

KEY MANAGEMENT PORTAL

User Guide

APRIL 2021



Contents

Acronyms.....	2
Application Overview	3
Introduction.....	3
Users.....	3
Core Modules.....	3
Certificate Requests (PKI) workflows	4
Security Officer User Functions	5
Registration and Access to the Key Management Portal.....	5
Requesting Access	5
Access Approval	5
Launching the KMP Application.....	6
Adding your Certificate Management Group email	7
Working with the PKI Certificate Inventory	8
About the Certificates Inventory.....	8
Viewing a Certificate/CA Chain/Key File	9
Renewing a certificate.....	10
Downloading a Certificate/CA Chain/File	11
Set a Certificate as 'not in use'	13
Working with Certificate Requests	14
About Certificate Requests	14
Creating a New Request	14
Creating request 'New Certificate'	15
Creating request 'Renew Certificate', the expiring certificate does not exist in KMP	16
Creating request 'Renew Certificate', the expiring certificate already exists in KMP	17
Creating request 'Submit Certificate'	19
Creating request 'Submit CA Chain'	19
Creating request 'Share File'	20
Viewing the List of Requests.....	21
Using the Certificate Request Details screen	22
Cancel Request.....	23
Attach Certificate to request coming from Mastercard KMD.....	23
Updating a request sent back from Mastercard KMD	25
Using Comments on Certificate Requests and Certificates	26
Viewing your Company and Security Officer Details	26
Appendix.....	28
Support Pages	28
Finding the Support area	28
DN Requirement Specifications for Certificate Signing Requests (CSR)	29
Automated Email Notifications	29
Supported file formats for uploading file	30



Acronyms

Term/Abbreviation	Definition
KMP	Key Management Portal
CSR	Certificate Signing Request
Certificate DN	Certificate Distinguished Name - This is a term describing the identifying information in a certificate and which is part of the certificate itself.
Request	This is an overarching term describing any process instance managed in the Key Management Portal.
Security Officer (SO)	Describes the people within client organizations responsible for keys and certificates exchange with Mastercard. This is also a type of user in the system.
Key Management Delivery (KMD)	The business function within Mastercard responsible for keys and certificates exchange. This is also a type of user in the system.
PKI	Public Key Infrastructure
MCC	Mastercard Connect
CA	Certificate Authority



Application Overview

Introduction

The Key Management Portal (KMP) is a new application available in Mastercard Connect. KMP provides external customers of Mastercard a self-service portal to request and exchange keys and certificates with Mastercard.

The portal provides guided workflows to create and manage requests for keys and certificates exchange, as well as an inventory of all PKI for Business Partners keys and certificates that have been exchanged between Mastercard and customers using KMP.

KMP replaces two existing business processes:

- The PKI for Business Partner registration process – before KMP, the registration was done using forms exchanged by email. With KMP, the registration is done through acquiring access to Mastercard Connect and access to the KMP application. Once a user has been granted access to KMP, they are considered a Security Officer and are registered for PKI processes in KMP.
- The exchange of PKI certificates – before KMP, the exchange was managed through emails with the certificates being exchanged using encrypted zip files. With KMP, there is no need for forms, emails or CSRs in encrypted zip files. Requests are initiated and managed through the portal, and the customer can download their certificates on the portal.

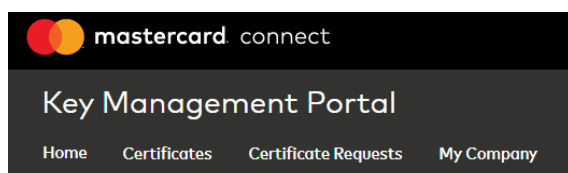
Users

User Type	Definition
Security Officer	Users within customer organizations responsible for keys and certificates exchange with Mastercard.
KMD user	A member of the Key Management Delivery (KMD) function in Mastercard, responsible for keys and certificate exchange with customer Security Officers.
Internal Mastercard	Internal employees of Mastercard who do not perform key management functions but who can visit KMP and view/track customer requests.

Core Modules

Feature	Description
Homepage	The welcome page providing links to main functions
Certificates	This module provides an inventory of certificates providing access to detailed information about previously exchanged certificates and some associated actions like download and renewal.
Certificate Requests	This module provides the full list of PKI requests with access to detailed information about each request and associated actions. The available actions vary depending on the stage in the lifecycle the request is at and on the role of the user. The workflows and actions are explained in the next section.
My Company	This module provides the customer organization name and CID (company identifier). It also contains the Certificate Management Group email registered by Key Management Portal Security Officers and the list of registered Security Officers for the company.

Each module is accessible from any page in the portal via the navigational tabs at the top of the screen:



Certificate Requests (PKI) workflows

Any exchange of keys and certificates in KMP is handled through a request, whether the request is initiated by a Security Officer (SO) or a Key Management Delivery (KMD) user.

Request Name	Initiated by	Description
New Certificate	Security Officer	A request for a new certificate to be signed and issued by Mastercard.
Renew Certificate	Security Officer	A request to renew a certificate previously signed and issued by Mastercard.
Submit Certificate	Security Officer	A request to submit/share an existing certificate with Mastercard.
Submit CA Chain	Security Officer	A request to submit/share a CA Chain with Mastercard.
Share File	Security Officer	A request to submit/share a CSR or a simple key file with Mastercard.
KMD Shares CSR to be Signed	KMD User	A request to share a CSR with a customer to be signed by the customer. This requires an action from a Security Officer to upload the signed certificate in KMP.
KMD Shares Certificate with customer	KMD User	KMD provides a certificate to the customer via the KMP to be installed on customer side.
KMD Shares CA Chain with customer	KMD User	KMD provides a CA chain to the customer via the KMP to be installed on customer side.



Security Officer User Functions

Registration and Access to the Key Management Portal

Requesting Access

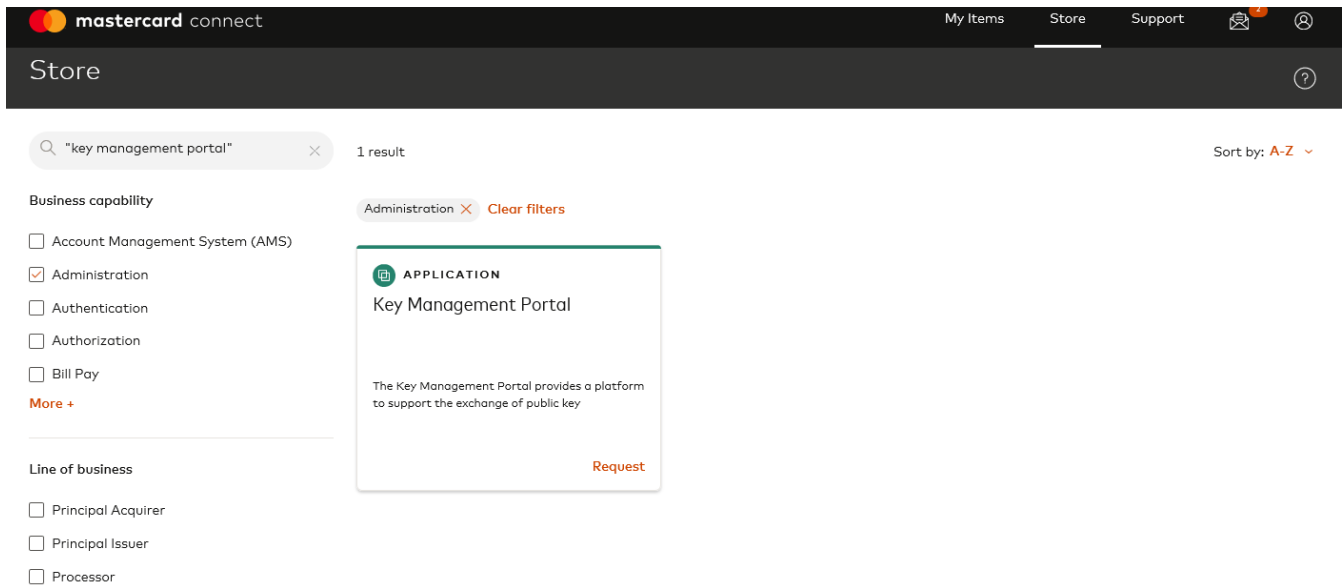
Before you begin

To access KMP, your company must be registered with Mastercard. Once your company has been setup and given a company identifier (CID), you can sign up for Mastercard Connect.

To sign up, go to www.Mastercardconnect.com then click **Sign up**.

Procedure

1. Sign in at www.Mastercardconnect.com
2. Click **Store** in the top menu.
3. Search for **Key Management Portal**. You can also select **Administration** under **Business capabilities** to narrow down the results.



The screenshot shows the Mastercard Connect Store interface. At the top, there is a navigation bar with 'mastercard connect' on the left and 'My Items', 'Store', and 'Support' on the right. Below the navigation bar, the 'Store' section is active. A search bar contains the text '"key management portal"'. To the right of the search bar, it says '1 result' and 'Sort by: A-Z'. On the left side, there are filter sections for 'Business capability' and 'Line of business'. Under 'Business capability', 'Administration' is selected. A 'Key Management Portal' application card is displayed in the center, with a 'Request' button at the bottom right.

4. On the Key Management Portal card, select **Request**.
5. Select **Security Officer Level 1** access.
6. Click **Request access**.

Result

A request for access to KMP was submitted to your Mastercard Connect Security Administrator.

Access Approval

The designated Security Administrators within your company must approve your request.



Launching the KMP Application

1. Sign in to **Mastercard Connect** (www.mastercardconnect.com)
2. Click **My Items**.

The screenshot shows the 'My Items' page in the Mastercard Connect interface. At the top, there is a navigation bar with the Mastercard logo, 'mastercard connect', and links for 'My Items', 'Store', and 'Support'. Below the navigation bar, the page title 'My Items' is displayed. A search bar labeled 'Search My Items' is on the left, and a 'Sort by: A-Z' dropdown menu is on the right. The main content area is titled 'All items (4)' and displays four application cards. Each card has a green header with 'APPLICATION' and a star icon. The cards are: 'Key Management Portal', 'KMP PreStage', 'My Company Manager', and 'Technical Resource Center - Announcements'. Each card also has a three-dot menu icon at the bottom right.

3. Click on the Key Management Portal card to **Open** it.

Tip: To add the KMP to your Mastercard Connect Home Page, click on the star on the right corner of the Key Management Portal application card.



Adding your Certificate Management Group email

About this task

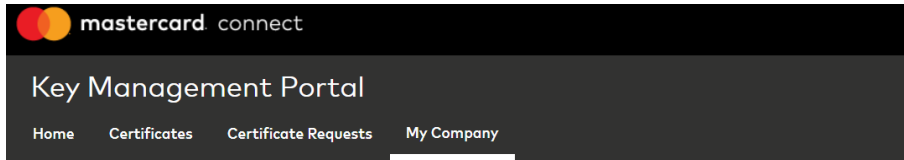
Your Certificate Management Group email is an alternative means of communication which the Mastercard Key Management Delivery team will use for crucial communication with your organization and in case there is no longer an active user on the Key Management Portal.

Avoid entering personal corporate email address as this entry should not be tied to an individual.

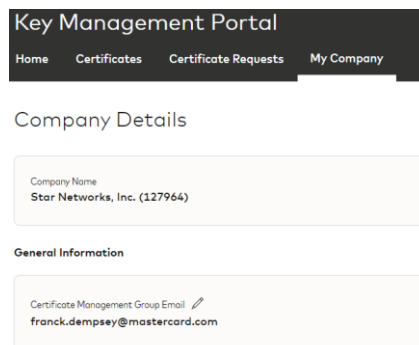
This step is required to complete your registration and begin to submit certificate requests in KMP.

Procedure

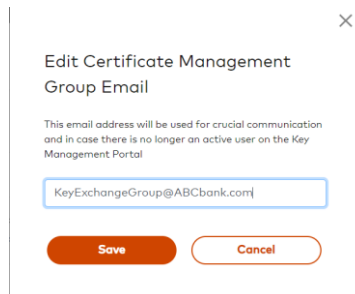
1. Click **My Company**



2. Click on the pencil icon next to **Certificate Management Group Email**



3. Enter your Certificate Management Group email and press **Save**



Working with the PKI Certificate Inventory

About the Certificates Inventory

The Certificates inventory provides a full history of all PKI objects exchanged between Mastercard and your company including certificates, CA Chains and key files (for example a CSR or a text file containing a public key).

Entries are added to the inventory following the successful completion of a request whether the request was initiated by a Security Officer from your company or by a KMD user in Mastercard.

An inventory entry in KMP contains the following data fields:

Data field	Description	Populated for
Reference	The internal reference of the record within KMP. This is the same reference as the request associated with the record.	All entries (certificate, CA Chain, file)
Subject DN	The subject DN of the certificate	Certificate, CA Chain
Application	The name of the Mastercard application.	All entries
Environment	The name of the environment.	All entries
Certificate Profile	The profile type.	All entries
Issue Date	The valid from date of the certificate.	Certificate, CA Chain
Expiry Date	The expiry date of the certificate.	Certificate, CA Chain
Serial Number	The serial number of the certificate.	Certificate, CA Chain
Status	The status (active/expired/revoked)	Certificate, CA Chain
Associated Request	The request which produced the inventory entry.	All entries
Renewal Of	Where the certificate being viewed was issued to replace an existing certificate in KMP, this is the KMP reference of the previous certificate version.	Certificate
Renewed By	Where the certificate being viewed was replaced by another certificate in KMP, this is the KMP reference of the next certificate version.	Certificate

The information is presented on screen as depicted below:

The screenshot shows the Mastercard Connect Key Management Portal interface. At the top, there is a navigation bar with 'Certificates' and 'Certificate Requests' tabs. The main content area is titled 'Certificate Detail' and includes an 'Actions' button. The certificate details are displayed in a grid format:

Serial Number OF330B5A6E07FDDA	Company Star Networks, Inc.	Application InControl Widget	Environment MTF	Certificate Profile
Associated Request PKI_198	Issue Date 13/11/2019	Expiry Date 14/05/2020	Status Active	Renewal Of
Renewed By				

Below the main details, there is a 'Subject DN' section with the following information:

- Common Name: KMP Testing 3
- Organization: My org name
- Organization Unit:



Viewing a Certificate/CA Chain/Key File

You can access the list of Certificates by clicking on the **Certificates** tab heading.

Key Management Portal							
Certificates Certificate Requests							
Start a New Request							
Reference	DN	Application	Environment	Certificate Profile	Expiry Date	Serial Number	Status
PKI_198	CN : KMP Testing OU : O : My org nam L : Iles de Franc CB : FR	InControl Widget	MTF		14/05/2020	0F330B5A6E0...	Active
PKI_190	CN : test_kmp_6 OU : KMP Team O : KMP testing L : CB : IE	Push Provisioning (PEPK)	MTF	Google	18/09/2020	0F330B5A6E1...	Active

From this list, you can open a record by clicking on the **Reference** hyperlink. Where the record being viewed is for a certificate or a key file, the screen is titled **Certificate Detail**:

Key Management Portal				
Certificates Certificate Requests				
Certificate Detail				
Actions				
Serial Number	Company	Application	Environment	Certificate Profile
0F330B5A6E07FDDA	Star Networks, Inc.	InControl Widget	MTF	
Associated Request	Issue Date	Expiry Date	Status	Renewal Of
PKI_198	13/11/2019	14/05/2020	Active	

Where the record is a CA Chain, the screen is titled **CA Chain Detail**:

Key Management Portal				
Certificates Certificate Requests				
CA Chain Detail				
Actions				
Serial Number	Company	Application	Environment	Certificate Profile
4c0e8c39	Star Networks, Inc.	SecurePlus - Mainframe		
Associated Request	Issue Date	Expiry Date	Status	Renewal Of
PKI_188	11/11/2011	12/11/2021	Active	



Renewing a certificate

Procedure

1. Find the certificate of interest in the Certificates Inventory
2. Open the certificate by clicking the Reference link.
3. On the Certificate Details screen, select Actions > **Renew Certificate**

Serial Number	Company	Application
0F330B5A6E18047F	Star Networks, Inc.	Tivoli Federated Identity Manager - Commercial I

4. Complete the request as described in section [Creating request 'Renew Certificate', the expiring certificate already exists in KMP](#)

Remark: If the certificate is not in the Certificate listing, refer to the section [Creating request 'Renew Certificate', the expiring certificate does not exist in KMP](#)



Downloading a Certificate/CA Chain/File

About downloading a certificate which was renewed

If you are viewing a certificate which has been renewed in the portal, you will not be able to download it. KMP allows you to download only the latest version of a given certificate.

To find the latest version of the certificate you're viewing, click the **Renewed By** link to open the next version.

The screenshot shows the 'Key Management Portal' header with navigation links: Home, Certificates, Certificate Requests, and My Company. The main content area is titled 'Certificate Detail' and features an orange 'Actions' button. Below this is a table with the following data:

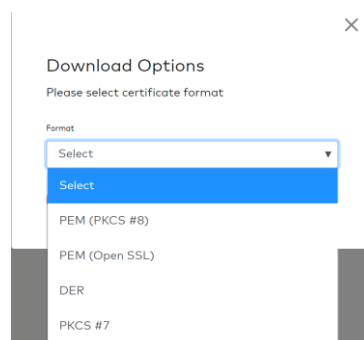
Serial Number 0F330B5A6E18047D	Company Star Networks, Inc.	Application Biometrics/IDCM	Environment Production	Certificate Profile Signing
Associated Request PKI_107	Issue Date 12/05/2020	Expiry Date 10/11/2020	Status Active	Renewal Of
Renewed By PKI_117				

Procedure

1. On the Detail screen, click **Actions**, then **Download**.

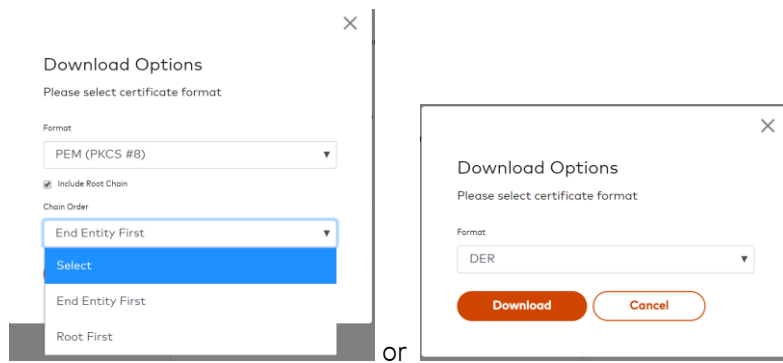
This screenshot shows the 'Key Management Portal' header with 'Certificates' and 'Certificate Requests' links. The 'Certificate Detail' section is visible, and the 'Actions' button is highlighted. A dropdown menu is open under 'Actions', showing a 'Download' option.

2. If you're downloading a certificate or a CA Chain, select a **Format** from list



3. Select the preferred ordering of Root CA (unless you select the DER format in which case the Root Chain cannot be included)





4. Press **Download**

Results

The downloaded file is saved in the default download folder of your browser.

Several different outcomes can be observed:

- For any certificate or CA chain being downloaded in the PEM (PKCS #8), PEM (Open SSL) or PKCS #7 format, the root chain is always included in the downloaded file containing the certificate and chaining:
 - For PEM (PKCS #8), PEM (Open SSL), the downloaded file is a .pem file
 - For PKCS #7, the downloaded file is a .p7b file
- Where the user is downloading a certificate for an application which requires mutual authentication, an extra CA Chain is delivered along with the certificate chaining inside a zip file.
- Where the DER format was selected, only the end entity certificate is provided in a .cer file, **the CA chain (Sub and Root CA) is not included.**



Set a Certificate as 'not in use'

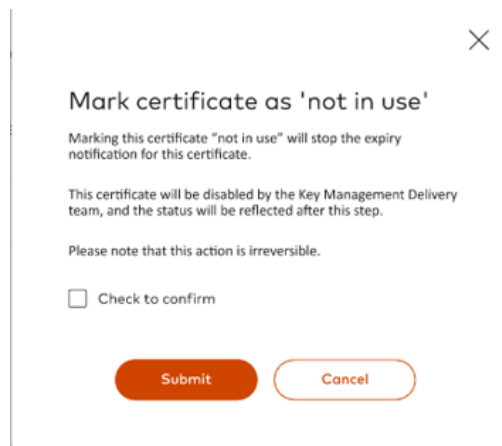
If you have a certificate in your inventory which is nearing its expiration and you do not wish to renew it, you can mark as it as 'not in use' and KMP will not be sending you automated expiry reminder emails in relation to this certificate. This also informs the Key Management Delivery team in Mastercard that the certificate is reaching its end life and can eventually be retired.

Procedure

1. Open the certificate of interest
2. Click **Actions**
3. Select **Set as 'not in use'**



4. Read the information and check the box to confirm you wish to proceed.



5. Click **Submit**

Results

The certificate is marked as 'not in use' in KMP. The KMP application will not be triggering expiry reminder emails for this certificate.



Working with Certificate Requests

About Certificate Requests

Certificate Requests represent all the PKI process instances in KMP. Requests can be initiated by Security Officers in your company or KMD users in Mastercard. Successful requests reach the state of Completed whilst unsuccessful requests typically finish in the Cancelled state.

A request in KMP contains the following data fields:

Data element	Description
Reference	The internal reference of the record within KMP.
Subject DN	The subject DN of the object being exchanged (can be CSR, CA Chain or certificate depending on the type of request).
Application	The name of the Mastercard application.
Environment	The name of the environment.
Certificate Profile	The profile type.
MasterCard Project Contact	The email address of the Mastercard project manager delivering the application specified in the request.
Requestor	The name of the user who created the request
Created On	The creation date of the request.
Closed On	The closure date of the request.
Status	The status of the request.
Uploaded Files	Files attached to the request.
Comments	Comments associated with the request.

Creating a New Request

Before you begin

Your company must have at least 2 active Security Officers on the Key Management Portal to be permitted to create new requests in KMP. If you see the following message when logging into KMP then your company needs to have at least 1 additional Security Officer registered on the Key Management Portal application in Mastercard Connect. To get registered, see [Registration and Access to the Key Management Portal](#).



Furthermore, a **Certificate Management Group email** must be added to your company profile, see [Adding your Certificate Management Group email](#).

Procedure

The following procedure is applicable to all requests initiated by a Security Officer. The available Application, Request Type, Environment and Certificate Profile value combinations are pre-configured per application.

1. On the Certificates page or on the Certificate Requests page, click **Start New Request**
2. Select the relevant **Application**
3. Select the **Request Type**
4. Select the **Environment**, if prompted
5. Select the **Certificate Profile**, if prompted
6. Enter **Mastercard Project Contact** email (not the KMD representative), if prompted. **The email must have the @mastercard.com domain.**



What to do next

Continue filling the request form. Subsequent steps vary based on the request type you have selected.

Creating request 'New Certificate'

This procedure begins after the user has filled out a new request up to the **Mastercard Project Contact** field.

Procedure

1. The **DN Requirements** appear

Note: you can view and print DN requirements for any application from the [Support Pages](#).

2. Upload your CSR file generated in compliance with the DN requirements which can be found in the Support Page

3. Click **Next**
4. Review the **CSR values** to ensure they adhere to the **DN requirements**.



Certificate Request Review

Please review your CSR Values against the DN Requirements to ensure they meet the mastercard requirements.

DN Requirements

Common Name
[Customer Name]-[environment]

Organization
MasterCard Worldwide - FSSO

Organization Unit
FSSO Message Signing

Country
must be a valid 2 characters ISO code

CSR DN Details

Common Name
www.mastercard.com

Organization
MasterCard International

Organization Unit

Country
BE

Subject Alt Name(s)

www1.mastercard.com	www.travelwithus.mastercard.com
www.summertimecrossborder.me	www.smartcommunitiescoalition.org
	g
www.smartcommunitiescoalition.co	www.mastercardweacceptdebit.com

Submit
Previous
Cancel

5. Enter **Subject Alternate Names (SAN)** if necessary (**domain names need to be comma-separated**)

Note: you can return to the previous screen to make corrections by clicking **Previous**

6. Click **Submit**

Results

The request status is set to **In Progress**.

An email notification is sent to every KMP Security Officer of your company informing them that the request was submitted.

Creating request 'Renew Certificate', the expiring certificate does not exist in KMP

This procedure begins after the user has filled out a new request up to the **Certificate Profile** field.

Procedure

1. Enter the **Expiring Certificate Serial Number**
2. The **Expiring Certificate DN** and the **DN Requirements** appear

Certificate Request Form

Mastercard Application Tivoli Federated Identity Manager - B2B FS	Request Type Renew Certificate	Environment Production
Certificate Profile Signing	Expiring Certificate Serial # 0f330b5a6e13daaa ✔	

Expiring Certificate DN

Common Name
test_kmp_6

Organization
KMP testing

Organization Unit
KMP Team

Country
IE

DN Requirements

Common Name
[Customer Name]-[environment]

Organization
MasterCard Worldwide - FSSO



Note: you can view and print DN requirements for any application from the [Support Pages](#).

3. Upload your CSR file generated in compliance with the DN requirements which can be found in the Support Page
4. Click **Next**
5. Review the **CSR values** to ensure they match the **DN Requirements**.

Certificate Request Review

Please review your CSR Values against the DN Requirements to ensure they meet the mastercard requirements.

DN Requirements	CSR DN Details
<p>Common Name [Customer Name]-[environment]</p> <p>Organization MasterCard Worldwide - FSSO</p> <p>Organization Unit FSSO Message Signing</p> <p>Country must be a valid 2 characters ISO code</p>	<p>Common Name test_kmp_6</p> <p>Organization KMP testing</p> <p>Organization Unit KMP Team</p> <p>Country IE</p>

Expiring Certificate DN

<p>Common Name test_kmp_6</p> <p>Organization KMP testing</p> <p>Organization Unit KMP Team</p> <p>Country IE</p>

Subject Alt Name(s)

Enter Alt Name(s) here (optional). Alt names are separated by comma.

Submit **Previous** **Cancel**

6. Enter **Subject Alternate Names (SAN)** if necessary (**domain names need to be comma-separated**)

Note: you can return to the previous screen to make corrections by clicking **Previous**

7. Click **Submit**

Results

The request status is set to **In Progress**.

An email notification is sent to every KMP Security Officer of your company informing them that the request was submitted.

Creating request 'Renew Certificate', the expiring certificate already exists in KMP

This procedure begins after the user clicked the **Renew Certificate** action on the **Certificate Details** screen

Procedure

1. The request form appears already prepopulated with information contained in the expiring certificate record in KMP

Mastercard Application	Request Type	Environment
MFE - FTPS (FTP with SSL)	Renew Certificate	Production
Certificate Profile	Expiring Certificate Serial #	
Client	0F330B5A6E13DAAA	
Expiring Certificate DN		
<p>Common Name test_kmp_6</p> <p>Organization KMP testing</p> <p>Organization Unit KMP Team</p> <p>Country IE</p>		

2. Upload your CSR file generated in compliance with the DN requirements which can be found in the Support Page



3. Click **Next**
4. Review the **CSR values** to ensure they match the **Expiring Certificate DN** Details and adhere to the **DN Requirements**.
5. Enter **Subject Alternate Names (SAN)** if necessary (**domain names need to be comma-separated**)

Note: you can return to the previous screen to make corrections by clicking **Previous**

6. Click **Submit**

Results

The request status is set to **In Progress**.

An email notification is sent to every KMP Security Officer of your company informing them that the request was submitted.



Creating request 'Submit Certificate'

This procedure begins after the user has filled out a new request up to the **Mastercard Project Contact** field.

Procedure

1. Upload your Certificate and CA Chain files

Note: the certificate and CA chain can be uploaded in 1 file or over multiple files. KMP will detect if an object is missing and display the relevant instruction as to what is left to upload. You just need to upload your file(s) until you see the success message.

Illustration of 1 file containing the certificate and chaining

Illustration of 1 file containing the end entity certificate and 1 file containing the CA chain

2. Click **Submit**

Results

The request status is set to **In Progress**.

An email notification is sent to every KMP Security Officer of your company informing them that the request was submitted.

Creating request 'Submit CA Chain'

This procedure begins after the user has filled out a new request up to the **Certificate Profile** field.

Procedure


1. Upload your CA Chain files

Note: the CA chain be uploaded in 1 single file or over multiple files. KMP will detect if an object is missing and display the relevant instruction as to what is left to upload. You just need to upload your file(s) until you see the success message.



Upload CA Chain

 Add attachment

 **3 CAs Root First.txt** Remove
4.9 KB

Root Details

CN
ECMS Sandbox Root CA (DO NOT USE)

Issuer
ECMS Sandbox Root CA (DO NOT USE)

Sub CA Details

CN
ECMS Sandbox Sub CA (DO NOT USE)

Issuer
ECMS Sandbox Root CA (DO NOT USE)

Sub CA Details

CN
ECMS Sandbox RSA Cloud Sub CA (DO NOT USE)

Issuer
ECMS Sandbox Sub CA (DO NOT USE)

 CA chain validated successfully

Submit

Cancel

2. Click **Submit**

Results

The request status is set to **In Progress**.

An email notification is sent to every KMP Security Officer of your company informing them that the request was submitted.

Creating request 'Share File'

This procedure begins after the user has filled out a new request up to the **Mastercard Project Contact** field.

Procedure

6. Upload your file
7. Click **Submit**

Results

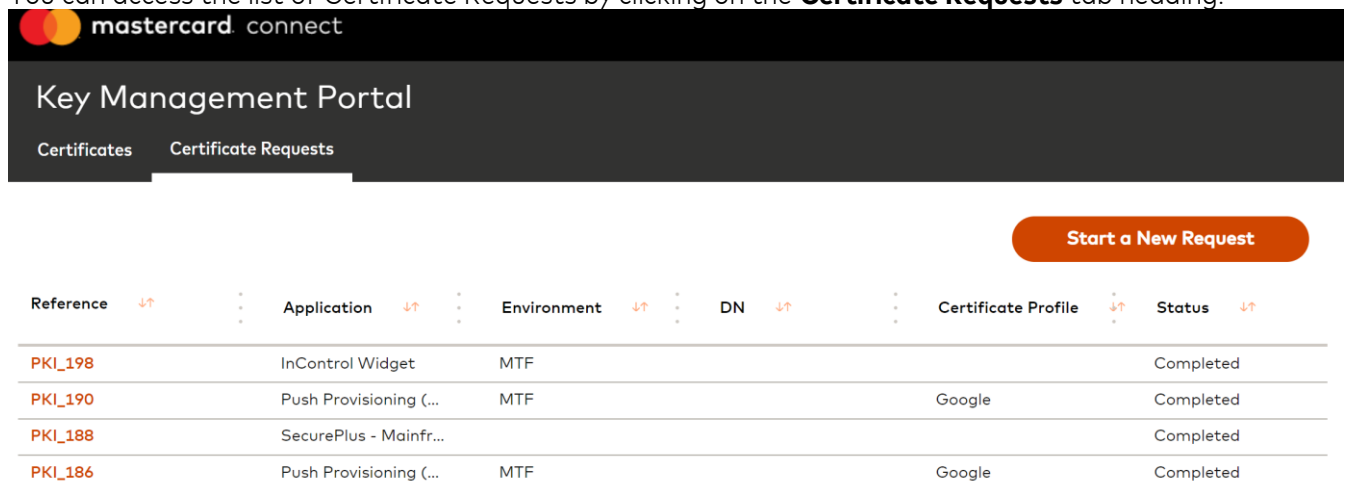
The request status is set to **In Progress**.

An email notification is sent to every KMP Security Officer of your company informing them that the request was submitted.



Viewing the List of Requests

You can access the list of Certificate Requests by clicking on the **Certificate Requests** tab heading.



The screenshot shows the 'Key Management Portal' interface. At the top left is the 'mastercard connect' logo. Below it, the title 'Key Management Portal' is displayed. There are two tabs: 'Certificates' and 'Certificate Requests', with the latter being the active tab. In the top right corner, there is an orange button labeled 'Start a New Request'. Below this is a table with the following columns: Reference, Application, Environment, DN, Certificate Profile, and Status. Each column has a small red icon indicating sorting options. The table contains four rows of data, all with a status of 'Completed'.

Reference	Application	Environment	DN	Certificate Profile	Status
PKI_198	InControl Widget	MTF			Completed
PKI_190	Push Provisioning (...)	MTF		Google	Completed
PKI_188	SecurePlus - Mainfr...				Completed
PKI_186	Push Provisioning (...)	MTF		Google	Completed

From this list, you can open a record by clicking on the **Reference** hyperlink.



Using the Certificate Request Details screen

The Request Details screen provides you with the necessary information to progress the request further.

Certificate Request PKI_184

Company Star Networks, Inc.	Application MDES - External Customer Wrapping Key - Outbound	Environment MTF	Certificate Profile Encryption			
Request Type New Certificate	Request ID PKI_184	Status In Progress	MasterCard Project Contact asd@asd.com	Requestor Mary Jones	Created On 03/04/2020	Closed On

DN Requirements

Common Name
[Customer name + free identifier, no FQDN]

Organization
[Customer Name]

Organization Unit
MDES Outbound Encryption MTF

Country
must be a valid 2 characters ISO code

CSR DN Details

Common Name
KMP

Organization
MC

Organization Unit
KMD

Country
BE

Uploaded Files

CSR - ECC test.csr

Download file 

Comments

Enter your comment here...

Area Description

Summary section

Company Star Networks, Inc.	Application MDES - External Customer Wrapping Key - Outbound	Environment MTF	Certificate Profile Encryption			
Request Type New Certificate	Request ID PKI_184	Status In Progress	MasterCard Project Contact asd@asd.com	Requestor Mary Jones	Created On 03/04/2020	Closed On

The subject DN of the object being exchanged (can be CSR, CA Chain or certificate depending on the type of request).

DN Requirements

Common Name
[Customer name + free identifier, no FQDN]

Organization
[Customer Name]

Organization Unit
MDES Outbound Encryption MTF

Country
must be a valid 2 characters ISO code

CSR DN Details

Common Name
KMP

Organization
MC

Organization Unit
KMD

Country
BE

Uploaded Files

Comments area where you post notes and comments to the request.

Actions menu. The available actions will vary based on the stage in the process that the request is at.

Certificate Request PKI_1902

[Attach Certificate and CA Chain](#)



Cancel Request

About this task

You can cancel a request if a KMD user has not started working on it. Once a request has been cancelled; it cannot be reopened.

Procedure

1. Open the request of interest
2. Click on **Cancel Request**
3. In the popup menu, fill out the mandatory **Comment**
4. Click **Submit**

Results

The request is now cancelled and permanently closed.

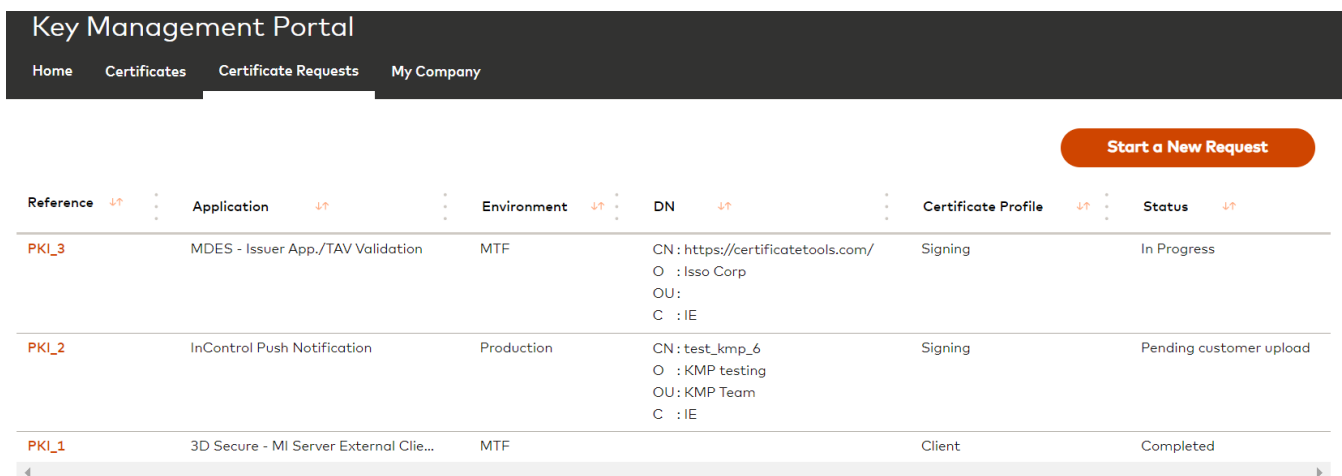
The cancelation comment is displayed under the **Comment** section.

An email notification is sent to the KMP Security Officers of your company informing them of the cancelation.

Attach Certificate to request coming from Mastercard KMD

About this task

There may be instances where the Mastercard KMD team requires a signed certificate from your company. In such scenario, a KMD user would create a request **KMD Shares CSR to be Signed** to which they will attach CSR file. An email notification is sent to every KMP security officer. Such requests would be in the status **Pending customer upload**. You will need to download the CSR and have it signed with the required CA.



The screenshot shows the Key Management Portal interface. At the top, there is a navigation bar with links for Home, Certificates, Certificate Requests, and My Company. A prominent orange button labeled "Start a New Request" is located in the top right corner. Below the navigation bar is a table with the following columns: Reference, Application, Environment, DN, Certificate Profile, and Status. The table contains three rows of data:

Reference	Application	Environment	DN	Certificate Profile	Status
PKI_3	MDES - Issuer App./TAV Validation	MTF	CN : https://certificatetools.com/ O : Issso Corp OU : C : IE	Signing	In Progress
PKI_2	InControl Push Notification	Production	CN : test_kmp_6 O : KMP testing OU : KMP Team C : IE	Signing	Pending customer upload
PKI_1	3D Secure - MI Server External Clie...	MTF		Client	Completed

Procedure

1. Open the request of interest
2. Click **Attach Certificate and CA Chain**
3. Upload your Certificate and CA Chain files

Note: the certificate and CA chain can be uploaded in 1 file or over multiple files. KMP will detect if an object is missing and display the relevant instruction as to what is left to upload.

You just need to upload your file(s) until you see the success message.




✕

Attach Certificate and CA Chain

Upload Certificate and CA Chain

[Add attachment](#)

 **test_kmp_6 (22).pem** Remove
5.0 KB

Root Details

CN
ECMS DO NOT USE ROOT CA 20190815330

Issuer
ECMS DO NOT USE ROOT CA 20190815330

Sub CA Details

CN
ECMS DO NOT USE SUB CA 20190815

Issuer
ECMS DO NOT USE ROOT CA 20190815330

End Entity DN

Common Name
test_kmp_6

Organization
KMP testing

Organization Unit
KMP Team

Country
IE

✔ Certificate chain validated successfully

SubmitCancel

4. Click **Submit**

Results

The request status is set to **In Progress** and is back with Mastercard KMD for processing.



Updating a request sent back from Mastercard KMD

About this task

If the Mastercard Key Management Delivery team finds a potential error with your request, they would send the request back to you with some review instructions (KMP would also send you an email notification about this). You will then need to open the request and make the necessary updates.

Procedure

1. Open the request of interest
2. Click **Update Request**
3. The request creation form is presented including your previous input and an information message with the instructions from KMD

The screenshot shows the 'Certificate Request Form' in the Mastercard Connect interface. At the top, a yellow warning banner reads: 'Dear Customer, the CSR contains some invalid information.' Below this, the form is divided into several sections:

- Mastercard Application:** A dropdown menu showing 'Way4Gate @ Trevica - MPTS Europe'.
- Request Type:** A dropdown menu showing 'New Certificate'.
- Environment:** A dropdown menu showing 'Production'.
- Certificate Profile:** A dropdown menu showing 'Client'.
- Mastercard Project Contact Person:** A text input field containing 'test22@mastercard.com'.
- DN Requirements:** A list of fields with instructions: 'Common Name [Issuer Name/Corporate Name]', 'Organization [Customer Organization]', 'Organization Unit: w4g-clientauth-prod', and 'Country: must be a valid 2 characters ISO code'.
- Notes:** A box containing two instructions: '- None of the DN fields can be blank.' and '- There must be NO special characters included in the value of any field.'
- Upload CSR:** A file upload area showing a file named 'CSR 5188-www.mastercard.comUPD ATED.pem' with a size of 3.8 KB and a 'Remove' button.

4. Make the necessary update and Click **Next/Submit**

Results

The request is updated with the new information and the status is set to **In Progress**.

An email notification is sent to every KMP Security Officer of your company informing them that the request was submitted.



Using Comments on Certificate Requests and Certificates

About comments

Comments are visible to all users who can view the request.

After a comment is added, an email notification is sent to the Security Officer who initiated the request. If other Security Officers from your company posted a comment on the request (and joined the conversation), they will also be notified about new comments.

Procedure

To create a comment

1. Open the request or the certificate of interest
2. Type a comment in the comment box. Clicking **Cancel** will clear any text entered in the comment box.
3. Press **Submit**

To delete a comment that you entered

1. Find the comment of interest
2. Click on the menu button next to the comment
3. Select **Delete**

Comments

Max. 500 characters allowed

Submit

Cancel

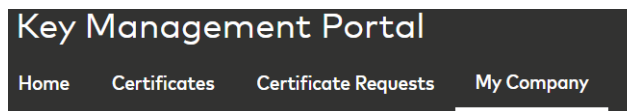
Test user

19/04/2020, 13:51:48

to Key Management - the certificate is in good order.

Viewing your Company and Security Officer Details

You can access your company details by clicking the **My Company** tab.




The screen shows some information about your company and who the registered Security Officers are.



Company Details

Company Name
Star Networks, Inc. (127964)

General Information

Certificate Management Group Email 
test@kmp.com

Security Officers

Full Name	Business Email	Security Level
Test User	lakshmi.adepu@mastercard.com	Level 1
Lakshmi Adepu	lakshmi.adepu@mastercard.com	Level 1

From the Security Officers grid, you can drill into a Security Officer record by clicking the name hyperlink.

[← Security Officers](#)

Security Officer Details

First Name Test	Last Name User	Security Level Level 1
---------------------------	--------------------------	----------------------------------

Contact Information

Business Email lakshmi.adepu@mastercard.com	Business Phone 2345789901
--	------------------------------

Address

Address 1 2200 mastercard blvd	Address 2	City o' fallon	Zip 63304
State UNITED STATES	Country UNITED STATES		

It's **important to note** that the information shown is a subset of all the information available in Mastercard Connect for your company and Security Officers. The full profile of your company can be accessed from the Mastercard Connect homepage. Information about users is maintained inside their profile in Mastercard Connect.



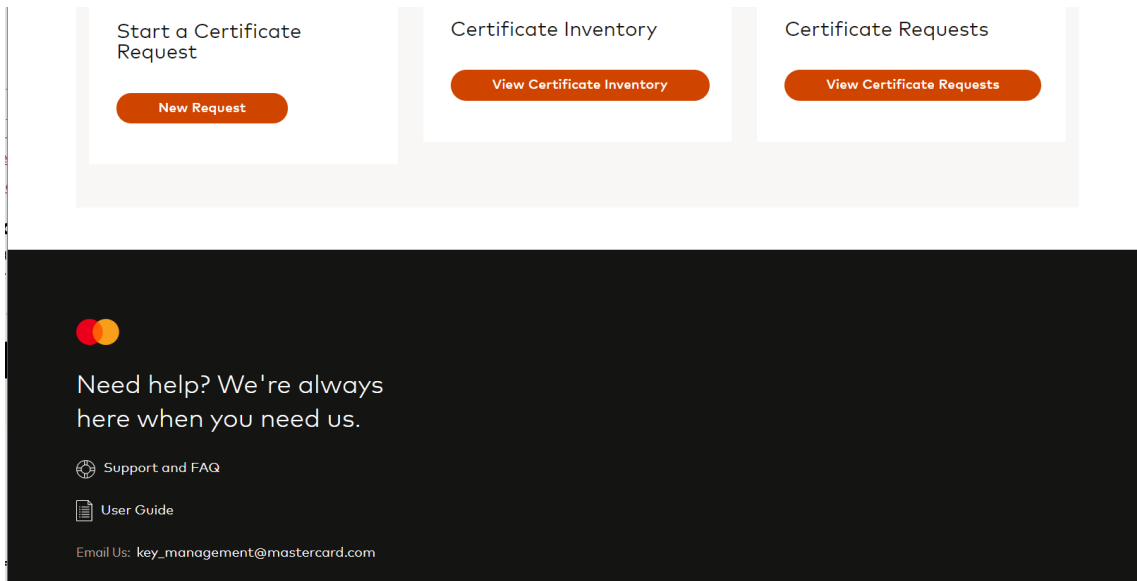
Appendix

Support Pages

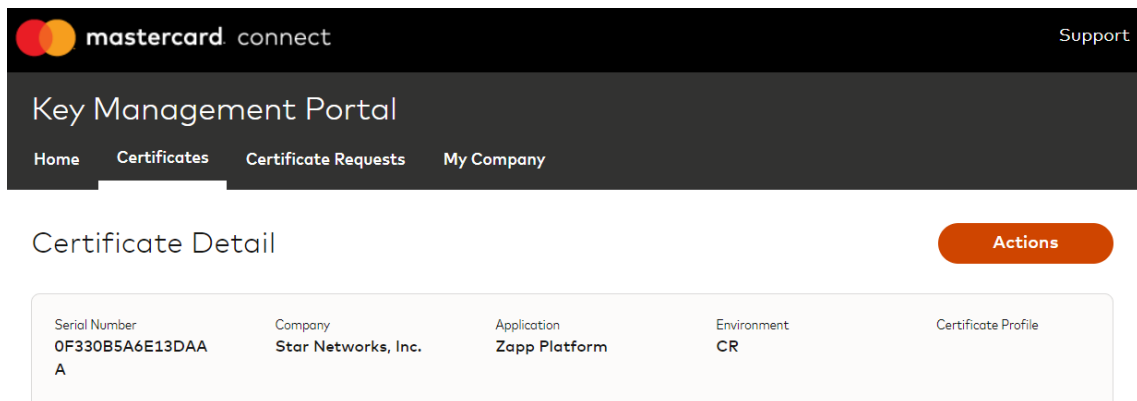
Finding the Support area

The Support area of KMP can be accessed from 2 places:

1. At the bottom of the Home page by clicking **Support and FAQ**

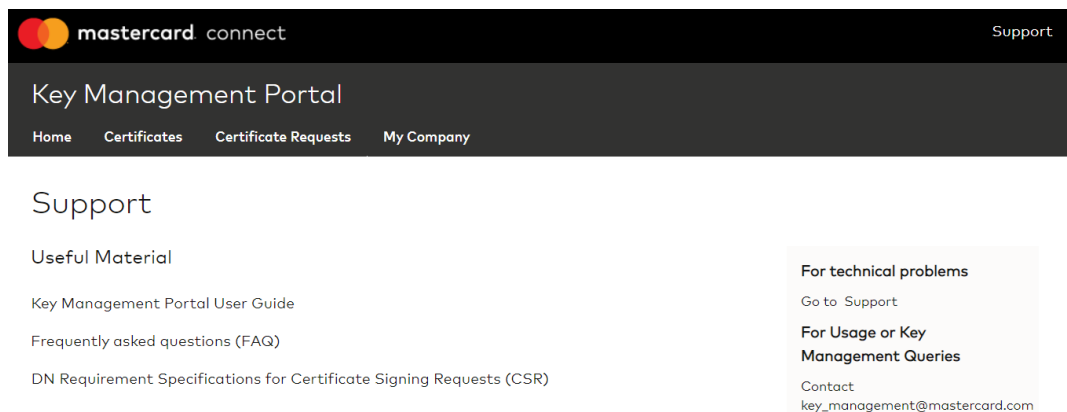


2. By clicking the **Support** link at the top right of any screen in the application



On the Support page, you can

- download the latest User Guide and Frequently Asked Questions (FAQ) documents.
- Access the **DN Requirement Specifications for Certificate Signing Requests (CSR)**
- Find some contact details to raise problems or questions



DN Requirement Specifications for Certificate Signing Requests (CSR)

On this page you can view and download the DN requirements for the relevant applications which you can choose when submitting a certificate request.

To view DN requirements, simply select the Mastercard Application of interest:

DN Requirements for PKI for Business Partners

View and export the DN requirement specification governing the submission of Certificate Signing Requests (CSR) for each relevant application.

Mastercard Application

MPTS API - MPTS Europe

[Download as PDF](#)

Certificate Profile: **Client** Environment: **Stage**

DN Requirements	Notes
<p>Common Name [Issuer Name/Corporate Name]</p> <p>Organization [Customer Organization]</p> <p>Organization Unit MPTS API-clientauth-stg</p> <p>Country must be a valid 2 characters ISO code</p>	<ul style="list-style-type: none">- None of the DN fields can be blank.- There must be NO special characters included in the value of any field.

You may download the content into a PDF document for printing.

Automated Email Notifications

The KMP application automatically sends email notifications to KMP Security Officers at key points of the workflows to keep them informed on progress or any required actions.

Each email contains some summary information about the request, as illustrated below:



Dear Security Officers,

Request ID: **PKI_930**

Requestor: **Test User**

Request Type: **New Certificate**

Application: **MasterCard Track**

Environment: **Prod**

Certificate Profile: **Client**

This request has been received by the Key Management Delivery team.

If the above information is incorrect or you believe that this request has been made in error, please contact

key_management@mastercard.com

Kind Regards,

The Mastercard Key Management Delivery Team



Supported file formats for uploading file

KMP enforces certain rules around files which can be uploaded to a certificate request.

- CSR files must be Base64 PEM (non-binary encoded, eg not DER)
- Certificate and CA Chain file requirements:
 - X.509 version 3
 - Base64 PEM encoding
 - Not expired
- The size does not exceed 100KB