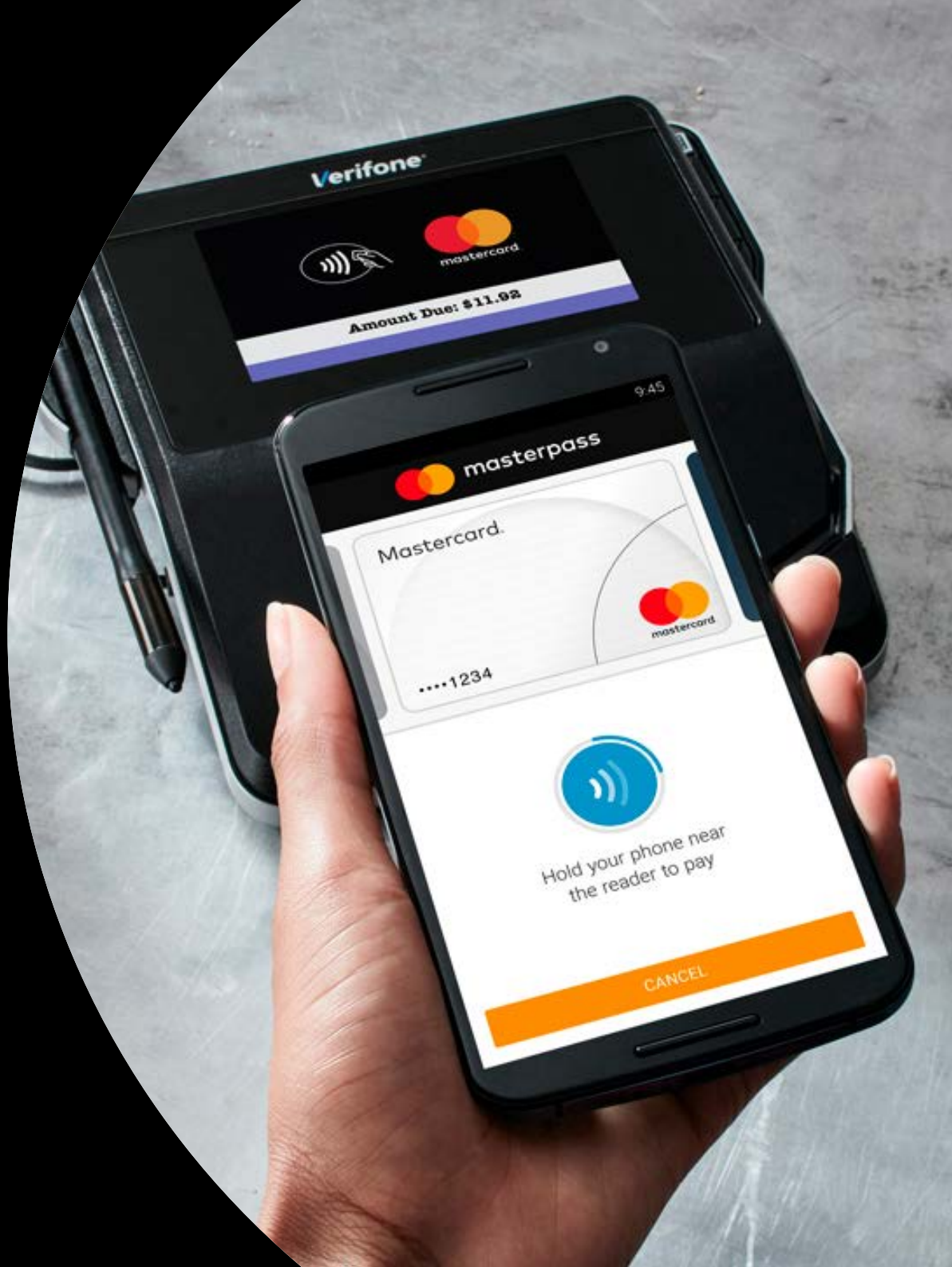
MDES Keys and Certificates

Mastercard Quick Reference Guide

March 2020



mastercard

How to read this document

WHO NEEDS IT?
Explains who the topic applies to.

PREREQUISITES
Lists the processes or actions that must be completed before you start a specific process.

ALSO KNOWN AS
Lists the alternative names that are used for certain terms.

GOOD TO KNOW
Provides additional background information to help you better understand the topic.

WANT TO KNOW MORE?
Provides information on helpful Mastercard documentation, available either from your Mastercard representative, or at Publications on Mastercard Connect™. You can find a specific manual by using the search function.

This page gives you a brief description of the different sections you will find in this document.

What is it?
Gives a high-level overview of the prerequisites or process.

Symbols

Symbol	Significance
	Key
	Certificate
	Applicable
	Not applicable
	Conditional

The process
Describes the tasks to follow to complete a process.

White circles indicate a task that must be performed by you, the customer.

Orange circles indicate a task that must be performed by Mastercard.

Contents

Welcome 4

Abbreviations and acronyms 5

Keys and Certificates 6

Overview 7


XML Gateway Client Certificate 9


Customer Wrapping Key 11


PEPK-PESK 13


Mastercard CMS-D Public Key 15


ECB and CCMOut Keys 16


SEPK 18


PTPK-PTSK 19


Mastercard XML Gateway Server Certificate 21


Consumer Key 22


Mastercard Encryption Public Key 23


Client Encryption Key 24


MDES Tokenization Authentication Value (TAV) Issuer App Certificate 26

Appendix 28

Support & feedback 29

Welcome to Mastercard Digital Enablement Service – Keys and Certificates

PREREQUISITES

- Access to Mastercard Connect™
- Implementing MDES with Mastercard

WANT TO KNOW MORE?

- MDES Information Center

This document provides an overview of the keys and certificates required to implement Mastercard Digital Enablement Service (MDES).

The primary intended audience of this guide are MDES Wallet Providers, Issuers, Digital Merchants and Commerce Platforms that want to exchange MDES keys and certificates. However, the document may be of interest to anybody wanting to learn more about MDES keys and certificates.

This document provides a relatively high-level overview with links to additional information where relevant.

Detailed MDES manuals are available on the **MDES Information Center** via Mastercard Connect™.

Abbreviations and acronyms

The following abbreviations and acronyms are used in this guide:

AES	Advanced Encryption Standard
API	Application Programming Interface
CA	Certificate Authority
CaaS	Cryptography as a Service
CASD	Controlling Authority Security Domain
CSR	Certificate Signing Request
CMS-D	Credentials Management System-Dedicated
DSRP	Digital Secure Remote Payment
ECB	Electronic Code Book
HCE	Host Card Emulation
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ICC	Integrated Circuit Card
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
KMS	Key Management Services
MCBP	Mastercard Cloud-Based Payments
MPA	Mobile Payment Application, which is also known as the wallet application
PEPK	Payload Encryption Public Key
PESK	Payload Encyrption Secret Key
PTPK	Personalization Transport Public Key
PTSK	Personalization Transport Secret Key
SE	Secure Element
SEPK	Secure Element Public Key
SSL	Secure Sockets Layers
SUK	Single Use Key
RGK	Randomly-Generated Key
TAV	Tokenization Authentication Value
TEE	Trusted Execution Environment
TLS	Transport Layer Security
XML	Extensible Markup Language

Keys and Certificates

XML Gateway Client Certificate

Certificate required to establish trust upon mutual connection to Mastercard XML Gateway.

Customer Wrapping Key

Wrapping Key used by MDES to encrypt one-time use Advance Encryption Standard (AES) key transmitted from MDES to wallet provider.

PEPK-PESK

Key used by a wallet provider to encrypt a one-time use Advance Encryption Standard (AES) key transmitted from a wallet provider to MDES.

Mastercard CMS-D Public Key

Key used by MDES to encrypt the Randomly-Generated Key (RGK) provided by the Mobile Payment Application (MPA) during registration.

ECB and CCMOut Keys

Key used by MDES to encrypt rawTransactionCredentials and Token CredentialData sent through the MDES Credentials Management API during Single Use Key (SUK) Provisioning.

SEPK

Key used by wallet provider to validate the signature made by the Controlling Authority Security Domain (CASD).

PTPK-PTSK

Key used by wallet provider to encrypt the Randomly-Generated Key (RGK).

Mastercard XML Gateway Server Certificate

Certificate required for the Customer's server to authenticate Mastercard's server during outbound requests (MDES to Customer).

Consumer Key

Key used to verify the identity of a client, who request access to the Mastercard Open API Gateway.

Mastercard Encryption Public Key

Key transmitted from MDES to Open API Client (Outbound Field Encryption).

Client Encryption Key

Key used by an Open API Client to encrypt a one-time use Advance Encryption Standard (AES) key transmitted from the Client to MDES.

MDES Tokenization Authentication Value (TAV) Issuer App Certificate

TAV key is a key that allows an issuer to provide authentication for a tokenization approved by the issuer's own app.

mastercard

Overview

GOOD TO KNOW

- The Credential Management System (CMS) has two parts: Core (CMS-C) and Dedicated (CMS-D).
- Credentials Management System-Core (CMS-C) is a secure component within MDES that stores the master keys for the tokens and generates session keys, which are converted into Transaction Credentials for use in transactions.
- Credentials Management System-Dedicated (CMS-D) is an optional component (depending on the use case), which can be provided by Mastercard, the wallet provider, or a third party. It uses the session keys to create Transaction Credentials and directly replenishes them to the wallet application so that it can transact.
- CMS-D is responsible for the registration of the user and the binding between the user and the Mobile Payment Application.

	Keys & Certificates	Issuer	Merchant and Commerce Platform	Wallet Provider	MCBP Mastercard CMS-D	MCBP Non-Mastercard CMS-D	Secure Element
1	**XML Gateway Client Certificate**	✗	✗	✓	✓	✓	✓
2	**Customer Wrapping Key**	✗	✗	✓	✓	✓	✓
3	**PEPK - PESK**	✗	✗	✓	✓	✓	✓
4	**Mastercard CMS-D Public Key**	✗	✗	?	?	✗	✗
5	**ECB and CCMOut Keys** (for non-Mastercard CMS-D)	✗	✗	✓	✗	✓	✗
6	**SEPK** (for Secure Element only)	✗	✗	✓	✗	✗	✓
7	**PTPK - PTSK** (for Secure Element only)	✗	✗	✓	✗	✗	✓
8	**Mastercard XML Gateway Server Certificate**	✓	✓	✓	✗	✗	✗
9	**Consumer Key**	✓	✓	✗	✗	✗	✗
10	**Mastercard Encryption Public Key**	✓	✓	✗	✗	✗	✗
11	**Client Encryption Key**	✓	✓	✗	✗	✗	✗
12	**MDES Tokenization Authentication Value (TAV) Issuer App Certificate**	✓	✗	✗	✗	✗	✗

Legend: ✓ applicable ✗ not applicable ? conditional

Keys and certificates used in respective API calls

Keys & Certificates	MDES Digitization API	MDES MPA Management API	MDES Remote Transaction API	MDES Credentials Management API
1 **XML Gateway Client Certificate**	✓	✓	✓	✓
2 **Customer Wrapping Key**	✓	✗	✓	✗
3 **PEPK-PESK**	✓	✗	✗	✗
4 **Mastercard CMS-D Public Key**	✗	✓	✗	✗
5 **ECB and CCMOut Keys** (for non-Mastercard CMS-D)	✗	✗	✗	?
6 **SEPK** (for Secure Element only)	✓	✗	✗	✗
7 **PTPK-PTSK** (for Secure Element only)	✓	✗	✗	✗

	MDES Pre-Digitization API	MDES Customer Service API	Digital Enablement API	MDES Token Connect API
8 **Mastercard XML Gateway Server Certificate**	✓	✗	✗	✗
9 **Consumer Key**	✓	✓	✓	✓
10 **Mastercard Encryption Public Key**	✓	✗	✓	✗
11 **Client Encryption Key**	✓	✗	✓	✓
12 **MDES Tokenization Authentication Value (TAV) Issuer App Certificate**	✗	✗	✗	✗

Note: The XML Gateway Client and Server Certificate are used to establish trust upon mutual connection to Mastercard XML Gateway. However, it is not used during the API call itself.

Legend: ✓ applicable ✗ not applicable ? conditional

The next section of this guide describes each key and certificate required for new wallet provider implementation along with the secure processes that must be followed to exchange or obtain them.

mastercard

XML Gateway Client Certificate

ALSO KNOWN AS

- MDES Wallet provider Certificate.
- MDES Inbound Gateway

WHO NEEDS IT?

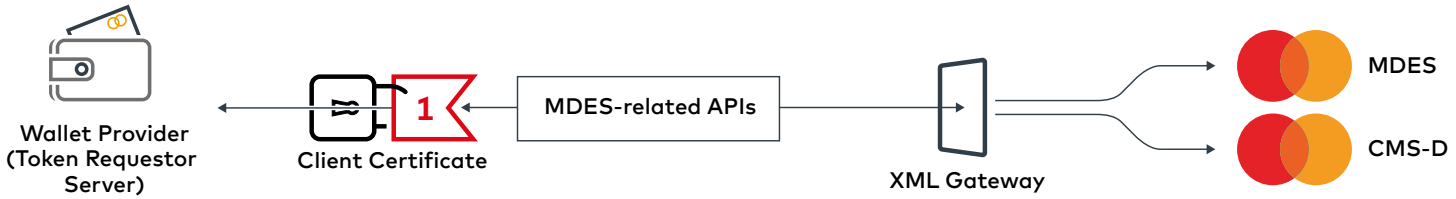
- All MDES wallet providers.

GOOD TO KNOW:

- This certificate is deployed to the Cryptography as a Service (CaaS) servers.

What is the XML Gateway Client Certificate?

The XML Gateway Client Certificate is a **certificate** used by MDES to establish a secure connection (trust) with a customer upon mutual **Transport Layer Security (TLS)** connection to Mastercard XML Gateway.



Below, you will find an overview of how the XML Gateway Client Certificate works for MDES.

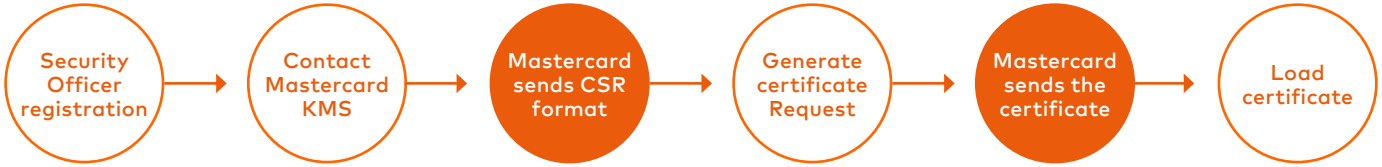
1. The wallet provider must follow the process to generate the XML Gateway Client Certificate with Mastercard (explained on the next page).

2. During the generation of this certificate, Mastercard will encrypt (sign) wallet provider information using the Mastercard private key.

3. Once the certificate is generated, the wallet provider needs to attach this certificate to messages that are sent to MDES platform.

4. When the client certificate is presented to Mastercard XML Gateway, Mastercard will then use its own public key (previously loaded in the XML Gateway) to validate the certificate and verify that the wallet provider who has sent the message is genuine.

The XML Gateway Client Certificate Exchange Process



GOOD TO KNOW

- You can reuse security officers previously registered for Business Partner PKI. To use the same security officers, sends an email request to key_management@mastercard.com with details of the previously registered security officers you want to reuse.
- More than one security officers will be required to ensure a contact remains active in case some officers change roles.
- Security officers must not include any other parties in their official communication with Mastercard KMS team (for example Mastercard project leads or similar).
- If your security officers have been registered, you can directly contact Mastercard KMS to initiate the certificate exchange process.
- The certificate request for Production environment must be zipped using WinZip and the security officer's password as specified during registration. Note: this password must be shared only with Mastercard KMS team.
- Unique client certificates are required for MTF and Production environments.
- A renewal notification email will be sent before your keys and certificates expire. Therefore, ensure that you think through the process and setup the security officers such that the relevant people will get the notification at the renewal time.

1 Security Officer Registration

Register your two security officers by completing Mastercard PKI Enrollment Form for Business Partners (Form 1075) and send the scanned version by email to key_management@mastercard.com. Mastercard KMS team will update its systems to register your named security officers.

2 Contact Mastercard KMS

Contact **Mastercard KMS team** by email at key_management@mastercard.com to inform them that you want to exchange XML Gateway Client Certificate.

3 Mastercard KMS Sends CSR Format

Mastercard KMS team will send you the details of the **Certificate Signing Request (CSR)** that you must use and other supporting certificate request documentation by email.

Note: This email also provides instruction to the wallet provider on what information is needed to request their MDES certificate, what format the CSR should be in, and how to submit their Certificate Request to KMS.

4 Generate Certificate Request

Your security officers should generate official Certificate Signing Request (CSR) using the format defined by Mastercard in the previous step and send it by email to key_management@mastercard.com, copying the other security officer in the email.

Note: During this process, you are required to create a (private and public) key pair using your **secure device** and send the public key, in form of a CSR, to Mastercard.

5 Mastercard Sends The Certificate

Mastercard will validate the request, create the certificate, and sign it with Mastercard digital signature (indicating this customer public key is really owned by a genuine customer), and send it to your two security officers by email along with confirmation that your certificate exchange process is now complete.

6 Load The Certificate

The Mastercard XML Gateway Client certificate must be loaded into your trust store (the device receiving the service call from MDES).

Renewal Process You will receive an email notification when the certificate is due for renewal. After you receive the email notification, send details as instructed in the email.

mastercard

Customer Wrapping Key

ALSO KNOWN AS

- MDES Wallet Provider – External Customer Wrapping Key
- MDES Outbound Encryption Public Key

WHO NEEDS IT

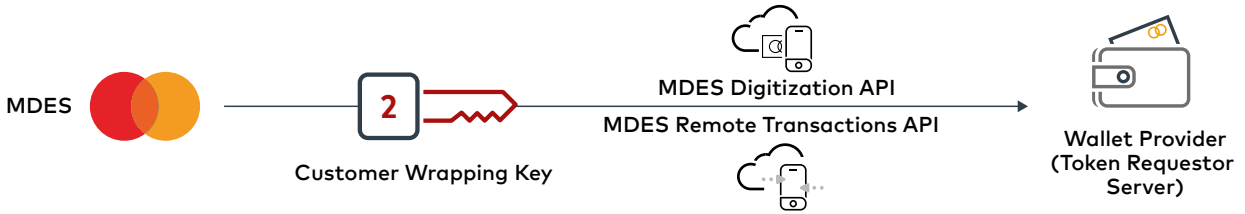
- All MDES Wallet Providers

GOOD TO KNOW

- A wrapping key is a key used to encrypt (or wrap) another key for transport or storage.

What is the Customer Wrapping Key?

The Customer Wrapping Key is an **asymmetric** wrapping key used by MDES (during MDES Digitization API and MDES Remote Transaction API) to encrypt another **'one-time use Advance Encryption Standard (AES) key'** as it is transmitted from MDES to a wallet provider.



Below, you will find an overview of how Customer Wrapping Key works for MDES.

1. The wallet provider needs to create a private and public key pair by using their secure device.

2. The wallet provider sends the public key part, in form of a CSR, to Mastercard. Mastercard will then return a CA signed certificate with added validity period to the wallet provider.

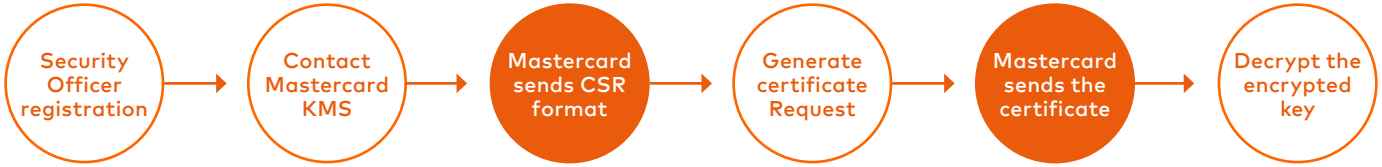
3. Mastercard then provides this public key to MDES, so that MDES can use this public key to encrypt 'one-time use AES key' as it is transmitted from MDES to a wallet provider in each API call that includes encrypted data from MDES.

4. The wallet provider then uses its private key component to decrypt the 'encrypted one-time use AES key'.

5. The wallet provider then uses the 'one-time use AES key' to decrypt the encrypted data.

The process ensures that all sensitive data is encrypted at all times as it is sent from MDES to a wallet provider.

2 The Customer Wrapping Key Exchange Process



GOOD TO KNOW

- If your security officers have been registered, you can directly contact Mastercard KMS to initiate the certificate exchange process.
- Unique client certificates are required for MTF and Production environments.
- The certificate request for Production environment must be zipped using WinZip and the security officer's password as specified during registration. Note: this password must be shared only with Mastercard KMS team.
- A renewal notification email will be sent before your keys and certificates expire. Therefore, ensure that you think through the process and setup the accounts such that the relevant people will get the notification at the renewal time.

1 Security Officer Registration

Register your two security officers by completing Mastercard PKI Enrollment Form for Business Partners (Form 1075) and send the scanned version by email to key_management@mastercard.com. Mastercard KMS team will update its systems to register your named security officers.

2 Contact Mastercard Key Management Service (KMS) Team

Contact **Mastercard KMS team** by email at key_management@mastercard.com to inform them that you want to exchange the Customer Wrapping Key.

3 Mastercard KMS Sends CSR Format

When security officer registration has been completed, Mastercard KMS team will send you the details of the **Certificate Signing Request (CSR)** that you must use and other supporting certificate request documentation by email.

Note: This email also provides instruction to the wallet provider on what information is needed to request their MDES certificate, what format the CSR should be in, and how to submit their Certificate Request to KMS.

4 Generate Certificate Request

Your security officers should generate official Certificate Signing Request (CSR) using the format defined by Mastercard in the step above and send it by email to key_management@mastercard.com, copying the other security officer in the email.

Note: During this process, you are required to create a private and public key pair using your **secure device** and send the public key, in form of a CSR, to Mastercard.

5 Mastercard signs the CSR with the CA

Mastercard will validate the request and then sign the CSR with the CA to create a certificate with an added validity period. This certificate is sent to your two security officers by email. Mastercard installs the signed certificate on MDES. This certificate (public key) is then used to encrypt the single use randomly generated AES keys. This single use AES key is in turn used to encrypt sensitive data transmitted from MDES to a wallet provider

6 Decrypt The Encrypted Key

Customer then uses their private key component to decrypt the encrypted 'one-time use AES' key and uses the same 'one-time use AES' key to decrypt the encrypted data returned in the notifyTokenUpdated API.

Renewal Process You will receive an email notification when the certificate is due for renewal. After you receive the email notification, send details as instructed in the email.

mastercard

PEPK-PESK

ALSO KNOWN AS

- Mastercard Public Key (PEPK)
- Key Alias Reference: 70 (Public) and 71 (Private)

WHO NEEDS IT

- All MDES wallet providers.

GOOD TO KNOW:

- This key is deployed to the Cryptography as a Service (CaaS) servers.

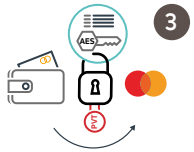
What is the PEPK-PESK

The PEPK (Payload Encryption Public Key)-PESK (Payload Encryption Secret Key) is an **asymmetric** wrapping key used by a wallet provider to encrypt another **'one-time use AES' key'**, as it is transmitted from a wallet provider to MDES.

Below, you will find an overview of how PEPK-PESK works for MDES.

1. Mastercard creates a private and public key pair by using the Mastercard secure device.

2. Mastercard provides the public key part, in form of a signed certificate, to the wallet provider.



3. The wallet provider then uses this PEPK to encrypt another one-time use AES key which is used to encrypt the FundingAccountData as it is transmitted from the wallet provider to MDES.

4. Mastercard will then use its private key component to decrypt the AES key in order to decrypt the encrypted payload message.

The process ensures that all sensitive data is encrypted at all times as it is sent from a wallet provider to MDES.

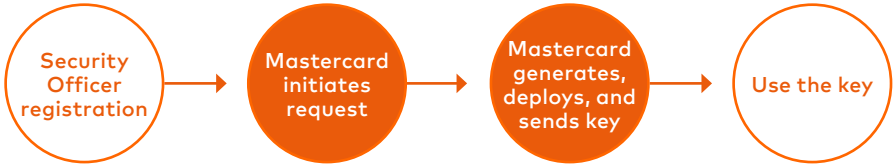
3 The PEPK-PESK Exchange Process

GOOD TO KNOW

- Unique keys are required for MTF and Production environments.
- A renewal notification email will be sent before your keys and certificates expire. Therefore, ensure that you think through the process and setup the accounts such that the relevant people will get the notification at the renewal time.

WANT TO KNOW MORE

- MDES—API Specification



1 Security Officer Registration

Register your two security officers by completing Mastercard PKI Enrollment Form for Business Partners (Form 1075) and send the scanned version by email to key_management@mastercard.com. **Mastercard KMS team** will update its systems to register your named security officers.

2 Mastercard Initiates Request

Your Mastercard Implementation Manager will initiate internal requests and assign them to the impacted teams.

3 Mastercard KMS Generates, Deploys, and Sends The Key

When security officer registration is completed and the key exchange process is initiated, Mastercard KMS generates the PEPK-PESK and deploys the PESK key on the Cryptography as a Service (CaaS) servers. Then, the Mastercard KMS team will send you the PEPK (the public key) to your registered security officers.

4 Use The Key

The PEPK is now ready to be used to encrypt your 'one-time use AES' key and data.

Renewal Process You will receive an email notification when the certificate is due for renewal. After you receive the email notification, send details as instructed in the email.

Mastercard CMS-D Public Key

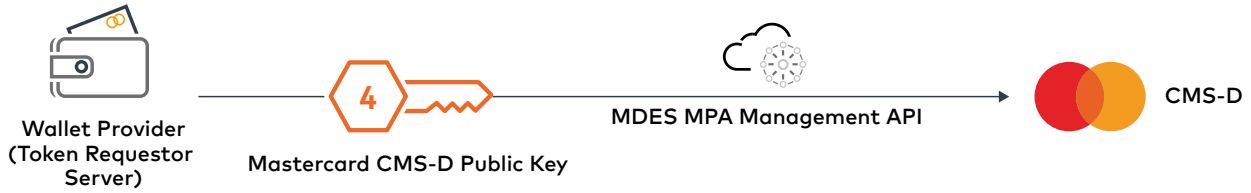
ALSO KNOWN AS
- MPA Management Key

WHO NEEDS IT?
- Mastercard CMS-D Public Key is a conditional key.
- MDES wallet providers who use **Mastercard CMS-D** and would like the wallet server to manage the **mobile PIN**.

WANT TO KNOW MORE?
- MDES—API Specification

What is the Mastercard CMS-D Public Key?

The Mastercard CMS-D Public Key is an **asymmetric key** used by MDES to encrypt the Randomly-Generated Key (RGK) provided by the Mobile Payment Application (MPA) during registration.



Below, you will find an overview of how Mastercard CMS-D Public Key works for MDES.

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 Mastercard CMS-D 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 Mastercard CMS-D Public Key, and supplies it in the registration request. Then, MDES returns the Mobile Keys encrypted using this random key in the registration response.

The Mastercard CMS-D Public Key Exchange Process

This key is generated automatically via '/pkCertificate' call within the MDES MPA Management API. When the Mastercard CMS-D public key has been obtained, it is recommended to periodically use the /pkCertificate call within the MPA management API to ensure the latest keys are always being used.

ECB and CCMOut Keys

WHO NEEDS IT

- MDES wallet providers who use **non-Mastercard CMS-D**.

GOOD TO KNOW

- Each tokenized transaction uses a set of payment keys. The wallet provider's Credentials Management System sends the payment keys to the wallet application and replenishes them each time they are used.
- When an issuer integrates with a wallet program that has a Cloud token type, the issuer can alter the maximum number of payment keys (Session Keys and SUKs) that can be stored simultaneously on a cardholder's device per digitized card.
- Unique keys are required for MTF and Production environments.

WANT TO KNOW MORE?

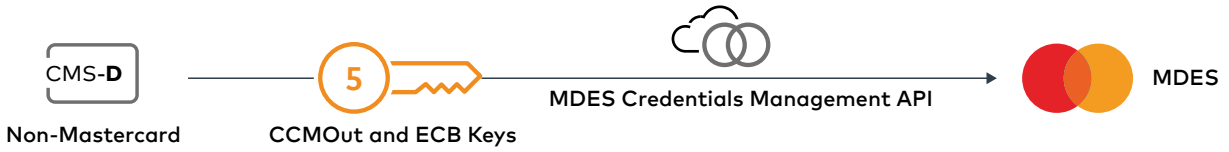
- MDES—API Specification
- Issuer Cryptographic Algorithms

What are the ECB and CCMOut Keys?

The CCMOut Key is a symmetric key used to encrypt TokenCredential data (card profile and iccKEK) and rawTransactionCredentials data sent through the MDES Credentials Management API during token provisioning.

The ECB (Electronic Code Book) Key is a symmetric transport key used by MDES to encrypt rawTransactionCredentials and TokenCredentialData sent through the MDES Credentials Management API.

The ECB Key is used by MDES to encrypt the following **rawTransactionsCredentials** during Single Use Key (SUK) replenishment:



rawTransactionsCredentials	Description
Idn	Integrated Circuit Card (ICC) Dynamic Number
contactlessMdSessionKey	Session key used for mobile device authentication for contactless transactions
contactlessUmdSessionKey	Session key used for user and mobile device authentication for contactless transactions
dsrpMdSessionKey	Session key used for mobile device authentication for Digital Secure Remote Payment (DSRP) transactions
dsrpUmdSessionKey	Session key used for user and mobile device authentication for Digital Secure Remote Payment (DSRP) transactions

This key is also used by MDES to encrypt the following TokenCredentialData during Token Provisioning:

TokenCredentialData	Description
iccKek	The key used to encrypt ICC private keys in the 'cardProfile'.

5 The ECB and CCMOut Keys Exchange Process

GOOD TO KNOW

- Unique keys are required for MTF and Production environments.

1 Security Officer Registration

Register your security officers by completing Key Management Services - Member Security Officers Registration/Update (Form 1029) and hand the form to the Mastercard representative during the face-to face meeting or scan the completed form and send it by email to key_management@mastercard.com. **Mastercard KMS team** will update its systems to register your named security officers.

For more detailed information on the Security Officer Registration Process, consult the Key Management – Implementation Quick Reference Guide.

2 Initiate Key Exchange Process

Contact your Mastercard Implementation Manager who will then raise an internal request to initiate the key exchange process with KMS team.

3 Mastercard KMS Generates and Sends The Key

When security officer registration is completed and the key exchange process is initiated, Mastercard will generate and send you the key.

4 Acknowledge Reception of The Key

Upon receipt of the key, complete the MDES Key Transfer Form – Form 1027, scan the completed form and send it by email to key_management@mastercard.com to acknowledge reception of the key.

5 Use The Key

The ECB and CCMOut Keys are now ready to be used.

SEPK

ALSO KNOWN AS

- Secure Element Public Key (SEPK)
- PK.CA.AUTH

WHO NEEDS IT?

- MDES wallet providers who implement MDES using the device's **Secure Element** (**SE**).

GOOD TO KNOW

- Unique keys are required for MTF and Production environments

What is the SEPK Key?

The SEPK (Secure Element Public Key) is a Certificate Authority (CA) public key pair used by a wallet provider to validate the signature on the Controlling Authority Security Domain (CASD) Certificate, as provided in the checkEligibility request, per the MDES Specification.

Mastercard extracts the public key (SEPK) from the CERT.CA.AUTH (on the Secure Element), then uses this extracted SEPK to validate the signature on the CASD Certificate.

The SEPK Key Exchange Process

1 Security Officer Registration

Register your two security officers by completing Mastercard PKI Enrollment Form for Business Partners (Form 1075) and send the scanned version by email to key_management@mastercard.com. **Mastercard KMS team** will update its systems to register your named security officers.

2 Mastercard Initiates Request

Your Mastercard Implementation Manager will initiate internal requests and assign them to the impacted teams.

3 Mastercard Contacts Customer

Mastercard KMS contacts customer requesting customer to provide the SEPK.

4 Customer Provides Key

Customer provides the SEPK to Mastercard KMS.

5 Mastercard Deploys Key

Mastercard deploys the SEPK on the Cryptography as a Service (CaaS) servers.

mastercard

PTPK-PTSK

ALSO KNOWN AS

- Personalization Transport Public Key (PTPK)

WHO NEEDS IT?

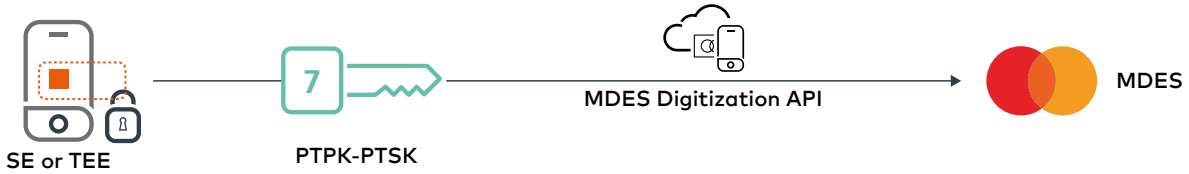
- MDES wallet providers who implement MDES using the device's physical **Secure Element** (**SE**).

GOOD TO KNOW

- The RGK uses the same principal as Advance Encryption Standard (AES).

What is the PTPK-PTSK Key?

The PTPK (Personalization Transport Public Key)-PTSK (Personalization Transport Secret Key) is an **asymmetric** transport key pair used by the wallet provider to encrypt (or wrap) the Randomly-Generated Key (RGK).



Below, you will find an overview of how PTPK-PTSK works for MDES.

1. Mastercard creates (private and public) key pair by using Mastercard secure device.

2. Mastercard provides the public key part, in form of a certificate, to the wallet provider.

3. The wallet provider uses this Mastercard public key (PTPK) to encrypt the Randomly-Generated Key (RGK), as it is transmited from the wallet provider to MDES.

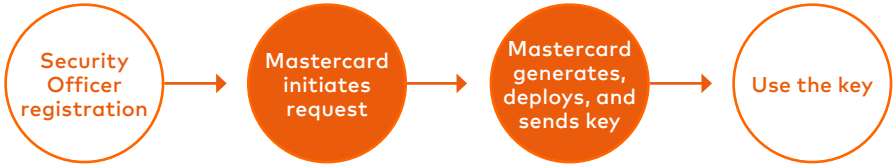
4. Mastercard will then use its private key component to decrypt the message.

The process ensures that all sensitive data is encrypted at all times as it is sent from a wallet provider to MDES.

The PTPK-PTSK Exchange Process

GOOD TO KNOW

- Unique keys are required for MTF and Production environments.
- You need to renew your certificate before it expires.



1 Security Officer Registration

Register your two security officers by completing Mastercard PKI Enrollment Form for Business Partners (Form 1075) and send the scanned version by email to key_management@mastercard.com. **Mastercard KMS team** will update its systems to register your named security officers.

2 Mastercard Initiates Request

Your Mastercard Implementation Manager will initiate internal requests and assign them to the impacted teams.

3 Mastercard Generates, Deploys, and Sends Key

Mastercard KMS generates the PTPK-PTSK and deploys the PTSK key on the Cryptography as a Service (CaaS) servers. Then, the Mastercard KMS team will send you the public key (PTPK) to your registered security officers.

4 Use The Key

The PTPK is now ready to be used.

Mastercard XML Gateway Server Certificate

ALSO KNOWN AS
- Entrust Certificate Authority (CA) Chain

WHO NEEDS IT?
- MDES API clients who would like to **receive outbound messages** from Mastercard.

GOOD TO KNOW
- Clients can optionally receive outbound messages from Mastercard.
- Outbound messages are mandatory for Merchants using Digital Enablement API.
- Unique client certificates are required for MTF and Production environments.

WANT TO KNOW MORE:
- Entrust

What is the Mastercard XML Gateway Server Certificate?

When a client receives outbound messages from Mastercard, a mutual TLS or SSL connection to Mastercard XML Gateway must be established. In this situation (where mutual TSL or SSL is used), each party must present its own certificate; Mastercard (the server) will provide an **XML Gateway Server Certificate** and the client will provide their **XML Gateway Client Certificate**.

Below, you will find an overview of how the XML Gateway Server Certificate works for MDES.

1 To establish this mutual connection, the client and Mastercard present their certificate to each other.

2 The client ensures that its internet appliance has access to its trust store which contains the Entrust Certificate Authority – L1K Chain Certificate.

3 The client validates the Mastercard XML Gateway Server Certificate by using the Entrust Certificate Authority - L1K Chain Certificate obtained previously.

At the same time, the Mastercard XML Gateway also validates the issuer server's certificate.

The Mastercard XML Gateway Server Certificate Exchange Process

To validate the Mastercard XML Gateway Server Certificate, clients need to download the Entrust Certificate Authority – L1K Chain Certificate directly from Entrust and import it into the appropriate trust store.

Consumer Key

ALSO KNOWN AS

- Open Standard for Authorization Key
- Open API Key

WHO NEEDS IT?

- MDES issuers using Pre-digitization API and/or MDES Customer Service API.

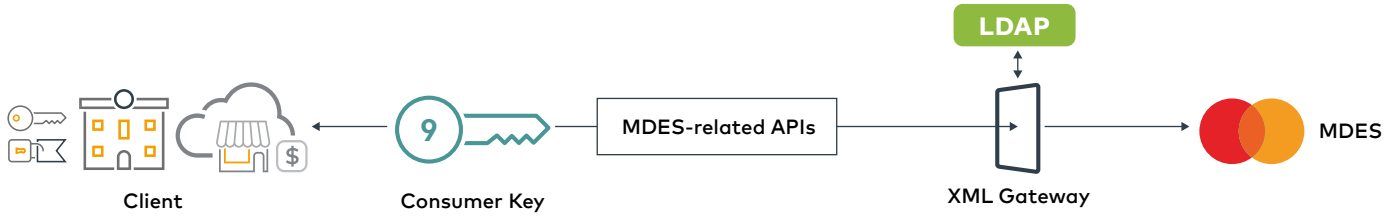
GOOD TO KNOW

- You can use the same or different Consumer key to access Production and MTF environments.

What is the Consumer Key?

The Consumer key is used to authenticate (verify) the identity of a client who requests access to the MDES APIs. This key is required for client authentication and HTTP requests to all MDES APIs.

When a client requests access to MDES APIs via Mastercard XML Gateway, XML Gateway communicates directly with the Lightweight Directory Access Protocol (LDAP) to verify the client's credentials, available in the Consumer key.



Notes:

LDAP is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.

A common use of LDAP is to provide a central place to store usernames and passwords (in this case for certificates). This allows many different applications and services to connect to the LDAP server to validate users. This has a major benefit that allows a central place to update and change user password.

The Consumer Key exchange Process

The Consumer Key can be generated via Mastercard Developers at the same time as Mastercard Encryption Public Key, explained next. For the detailed process, see the **Consumer Key and Encryption Key Exchange Process on page page 25.**

Mastercard Encryption Public Key

ALSO KNOWN AS

- MDES Outbound Encryption Public Key
- Issuer Encryption Private and Public Keys
- Issuer Encryption Key Pair
- Issuer Key Pair and Certificate (Open API)

WHO NEEDS IT?

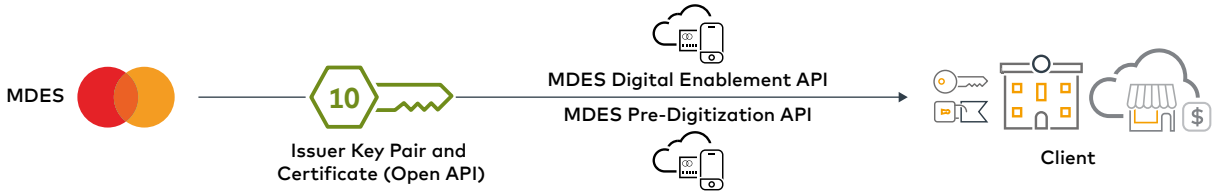
- MDES clients using Pre-digitization API and Digital Enablement API.
- Issuers implementing "Issuer-Initiated Digitization" for Android devices.

GOOD TO KNOW

- By using the publicKeyFingerprint of the key alias, the client can identify which private key is used to unwrap the encrypted key.
- The Mastercard Encryption Public Key is used to encrypt any MDES requests sent to the client, such as: Request Activation, Notify Service Updated, and Authorize Service.

What is the Mastercard Encryption Public Key?

The **Mastercard Encryption Public Key** is a public **asymmetric** wrapping key used by MDES when required to transmit sensitive information to a client (Outbound Field Encryption). It is used to encrypt the 'one-time use AES key' that further encrypts the payload that has sensitive information.



Below, you will find an overview of how the key works for MDES.

1. The client creates (private and public) key pair by using the secure device.

2. The client provides the public key part to Mastercard by uploading it to the Project created in Mastercard Developers. Refer to the key exchange process on page 25.

3. Mastercard provides this public key to MDES that uses this public key to encrypt the 'one-time use AES key' and that is further used to encrypt the payload that contains sensitive information (such as token details).

4. MDES sends the encrypted 'one-time use AES key' and the encrypted payload to the client.

5. The client uses its private key to decrypt the encrypted one-time use AES. Then it uses the AES key to recover the sensitive information in the payload.

The process ensures that all sensitive data is encrypted at all times as it is sent from MDES to the client.

Client Encryption Key

ALSO KNOWN AS

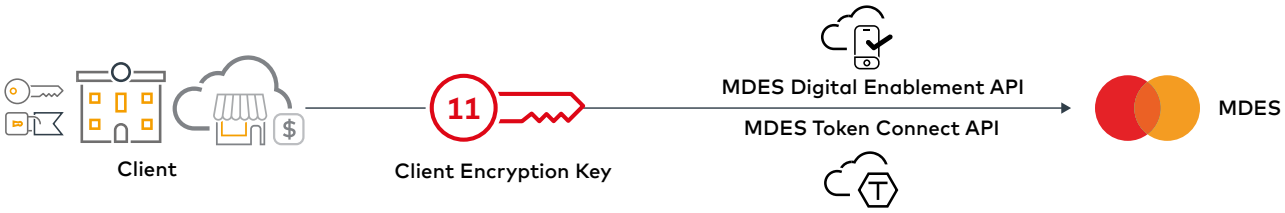
- Mastercard Public Key (Client Encryption Key)

WHO NEEDS IT

- All MDES clients.

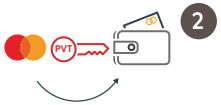
What is the Client Encryption Key?

The Client Encryption Key is a public **asymmetric** wrapping key used by a Client when they need to transmit sensitive information to MDES (Inbound Field Encryption). It is used to encrypt another **'one-time use AES' key'**, as it is transmitted from the Client to MDES.



Below, you will find an overview of how the Client Encryption Key works for MDES.

1. When a Client moves their project in Mastercard Developers from Sandbox to MTF or Production, Mastercard creates a private and public key pair.



2. Mastercard provides the public key part, in form of a certificate, to the wallet provider.

3. The client then uses this Mastercard public key (Client Encryption Key) to encrypt another 'one-time use AES' key. The AES key is further used to encrypt sensitive information (such as card details or PII data) that the Client transmits to MDES.

4. Mastercard will then use its private key component to decrypt the AES key, to retrieve the sensitive data.

The process ensures that all sensitive data is encrypted at all times as it is sent from a client to MDES.

The Consumer Key, Mastercard Encryption Public Key, and Client Encryption Key Exchange Process

PREREQUISITES

- Registered with Mastercard Developers.
- Access to MDES related APIs Documentation is available on Mastercard Developers.

GOOD TO KNOW

- Sandbox environment is not available for Pre-digitization API.

WANT TO KNOW MORE?

- Mastercard Developers

1 Create a New Project

Sign-in to Mastercard Developers and create a new project by using 'Create Project' functionality. Refer to the following links for creating a Project:

Digital Enablement API - https://developer.mastercard.com/tutorial/creating-a-new-digital-enablement-api-project?lang=#overview

Token Connect API - https://developer.mastercard.com/tutorial/creating-a-new-mdes-token-connect-api-project?lang=#overview

Pre-Digitization API - https://developer.mastercard.com/mdes/tutorial/predigapi/

2 Move Project to Production

To test your project in MTF environment, you need to move your project from Sandbox environment to production environment.

a. Configure Your Project

b. Create the Consumer Key

c. Create the Mastercard Encryption Public Key for Production and MTF

To move your project to production for

Digital Enablement API - https://developer.mastercard.com/tutorial/digital-enablement-api-move-a-project-to-the-production-environment?lang=#overview

MDES Token Connect API - https://developer.mastercard.com/tutorial/mdes-token-connect-api-move-a-project-to-the-production-environment?lang=#overview

Pre-Digitization API - https://developer.mastercard.com/mdes/tutorial/predigapi/step4/

d. Confirm and Download Keys

To finalize your request and download the keys you obtain the publicKeyFingerprint of the Mastercard Encryption Public Key.

3 Provide Client ID to Mastercard

Renewal Process

To renew the Consumer Key, Mastercard Encryption Public Key, and Client Encryption Key Exchange, follow the instructions on the following pages:

- https://developer.mastercard.com/page/b2-oauth-key-renewal-process
- https://developer.mastercard.com/page/b3-issuer-key-pair-and-certificate-open-api-renewal-process
- https://developer.mastercard.com/page/b5-client-encryption-key-renewal-process

12 MDES Tokenization Authentication Value (TAV) Issuer App Certificate

ALSO KNOWN AS

- MDES TAV Issuer App Certificate.
- Token Authentication Value (TAV) Validation - MDES

WHO NEEDS IT?

- MDES issuers who wish to implement In-App Token activation and/or In-App Digitization via TAV.
- Issuer TAV Certificate is conditional.

GOOD TO KNOW

- TAV certificate can be used across all wallets, across several Customer IDs, and across several countries.

WANT TO KNOW MORE?

- MDES – Issuer Implementation Guide

What is MDES Tokenization Authentication Value (TAV) Issuer App Certificate?

Depending on the implementation and options functionally supported by Wallet Providers, an issuer may generate a Tokenization Authentication Value (TAV) to push a digitization request to selected Wallet Providers.

The TAV allows an issuer to provide authentication for a tokenization pre-approved by the issuer's own app, it contains the issuer's digital signature using an asymmetric key algorithm that approves the digitization of a token for an Account PAN.

The TAV can be used to indicate an issuer's pre-authorization for a particular card to be digitized prior to the creation of a token, or can be used to activate a token.

Below, you will find an overview of how TAV Issuer App Certificate works for MDES.

1. The issuer creates (private and public) key pair by using the issuer the secure device.

2. The issuer provides the public key part to Mastercard.

3. Mastercard then creates the TAV Public Key Certificate (from the TAV Public Key) and signs it with Mastercard digital signature to indicate that this issuer public key is really owned by a genuine customer. Mastercard associates the certificate to the issuer's account range(s) in MDES using a Key Unique Reference, for future use.

4. During an in-app digitization or activation, the Issuer creates a TAV signature for the PAN being tokenized, using the TAV Private Key. This authenticates the issuer's approval for activation or digitization.

5. The issuer transmits the TAV signature to the wallet provider, and the wallet provider supplies the TAV signature to MDES during digitization or activation.

6. Mastercard retrieves the TAV Public Key certificate of the issuer, retrieves the TAV Public Key from the certificate, and uses the TAV Public Key to validate the Issuer's TAV signature for the account PAN.

12 The MDES TAV Issuer App Certificate Exchange Process

GOOD TO KNOW

- You can reuse security officers previously registered for Business Partner PKI.
- To use the same security officers, sends an email request to key_management@mastercard.com with details of the previously registered security officers you want to reuse.
- More than one security officers will be required to ensure a contact remains active in case some officers change roles.
- Security officers must not include any other parties in their official communication with Mastercard KMS team (for example Mastercard project leads or similar) .
- If your security officers have been registered, you can directly contact Mastercard KMS to initiate the certificate exchange process.
- The certificate request for Production environment must be zipped using WinZip and the security officer's password as specified during registration. Note: this password must be shared only with Mastercard KMS team.
- Unique TAV Certificate is required for MTF and Production environments.
- A renewal notification email will be sent before your keys and certificates expire. Therefore, ensure that you think through the process and setup the security officers such that the relevant people will get the notification at the renewal time.

1 Security Officer Registration

Register your two security officers by completing Mastercard PKI Enrollment Form for Business Partners (Form 1075) and send the scanned version by email to key_management@mastercard.com. Mastercard KMS team will update its systems to register your named security officers.

2 Contact Mastercard Key Management Service (KMS) Team

Contact **Mastercard KMS team** by email at key_management@mastercard to inform them that you want to exchange TAV certificate.

3 Mastercard KMS Sends CSR Format

Mastercard KMS team will send you the details of the **Certificate Signing Request (CSR)** that you must use and other supporting certificate request documentation by email.

Note: This email also provides instruction to the issuer on what information is needed to request their MDES certificate, what format the CSR should be in, and how to submit their Certificate Request to KMS.

4 Generate Certificate Request

Your security officers should generate official Certificate Signing Request (CSR) using the format defined by Mastercard in the step above and send it by email to key_management@mastercard.com, copying the other security officer in the email.

Note: During this process, you are required to create a (private and public) key pair using your **secure device** and send the public key, in form of a CSR, to Mastercard.

5 Mastercard Sends The Certificate

Mastercard will validate the request, create the certificate, and sign them with Mastercard digital signature (indicating this customer public key is really owned by a genuine customer), and send them to your two security officers by email along with confirmation that your certificate exchange process is now complete.

At this point, Mastercard is ready to use the Issuer Public Key in TAV signature validation.

Renewal Process You will receive an email notification when the certificate is due for renwal. After you receive the email notification, send details as instructed in the email.

Appendix

Asymmetric cryptography

A cryptographic system that uses public and private keys to encrypt and decrypt data (also known as public key cryptography). The public key can be shared with everyone, while the other key pair (the private key) is kept secret.

Certificate

An electronic document used to identify an individual, a server, a company, or other entity, and to bind that identity with a public key. A certificate always includes:

- A public key and the name of the entity it identifies
- An expiration date
- A serial number
- The digital signature and name of the issuing Certificate Authorities (CA)

Mastercard as the Certificate Authorities (CA), certifies ownership of key pairs and certificates.

Notes: Certificates have a limited lifetime, maximum four years. It is the client's responsibility to ensure that another key is certified and configured within the MDES client enablement process in advance of certificate expiry.

Certificate Signing Request (CSR)

A specific formatted file that must zipped using WinZip and the security officer's password as specified during registration. A Mastercard security officer will send you the details of the format that you must use.

'One-time use AES' key

A key used to encrypt the sensitive information, such as the Primary Account Number (PAN), also known as FundingAccountData. This key is generated automatically from a master key and generated by the party that sends the sensitive information (either the customer or MDES). 'One time use AES key' is only being used when the FundingAccountData (PAN) is present in the API call.

Mastercard Key Management Service (KMS)

A Mastercard service for the generation, storage and management of Mastercard keys and certificate.

MDES APIs

MDES provides a set of services to clients to support Pre-digitization, Digitization, Transaction Details, and Life Cycle Management. To fulfill these needs, Mastercard provides MDES API definitions in the MDES—API Specification.

Secure Device

A special type of computer used to generate and store cryptographic keys. Also known as a Hardware Security Module (HSM).

Symmetric cryptography

A cryptographic system that uses the same key to encrypt and decrypt data. Symmetric encryption is typically more efficient than asymmetric encryption.

Transport Layer Security (TLS)

Cryptographic protocols that provide communications security over a computer network. In a mutual TLS or SSL authentication, both the client and the server authenticate each other through the digital certificate, so that both parties are assured of the other's identity. TLS and its predecessor, SSL, both frequently referred to as SSL.

Support & feedback

Support

If you have questions about initiating a MDES Project or MDES Keys and certificates.

- contact your Mastercard representative

During implementation, and up to 30 days after

- contact your Mastercard Implementation Manager.

After 30 days

- contact the Digital Support by:
  - email at digital.support@mastercard.com
  - phone at +1-636-722-6176 or +32-2-352-5403 - select option 5 and followed by option 1.

Documentation

- Mastercard manuals and documentation are available on the **MDES Information Center** via Mastercard Connect™/My Apps/Publications.

Feedback

If you have suggestions for improving this document, please email us at: digital.support@mastercard.com