRhdGEgZW5jcnlwdGVkIHVzaW5nIHRoZSBNb2JpbGUgS2V5cw=="
}
```


Where the "encryptedData" would decrypt to:


```
{
	"responseId" : "7000000001",
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
        "responseHost" : "site2.Mastercard.com"
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

5.3.8 Get Task Status

5.3.8.1 Overview

This API is used to check the status of a task that was previously requested.

5.3.8.2 URL Endpoint

/getTaskStatus

5.3.8.3 HTTP Method

POST

5.3.8.4 Encrypted Request Parameters

taskId

Description:	Unique identifier for this task as assigned by the Mobile Payment App. Must be an identifier previously used when requesting a task.
Data Type:	String
Max Length:	64
Required:	Yes

5.3.8.5 Encrypted Response Values

status

Description: The status of the specified task. Must be one of:

Value	Meaning
PENDING	The task has been received and is pending processing.
IN_PROGRESS	The task is currently in progress
COMPLETED	The task was completed successfully
FAILED	The task was processed but failed to complete successfully.

Data Type:	String
Max Length:	64
Required:	Yes

5.3.8.6 Examples

5.3.8.6.1 Sample Request

```
{
      "mobileKeysetId" : "e279760f-f4cd-4683-ba42-4d8053817a69",
      "authenticationCode" :
"94c46d98ecdeed2957e45c576bc2e0e97ce326e9715d2b99832608472950b7f3"
      "encryptedData" :
"Tk9UIFJFQUwgREFUQSAtIHRoaXMgd2lsbCBiZSB0aGUgYWN0dWFsIGRhdGEgZW5jcnlwdGVkIHVzaW5nIHRo
ZSBNb2JpbGUgS2V5cw=="
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

Where the "encryptedData" would decrypt to:

```
{
	"requestId" : "800000000001",
	"taskId": "123456"
}
```

5.3.8.6.2 Sample Response

```
{
	"encryptedData" :
"Tk9UIFJFQUwgREFUQSAtIHRoaXMgd2lsbCBiZSB0aGUgYWN0dWFsIGRhdGEgZW5jcnlwdGVkIHVzaW5nIHRo
ZSBNb2JpbGUgS2V5cw=="
}
```

Where the "encryptedData" would decrypt to:

```
{

	"responseId": "800000000001",
	"status": "FAILED"
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

5.3.9 Get System Health

5.3.9.1 Overview

This API is used to check the general status of a Mobile Payment API host.

A successful response contains an HTTP response code of 200 with an empty body, and indicates that the service is running and accepting requests.

Note that this API may only be used by authenticated clients – it is not generally accessible publicly.

5.3.9.2 URL Endpoint

/health

5.3.9.3 HTTP Method

GET

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

6 MPA Management API

6.1 General

The MDES MPA Management API encompasses a set of APIs that are either initiated by the Wallet Server to the Mastercard CMS-D (inbound), or asynchronous API (outbound) calls made from the Mastercard CMS-D to the Wallet Server.

MDES MPA Mangement API supports MCBP implementations from 1.0 to 2.0.

6.1.1 API Design Principles

The MPA Management APIs are designed as 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 will specify the HTTP Method used to access it. All strings in request and response objects are to be UTF-8 encoded. Each API URI includes the major and minor version of API that it conforms to. This will allow multiple concurrent versions of the API to be deployed simultaneously.

The client must handle any standard HTTP response code that could result from a web service call including but not limited to 302, 401, 404, or 500.

All APIs return an HTTP response code of 200 if the call was successfully received and accepted for processing. Any errors that subsequently occur during processing are returned in the response payload (see Sections 6.1.4 and 6.1.5 and for more information on error code elements and error handling).

To ensure forward-compatibility, all API client implementations must be resilient to new elements being added to outbound requests and responses from MDES.

6.1.2 URL Scheme

All API URLs follow the format:

scheme://host[:port]/contextRoot/api/majorVer/minorVer/apiName

URL Element	Definition
scheme	https
host[:port]	Hostname (and port number if required) for the environment. services.Mastercard.com
contextRoot	mdes
api	mpamanagement

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

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.

6.1.3 Security Overview and Encryption

All communication between the client and the Credentials Management Dedicated will be secured using mutually authenticated TLS.

6.1.4 API Request / Response Common Elements and Headers

All requests and responses from MDES contain an element ‘responseHost’. This identifies the specific MDES host that originated a request or response. It should be used by the client in the URL for future calls in order to direct the call to a specific host. As MDES is deployed in a dual active environment, this ensures that when a client makes a series of API calls, they must direct all calls within the same conversation to the same host. This minimizes the risk of some calls being routed to a different site, where data from a previous call may not yet have been replicated. When a conversation is complete, the client should revert back to the default host (provided during onboarding) to ensure that it is not locked permanently to one host.

The client may also provide its 'responseHost' in requests and responses originating from the client, and MDES will honor the responseHost per the above. Note that all valid client hosts must be pre-configured in MDES. Should a 'responseHost' value be submitted that is not yet configured, MDES will respond with an error.

In addition every inbound and outbound request contains an element ‘requestId’ which uniquely identifies the request. Every response contains an element ‘responseId’ which uniquely identifies the response. The responseId may optionally use the corresponding requestId. Note that the format and uniqueness of the requestId and responseId are not necessarily validated on the MPA Management API.

In the case of an operation reporting an error, a response contains one or more errors with the elements ‘errorCode’ and ‘errorDescription’ as defined in Section 6.1.5. Unless explicitly stated otherwise, other elements (including 'Required' fields) are not present if an error is reported.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

6.1.4.1 Common Request Elements

responseHost	
Description:	The host that originated the request. Future calls in the same conversation may be routed to this host. Must be provided as: host[:port][/contextRoot] Where port and contextRoot are optional. If contextRoot is not provided, the default (per the URL Scheme) is assumed and must be used.
Data Type:	String
Max Length:	64
Required:	No

requestId	
Description:	Unique identifier for the request.
Data Type:	String
Max Length:	64
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

6.1.4.2 Common Response Elements

responseHost	
Description:	The host that originated the response. Future calls in the same conversation must be routed to this host. Must be provided as: host[:port][/contextRoot] Where port and contextRoot are optional. If contextRoot is not provided, the default (per the URL Scheme) is assumed and must be used.
Data Type:	String
Max Length:	64
Required:	Conditional – See Section 6.1.4. In Production, the responseHost supplied by MDES must be used by the client for future API calls within a conversation. When the conversation is complete, the client will revert back to the default host supplied during onboarding.

responseId	
Description:	Unique identifier for the response.
Data Type:	String
Max Length:	64
Required:	Yes

errors	
Description:	One or more errors for the reasons the operation failed.
Data Type:	Array[Error object]
Max Length:	N/A
Required:	Conditional – required if one or more errors occurred performing the operation.

6.1.5 Error Codes

Error Code	Error Description	Detail
INVALID_JSON	Invalid JSON	The JSON could not be parsed.
AUTHORIZATION_FAILED	Authorization failed.	The request failed to present a valid cert to access the API.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

Error Code	Error Description	Detail
INVALID_FIELD_FORMAT	Invalid Field Format - {fieldName}	The field is not in the correct format. For instance, it should be a number but is a string.
INVALID_FIELD_LENGTH	Invalid Field Length - {fieldName}	The value does not fall between the minimum and maximum length for the field.
INVALID_FIELD_VALUE	Invalid Field Value - {fieldName}	The value is not allowed for the field.
INVALID_RESPONSE_HOST	Invalid Response Host	The requested response host is invalid.
MISSING_REQUIRED_FIELD	Missing Required Field - {fieldName}	A required field is missing.
INVALID_OPERATION	Invalid Operation	The requested operation is invalid. For example, if a token-level PIN management operation is invoked on a token using a wallet-level PIN.
CRYPTOGRAPHY_ERROR	Cryptography Error	There was an error decrypting the encrypted payload.
INTERNAL_SERVICE_FAILURE	Internal Service Failure	MDES had an internal exception.
INVALID_PAYMENT_APP_INSTANCE_ID	Invalid Payment App Instance ID	The Payment App Instance ID could not be found.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

Error Code	Error Description	Detail
INVALID_PAYMENT_APP_PROVIDER_ID	Invalid Payment App Provider ID	The Payment App Provider Id (Wallet Identifier) could not be found

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

6.1.6 Retry Strategy

For outbound calls that fail with a timeout, connection failure, or an HTTP response code of 302, 500, or 503 MDES will automatically retry 3 times with up to a 5-second wait between each try. 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.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

6.2 Inbound APIs (to MDES)

6.2.1 Register

6.2.1.1 Overview

This API is used by a server to register a new Mobile Payment App instance with MDES for use; or for existing Mobile Payment App instances which are already registered, this API is used to re-register the Mobile Payment App instance in order to update any registration details (such as its RNS information or device fingerprint) and generate new Mobile Keys.

MDES supports two methods for registering a Mobile Payment App, either it is performed by a server on behalf of the Mobile Payment App using this API; or it is performed directly by the Mobile Payment App in response to a remote notification (for the latter, see Section 5.3.1 for more information on the ~~Register~~ API on the Mobile Payment API).

6.2.1.2 URL Endpoint

/register

6.2.1.3 HTTP Method

POST

6.2.1.4 Request Parameters

paymentAppId	
Description:	Identifier for the Payment App, unique per app as assigned by Mastercard for this Payment App.
Data Type:	String
Max Length:	30
Required:	Yes

paymentAppInstanceId	
Description:	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization.
Data Type:	String
Max Length:	48
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

rnsInfo	
Description:	Contains information about the Remote Notification Service to be used to deliver credentials to the target application instance.
Data Type:	RnsInfo object.
Max Length:	N/A
Required:	Conditional – required if remote notification is via Google Cloud Messaging. Not present if remote notification is via a server using the Send Remote Notification Message API (see Section 6.3.1).
~~certificateFingerprint~~	
Description:	The certificate fingerprint identifying the public key used to encrypt the randomly-generated AES key ('rgk').
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	64
Required:	**Deprecated** – use publicKeyFingerprint instead.
publicKeyFingerprint	
Description:	The certificate fingerprint identifying the public key used to encrypt the randomly-generated AES key ('rgk').
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	64
Required:	Yes
rgk	
Description:	The randomly-generated 128-bit AES key, encrypted by the Mastercard public key (provided during onboarding) using OAEP with SHA-256 hashing algorithm.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	512
Required:	Yes
deviceFingerprint	
Description:	The unique device fingerprint, which is a SHA-256 hash computed over a list of data elements retrieved from the Mobile Payment App and the Mobile Device.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	64 (Exact)
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

newMobilePin	
Description:	The new Mobile PIN value as chosen by the user, to be updated in MDES. The Mobile PIN value is supplied as a Format 4 PIN Block using a substitute value for the PAN as specified in Section 5.1.3.2, encrypted using the given 'rgk'.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	64
Required:	Conditional – optional if the Mobile Payment App supports Mobile PIN and if the Mobile PIN is supplied by a server. Not present if the Mobile Payment App does not support Mobile PIN. Not present if the Mobile PIN is supplied directly by the Mobile Payment App using the Mobile Payment API (see Section 5.3.6 – Change Mobile PIN).

6.2.1.5 Response Values

mobileKeysetId	
Description:	The identifier for the Mobile Keys used to manage the CLOUD credentials, as assigned by MDES upon successful registration.
Data Type:	String
Max Length:	64
Required:	Yes

mobileKeys	
Description:	Contains the mobile keys used to secure the communication during subsequent remote management sessions.
Data Type:	MobileKeys object.
Max Length:	N/A
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

remoteManagementUrl	
Description:	The URL endpoint for subsequent remote management sessions. The Mobile Payment App must store this URL for future use in order to be able to request new remote management sessions. Must be provided as: host[:port][/contextRoot] Where port and contextRoot are optional. If contextRoot is not provided, the default (per the URL Scheme) is assumed and must be used.
Data Type:	String
Max Length:	128
Required:	Yes

6.2.1.6 Examples

6.2.1.6.1 Sample Request

```
{
"responseHost" : "site2.your-server.com",
"requestId" : "123456",
       "paymentAppId" : "WalletApp1",
       "paymentAppInstanceId" : "123456789",
"rnsInfo" : {
"gcmRegistrationId" : "APA91bHPRgkF3JUikC4ENAHEeMrd41Zxv3hVZjC9KtT8OvPVGJ-
hQMRKRrZuJAEcl7B338qju59zJMjw2DELjzEvxwYv7hH5Ynpc1ODQ0aT4U4OFEeco8ohsN5PjL1iC2dNtk2BA
okeMCg2ZXKqpc8FXKmhX94kIxQ",
       },
       "publicKeyFingerprint" : "4c4ead5927f0df8117f178eea9308daa58e27c2b",
       "rgk" :
"4E4F54205245414C2044415441202D20746869732077696C6C2062652072616E646F6D206B6579206765
6E657261746564206279207468652045504D504120616E6420656E6372797074656420757369E67207468652
04D617374657243617264207075626C6963206B6579",
       "deviceFingerprint" :
"1bbefaa95b26b9e82e3fdd37b20050fc782b2f229a8f8bcbbcb6aa6abe4c851e",
       "newMobilePin" : "4E4F54205245414C2050494E20424C4F434B"
}
```

6.2.1.6.2 Sample Response

```
{
       "responseHost" : "site1.Mastercard.com",
       "responseId" : "123456",
       "mobileKeysetId" : "e279760f-f4cd-4683-ba42-4d8053817a69",
       "mobileKeys" : {
              "transportKey" :
"4E4F54205245414C2044415441202D20746869732077696C6C206265207468",
              "macKey" :
"4E4F54205245414C2044415441202D20746869732077696C6C206265207468",
              "dataEncryptionKey" :
"4E4F54205245414C2044415441202D20746869732077696C6C2062652074686"
       },
       "remoteManagementUrl" : "loadbalanced.Mastercard.com"
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

6.2.2 Unregister

6.2.2.1 Overview

This API is used by a server to unregister an existing Mobile Payment App instance with MDES.

Any existing registration data and/or any Token credentials associated with that Mobile Payment App instance are deleted from MDES.

6.2.2.2 URL Endpoint

/unregister

6.2.2.3 HTTP Method

POST

6.2.2.4 Request Parameters

paymentAppInstanceId	
Description:	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization.
Data Type:	String
Max Length:	48
Required:	Yes

6.2.2.5 Response Values

Only common response elements.

6.2.2.6 Examples

6.2.2.6.1 Sample Request

```
{
"responseHost" : "site2.your-server.com",
"requestId" : "123456",
      "paymentAppInstanceId" : "123456789"
}
```

6.2.2.6.2 Sample Response

```
{
      "responseHost" : "site1.Mastercard.com",
      "responseId" : "123456"
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

6.2.3 Set Mobile PIN

6.2.3.1 Overview

This API is used by a server to set the Mobile PIN for a given Mobile Payment App instance.

Applicable only if the Mobile PIN is supplied by a server. Not applicable if the Mobile PIN is supplied directly by the Mobile Payment App using the Mobile Payment API (see Section 5.3.6 – Change Mobile PIN).

For Mobile Payment Applications that support a Locally-verified Consumer Device CVM (CDCVM) instead of Mobile PIN, this API is also used to notify a successful reset of the Locally-verified CDCVM on the device. In this case, the Mobile PIN value embedded in parameter newMobilePin is a dummy value. MDES will reset the Mobile PIN try counters and unsuspend the Tokens as necessary

6.2.3.2 URL Endpoint

/setMobilePin

6.2.3.3 HTTP Method

POST

6.2.3.4 Request Parameters

paymentAppInstanceId	
Description:	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization.
Data Type:	String
Max Length:	48
Required:	Yes

newMobilePin	
Description:	The new Mobile PIN value as chosen by the user, to be updated in MDES. The Mobile PIN value is supplied as a Format 4 PIN Block using a substitute value for the PAN as specified in Section 5.1.3.2, encrypted using the Mobile Data Encryption Key.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	64
Required:	Yes

6.2.3.5 Response Values

Only common response elements.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

6.2.3.6 Examples

6.2.3.6.1 Sample Request

```
{
"responseHost" : "site2.your-server.com",
"requestId" : "123456",
       "paymentAppInstanceId" : "123456789",
       "newMobilePin" : "4E4F54205245414C2050494E20424C4F434B"
}
```

6.2.3.6.2 Sample Response

```
{
       "responseHost" : "site1.Mastercard.com",
       "responseId" : "123456"
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

6.2.4 Get Public Key Certificate

6.2.4.1 Overview

This API is used to download the public key certificate which is used to wrap the randomly-generated key (RGK) during the MPA registration process.

6.2.4.2 URL Endpoint

/pkCertificate

6.2.4.3 HTTP Method

GET

6.2.4.4 Response Data

Response data contains a file of MIME type "application/pkix-cert" according to RFC 2585.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

6.2.5 Get System Health

6.2.5.1 Overview

This API is used to check the general status of an MPA Management API host.

A successful response contains an HTTP response code of 200 with an empty body, and indicates that the service is running and accepting requests.

6.2.5.2 URL Endpoint

/health

6.2.5.3 HTTP Method

GET

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

6.3 Outbound APIs (from MDES)

6.3.1 Send Remote Notification Message

6.3.1.1 Overview

This API is used by MDES to send a Remote Notification Message to the Mobile Payment App via a server,

MDES supports two methods of sending remote notification messages, they are either sent to the Mobile Payment App via Google Cloud Messaging, or they are sent to the Mobile Payment App via a server using this API.

The server may deliver the remote notification message payload to the Mobile Payment App using its own preferred channel or mechanism, but the remote notification message payload must be delivered to the Mobile Payment App as is without changing any of its content.

6.3.1.2 URL Endpoint

/sendRemoteNotificationMessage

6.3.1.3 HTTP Method

POST

6.3.1.4 Request Parameters

paymentAppProviderId	
Description:	Globally unique identifier for the Wallet Provider, as assigned by MDES. Commonly known as the Wallet Identifier.
Data Type:	String
Max Length:	64
Required:	Yes

paymentAppInstanceId	
Description:	Identifier for this specific Mobile Payment App instance, unique across a given Wallet Identifier.
Data Type:	String
Max Length:	48
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

notificationData	
Description:	Contains the Base64 encoded NotificationData object. This is the message that will be sent to the device.
Data Type:	String. Base64-encoded data.
Max Length:	N/A
Required:	Yes

6.3.1.5 Response Values

Only common response elements.

6.3.1.5.1 Sample Notification for Provisioning


```
{
	"paymentAppProviderId": "123456789",
	"requestId": "123456",
	"paymentAppInstanceId": "123456789",
	"notificationData":
"ew0KCSJyZXNwb25zZUhvc3QiIDogInNpdGUxLm1hc3RlcmNhcmQuY29tIiwNCgkicmVnaXN0cmF0aW9uRGF0
YSIgOiB7DQoJCSJyZWdpc3RyYXRpb25Db2RlIiA6ICI2Y2MwNjNmYi03NjZkLTQ4NDktOTMwZC1lYjBmZGY0Z
TE1YTUiLCANCgkJInB1YmxpY0tleSIgOiAiNEU0RjU0MjA1MjQ1NDE0QzIwNDQ0MTU0NDEyMDJEMjA3NDY4Nj
k3MzIwNzc2OTZDNkMyMDYyNjUyMDYxMjA3MDc1NjI2QzY5NjMyMDZCNjU3OTIwNzA3MjZGNzY2OTY0NjU2NDI
wNjI3OTIwNzQ2ODY1MjA0MzcyNjU2NDY1NkU3NDY5NjE2QzczMjA0RDYxNkU2MTY3NjU2RDY1NkU3NDIwMjg0
NDY1NjQ2OTYzNjE3NDY1NjQyOSIsDQogICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICJ
wa0NlcnRpZmljYXRlVXJsIiA6ICJodHRwczovL3NlcnZpY2VzLm1hc3RlcmNhcmQuY29tL21kZXMvcGF5bWVudGFwcC8xLzAvcGtDZXJ0aWZpY2F0ZSINCgl9LA0KCSJtb2JpbGVLZXlzZXRJZCIgOiAiZTI3OTc2MGYtZjRjZC00NjgzLWJhNDItNGQ4MDUzODE3YTY5Iiw
NCgkiZW5jcnlwdGVkRGF0YSIgOiAiVGs5VUlGSkZRVXdnUkVGVVFTQXRJSFJvYVhNZ2QybHNiQ0JpWlNCMGFH
VWdZV04wZFdGc0lHUmhkR0VnWlc1amNubHdkR1ZrSUhWemFXNW5JSFJvWlNCTmIySnBiR1VnUzJWNWN5QT0iD
Qp9DQo="
}
```


Where "notificationData" would decode to:


```
{
	"responseHost" : "site1.Mastercard.com",
	"mobileKeysetId" : "e279760f-f4cd-4683-ba42-4d8053817a69",
	"encryptedData" :
"Tk9UIFJFQUwgREFUQSAtIHRoaXMgd2lsbCBiZSB0aGUgYWN0dWFsIGRhdGEgZW5jcnlwdGVkIHVzaW5nIHRo
ZSBNb2JpbGUgS2V5cyA="
}
```


Where "encryptedData" would decrypt to:


```
{
	"version" : "1.0",
	"sessionCode" : "92d60ba5-dd1f-4bb8-b08e-0648b3098d1e",
	"expiryTimeStamp" : "2015-03-06T03:23:26Z",
	"validForSeconds" : "3600",
	"pendingAction" : "PROVISION",
	"tokenUniqueReference" : "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45"
```


© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
}
```

6.3.1.5.2 Sample Notification in response to a Request Session

```
{
      "paymentAppProviderId": "123456789",
      "requestId": "123456",
      "paymentAppInstanceId": "123456789",
      "notificationData":
"ew0KCSJyZXNwb25zZUhvc3QiIDogInNpdGUxLm1hc3RlcmNhcmQuY29tIiwNCgkibW9iaWxlS2V5c2V0SWQi
IDogImUyNzk3NjBmLWY0Y2QtNDY4My1iYTQyLTRkODA1MzgxN2E2OSIsDQoJImVuY3J5cHRlZERhdGEiIDogI
lRrOVVJRkpGUVV3Z1JFRlVRU0F0SUhSb2FYTWdkMmxzYkNCaVpTQjBhR1VnWVdOMGRXRnNJR1JoZEdFZ1pXNW
pjbmx3ZEdWa0lIVnphVzVuSUhSb1pTQk5iMkpwYkdVZ1MyVjVjeUE9Ig0KfQ0K"
}
```

Where "notificationData" would decode to:

```
{
      "responseHost" : "site1.Mastercard.com",
      "mobileKeysetId" : "e279760f-f4cd-4683-ba42-4d8053817a69",
      "encryptedData" :
"Tk9UIFJFQUwgREFUQSAtIHRoaXMgd2lsbCBiZSB0aGUgYWN0dWFsIGRhdGEgZW5jcnlwdGVkIHVzaW5nIHRo
ZSBNb2JpbGUgS2V5cyA=="
}
```

Where the "encryptedData" would decrypt to:

```
{
      "version" : "1.0",
      "sessionCode" : "92d60ba5-dd1f-4bb8-b08e-0648b3098d1e",
      "expiryTimeStamp" : "2015-03-06T03:23:26Z",
      "validForSeconds" : "3600"
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

7 Transaction Details API

This section specifies the public API provided by the Transaction Details Service.

7.1 General

7.1.1 API Design Principles

The Transaction Detail APIs are designed as 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 to be UTF-8 encoded. Each API URI includes the major and minor version of API that it conforms to. This will allow multiple concurrent versions of the API to be deployed simultaneously.

The client must handle any standard HTTP response code that could result from a web service call including but not limited to 302, 401, 404, or 500.

All APIs return an HTTP response code of 200 if the call was successfully received and accepted for processing. Any errors that subsequently occur during processing are returned in the response payload (see Sections 7.1.4 and 7.1.5 on error code elements and error handling).

To ensure forward-compatibility, all API client implementations must be resilient to new elements being added to outbound requests and responses from the Transaction Details Service.

7.1.2 URL Scheme

All API URLs follow the format:

scheme://host[:port]/contextRoot/api/majorVer/minorVer/paymentAppInstanceId/apiName

URL Element	Definition
scheme	https
host[:port]	Hostname (and port number if required) for the environment. services.Mastercard.com ~~ws.Mastercard.com~~ **(deprecated)**
contextRoot	mdes
api	tds

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

majorVer	The major version of the APIs. This is not related to the version of this document. 1 ~~Not present for the Get System Health API~~ **(deprecated)**
minorVer	The minor version of the APIs. 0 ~~Not present for the Get System Health API~~ **(deprecated)**
paymentAppInstanceId	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization. This field is alphanumeric and additionally web-safe base64 characters per RFC 4648 (minus "-", underscore "_" and URL-encoded equals sign "%3D") up to a maximum length of 48 (after URL-decoding). Not present for the Get System Health API.
apiName	The URL endpoint as defined in the respective section for the API operation.

7.1.3 Security Overview and Encryption

All communications between the client and the Transaction Details APIs are secured using an HTTPS connection. Upon request, the Transaction Details API returns half of a registration code directly to the device. The other half is delivered via the Token Requestor. This allows for the device to be securely identified as the provisioned device. Both halves of the registration code is then hashed and used to register for the Transaction Details API. An authentication code is issued once the registration code is confirmed. The authentication code is required on all subsequent requests.

7.1.4 API Request / Response Common Elements and Headers

All requests and responses from MDES contain an element 'responseHost'. This identifies the specific MDES host that originated a request or response. It should be used by the client in the URL for future calls in order to direct the call to a specific host. As MDES is deployed in a dual active environment, this ensures that when a client makes a series of API calls, they must direct all calls within the same conversation to the same host. This minimizes the risk of some calls being routed to a different site, where data from a previous call may not yet have been replicated. When a conversation is complete, the client should revert back to the default host (provided during onboarding) to ensure that it is not locked permanently to one host.

In the case of an operation reporting an error, the response contains the elements "errorCode" and "errorDescription" as defined in Section 7.1.5. Unless explicitly stated

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

otherwise, other elements (including 'Required' fields) are not present if an error is reported.

7.1.4.1 Common Request Elements

No common request elements.

7.1.4.2 Common Response Elements

responseHost	
Description:	The host that originated the response. Future calls in the same conversation must be routed to this host. Must be provided as: host[:port][/contextRoot] Where port and contextRoot are optional. If contextRoot is not provided, the default (per the URL Scheme) is assumed and must be used.
Data Type:	String
Max Length:	64
Required:	Conditional – See Section 7.1.4. In Production, the responseHost supplied by MDES must be used by the client for future API calls within a conversation. When the conversation is complete, the client will revert back to the default host supplied during onboarding.
errorCode	
Description:	Error code for the reason the operation failed.
Data Type:	String
Max Length:	32
Required:	Conditional – required if an error occurred performing the operation.
errorDescription	
Description:	Error description of the reason the operation failed.
Data Type:	String
Max Length:	256
Required:	No

7.1.5 Error Codes

Error Code	Error Description	Detail
INVALID_JSON	Invalid JSON	The JSON could not be parsed.
UNRECOGNIZED_FIELD	Unrecognized Field - {fieldName}	The field name is not valid for the object.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

Error Code	Error Description	Detail
INVALID_FIELD_FORMAT	Invalid Field Format - {fieldName}	The field is not in the correct format. For instance, it should be a number but is a string.
INVALID_FIELD_LENGTH	Invalid Field Length - {fieldName}	The value does not fall between the minimum and maximum length for the field.
INVALID_FIELD_VALUE	Invalid Field Value - {fieldName}	The value is not allowed for the field.
MISSING_REQUIRED_FIELD	Missing Required Field - {fieldName}	A required field is missing.
INTERNAL_SERVICE_FAILURE	Internal Service Failure	MDES had an internal exception.
INVALID_TOKEN_UNIQUE_REFERENCE	Invalid Token Unique Reference	The token unique reference could not be found or does not match the paymentAppInstanceId provided.
INVALID_AUTHENTICATION_CODE	Invalid Authentication Code	The authentication code is invalid for the mapping or device indicated
INVALID_REGISTRATION_CODE	Invalid Registration Code	The registration code hash provided could not be validated.
TOKEN_INELIGIBLE	Token Ineligible For Transaction Details	Token is not eligible for the service and cannot be registered.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

7.2 Inbound APIs (to Transaction Details Service)

7.2.1 Get Registration Code

7.2.1.1 Overview

This API is used by the Mobile Payment App to generate a unique and random registration code for the registration process (see Section 7.2.2 – Register), ensuring that registration requests cannot be replayed.

A second registration code is sent over a separate channel via the Token Requestor using the Notify Transaction Details API (see Section 3.3.2) to the Mobile Payment App. The Mobile Payment App combines the two registration codes, performs a hash and uses the hash to authenticate itself to the service. In case of retry scenarios, the Mobile Payment App should always use the most recent two registration codes received.

7.2.1.2 URL Endpoint

/getRegistrationCode

7.2.1.3 HTTP Method

POST

7.2.1.4 Request Parameters

tokenUniqueReference

Description:	The Token for which to register for transaction details. Must be a valid reference as assigned by MDES.
Data Type:	String
Max Length:	64
Required:	Yes

7.2.1.5 Response Values

registrationCode1

Description:	The first part of the registration code that must be used in the registration request.
Data Type:	String
Max Length:	64
Required:	Yes

7.2.1.6 Examples

7.2.1.6.1 Sample Request

```
{
      "tokenUniqueReference" : "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45"
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

7.2.1.6.2 Sample Response

```
{
"responseHost" : "site1.Mastercard.com",
"registrationCode1" : "c1b1f68a-5d0e-4a38-8597-420d85301c46"
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

7.2.2 Register

7.2.2.1 Overview

This API is used by the Mobile Payment App to opt into the Transaction Details Service.

The Mobile Payment App must authenticate itself to the Transaction Details Service to be authorized and registered to access transaction details. To achieve this, the Mobile Payment App must first use the Get Registration Code API and provide a hash of the two registration codes generated (see Section 7.2.1).

In response to a successful Register request, the Transaction Details Service will generate an authentication code which is used subsequently to access the service. The authentication code is time-limited and will expire after 90 days. Note that the registration is only considered valid for as long as the authentication code remains valid. If the authentication code expires, the app must register again using this API to continue accessing the service. Outbound transaction notifications shall cease to be sent if registration expires.

All Tokens on the same Mobile Payment App instance share the same authentication code. In the case of an expired authentication code, obtaining a new valid authentication code for any registered Token will allow the retrieval of transaction details for all registered Tokens.

Once registered, the Transaction Details Service will notify the Mobile Payment App of new transaction details via the Token Requestor, using the Notify Transaction Details API (see Section 3.3.2). Each Token must be individually registered with the Transaction Details Service to receive notifications.

7.2.2.2 URL Endpoint

/register

7.2.2.3 HTTP Method

POST

7.2.2.4 Request Parameters

tokenUniqueReference	
Description:	The Token for which to register for transaction details. Must be a valid reference as assigned by MDES.
Data Type:	String
Max Length:	64
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

registrationHash	
Description:	The SHA-256 hash generated from the registration codes.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	64 (Exact)
Required:	Yes

7.2.2.5 Response Values

authenticationCode	
Description:	The authentication code used subsequently to access the service.
Data Type:	String
Max Length:	64
Required:	Yes

tdsUrl	
Description:	The URL used to get transaction details. The Mobile Payment App should store URL for future use to access the Transaction Details Service. Must be provided as: host[:port][/contextRoot] Where port and contextRoot are optional. If contextRoot is not provided, the default (per the URL Scheme) is assumed and must be used.
Data Type:	String
Max Length:	128
Required:	Yes

7.2.2.6 Examples

7.2.2.6.1 Sample Request

```
{
      "tokenUniqueReference" : "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
      "registrationHash" :
"a7265919d0e8e8b44f955e8a38afbc80aab800a699959f31a992050633b44ff7"
}
```

7.2.2.6.2 Sample Response

```
{
"responseHost" : "site1.Mastercard.com",
      "authenticationCode" : "800200c9-629d-11e3-949a-0739d27e5a66",
"tdsUrl" : "loadbalanced.Mastercard.com"
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

7.2.3 Get Transactions

7.2.3.1 Overview

This API is used by the Mobile Payment App to get recent transactions for one or more Tokens. To get recent transactions for a specific Token, the Token Unique Reference is optionally provided in the request.

The Mobile Payment App must have already been registered to use the service. If the Mobile Payment App is not yet registered, it must first use the Register API (see Section 7.2.2) to register for the service prior to getting transactions.

This API may be called in response to a notification from the Transaction Details Service, or it may be called independently (for example, in response to the Cardholder manually refreshing the transaction history from the user interface).

This API will also 'roll' the authentication code and return a new authentication code in the response. Any new authentication code returned shall have a 90 day validity after which it expires.

7.2.3.2 URL Endpoint

/getTransactions

7.2.3.3 HTTP Method

POST

7.2.3.4 Request Parameters

tokenUniqueReference	
Description:	The Token for which to get transaction details. Must be a valid reference as assigned by MDES, which is currently registered for the service. If not present, transaction details will be provided for all registered Tokens.
Data Type:	String
Max Length:	64
Required:	No

authenticationCode	
Description:	Authentication code used to access the service. Must be a valid authentication code as provided by the TDS.
Data Type:	String
Max Length:	64
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

lastUpdatedTag

Description:	The 'lastUpdatedTag' as returned in any previous request by the TDS. This can optionally be used to filter the list of records to be returned – when supplied, the transaction details returned shall be filtered to include only those transactions which are new or have been updated since that 'lastUpdatedTag' was returned. Note that the 'lastUpdatedTag' is not bound to a specific 'tokenUniqueReference'. The 'lastUpdatedTag' also has no time limit so any 'lastUpdatedTag' from any previous request shall be honored.
Data Type:	String
Max Length:	128
Required:	No

7.2.3.5 Response Values

authenticationCode

Description:	New authentication code. The authentication code may be 'rolled' on every use.
Data Type:	String
Max Length:	64
Required:	Yes

lastUpdatedTag

Description:	Opaque value to be optionally supplied in the next call to filter the list of records returned. See the 'lastUpdatedTag' definition in the request for more information on usage.
Data Type:	String
Max Length:	128
Required:	No

transactions

Description:	All the transaction details for the Token, filtered by the 'lastUpdatedTag' if one was provided in the request.
Data Type:	Array[TransactionDetails object]
Max Length:	N/A
Required:	Yes

7.2.3.6 Examples

7.2.3.6.1 Sample Request

```
{
       "tokenUniqueReference" : "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
       "authenticationCode" : "800200c9-629d-11e3-949a-0739d27e5a66",
       "lastUpdatedTag" : "eXl5eS1NTS1kZCdUJ0hIOm1tOnNzWg=="
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
}
```

7.2.3.6.2 Sample Response

```
{
"responseHost" : "site2.Mastercard.com",
      "authenticationCode" : "800200c9-629d-11e3-949a-0739d27e5a66",
      "lastUpdatedTag" : "eXl5eS1NTS1kZCdUJ0hIOm1tOnNzWg==",
      "transactions" : [
            {
                  "tokenUniqueReference" :
"DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
                  "recordId" : "123456",
"transactionIdentifier" :
"6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b",
"transactionType" : "PURCHASE",
"amount" : 123.45,
"currencyCode" : "USD",
"authorizationStatus" : "CLEARED",
"transactionTimestamp" : "2014-12-25T12:00:00.000-07:00",
"merchantName" : "Bob's Burgers",
"merchantType" : "5812",
"merchantPostalCode" : "61000"
            },
            {
                  "tokenUniqueReference" :
"DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
                  "recordId" : "123457",
"transactionIdentifier" :
"d4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35",
"transactionType" : "REFUND",
"amount" : -54.23,
"currencyCode" : "USD",
"authorizationStatus" : "CLEARED",
"transactionTimestamp" : "2014-12-25T12:01:32.000-07:00",
"merchantName" : "Bob's Burgers",
"merchantType" : "5812",
"merchantPostalCode" : "61000"
            },
{
                  "tokenUniqueReference" :
"DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
                  "recordId" : "123458",
"transactionIdentifier" :
"4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b49fce",
"transactionType" : "PURCHASE",
"amount" : 10.1,
"currencyCode" : "USD",
"authorizationStatus" : "REVERSED",
"transactionTimestamp" : "2014-12-26T12:05:10.000-07:00",
"merchantName" : "Bob's Burgers",
"merchantType" : "5812",
"merchantPostalCode" : "61000"
            }
      ]
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

7.2.4 Unregister

7.2.4.1 Overview

This API is used by the Mobile Payment App to unregister a specific Token from the Transaction Details Service, or to opt out of the Transaction Details Service altogether.

To unregister for a specific Token, the Token Unique Reference is optionally provided in the request. The specified Token will be unregistered from the service, but the authentication code remains valid for retrieval of transaction details for other Tokens that have not been unregistered.

If no Token Unique Reference is specified, all Tokens will be unregistered and the authentication code is revoked to prevent further access to the service. The Mobile Payment App can opt back into the service later by using the Register API (see Section 7.2.2) again.

Note that the deactivation of a Token does not automatically unregister the Token from the Transaction Details Service.

7.2.4.2 URL Endpoint

/unregister

7.2.4.3 HTTP Method

POST

7.2.4.4 Request Parameters

tokenUniqueReference	
Description:	The Token for which to unregister from transaction details. Must be a valid reference as assigned by MDES, which is currently registered for the service. If not present, all Tokens for the Mobile Payment App instance will be unregistered.
Data Type:	String
Max Length:	64
Required:	No

authenticationCode	
Description:	Authentication code used to access the service. Must be a valid authentication code as provided by the TDS.
Data Type:	String
Max Length:	64
Required:	Yes

7.2.4.5 Response Values

Only common response elements.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

7.2.4.6 Examples

7.2.4.6.1 Sample Request

```
{
       "tokenUniqueReference" : "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
       "authenticationCode" : "800200c9-629d-11e3-949a-0739d27e5a66"
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

7.2.5 Get System Health

7.2.5.1 Overview

This API is used to check the general status of a Transaction Details API host.

A successful response contains an HTTP response code of 200 with an empty body, and indicates that the service is running and accepting requests.

Note that this API may only be used by authenticated clients – it is not generally accessible publicly.

7.2.5.2 URL Endpoint

/health

Note that paymentAppInstanceId is omitted from the URL scheme for this API.

7.2.5.3 HTTP Method

GET

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

7.3 Transaction Identifier Algorithm

7.3.1 Overview

A transaction details record returned by the Transaction Details Service contains a unique Transaction Identifier that is calculated as a hash of dynamic data from the transaction.

When the transaction is first generated by the Mobile Payment App, it calculates the Transaction Identifier from the transaction data. When the same transaction data is received by the Transaction Details Service, it also performs the same calculation and stores the Transaction Identifier with the transaction details record. When the Mobile Payment App is notified of the transaction (using the Notify Transaction Details API – see Section 3.3.2) and calls the Get Transactions API (see Section 7.2.3) to fetch transaction details, the Transaction Identifier can be used by the Mobile Payment App to match the original transaction event (for example: contactless tap, or a DSRP payment) to the transaction details record provided by the Transaction Details Service.

Note that it may not always be possible to calculate a Transaction Identifier – in these cases, it is recommended that the client uses other transaction data (such as the amount, timestamp) for matching purposes. There are also cases where there may not be a transaction event on the Mobile Payment App (for example, refunds) – in these cases, the Transaction Identifier will also be omitted.

There are three variations of the Transaction Identifier Algorithm, and are as specified below:

1. Algorithm for M/Chip transactions (contactless and DSRP with full EMV data)
2. Algorithm for Magnetic Stripe transactions (contactless and Dynamic Magnetic Stripe Data)
3. Algorithm for DSRP transactions with UCAF data

7.3.2 Algorithm for M/Chip transactions

7.3.2.1 Applicability

This algorithm applies to:

- Contactless M/Chip transactions
- DSRP transactions with full EMV data:

7.3.2.2 Definition

SHA-256 (Token PAN || ATC || Application Cryptogram)

Where:

- **||** represents concatenation of byte arrays
- **Token PAN** is encoded per EMV specifications tag '5A' as a compressed numeric – two numeric digits (having values in the range Hex '0' to '9') per byte, which are

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

left justified and padded with trailing hexadecimal 'F's. To avoid any possible ambiguity, any excessive trailing 'FF' bytes are trimmed from the end so that the Token PAN contains a maximum of one 'F' nibble at the end when the PAN has an odd length.

- **ATC** is the Application Transaction Counter, exactly two bytes and encoded per EMV specifications tag '9F36'.
- **Application Cryptogram** is exactly eight bytes and encoded per EMV specifications tag '9F26'.
- All input fields are mandatory – if any input field is missing or otherwise unavailable, then the Transaction Identifier is not calculated.

7.3.2.3 Example

Given:

- Token PAN (numeric value): 123456789012345
- ATC (hex value): 0001
- Application Cryptogram (hex value): 1122334455667788

Then:

1. Encode the Token PAN as compressed numeric with only a single trailing 'F' nibble and no excessive trailing 'FF' bytes, giving an 8-byte hex value of 123456789012345F
2. Concatenate the three byte arrays together, giving an 18-byte hex value of 123456789012345F00011122334455667788
3. SHA-256 hash the 18-byte value to give a Transaction Identifier value of 94e09c05c05aa8d183d14aeac628ebb7c0325e80881811f2ac53e81db86eb0b6

7.3.3 Algorithm for Magnetic Stripe transactions

7.3.3.1 Applicability

This algorithm applies to:

- Contactless magnetic stripe transactions
- Dynamic Magnetic Stripe Data transactions

7.3.3.2 Definition

16-LSB (SHA-256 (Track 1 Data)) || 16-LSB (SHA-256 (Track 2 Data))

Where:

- **16-LSB** represents an operation to take the 16 least significant bytes
- **||** represents concatenation of byte arrays

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

- **Track 1 Data** is encoded in ASCII format excluding the start sentinel, end sentinel, and Longitudinal Redundancy Check (LRC). All other separator and special characters including spaces are preserved.
- **Track 2 Data** is encoded in binary format excluding the start sentinel, end sentinel, and Longitudinal Redundancy Check (LRC); generally following the compressed numeric format with two numeric digits (having values in the range Hex '0' to '9') per byte; Field Separator encoded as a single 'D' nibble; and odd length data padded with a single trailing 'F' nibble.
- **Partial matching must be supported** – it is conceivable the Transaction Details Service only has one of either the Track 1 Data or Track 2 Data available. To cater for this scenario, the first or last 16 bytes shall be filled with zeroes. The Mobile Payment App must accept a partial match of either the first 16 or last 16 bytes if the rest of the data is filled with zeroes.
- If both Track 1 Data and Track 2 Data are missing, then the Transaction Identifier is not calculated.

7.3.3.3 Example

Given:

- Track 1 Data (ASCII value – note the two spaces):
  B1234987623458765^RULES/MDES ^1509123000000000
- Track 2 Data (ASCII value): 1234987623458765=15091230000000000000

Then:

1. SHA-256 hash the 47-byte Track 1 Data, giving a hex value of
   272d11c54b10af21bd1c2e93cfa7cfbbea6fe411a4307fcff5f10f039d1f74f5
2. Encode the Track 2 Data as compressed numeric, giving a 19-byte hex value of
   1234987623458765D150912300000000000000F
3. SHA-256 hash the 19-byte value, giving a hex value of
   b75c0ff874d16e55727b0a498b3306cea334daeee4f7a991c5def7510ed4fb04
4. Take the least significant 16 bytes of each hash and concatenate them together to form the Transaction Identifier value of
   ea6fe411a4307fcff5f10f039d1f74f5a334daeee4f7a991c5def7510ed4fb04.

Note that partial matching must be supported, so the following values would also be considered a match:

- 00000000000000000000000000000000a334daeee4f7a991c5def7510ed4fb04
- ea6fe411a4307fcff5f10f039d1f74f500000000000000000000000000000000

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

7.3.4 Algorithm for DSRP transactions with UCAF data

7.3.4.1 Applicability

This algorithm applies to:

- DSRP transactions with UCAF data

7.3.4.2 Definition

SHA-256 (Token PAN || UCAF)

Where:

- || represents concatenation of byte arrays
- **Token PAN** is encoded per EMV specifications tag '5A' as a compressed numeric – two numeric digits (having values in the range Hex '0' to '9') per byte, which are left justified and padded with trailing hexadecimal 'F's. To avoid any possible ambiguity, any excessive trailing 'FF' bytes are trimmed from the end so that the Token PAN contains a maximum of one 'F' nibble at the end when the PAN has an odd length.
- **UCAF** is encoded in binary format (before applying any base-64 or other encoding when being sent on to the Mastercard network).

7.3.4.3 Example

Given:

- Token PAN (numeric value): 5413339000001513
- UCAF (base64 value): AHRbjBgsn2DeAAXsy27/AgBVFA==

Then:

1. Encode the Token PAN as compressed numeric, giving an 8-byte hex value of 5413339000001513
2. Encode the UCAF as binary, giving a 19-byte hex value of 00745B8C182C9F60DE0005ECCB6EFF02005514
3. Concatenate the two values together to form a 27-byte hex value of 5413339000001513007 45B8C182C9F60DE0005ECCB6EFF02005514
4. SHA-256 hash the 27-byte value, giving a Transaction Identifier value of f2a491c260e132989522d3748dfcce9361d74e821ca40dda43b74d9ca470546a

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

8 Remote Transaction API

8.1 General

8.1.1 API Design Principles

The Remote Transaction APIs are designed as 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 will specify the HTTP Method used to access it. All strings in request and response objects are to be UTF-8 encoded. Each API URI includes the major and minor version of API that it conforms to. This will allow multiple concurrent versions of the API to be deployed simultaneously.

The client must handle any standard HTTP response code that could result from a web service call including but not limited to 302, 401, 404, or 500.

All APIs return an HTTP response code of 200 if the call was successfully received and accepted for processing. Any errors that subsequently occur during processing are returned in the response payload (see Sections 8.1.4 and 8.1.5 for more information on error code elements and error handling).

To ensure forward-compatibility, all API client implementations must be resilient to new elements being added to outbound requests and responses from MDES.

8.1.2 URL Scheme

All API URLs follow the format:

scheme://host[:port]/contextRoot/api/majorVer/minorVer/apiName

URL Element	Definition
scheme	https
host[:port]	Hostname (and port number if required) for the environment. services.Mastercard.com
contextRoot	mdes
api	remotetransaction
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

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

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.

8.1.3 Security Overview and Encryption

All communication between the client and the Credentials Management Dedicated will be secured using mutually authenticated TLS.

8.1.4 API Request / Response Common Elements and Headers

All requests and responses from MDES contain an element ‘responseHost’. This identifies the specific MDES host that originated a request or response. It should be used by the client in the URL for future calls in order to direct the call to a specific host. As MDES is deployed in a dual active environment, this ensures that when a client makes a series of API calls, they must direct all calls within the same conversation to the same host. This minimizes the risk of some calls being routed to a different site, where data from a previous call may not yet have been replicated. When a conversation is complete, the client should revert back to the default host (provided during onboarding) to ensure that it is not locked permanently to one host.

The client may also provide its 'responseHost' in requests and responses originating from the client, and MDES will honor the responseHost per the above. Note that all valid client hosts must be pre-configured in MDES. Should a 'responseHost' value be submitted that is not yet configured, MDES will respond with an error.

In addition every inbound and outbound request contains an element ‘requestId’ which uniquely identifies the request. Every response contains an element ‘responseId’ which uniquely identifies the response. The responseId may optionally use the corresponding requestId. Note that the format and uniqueness of the requestId and responseId are not necessarily validated on the Remote Transaction API.

In the case of an operation reporting an error, a response contains one or more errors with the elements ‘errorCode’ and ‘errorDescription’ as defined in Section 8.1.5. Unless explicitly stated otherwise, other elements (including 'Required' fields) are not present if an error is reported.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

8.1.4.1 Common Request Elements

responseHost	
Description:	The host that originated the request. Future calls in the same conversation may be routed to this host. Must be provided as: host[:port][/contextRoot] Where port and contextRoot are optional. If contextRoot is not provided, the default (per the URL Scheme) is assumed and must be used.
Data Type:	String
Max Length:	64
Required:	No

requestId	
Description:	Unique identifier for the request.
Data Type:	String
Max Length:	64
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

8.1.4.2 Common Response Elements

responseHost	
Description:	The host that originated the response. Future calls in the same conversation must be routed to this host. Must be provided as: host[:port][/contextRoot] Where port and contextRoot are optional. If contextRoot is not provided, the default (per the URL Scheme) is assumed and must be used.
Data Type:	String
Max Length:	64
Required:	Conditional – See Section 8.1.4. In Production, the responseHost supplied by MDES must be used by the client for future API calls within a conversation. When the conversation is complete, the client will revert back to the default host supplied during onboarding.

responseId	
Description:	Unique identifier for the response.
Data Type:	String
Max Length:	64
Required:	Yes

errors	
Description:	One or more errors for the reasons the operation failed.
Data Type:	Array[Error object]
Max Length:	N/A
Required:	Conditional – required if one or more errors occurred performing the operation.

8.1.5 Error Codes

Error Code	Error Description	Detail
INVALID_JSON	Invalid JSON	The JSON could not be parsed.
AUTHORIZATION_FAILED	Authorization failed.	The request failed to present a valid cert to access the API.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

Error Code	Error Description	Detail
INVALID_FIELD_FORMAT	Invalid Field Format - {fieldName}	The field is not in the correct format. For instance, it should be a number but is a string.
INVALID_FIELD_LENGTH	Invalid Field Length - {fieldName}	The value does not fall between the minimum and maximum length for the field.
INVALID_FIELD_VALUE	Invalid Field Value - {fieldName}	The value is not allowed for the field.
INVALID_RESPONSE_HOST	Invalid Response Host	The requested response host is invalid.
MISSING_REQUIRED_FIELD	Missing Required Field - {fieldName}	A required field is missing.
CRYPTOGRAPHY_ERROR	Cryptography Error	There was an error decrypting the encrypted payload.
INTERNAL_SERVICE_FAILURE	Internal Service Failure	MDES had an internal exception.
INVALID_TOKEN_UNIQUE_REFERENCE	Invalid Token Unique Reference	The token unique reference could not be found or does not match the details provided.
INVALID_TOKEN_STATUS	Invalid Token status.	The token is in an invalid status for the requested operation. For instance, trying to transact with a suspended token.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

8.2 Inbound APIs (to MDES)

8.2.1 Transact

8.2.1.1 Overview

This API is used by the Token Requestor to create a Digital Secure Remote Payment ("DSRP") transaction cryptogram using the credentials stored within MDES in order to perform a DSRP transaction. The entire response is encrypted.

The caller may only transact using the Tokens belonging to them.

8.2.1.2 URL Endpoint

/transact

8.2.1.3 HTTP Method

POST

8.2.1.4 Request Parameters

tokenUniqueReference

Description:	Globally unique identifier for the Token, as assigned by MDES.
Data Type:	String
Max Length:	64
Required:	Yes

dsrpType

Description: What type of DSRP cryptogram to create.
Must be one of:

Value	Meaning
UCAF	Universal Cardholder Authentication Field (Data Element 48 Subelement 43)
M_CHIP	M/Chip ICC data (Data Element 55) Valid only if M/Chip data generation is enabled for the DSRP application for the given tokenUniqueReference

Data Type:	String
Max Length:	64
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

unpredictableNumber	
Description:	Value provided by the merchant or wallet server to provide variability and unique to the generation of a cryptogram.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	8 (Exact)
Required:	Yes

amount	
Description:	Transaction amount to be authorized. Note that refund transactions are not supported – this value must be a positive amount and can contain up to 12 digits, inclusive of any digits in the currency exponent.
Data Type:	Number (greater or equal to zero)
Max Length:	13
Required:	Conditional – required if dsrpType = M_CHIP. Not present otherwise.

currencyCode	
Description:	The transaction currency. Expressed as a 3-character ISO 4217 currency code.
Data Type:	String
Max Length:	3 (Exact)
Required:	Conditional – required if dsrpType = M_CHIP. Not present otherwise.

8.2.1.5 Response Values

encryptedPayload	
Description:	Contains an encrypted TransactRequest object.
Data Type:	EncryptedPayload Object encrypted using the Wallet Provider Public Key containing a TransactRequest object
Max Length:	N/A
Required:	Yes

8.2.1.6 Examples

8.2.1.6.1 Sample Request (UCAF)

```
{
    "requestId": "111111",
    "tokenUniqueReference": "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
    "dsrpType": "UCAF",
    "unpredictableNumber": "A1B2C3D4"
}
```

8.2.1.6.2 Sample Request (M/Chip)

```
{
    "requestId": "222222",
    "tokenUniqueReference": "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

```
    "dsrpType": "M_CHIP",
    "amount": 10.99,
    "currencyCode": "USD",
    "unpredictableNumber": "A1B2C3D4"
}
```

8.2.1.6.3 Sample Response (UCAF)

```
{
  "responseId" : "123456",
  "encryptedPayload" : {
"encryptedData" :
"4545433044323232363739304532433610DE1D1461475BEB6D815F31764DDC20298BD779FBE37EE5AB3C
BDA9F9825E1DDE321469537FE461E824AA55BA67BF6A",
"publicKeyFingerprint" :  "4c4ead5927f0df8117f178eea9308daa58e27c2b",
"encryptedKey" : "A1B2C3D4E5F6112233445566",
"oaepHashingAlgorithm" : "SHA512"
  }
}
```

8.2.1.6.4 Sample contents of encryptedData in encryptedPayload

```
{
      "accountNumber": "5480981500100002",
      "applicationExpiryDate": "181130",
      "panSequenceNumber": "01",
      "track2Equivalent": "5480981500100002D18112011000000000000F",
      "de48se43Data": "112233445566778899001122334455667788 99"
}
```

8.2.1.6.5 Sample Response (M/Chip)

```
{
  "responseId" : "123456",
  "encryptedPayload" : {
"encryptedData" :
"4545433044323232363739304532433610DE1D1461475BEB6D815F31764DDC20298BD779FBE37EE5AB3C
BDA9F9825E1DDE321469537FE461E824AA55BA67BF6A",
"publicKeyFingerprint" :  "4c4ead5927f0df8117f178eea9308daa58e27c2b",
"encryptedKey" : "A1B2C3D4E5F6112233445566",
"oaepHashingAlgorithm" : "SHA512"
  }
}
```

8.2.1.6.6 Sample contents of encryptedData in encryptedPayload

```
{
      "accountNumber": "5480981500100002",
"applicationExpiryDate": "181130",
      "panSequenceNumber": "01",
      "track2Equivalent": "5480981500100002D18112011000000000000F",
      "de55Data" :
"1122334455667788990011223344556677889900112233445566778899001122
3344556677889900"
}
```

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

8.2.2 Get System Health

8.2.2.1 Overview

This API is used to check the general status of a Remote Transaction API host.

A successful response contains an HTTP response code of 200 with an empty body, and indicates that the service is running and accepting requests.

8.2.2.2 URL Endpoint

/health

8.2.2.3 HTTP Method

GET

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

Appendix A Common Objects

A.1 ~~ActivationMethod~~ (deprecated – use AuthenticationMethod)

id

Description: Unique identifier assigned to this Activation Method.

Data Type: Number

Max Length: 32

Required: Yes

type

Description: Specifies the activation method type.

Must be one of:

Type	Meaning	Value Required
TEXT_TO_CARDHOLDER_NUMBER	Text message to Cardholder's mobile phone number. Value will be the Cardholder's masked mobile phone number.	Yes
EMAIL_TO_CARDHOLDER_ADDRESS	Email to Cardholder's email address. Value will be the Cardholder's masked email address.	Yes
CARDHOLDER_TO_CALL_AUTOMATED_NUMBER	Cardholder-initiated call to automated call center phone number. Value will be the phone number for the Cardholder to call.	Yes
CARDHOLDER_TO_CALL_MANNED_NUMBER	Cardholder-initiated call to manned call center phone number. Value will be the phone number for the Cardholder to call.	Yes
CARDHOLDER_TO_VISIT_WEBSITE	Cardholder to visit a website. Value will be the website URL.	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

	CARDHOLDER_TO_USE_MOBILE_APP	Cardholder to use a specific mobile app to activate Token. Value will be a String containing a JSON object AndroidIntent. This AndroidIntent contains an extraTextValue of type MobileAppActivationParameters	Yes
	ISSUER_TO_CALL_CARDHOLDER_NUMBER	Issuer-initiated voice call to Cardholder's phone. Value will be the Cardholder's masked voice call phone number.	Yes

Data Type: String

Max Length: 64

Required: Conditional – required in Digitize Response

value

Description: Specifies the activation method value (meaning varies depending on the activation method type).

Data Type: String

Max Length: N/A

Required: Conditional – required in Digitize response depending on 'type'.

A.2 AlternatePaymentCredentialsRequest

tokenNumber

Description: The Token PAN.

Data Type: String (Numeric)

Max Length: 19 (min length 9)

Required: Yes

tokenExpiry

Description: Expiry date for the Token. Expressed in YYMM format.

Data Type: String (Numeric)

Max Length: 4 (Exact)

Required: Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

cryptographicData

Description:	The cryptographic data being swapped with alternate payment credentials. Cryptographic data must have the format of Digital Secure Remote Payment cryptogram expected in an Authorization Request/0100 message or in an Financial Transaction Request/0200 message in DE 48, subelement 43 (Universal Cardholder Authentication Field (UCAF)).
Data Type:	String
Max Length:	28
Required:	Yes

dataValidUntilTimestamp

Description:	The date/time after which this encrypted payload object is considered invalid. If present, all systems must reject this encrypted object after this time and treat it as invalid data. 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. 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

A.3 AndroidIntent

action

Description:	The name of the action to be performed. This is a fully qualified name including the package name in order to create an explicit intent.
Data Type:	String
Max Length:	128
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

packageName	
Description:	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 can be used to open a link to the appropriate Android app store for the user to download and install the app.
Data Type:	String
Max Length:	128
Required:	Yes

extraTextValue	
Description:	Contains the data to be passed through to the target app in the intent as an extra key/value pair with key 'android.intent.extra.TEXT'. This is Base64-encoded data of a JSON object. The object type of this extraTextValue will depend on context, and is documented wherever AndroidIntent is being used.
Data Type:	String. Base64-encoded data.
Max Length:	N/A
Required:	Yes

A.4 APDUCommand

messageId	
Description:	Uniquely identifies this command within a set of commands in the provisioning data.
Data Type:	String
Max Length:	64
Required:	Yes

apduCommand	
Description:	The APDU command to be submitted to the secure element.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	2000
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

A.5 APDUResponse

messageId

Description: Correlates to the messageId in the original command.

Data Type: String

Max Length: 64

Required: Yes

apduResponse

Description: The APDU response from the secure element.

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

Max Length: 2000

Required: Yes

A.6 ApplicableCardInfo

isSecurityCodeApplicable

Description: Whether a CVC2 is applicable for this card product being digitized.
Must be one of:

Value	Meaning
true	CVC2 is applicable
false	CVC2 is not applicable

Data Type: Boolean

Max Length: 5

Required: Yes

~~A.7~~ AuthenticationMethod

id

Description: Unique identifier assigned to this Authentication Method.

Data Type: Number

Max Length: 32

Required: Yes

type

Description: Specifies the authentication method type.
Must be one of:

Type	Meaning	Value Required

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

	TEXT_TO_CARDHOLDER_NUMBER	Text message to Cardholder's mobile phone number. Value will be the Cardholder's masked mobile phone number.	Yes
	EMAIL_TO_CARDHOLDER_ADDRESS	Email to Cardholder's email address. Value will be the Cardholder's masked email address.	Yes
	CARDHOLDER_TO_CALL_AUTOMATED_NUMBER	Cardholder-initiated call to automated call center phone number. Value will be the phone number for the Cardholder to call.	Yes
	CARDHOLDER_TO_CALL_MANNED_NUMBER	Cardholder-initiated call to manned call center phone number. Value will be the phone number for the Cardholder to call.	Yes
	CARDHOLDER_TO_VISIT_WEBSITE	Cardholder to visit a website. Value will be the website URL.	Yes
	CARDHOLDER_TO_USE_ISSUER_MOBILE_APP	Cardholder to use a specific mobile for authentication. Value will be an IssuerMobileApp object with the applicable activation app method for the device.	Yes
	ISSUER_TO_CALL_CARDHOLDER_NUMBER	Issuer-initiated voice call to Cardholder's phone. Value will be the Cardholder's masked voice call phone number.	Yes
Data Type:	String		
Max Length:	64		
Required:	Conditional – required in Digitize or Tokenize Response		

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

value	
Description:	Specifies the authentication method value (meaning varies depending on the authentication method type).
Data Type:	String
Max Length:	N/A
Required:	Conditional – required in Digitize or Tokenize response depending on 'type'.

A.8 BillingAddress

line1	
Description:	First line of the billing address.
Data Type:	String
Max Length:	64
Required:	No

line2	
Description:	Second line of the billing address.
Data Type:	String
Max Length:	64
Required:	No

city	
Description:	The city of the billing address.
Data Type:	String
Max Length:	32
Required:	No

countrySubdivision	
Description:	The country subdivision (for example, the state in the U.S.) of the billing address.
Data Type:	String
Max Length:	12
Required:	No

postalCode	
Description:	The postal code (for example, zipcode in the U.S.) of the billing address.
Data Type:	String
Max Length:	16
Required:	No

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

country

Description:	The country of the billing address. Expressed as a 3-letter (alpha-3) country code as defined in ISO 3166-1.
Data Type:	String
Max Length:	3 (Exact)
Required:	No

A.9 CardInfo

panUniqueReference

Description:	For repeat digitizations, the unique reference allocated to the Account Primary Account Number. When supplied, the tokenUniqueReferenceForPanInfo, accountNumber, expiryMonth and expiryYear are omitted from CardInfoData.
Data Type:	String
Max Length:	64
Required:	Conditional – optional in a Check Eligibility or Tokenize request, not present otherwise. Only allowed if tokenUniqueReferenceForPanInfo is not present and encrypted data does not contain the account information.

tokenUniqueReferenceForPanInfo

Description:	For repeat digitizations, the unique reference allocated to the token will be used to retrieve the account number and expiration date. When supplied, the panUniqueReference, accountNumber, expiryMonth and expiryYear are omitted from CardInfoData.
Data Type:	String
Max Length:	64
Required:	Conditional – optional in a Check Eligibility or Tokenize request, not present otherwise. Only allowed if panUniqueReference is not present and encrypted data does not contain the account information.

~~certificateFingerprint~~

Description:	The certificate fingerprint identifying the public key used to encrypt the ephemeral AES key.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	64
Required:	**Deprecated** – use publicKeyFingerprint instead.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

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:	Conditional – required if encryptedData is present

encryptedKey

Description:	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).
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	512
Required:	Conditional – required if encryptedData is present

oaepHashingAlgorithm

Description: 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:

Value	Meaning
SHA256	Use the SHA-256 algorithm
SHA512	Use the SHA-512 algorithm

Data Type:	String
Max Length:	6
Required:	No.

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

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

encryptedData	
Description:	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. (See also C.1 Encryption of PCI/PII Sensitive Data)
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	256 K
Required:	Conditional – required if panUniqueReference and tokenUniqueReferenceForPanInfo are not present

A.10 CardInfoData

accountNumber	
Description:	The Account Primary Account Number of the card to be digitized
Data Type:	String (Numeric)
Max Length:	19 (min length 9)
Required:	Conditional – required in a Check Eligibility, Tokenize, or Get Digital Asset request, unless a valid panUniqueReference or tokenUniqueReferenceForPanInfo was given in CardInfo.

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:	Conditional – required in a Check Eligibility or Tokenize request if the card has an expiry date. Not present if a valid panUniqueReference or tokenUniqueReferenceForPanInfo was given in CardInfo.

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:	Conditional – required in a Check Eligibility or Tokenize request if the card has an expiry date. Not present if a valid panUniqueReference or tokenUniqueReferenceForPanInfo was given in CardInfo.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

source

Description: The source of this card information.

Must be one of:

Value	Meaning
CARD_ON_FILE	Source was an existing card on file.
CARD_ADDED_MANUALLY	Source was a new card entered manually be the Cardholder.
CARD_ADDED_VIA_APPLICATION	Source was a new card added by another application (for example, Issuer banking app).

Data Type: String

Max Length: 32

Required: Conditional – required in a Check Eligibility or Tokenize request.

cardholderName

Description: The name of the Cardholder in the format LASTNAME/FIRSTNAME or FIRSTNAME LASTNAME.

Data Type: String

Max Length: 27

Required: Conditional – optional in a Check Eligibility or Tokenize request, not present otherwise.

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: Conditional – optional in a Digitize or Tokenize request, not present otherwise.

billingAddress

Description: The billing address for the card to be digitized. Verified as part of reaching the digitization decision.

Data Type: BillingAddress object

Max Length: N/A

Required: Conditional – optional in a Digitize or Tokenize request, not present otherwise.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

dataValidUntilTimestamp	
Description:	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: 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. 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

consumerIdentifier	
Description:	Consumer Identifier that may be required in some regions or flows.
Data Type:	String
Max Length:	88
Required:	Conditional – may be present in Digitize request, not present otherwise.

A.11 DigitizeResponsePayload

paymentAccountReference	
Description:	The PAR assigned to the PAN.
Data Type:	String(AlpahaNumeric)
Max Length:	29 (Exact)
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

dataValidUntilTimestamp

Description:	The date/time after which this encrypted payload object is considered invalid. If present, all systems must reject this encrypted object after this time and treat it as invalid data. 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. 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

A.12 EligibilityReceipt

value

Description:	The Eligibility Receipt value to be passed back to MDES in the Digitize API (see Section 3.2.2). MDES guarantees the Eligibility Receipt value to be a cryptographically strong random number. Opaque value to be passed back to MDES as is.
Data Type:	String
Max Length:	64
Required:	Yes

validForMinutes

Description:	How long this Eligibility Receipt is valid for, in minutes.
Data Type:	Number
Max Length:	6
Required:	Conditional – required in a Check Eligibility response.

A.13 EncryptedPayload

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

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

encryptedKey

Description: 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).

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

Max Length: 512

Required: Yes

oaepHashingAlgorithm

Description: 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:

Value	Meaning
SHA256	Use the SHA-256 algorithm
SHA512	Use the SHA-512 algorithm

Data Type: String

Max Length: 6

Required: No.

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 an encrypted 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.

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

Max Length: 256 K

Required: Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

A.14 Error

source

Description: An element used to indicate the source of the issue causing this error. Must be one of:

Value	Meaning
INPUT	Service inputs triggered an error.
MDES	MDES reported an error

Data Type: String

Max Length: 32

Required: Yes

errorCode

Description: Only generated by Open API. See Open API documentation for use cases.

Data Type: String

Max Length: 100

Required: No

description

Description: Description of the reason the operation failed.

Data Type: String

Max Length: 256

Required: No

~~**errorDescription**~~

Description: Description of the reason the operation failed.

Data Type: String

Max Length: 256

Required: **Deprecated** – use description instead.

reasonCode

Description: A reason code for the error that has occurred. See Error Reason Code definitions for the appropriate API service.

Data Type: String

Max Length: 100

Required: Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

recoverable	
Description:	Only generated by Open API. See Open API documentation.
Data Type:	Boolean
Max Length:	16
Required:	No

A.15 IssuerMobileApp

openIssuerMobileAppAndroidIntent	
Description:	AndroidIntent object can be used to open the issuer mobile app. This AndroidIntent contains an extraTextValue of type OpenMobileAppParameters
Data Type:	AndroidIntent object (extraTextValue of type OpenMobileAppParameters)
Max Length:	N/A
Required:	Conditional – optional in ProductConfig. Not present otherwise.

activateWithIssuerMobileAppAndroidIntent	
Description:	AndroidIntent object can be used to open the issuer mobile app. This AndroidIntent contains an extraTextValue of type MobileAppActivationParameters
Data Type:	AndroidIntent object (extraTextValue of type MobileAppActivationParameters)
Max Length:	N/A
Required:	Conditional – optional in AuthenticationMethod. Not present otherwise.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

A.16 JsonWebKey

The JsonWebKey object is a JSON Web Key (JWK) data structure as specified in RFC 7517. The following is a subset of JWK parameters as supported by MDES:

kty

Description: The "kty" (key type) parameter identifies the cryptographic algorithm family used with the key, such as "RSA" or "EC".

Must be one of the following supported key types:

Value	Meaning
EC	Elliptic Curve
RSA	RSA

Data Type: String

Max Length: 3

Required: Yes

x5c

Description: The "x5c" (X.509 certificate chain) parameter contains a chain of one or more PKIX certificates. The certificate chain is represented as a JSON array of certificate value strings. Each string in the array is a base64-encoded DER PKIX certificate value. The PKIX certificate containing the key value MUST be the first certificate. This MAY be followed by additional certificates, with each subsequent certificate being the one used to certify the previous one.

Data Type: Array[Base64-encoded String]

Max Length: N/A

Required: Yes

A.17 MediaContent

type

Description: What type of media this is. Specified as a MIME type, which will be one of the following supported types:

Value	Any additional meaning
application/pdf	For images, must be a vector PDF image.
image/png	Includes alpha channel
text/plain	
text/html	

Data Type: String

Max Length: 32

Required: Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

data	
Description:	The data for this item of media. Base64-encoded data, given in the format as specified in 'type'
Data Type:	String
Max Length:	N/A
Required:	Yes
width	
Description:	For image assets, the width of this image. Specified in pixels.
Data Type:	String (Numeric)
Max Length:	6
Required:	Conditional – required only for images.
height	
Description:	For image assets, the height of this image. Specified in pixels.
Data Type:	String (Numeric)
Max Length:	6
Required:	Conditional – required only for images.

A.18 MobileAppActivationParameters

paymentAppProviderId	
Description:	Globally unique identifier for the Wallet Provider, as assigned by MDES. Commonly known as the Wallet Identifier.
Data Type:	String
Max Length:	64
Required:	Yes
paymentAppInstanceId	
Description:	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization.
Data Type:	String
Max Length:	48
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

tokenUniqueReference	
Description:	Globally unique identifier for the Token to be activated, as assigned by MDES.
Data Type:	String
Max Length:	64
Required:	Yes

accountPanSuffix	
Description:	The last few digits (typically four) of the Account PAN being digitized.
Data Type:	String
Max Length:	8
Required:	Yes

accountExpiry	
Description:	The expiry of the Account PAN being digitized, given in MMYY format.
Data Type:	String
Max Length:	4
Required:	Yes

A.19 MobileKeys

transportKey	
Description:	The Mobile Transport Key used to provide confidentiality of data at the transport level between the Mobile Payment App and MDES. This is a 128-bit AES key (M_KEY_CONF as described in Mastercard Cloud-Based Payments – Issuer Cryptographic Algorithms), and is encrypted by the randomly-generated key (RGK) provided by the Mobile Payment App using ECB mode with no padding.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	64
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

macKey	
Description:	The Mobile MAC Key used to provide integrity of data at the transport level between the Mobile Payment App and MDES. This is a 128-bit AES key (M_KEY_MAC as described in Mastercard Cloud-Based Payments – Issuer Cryptographic Algorithms), and is encrypted by the randomly-generated key (RGK) provided by the Mobile Payment App using ECB mode with no padding.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	64
Required:	Yes

dataEncryptionKey	
Description:	The Mobile Data Encryption Key used to encrypt any sensitive data at the data field level between the Mobile Payment App and MDES. This is a 128-bit AES key and is encrypted by the randomly-generated key (RGK) provided by the Mobile Payment App using ECB mode with no padding.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	64
Required:	Yes

A.20 NotificationData

responseHost	
Description:	The host that the Mobile Payment App should route requests to. This allows MDES to control requests related to a specific conversation to the desired location. If omitted, then the default host (provided during registration) should be assumed. Must be provided as: host[:port][/contextRoot] Where port and contextRoot are optional. If contextRoot is not provided, the default (per the URL Scheme) is assumed and must be used.
Data Type:	String
Max Length:	64
Required:	Conditional – required for initial registration, optional otherwise.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

mobileKeysetId	
Description:	Identifies the Mobile Keys used for this remote management session.
Data Type:	String
Max Length:	64
Required:	Yes

encryptedData	
Description:	Contains the encrypted RemoteManagementSessionData object. The plaintext data is prepended with a random 16-byte value before it is encrypted by the Mobile Transport Key using CBC mode padded with '80' followed by '00' bytes until the end of the block. The MAC is then computed over the output, which is appended to the end.
Data Type:	String. Base64-encoded data.
Max Length:	256 K
Required:	Yes

A.21 NotifyTokenUpdatedRequest

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

paymentAppInstanceId	
Description:	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization. This field is alphanumeric and additionally web-safe base64 characters per RFC 4648 (minus "-", underscore "_") up to a maximum length of 48, = should not be URL encoded.
Data Type:	String
Max Length:	48
Required:	Conditional – not applicable for server-based tokens. Required otherwise.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

dataValidUntilTimestamp

Description:	The date/time after which this encrypted payload object is considered invalid. If present, all systems must reject this encrypted object after this time and treat it as invalid data. 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. 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

A.22 OpenMobileAppParameters

paymentAppProviderId

Description:	Globally unique identifier for the Wallet Provider, as assigned by MDES. Commonly known as the Wallet Identifier.
Data Type:	String
Max Length:	64
Required:	Yes

paymentAppId

Description:	Identifier for the Payment App, unique per app as assigned by Mastercard for this Payment App.
Data Type:	String
Max Length:	30
Required:	Yes

paymentAppInstanceId

Description:	Identifier for the specific Mobile Payment App instance, unique across a given Wallet Identifier. This value cannot be changed after digitization.
Data Type:	String
Max Length:	48
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

tokenUniqueReference	
Description:	Globally unique identifier for the Token to be activated, as assigned by MDES.
Data Type:	String
Max Length:	64
Required:	Yes

A.23 PaymentAppRegistrationData

registrationCode	
Description:	A one-time registration code that authorizes the Mobile Payment App to register itself with MDES.
Data Type:	String
Max Length:	64
Required:	Yes

~~publicKey~~	
Description:	The public key to be used to encrypt the randomly-generated key provided by the Mobile Payment App during registration.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	256
Required:	**Deprecated** – use pkCertificateUrl instead.

pkCertificateUrl	
Description:	URL to the public key certificate to be used to encrypt the randomly-generated key provided by the Mobile Payment App during registration. The public key certificate can be downloaded by performing a HTTP GET using the given URL. The certificate will be provided as a file of MIME type "application/pkix-cert" according to RFC 2585.
Data Type:	String
Max Length:	128
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

A.24 ProductConfig

brandLogoAssetId

Description: The Mastercard or Maestro brand logo associated with this card. Provided as an Asset ID – use the Get Asset API (See Section 3.2.5) to retrieve the actual asset.

Data Type: String

Max Length: 64

Required: Yes

issuerLogoAssetId

Description: The logo of the issuing bank. Provided as an Asset ID – use the Get Asset API (See Section 3.2.5) to retrieve the actual asset.

Data Type: String

Max Length: 64

Required: Yes

isCoBranded

Description: Whether the product is co-branded.

Must be one of:

Value	Meaning
true	This is a co-branded product.
false	This is not a co-branded product.

Data Type: String

Max Length: 5

Required: Yes

coBrandName

Description: Textual name of the co-brand partner.

Data Type: String

Max Length: 128

Required: Conditional – required if isCoBranded = "true". Not present otherwise.

coBrandLogoAssetId

Description: The co-brand logo (if any) for this product. Provided as an Asset ID – use the Get Asset API (See Section 3.2.5) to retrieve the actual asset.

Data Type: String

Max Length: 64

Required: No

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

cardBackgroundCombinedAssetId

Description:	The card image used to represent the digital card in the wallet. This 'combined' option contains the Mastercard, bank and any co-brand logos. Provided as an Asset ID – use the Get Asset API (See Section 3.2.5) to retrieve the actual asset.
Data Type:	String
Max Length:	64
Required:	Conditional – either CardBackgroundCombined or CardBackground will be provided.

cardBackgroundAssetId

Description:	The card image used to represent the digital card in the wallet. This 'non-combined' option does not contain the Mastercard, bank, or co-brand logos. Provided as an Asset ID – use the Get Asset API (See Section 3.2.5) to retrieve the actual asset.
Data Type:	String
Max Length:	64
Required:	Conditional – either CardBackgroundCombined or CardBackground will be provided.

iconAssetId

Description:	The icon representing the primary brand(s) associated with this product. Provided as an Asset ID – use the Get Asset API (See Section 3.2.5) to retrieve the actual asset.
Data Type:	String
Max Length:	64
Required:	Yes

foregroundColor

Description:	Foreground color, used to overlay text on top of the card image.
Data Type:	String - Hexadecimal RGB color format (case-insensitive).
Max Length:	6
Required:	Yes

issuerName

Description:	Name of the issuing bank.
Data Type:	String
Max Length:	64
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

shortDescription

Description:	A short description for this product.
Data Type:	String
Max Length:	128
Required:	Yes

longDescription

Description:	A long description for this product.
Data Type:	String
Max Length:	256
Required:	No

customerServiceUrl

Description:	Customer service website of the issuing bank.
Data Type:	String
Max Length:	128
Required:	No

customerServiceEmail

Description:	Customer service email address of the issuing bank.
Data Type:	String
Max Length:	64
Required:	No

customerServicePhoneNumber

Description:	Customer service phone number of the issuing bank.
Data Type:	String
Max Length:	64
Required:	No

issuerMobileApp

Description:	Mobile app of the issuing bank. Contains one or more mobile app details that may be used to deep link from the Mobile Payment App to the issuer mobile app.
Data Type:	IssuerMobileApp object
Max Length:	N/A
Required:	No

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

onlineBankingLoginUrl	
Description:	Logon URL for the issuing bank's online banking website.
Data Type:	String
Max Length:	128
Required:	No
termsAndConditionsUrl	
Description:	URL linking to the issuing bank's terms and conditions for this product.
Data Type:	String
Max Length:	128
Required:	No
privacyPolicyUrl	
Description:	URL linking to the issuing bank's privacy policy for this product.
Data Type:	String
Max Length:	128
Required:	No
issuerProductConfigCode	
Description:	Freeform identifier for this product configuration as assigned by the issuer.
Data Type:	String
Max Length:	64
Required:	No

A.25 RawTransactionCredential

atc	
Description:	Application Transaction Counter unique for this transaction using this set of keys.
Data Type:	Number
Max Length:	5
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

idn

Description:	The ICC dynamic number for this transaction (see Mastercard Cloud-Based Payments – Issuer Cryptographic Algorithms for more information on how this field is derived). Encrypted by a transport key identified by 'kekId' using ECB mode with no padding.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	48
Required:	Yes

contactlessMdSessionKey

Description:	Session key used for mobile device authentication (MD) for contactless transactions (see Mastercard Cloud-Based Payments – Issuer Cryptographic Algorithms for more information on how this field is derived). Encrypted by a transport key identified by 'kekId' using ECB mode with no padding.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	48
Required:	Conditional – required if contactless is supported

contactlessUmdSessionKey

Description:	Session key used for user and mobile device authentication (UMD) for contactless transactions (see Mastercard Cloud-Based Payments – Issuer Cryptographic Algorithms for more information on how this field is derived). Encrypted by a transport key identified by 'kekId' using ECB mode with no padding.
Data Type:	String. Hex-encoded data
Max Length:	48
Required:	Conditional – required if contactless is supported except with a Card-like User Experience, when the Wallet application supports Mobile PIN for DSRP

dsrpMdSessionKey

Description:	Session key used for mobile device authentication (MD) for DSRP transactions (see Mastercard Cloud-Based Payments – Issuer Cryptographic Algorithms for more information on how this field is derived). Encrypted by a transport key identified by 'kekId' using ECB mode with no padding.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	48
Required:	Conditional – required if DSRP is supported

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

dsrpUmdSessionKey	
Description:	Session key used for user and mobile device authentication (UMD) for DSRP transactions (see Mastercard Cloud-Based Payments – Issuer Cryptographic Algorithms for more information on how this field is derived). Encrypted by a transport key identified by 'kekId' using ECB mode with no padding.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	48
Required:	Conditional – required if DSRP is supported

A.26 RawTransactionCredentials

encryptedData	
Description:	Contains an encrypted RawTransactionCredentialsData object. Encrypted using CCM as specified in Mastercard Cloud-Based Payments – Issuer Cryptographic Algorithms.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	256 K
Required:	Yes

ccmNonce	
Description:	The nonce used to CCM encrypt the raw Transaction Credentials data.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	64
Required:	Yes

ccmKeyId	
Description:	The identifier of the key used to CCM encrypt the raw Transaction Credentials data.
Data Type:	String
Max Length:	50
Required:	Yes

ccmMac	
Description:	The message authentication code computed over the data that was encrypted.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	24
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

A.27 RawTransactionCredentialsData

rawTransactionCredentials	
Description:	Contains the raw Transaction Credential data to be replenished.
Data Type:	Array[RawTransactionCredential object]
Max Length:	N/A
Required:	Yes

kekId	
Description:	Identifier for the key used to encrypt the individual MD and UMD session keys and the IDN within the raw Transaction Credentials.
Data Type:	String
Max Length:	50
Required:	Yes

A.28 RemoteManagementSessionData

version	
Description:	Version number of the Mobile Payment APIs. This is not related to the version of this document.
Data Type:	String
Max Length:	16
Required:	Yes

sessionCode	
Description:	The 29-byte remote management session code used by the Mobile Payment App to generate an authentication code and to derive the Mobile Session Keys when communicating with MDES.
Data Type:	String
Max Length:	64
Required:	Yes

expiryTimestamp	
Description:	The date/time when the remote management session code will expire. 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

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

validForSeconds

Description:	The number of seconds after which the remote management session code will expire after first use.
Data Type:	Number
Max Length:	16
Required:	No

pendingAction

Description: The pending action requested by MDES for a Token on the Mobile Payment App.

Must be one of:

Value	Meaning
PROVISION	A new Token credential is ready to be provisioned to the Mobile Payment App
RESET_MOBILE_PIN	The Mobile PIN has been reset. The Mobile Payment App must set a new Mobile PIN.

Data Type:	String
Max Length:	64
Required:	No

tokenUniqueReference

Description:	The Token Credential on which the action is requested. Must be a valid reference as assigned by MDES.
Data Type:	String
Max Length:	64
Required:	Conditional – required if the pendingAction relates to a specific Token. Not present otherwise.

A.29 RnsInfo

gcmRegistrationId

Description:	The Google Cloud Messaging Registration ID.
Data Type:	String
Max Length:	2000
Required:	Conditional – required if the RNS used is Google Cloud Messaging.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

A.30 SeInfo

seId	
Description:	Identifier of the target SE to be provisioned.
Data Type:	String
Max Length:	128
Required:	Yes

seCapabilities	
Description:	Contains information about the capabilities of this SE, which are checked for device eligibility.
Data Type:	Map
Max Length:	N/A
Required:	No

A.31 SpsdInfo

aid	
Description:	The AID for the Service Provider Security Domain.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	64
Required:	Conditional – required in a Check Eligibility request.

appletInstanceAid	
Description:	The AID for the Mastercard applet instance.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	64
Required:	Yes

spsdSequenceCounter	
Description:	The current value of Secure Channel Sequence Counter as maintained by the Security Domain.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	32
Required:	Conditional – required in a Check Eligibility request.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

rgk	
Description:	The randomly-generated key per GlobalPlatform specifications, encrypted by the Mastercard public key (PK.AP.CT) and signed by the CASD; as described in the Mastercard Digital Enablement Service – Embedded Mobile PayPass Payments Configuration Description.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	2000
Required:	Conditional – required in a Check Eligibility request.
casdPkCertificate	
Description:	The public key certificate for the CASD which signs the RGK, used to verify the signature of the RGK. This is CERT.CASD.AUT as described in the Mastercard Digital Enablement Service – Embedded Mobile PayPass Payments Configuration Description.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	2000
Required:	Conditional – one of 'casdPkCertificate', 'casdPkJwk', or 'semsPkCertificate' is required in a Check Eligibility request.
casdPkJwk	
Description:	The public key certificate chain for the CASD which signs the RGK, used to verify the signature of the RGK, provided in JSON Web Key (JWK) format. Note that the trusted root CA is not part of the JWK.
Data Type:	JsonWebKey object.
Max Length:	N/A
Required:	Conditional – one of 'casdPkCertificate', 'casdPkJwk', or 'semsPkCertificate' is required in a Check Eligibility request
semsPkCertificate	
Description:	The public key certificate for a Secure Element Management Service provisioning.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	2000
Required:	Conditional – one of 'casdPkCertificate', 'casdPkJwk', or 'semsPkCertificate' is required in a Check Eligibility request

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

A.32 Token

tokenUniqueReference

Description: The unique reference allocated to the Token.

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:

Value	Meaning
INACTIVE	Token has not yet been activated
ACTIVE	Token is active and ready to transact
SUSPENDED	Token is suspended and unable to transact
DEACTIVATED	Token has been permanently deactivated

Data Type: String

Max Length: 32

Required: Yes

statusTimestamp

Description: The date and time the token status was updated.
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: No

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

suspendedBy

Description: Who or what caused the Token to be suspended.

One or more values of:

Value	Meaning
ISSUER	Suspended by the Issuer.
~~PAYMENT_APP_PROVIDER~~	Suspended by the Payment App Provider. **Deprecated** – use TOKEN_REQUESTOR instead.
TOKEN_REQUESTOR	Suspended by the Token Requestor.
MOBILE_PIN_LOCKED	Suspended due to the Mobile PIN being locked.
CARDHOLDER	Suspended by the Cardholder

Data Type: Array[String]

Max Length: N/A

Required: Conditional – required if status = SUSPENDED.

productConfig

Description: Updated product configuration for the token.

Data Type: ProductConfig object

Max Length: N/A

Required: Conditional – required only if any product configuration has changed, or when querying a specified Token using Get Token (Section 3.2.14). Not present otherwise.

tokenInfo

Description: Updated token information.

Data Type: TokenInfo object

Max Length: N/A

Required: Conditional – required only if any token information has changed, or when querying a specified Token using Get Token (Section 3.2.14). Not present otherwise.

tdsRegistrationUrl

Description: The URL endpoint for the Transaction Details Service.

Must be provided as:

host[:port][/contextRoot]

Where port and contextRoot are optional.

If contextRoot is not provided, the default (per the URL Scheme) is assumed and must be used.

Data Type: String

Max Length: 128

Required: No

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

~~errorCode~~	
Description:	Error code for reason the requested operation failed.
Data Type:	String
Max Length:	32
Required:	**Deprecated** – use errors instead.

~~errorDescription~~	
Description:	Error description for reason the requested operation failed.
Data Type:	String
Max Length:	256
Required:	**Deprecated** – use errors instead.

errors	
Description:	An element used to encapsulate a collection of errors that occurred during a single request.
Data Type:	Array[Error object]
Max Length:	N/A
Required:	Conditional – required if one or more errors occurred performing the operation. Not present if the operation was successful.

A.33 TokenCredential

encryptedData	
Description:	Contains the encrypted TokenCredentialData object. Encrypted using CCM as described in Mastercard Cloud-Based Payments – Issuer Cryptographic Algorithms.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	256 K
Required:	Yes

ccmNonce	
Description:	The nonce used to CCM encrypt the Token Credential data.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	64
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

ccmKeyId	
Description:	The identifier of the key used to CCM encrypt the Token Credential data.
Data Type:	String
Max Length:	50
Required:	Yes
ccmMac	
Description:	The message authentication code computed over the data that was encrypted.
Data Type:	String
Max Length:	24
Required:	Yes

A.34 TokenCredentialData

cardProfile	
Description:	The card profile for this Token Credential.
Data Type:	See Mastercard Digital Enablement Service – Mastercard Cloud-Based Payments Card Profile Specification. Please use the document version that corresponds to the MCBP version supported by the mobile wallet app.
Max Length:	N/A
Required:	Yes
iccKek	
Description:	The 128-bit AES key used to encrypt the ICC private keys in the 'cardProfile'. Provided as a 32-byte field, encrypted by a transport key identified by 'kekId' using ECB mode padded with '80' followed by '00' bytes until the end of the block.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	64
Required:	Conditional. Not present when the profile does not contain contactless data
kekId	
Description:	The identifier for the key used to encrypt 'iccKek'.
Data Type:	String
Max Length:	50
Required:	Conditional. Not present when the profile does not contain contactless data

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

dataValidUntilTimestamp	
Description:	The date/time after which this encrypted payload object is considered invalid. If present, all systems must reject this encrypted object after this time and treat it as invalid data. 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. 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

A.35 TokenDetail

tokenUniqueReference	
Description:	Globally unique identifier for the Token, as assigned by MDES.
Data Type:	String
Max Length:	64
Required:	Yes

publicKeyFingerprint	
Description:	The certificate fingerprint identifying 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 Mastercard public key (as identified by 'publicKeyFingerprint') using the OAEP or RSA Encryption Standard PKCS #1 v1.5 scheme (depending on the value of 'oaepHashingAlgorithm'. 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

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

oaepHashingAlgorithm

Description: 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:

Value	Meaning
SHA256	Use the SHA-256 algorithm
SHA512	Use the SHA-512 algorithm

Data Type: String

Max Length: 6

Required: No.

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 TokenDetailData object. Encrypted by the ephemeral AES key using CBC mode (IV as provided in 'iv', or zero if none provided) and PKCS#7 padding.

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

Max Length: 256 K

Required: Yes

A.36 TokenDetailData

tokenNumber

Description: The Token Primary Account Number of the card

Data Type: String (Numeric)

Max Length: 19 (min length 9)

Required: Conditional – required if tokenType = STATIC

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

expiryMonth	
Description:	The month of the token expiration date.
Data Type:	String (Numeric)
Max Length:	2 (Exact)
Required:	Conditional – required if tokenType = STATIC
expiryYear	
Description:	The year of the token expiration date.
Data Type:	String (Numeric)
Max Length:	2 (Exact)
Required:	Conditional – required if tokenType = STATIC
paymentAccountReference	
Description:	The unique account reference assigned to the PAN. Conditionally returned if the Token Requestor has opted to receive PAR and providing PAR is assigned by Mastercard or the Issuer provides PAR in the authorization message response.
Data Type:	String
Max Length:	29(exact)
Required:	No
dataValidUntilTimestamp	
Description:	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: 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. 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

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

A.37 TokenInfo

tokenPanSuffix

Description: The last few digits (typically four) of the Token PAN.

Data Type: String

Max Length: 8

Required: Yes

accountPanSuffix

Description: The last few digits (typically four) of the Account PAN.

Data Type: String

Max Length: 8

Required: Yes

alternateAccountIdentifierSuffix

Description: The last few digits (typically four) of the Alternate account identifier.

Data Type: String

Max Length: 8

Required: No

tokenExpiry

Description: The expiry of the Token PAN, given in MMYY format.

Data Type: String

Max Length: 4

Required: Yes

dsrpCapable

Description: Whether DSRP transactions are supported by this Token.
Must be one of:

Value	Meaning
true	DSRP capable
false	Not DSRP capable

Data Type: Boolean

Max Length: 5

Required: Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

tokenAssuranceLevel	
Description:	A value indicating the confidence level of the token to Account PAN binding.
Data Type:	Numeric
Max Length:	2
Required:	No

A.38 TokenTransaction

tokenUniqueReference	
Description:	Globally unique identifier for the Token, as assigned by MDES.
Data Type:	String
Max Length:	64
Required:	Yes

transactions	
Description:	Transaction details of the tokenUniqueReference.
Data Type:	Array[TransactionDetails object]
Max Length:	N/A
Required:	Yes

errors	
Description:	An element used to encapsulate a collection of errors that occurred during a single request.
Data Type:	Array[Error object]
Max Length:	N/A
Required:	Conditional – required if one or more errors occurred performing the operation. Not present if the operation was successful.

A.39 TransactionCredential

atc	
Description:	Application Transaction Counter unique for this transaction using this set of keys.
Data Type:	Number
Max Length:	5
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

idn

Description:	The ICC dynamic number for this transaction (see Mastercard Cloud-Based Payments – Issuer Cryptographic Algorithms for more information on how this field is derived). Encrypted by the Mobile Data Encryption Key using ECB mode with no padding.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	48
Required:	Yes

contactlessMdSessionKey

Description:	Session key used for mobile device authentication (MD) for contactless transactions (see Mastercard Cloud-Based Payments – Issuer Cryptographic Algorithms for more information on how this field is derived). Encrypted by the Mobile Data Encryption Key using ECB mode with no padding.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	48
Required:	Conditional – required if contactless is supported

contactlessUmdSessionKey

Description:	Session key used for user and mobile device authentication (UMD) for contactless transactions (see Mastercard Cloud-Based Payments – Issuer Cryptographic Algorithms for more information on how this field is derived). Encrypted by a transport key identified by 'kekId' using ECB mode with no padding.
Data Type:	String. Hex-encoded data
Max Length:	48
Required:	Conditional – required if contactless is supported and the wallet application supports no CDCVM or a locally-verified CDCVM

contactlessUmdSingleUseKey

Description:	Single use key used for user and mobile device authentication (UMD) for contactless transactions (see Mastercard Cloud-Based Payments – Issuer Cryptographic Algorithms for more information on how this field is derived). Encrypted by the Mobile Data Encryption Key using ECB mode with no padding.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	48
Required:	Conditional – required if contactless is supported with Mobile PIN (for contactless User Experiences 'CDCVM Always' and 'Flexible CDCVM')

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

dsrpMdSessionKey	
Description:	Session key used for mobile device authentication (MD) for DSRP transactions (see Mastercard Cloud-Based Payments – Issuer Cryptographic Algorithms for more information on how this field is derived). Encrypted by the Mobile Data Encryption Key using ECB mode with no padding.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	48
Required:	Conditional – required if DSRP is supported

dsrpUmdSessionKey	
Description:	Session key used for user and mobile device authentication (UMD) for DSRP transactions (see Mastercard Cloud-Based Payments – Issuer Cryptographic Algorithms for more information on how this field is derived). Encrypted by a transport key identified by 'kekId' using ECB mode with no padding.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	48
Required:	Conditional – required if DSRP is supported with locally-verified CDCVM

dsrpUmdSingleUseKey	
Description:	Single use key used for user and mobile device authentication (UMD) fo DSRP transactions (see Mastercard Cloud-Based Payments – Issuer Cryptographic Algorithms for more information on how this field is derived). Encrypted by the Mobile Data Encryption Key using ECB mode with no padding.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	48
Required:	Conditional – required if DSRP is supported with Mobile PIN

A.40 TransactionCredentialStatus

atc	
Description:	The Application Transaction Counter (ATC) identifying this Transaction Credential.
Data Type:	Number
Max Length:	5
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

status

Description: The status of this Transaction Credential.

Must be one of:

Value	Meaning
UNUSED_ACTIVE	This Transaction Credential has not yet been used and remains active.
UNUSED_DISCARDED	This Transaction Credential was not used but has been discarded.
USED_FOR_CONTACTLESS	This Transaction Credential has been used for a contactless transaction.
USED_FOR_DSRP	This Transaction Credential has been used for a digital secure remote payment transaction.

Data Type: String

Max Length: 64

Required: Yes

timestamp

Description: The date/time stamp for this status. For UNUSED_ACTIVE credentials, the timestamp must be the current time as the status is being reported. For used or discarded credentials, the timestamp must be the time when the credentials were used or discarded.

Must be 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

A.41 TransactionDetails

tokenUniqueReference

Description: The Token for this transaction.

Data Type: String

Max Length: 64

Required: Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

recordId

Description:	Unique identifier for this transaction record. Opaque value.
Data Type:	String
Max Length:	64
Required:	Yes

transactionIdentifier

Description:	A unique identifier for the transaction that is used to match a transaction event on the device (for example, a contactless tap, or a DSRP payment) to a transaction details record provided by the TDS. See Section 7.3 – Transaction Identifier Algorithm for details of how this identifier is calculated.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	64
Required:	No

transactionType

Description: The transaction type. Must be one of:

Value	Meaning
PURCHASE	Purchase transaction
REFUND	Refund transaction

Data Type:	String
Max Length:	32
Required:	Yes

amount

Description:	The transaction amount. Negative amounts indicate a refund. REFUND transaction types will always have a negative amount.
Data Type:	Number
Max Length:	13
Required:	No

currencyCode

Description:	The transaction currency. This is the local currency at the source location of the transaction.
Data Type:	3-digit ISO 4217 currency code.
Max Length:	3 (Exact)
Required:	Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

authorizationStatus

Description: The authorization status of the transaction. Must be one of:

Value	Meaning
AUTHORIZED	Transaction has been authorized, pending to be cleared.
DECLINED	Transaction was declined.
CLEARED	Transaction has been cleared.
REVERSED	Transaction has been reversed.

Data Type: String

Max Length: 16

Required: Yes

transactionTimestamp

Description: The date/time when the transaction occurred. 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

merchantName

Description: The merchant ("doing business as") name.

Data Type: String

Max Length: 64

Required: No

merchantType

Description: The merchant's type of business or service. Must be a valid Merchant Category Code (MCC).

Data Type: String

Max Length: 4

Required: No

merchantPostalCode

Description: The postal code (for example, zipcode in the U.S.) of the merchant.

Data Type: String

Max Length: 16

Required: No

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

installments

Description: The number of installments for the transaction.

Data Type: Number

Max Length: 3

Required: No

transactionCountryCode

Description: The country in which the transaction was performed. Expressed as a 3-letter (alpha-3) country code as defined in ISO 3166-1.

Data Type: String

Max Length: 3(Exact)

Required: No

comboCardAccountType

Description: Indicator if Credit or Debit was chosen for a tokenized combo card at the time of the transaction.

Value	Meaning
CREDIT	CREDIT was chosen at the time of transaction.
DEBIT	DEBIT was chosen at the time of transaction.

Data Type: String

Max Length: 6

Required: No

A.42 TransactRequest

accountNumber

Description: The Primary Account Number for the transaction – this is the Token PAN.

Data Type: String (Numeric)

Max Length: 19 (min length 9)

Required: Yes

applicationExpiryDate

Description: Application expiry date for the Token. Expressed in YYMMDD format.

Data Type: String (Numeric)

Max Length: 6 (Exact)

Required: Yes

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

panSequenceNumber

Description:	Application PAN sequence number for the Token.
Data Type:	String (Numeric)
Max Length:	2 (Exact)
Required:	Yes

track2Equivalent

Description:	Track 2 equivalent data for the Token. Expressed according to ISO/IEC 7813, excluding start sentinel, end sentinel, and Longitudinal Redundancy Check (LRC), using hex nibble 'D' as field separator, and padded to whole bytes using one hex nibble 'F' as needed.
Data Type:	String. Hex-encoded data (case-insensitive).
Max Length:	38
Required:	Yes

de48se43Data

Description:	Data for DE 48 Subelement 43 containing the cryptogram.
Data Type:	String
Max Length:	32
Required:	Conditional – required if dsrpType = UCAF. Not present otherwise.

de55Data

Description:	Data for DE 55 containing the cryptogram.
Data Type:	String
Max Length:	200
Required:	Conditional – required if dsrpType = M_CHIP. Not present otherwise.

dataValidUntilTimestamp

Description:	The date/time after which this encrypted payload object is considered invalid. If present, all systems must reject this encrypted object after this time and treat it as invalid data. 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. 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

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

Appendix B Maps

B.1 DeviceInfo

deviceName

Description:	The name that the Cardholder has associated to the target provisioned device (or device being provisioned).
Data Type:	String
Max Length:	64
Required:	Conditional – required in a Check Eligibility request, except when Storage Technology is specified as "SERVER".

serialNumber

Description:	The serial number of the target provisioned device (or device being provisioned). May be masked.
Data Type:	String
Max Length:	64
Required:	No

~~deviceType~~

Description: The form factor of the target provisioned device (or device being provisioned).

Must be one of:

Value	Meaning
PHONE	Mobile phone.
TABLET	Tablet computer.
WATCH	Watch.

Data Type:	String
Max Length:	64
Required:	**Deprecated** – use formFactor instead.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

formFactor

Description: The form factor of the target provisioned device (or device being provisioned).

Must be one of:

Value	Meaning
PHONE	Mobile phone.
~~TABLET~~	Tablet computer **Deprecated** – use TABLET_OR_EREADER instead.
TABLET_OR_EREADER	Tablet computer or e-reader.
~~WATCH~~	Watch **Deprecated –** use WATCH_OR_WRISTBAND instead.
WATCH_OR_WRISTBAND	Watch or wristband, including a fitness band, smart strap, disposable band, watch add-on, security / ID Band
CARD	Card
STICKER	Sticker
PC	PC or Laptop
DEVICE_PERIPHERAL	Device peripherals, such as a mobile phone case or sleeve
TAG	Tag, such as a key fob or mobile tag
JEWELRY	Jewelry, such as a ring, bracelet, necklace and cuff links
FASHION_ACCESSORY	Fashion accessory, such as a handbag, bag charm, glasses
GARMENT	Garment, such as a dress
DOMESTIC_APPLIANCE	Domestic appliance, such as a refrigerator, washing machine
VEHICLE	Vehicle, including vehicle attached devices
MEDIA_OR_GAMING_DEVICE	Media or gaming device, including a set top box, media player, television

Data Type: String

Max Length: 64

Required: Conditional – required in a Check Eligibility request, except when Storage Technology is specified as "SERVER".

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

storageTechnology

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

Value	Meaning
DEVICE_MEMORY	Device memory.
DEVICE_MEMORY_PROTECTED_TPM	Device memory using a protected trust platform module.
TEE	Trusted execution environment.
SE	Secure element.
SERVER	Server host.
VEE	Virtual execution environment

Data Type: String

Max Length: 32

Required: Yes

~~tokenStorageType~~

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

Value	Meaning
DEVICE_MEMORY	Device memory.
DEVICE_MEMORY_PROTECTED_TPM	Device memory using a protected trust platform module.
TEE	Trusted execution environment.
SE	Secure element.
SERVER	Server host.

Data Type: String

Max Length: 32

Required: **Deprecated** – use storageTechnology instead.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

osName

Description: The name of the operating system of the target provisioned device (or device being provisioned).

Must be one of:

Value	Meaning
ANDROID	Google Android operating system.
WINDOWS	Microsoft Windows operating system.
TIZEN	Tizen operating system.
PAGARE_EMBEDDED_OS	FitPay embedded operating system
ANDROID_WEAR	Android wear operating system
EMBEDDED_OS	All Embedded operating system and Real time Operating systems

Data Type: String

Max Length: 32

Required: Conditional – required in a Check Eligibility request, except when Storage Technology is specified as "SERVER".

osVersion

Description: The version of the operating system of the target provisioned device (or device being provisioned).

Data Type: String (supports numbers and decimals).

Max Length: 32

Required: Conditional – required in a Check Eligibility request, except when Storage Technology is specified as "SERVER".

nfcCapable

Description: Whether the target provisioned device (or device being provisioned) has NFC capability.

Must be one of:

Value	Meaning
true	The device is NFC capable
false	The device is not NFC capable

Data Type: Boolean

Max Length: N/A

Required: Conditional – required in a Check Eligibility request, except when Storage Technology is specified as "SERVER.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

imei

Description:	The IMEI number of the target provisioned device (or device being provisioned).
Data Type:	String (Numeric)
Max Length:	15 (exact)
Required:	No

msisdn

Description:	The MSISDN of the target provisioned device (or device being provisioned).
Data Type:	String
Max Length:	15
Required:	No

B.2 DecisioningData

recommendation

Description: Digitization decision recommended by the Token Requestor.
Must be one of:

Value	Meaning
APPROVED	Recommend a decision of "Approved"
DECLINED	Recommend a decision of "Declined"
REQUIRE_ADDITIONAL_AUTHENTICATION	Recommend additional authentication

Data Type:	String
Max Length:	64
Required:	No

recommendationAlgorithmVersion

Description:	Version of the algorithm used by the Token Requestor to determine its recommendation.
Data Type:	String
Max Length:	16
Required:	No

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

deviceScore	
Description:	Score assigned by the Token Requestor for the target device being provisioned. Must be a value from 1 to 5.
Data Type:	Number
Max Length:	1
Required:	No
accountScore	
Description:	Score assigned by the Token Requestor for the consumer account or relationship. Must be a value from 1 to 5.
Data Type:	Number
Max Length:	1
Required:	No

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

recommendationReasons

Description: Code indicating the reasons the Token Requestor is suggesting the digitization decision.

Data Type: Array[String]

Recommendation reasons for an 'APPROVED' recommendation must be one or more of:

Value	Meaning
LONG_ACCOUNT_TENURE	Account has existed for an extended period of not less than one year. A Token Requestor may determine a longer account tenure to qualify for this reason.
GOOD_ACTIVITY_HISTORY	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.
ADDITIONAL_DEVICE	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.
SOFTWARE_UPDATE	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 paymentAppInstanceId to which a Token was previously digitized and activated for the same Account PAN and consumer account.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

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

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

Max Length: N/A

Required: No

deviceCurrentLocation

Description: Latitude and longitude in the format "(sign) latitude, (sign) longitude" with a precision of 2 decimal places. Ex: "38.63, -90.25" Latitude is between -90 and 90. Longitude between -180 and 180.

Relates to the target device being provisioned.

If there is no target device, then this should be the current consumer location, if available.

Data Type: String

Max Length: 14

Required: No

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

deviceIpAddress	
Description:	The IP address of the device through which the device reaches the internet. This may be a temporary or permanent IP address assigned to a home router, or the IP address of a gateway through which the device connects to a network. IPv4 address format of 4 octets separated by "." Ex: 127.0.0.1 Relates to the target device being provisioned. If there is no target device, then this should be the current consumer IP address, if available.
Data Type:	String
Max Length:	15
Required:	No

mobileNumberSuffix	
Description:	The last few digits (typically four) of the consumer's mobile phone number as available on file or on the consumer's current device, which may or may not be the mobile number of the target device being provisioned.
Data Type:	String
Max Length:	32
Required:	No

accountIdHash	
Description:	SHA-256 hash of the Cardholder's account ID with the Token Requestor. Typically expected to be an email address.
Data Type:	String (Alpha-Numeric). Hex-encoded data (case-insensitive).
Max Length:	64
Required:	No

B.3 SeCapabilities

Placeholder for data elements to be added.

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

Appendix C Implementation Information

C.1 Encryption of PCI/PII Sensitive Data

PCI sensitive data and all Cardholder personally identifiable information (PII) sent to MDES is encrypted for transport by the Token Requestor. 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.

Encrypted PCI/PII data is submitted in CardInfoData object which can be used in the following API's:

- Check Eligibility (See 3.2.1)
- Digitize (See 3.2.2)
- Tokenize (See 3.2.3)
- Search Tokens (See 3.2.13)

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 applicable MDES API's and the External Partner's web service are secured using mutually authenticated TLS.
- Sensitive data is encrypted using a one-time use encryption key, and is exposed as *encryptedData* within the TLS tunnel. The one-time use encryption key is wrapped with the Public Key, in an RSA digital envelope, exposed by the API in *encryptedKey*.

The one time use encryption key is generated by a strong pseudorandom number generator built into the HSM. The one time use encryption key is wrapped with the Token Requestor Encryption Public Key, in an RSA digital envelope computed using PKCS#11's C_WrapKey method (section 11.14), which is defined on page 178 of the PKCS#11 v2.20 standard (https://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs-11-cryptographic-token-interface-standard.htm). MDES supports two wrapping mechanisms:

- When the "oaepHashingAlgorithm" parameter is omitted during the Token Requestor onboarding procedure, MDES uses the PKCS#1 v1.5 RSA mechanism (section 12.1.6) denoted CKM_RSA_PKCS, defined on page 197 of the PKCS#11 v2.20 standard.
- When the "oaepHashingAlgorithm" parameter is setup during the Token Requestor onboarding procedure with either "SHA-256" or "SHA-512", MDES uses the

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

PKCS#1 RSA OAEP mechanism (section 12.1.8) denoted CKM_RSA_PKCS_OAEP, defined on page 200 of the PKCS#11 v2.20 standard.

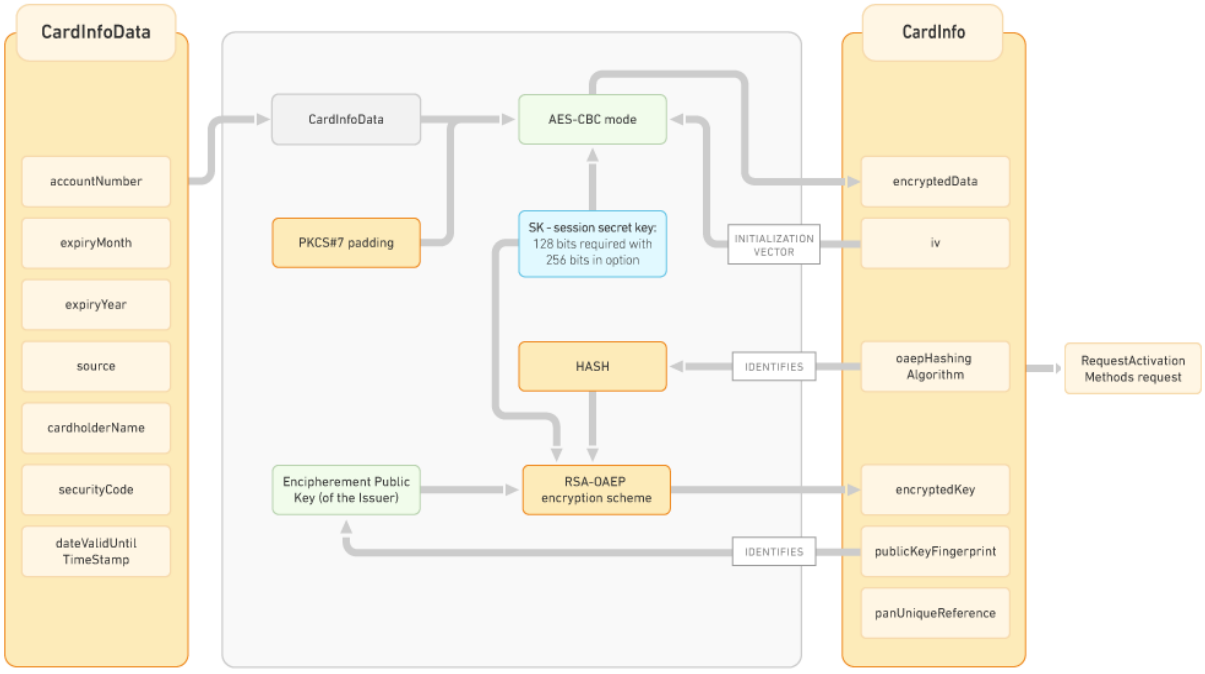
Within the mechanism parameters table CK_RSA_PKCS_OAEP_PARAMS (section 12.1.7) defined on page 200 of the PKCS#11 v2.20 standard, the following two parameters are considered:

- CK_MECHANISM_TYPE indicates the message digest algorithm used to calculate the digest of the encoding parameter;
- CK_RSA_PKCS_MGF_TYPE indicates the Mask Generation Function (MGF) to use on the encoded block.

MDES fills in these parameters as follows:

a) If during the onboarding Token Requestor has chosen "oaepHashingAlgorithm" = "SHA256", then MDES sets CK_MECHANISM_TYPE = CKM_SHA256 and CK_RSA_PKCS_MGF_TYPE = CKG_MGF1_SHA256.

b) If during the onboarding Token Requestor has chosen "oaepHashingAlgorithm" = "SHA512", then MDES sets CK_MECHANISM_TYPE = CKM_SHA512 and CK_RSA_PKCS_MGF_TYPE = CKG_MGF1_SHA512.



© 2017 Mastercard. Proprietary and Confidential. All rights reserved.

The MDES API exposes the hashing algorithm used by the OAEP scheme - *oaepHashingAlgorithm*.

The MDES API also exposes:

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

© 2017 Mastercard. Proprietary and Confidential. All rights reserved.