Mastercard Identity Check Onboarding Guide for 3-D Secure Acquirers, Merchants, and Service Providers

15 October 2019

MIPTS

Contents

Chapter 1 Overview of Identity Check with EMV 3-D Secure

The Mastercard Identity Check® program provides merchants, acquirers, cardholders, and issuers with the benefits of authentication utilizing the Mastercard authentication network.

Introduction to Identity Check and EMV 3-D Secure

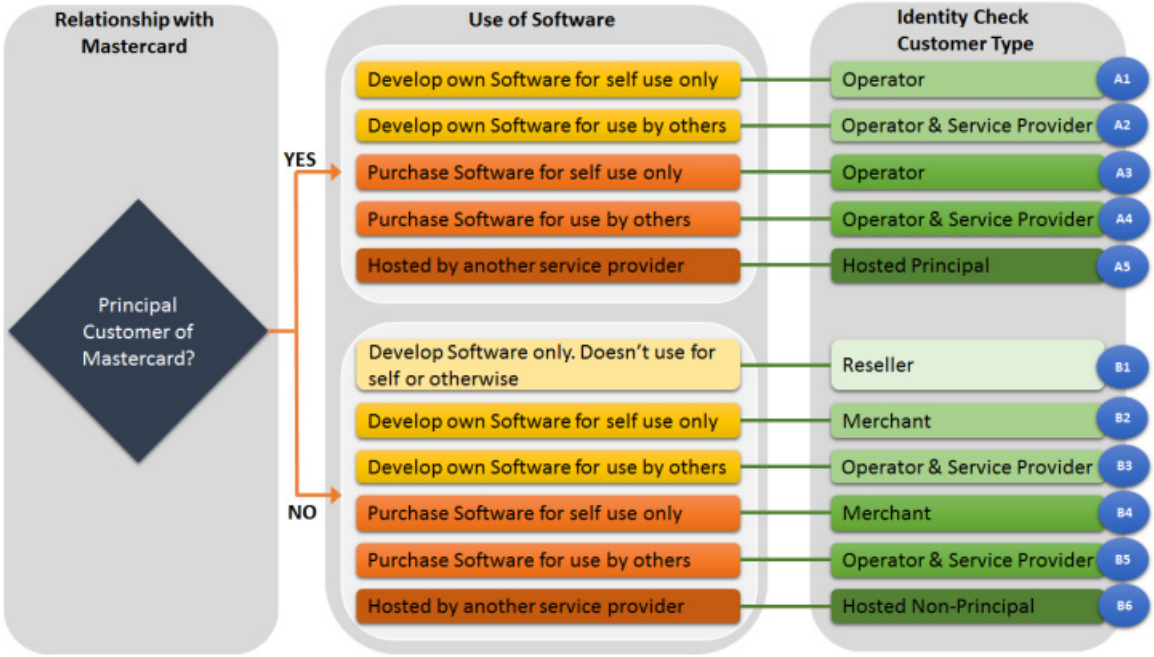
Mastercard Identity Check is a global authentication program that utilizes the Mastercard authentication network in conjunction with the EMV 3-D Secure® protocol. It is designed to help provide additional security for digital transactions and to help facilitate higher approval rates, by improving the authentication experience for merchants, issuers, and cardholders.

The purpose of this guide is to assist 3-D Secure Service Providers, Acquirers, and Merchants through the onboarding processes of program registration, testing, and production readiness. For more specifics regarding the Mastercard Identity Check program, please refer to *Mastercard Identity Check Program Guide* available on Mastercard Connect publication library.

Intended Audience

To help determine the steps required to onboard with Mastercard Identity Check, it will be important to determine your appropriate Identity Check customer type and associated scenario before you read through this Onboarding Guide.

The figure below represents the decision tree to help determine the customer type and scenario.



After determining the customer type and scenario, please refer to the table in the Scope section to understand the summary of the required onboarding steps.

Customer Type Definitions

The definitions listed below relate to Mastercard Identity Check onboarding for acquirers, merchants, and 3DS service providers.

Principal Licensed Customer of Mastercard—A customer licensed by Mastercard to offer branded products and services.

Mastercard 3DS Service Provider—This is a new category within the Mastercard service provider program. An entity that hosts 3DS authentication solutions for Mastercard principal customers and their merchants. Non-customers that provide authentication service such as Identity Check using EMV 3-D Secure are required to register in the program.

Acquirer—The Mastercard principal customer that provides the authorization and/or clearing functions for their merchants using Mastercard Identity Check and EMV 3DS.

Merchant—A 3DS requester using authentication services from a 3DS server. The 3DS requester may use a 3DS SDK.

Reseller—Entity that develops software for resale only and does not operate the software.

3DS Server Operator—Any party operating a 3DS server that will connect to the Mastercard Identity Check directory server.

3DS Service Provider—This is the 3DS Server Operator that offers a hosted service for other Mastercard principal customers.

Hosted Principal—An acquirer, issuer, or processor that uses a service hosted by a third party ACS or 3DS Server solution.

Operator—A customer that operates ACS software, who bought the ACS software from a reseller, and wants to connect to the EMV 3-D directory server.

Scope

In general, onboarding with Mastercard Identity Check consists of five major steps.

These steps vary depending upon the relationship with Mastercard, use of software and the customer type.

Each step has multiple activities and prerequisites. This guide will walk through those steps. A complete checklist is provided in *Appendix A: Onboarding Checklist*. The major steps are as follows:

Identity Check Scenario/Customer Type		Prerequisite	Mastercard Identity Check Onboarding Steps				
		EMVCo Certification Testing Required?	Register as a Mastercard 3DS service provider	PCI Compliance Required	Register on Mastercard Identity Check platform as	Mastercard Identity Check Compliance testing required	Complete Enrollment Process
A1	Operator	Yes	No	Yes	Principal	Yes	Yes
A2	Operator & Service Provider	Yes	Yes	Yes	Principal	Yes	Yes
A3	Operator	No	No	Yes	Principal	Yes	Yes
A4	Operator & Service Provider	No	Yes	Yes	Principal	Yes	Yes
A5	Hosted Principal	No	No	No	Principal	No	Yes
B1	Reseller	Yes	No	No	N/A	No	No
B2	Merchant	Yes	No	Yes	Merchant	Yes	Yes
B3	Operator & Service Provider	Yes	Yes	Yes	Service Provider	Yes	Yes
B4	Merchant	No	No	No	Merchant	Yes	Yes
B5	Operator & Service Provider	No	Yes	Yes	Service Provider	Yes	Yes
B6	Hosted Non-Principal (Merchant or payment gateway)	No Onboarding required with Mastercard Identity Check program					

NOTE: A1, A3, and B2 have to be PCI compliant but does not require proof A2, A4, B3, and B5 have 30 days to submit their AOC to Mastercard.

1. EMV 3-D Secure Compliance Testing and Approvals

Although this is a requirement of EMVCo, in many cases, this is also a prerequisite to entry onto the Mastercard Identity Check testing platform. Successful EMVCo testing results in a Letter of Approval and a 3DS Server Reference Number or SDK Reference Number assignment. This prerequisite is noted when applicable.

2. Mastercard 3-D Secure Service Provider Registration

This is a category within the Mastercard Service Provider Program. This registration is specific for service providers and is used to manage 3DS PCI Compliance. This registration also enables service providers to access Mastercard Connect and the testing platform for registration and testing. Once the Service Provider Registration is complete, a Company ID, Operator ID, a billable ICA number, and 3DS Requestor ID prefix is issued.

NOTE: The only exception to this rule is if a Mastercard acquiring customer operates the software (Customer Types A1 and A3). These customers will fall under the Mastercard PCI Compliance rules.

NOTE: The 3DS Server must use the 3DS Requestor ID prefix as a traceability mechanism to clearly identify the PSP at the Merchant level. Refer to Chapter 4—*Mastercard Identity Check Required Data Elements* section of the Mastercard Identity Check Program Guide for more information.

3. Mastercard Identity Check Registration

Mastercard Identity Check registration enables the principal customers to accept the terms and conditions and declare their ability to support their merchant participation. This step will include requesting Mastercard Connect (MCC) access, along with getting access to the applications needed to support the Identity Check Program. Program registration is completed through the Mastercard Identity Check Test Platform application found on Mastercard Connect. Customers will need to request this access through the MC Connect store prior to completing program registration. Mastercard Identity Check program registration is completed with the customer's Company ID(s) (CIDs) and billable ICA numbers for Mastercard principal customers (acquirers). The merchant's acquirer must be registered before a merchant and merchant ID can be enrolled on the directory server.

4. Mastercard Identity Check Compliance Testing

The Mastercard Identity Check Test Platform is used to register and test operators, service providers, and merchants, as defined by the Mastercard Identity Check Customer type. All entities requesting a connection to the Mastercard Identity Check directory server are required to register and complete compliance testing. A Letter of Compliance is issued when compliance testing is successfully completed.

NOTE: Connecting to the Mastercard Identity Check Test Platform will require development to proprietary APIs to establish full connection to the test platform. More information can be found in the *Mastercard Identity Check Test Platform User Guide Appendix A*.

5. Enrollment, Production Preparation, and Deployment

The Mastercard Identity Check directory server enrollment enables production loading of acquiring Bank Identification Numbers (BIN) with merchant IDs. Production certificate connectivity is unrelated to merchant enrollment and all of the previous steps described above must be completed prior to merchant enrollment in production.

NOTE: Identity Check Program Registration is a prerequisite for Directory Server Enrollment. If program registration does not occur or registration data does not match enrollment data, directory server enrollment will fail and enrollment will not be possible.

Contacts and Related Reference Materials

This is a list of contacts and related reference materials for Mastercard Identity Check.

Global Customer Service

U.S., Canada, Caribbean, Latin America, and Middle East/Africa regions

- Phone
  - 800-999-0363 (Inside U.S.)
  - 636-722-6176 (Outside U.S.)

  - 636-722-6292 (Spanish Language Support)
- Fax: 636-722-7192
- Email: IDC_Customer_Support@mastercard.com

Mailboxes

- Mastercard Identity Check program queries: 3DS2@mastercard.com
- For questions concerning compliance: Identity_Solutions_Compliance@mastercard.com

Related Mastercard Publications

- Mastercard Identity Check Test Platform User Guide
- Identity Solutions Services Management (ISSM) User Guide
- Mastercard Identity Check Program Guide (includes Processing Matrix)
- Mastercard Transaction Processing Rules
- Mastercard Rules - Chapter 7 Service Providers

Quick Reference Booklet – Merchant Edition

https://www.mastercard.us/en-us/about-mastercard/what-we-do/rules.html

EMVCo

https://www.emvco.com/

PCI Security Standards Council

https://www.pcisecuritystandards.org/

Mastercard Connect

www.mastercardconnect.com

Mastercard Identity Check and EMV 3-D Secure Terms

This section describes the acronyms used in this guide.

Acronym	Description
3DS	Three Domain Secure
3DS SDK	3-D Secure Software Development Kit
3DS Server	The system that facilitates communication between the 3DS requestor and the Mastercard Identity Check directory server.
3DS Server Reference Number	Reference number assigned by EMVCo

Acronym	Description
3DS Server Hosted Service Provider	A 3DS server operator that hosts the service for other entities.
3DS Server Operator	The entity that operates the 3DS server.
3DS Server Operator ID	Reference number assigned by Mastercard
3-DSS	3DS Server
ACS	Access Control Server
BIN	Bank Identification Number
CID	Company ID
CAI	Cyber and Intelligence Solutions
CIS	Customer Implementation Services
CSR	Certificate Signing Request
DS	Mastercard Identity Check Directory Server
EMVCo	EMVCo, LLC is a technical body that facilitates the worldwide interoperability and acceptance of secure payment transactions by managing and evolving the EMV specifications and related testing processes. It is the governing body for the EMV 3-D Secure Protocol.
EMV 3-D Secure	Specification published by EMVCo (3DS 2.0)
GCS	Global Customer Service
GIS	Global Information Security
IAV	Issuer Authentication Value
IDC	Mastercard Identity Check
ISSM	Identity Solutions Services Management
KMS	Key Management Services
KPI	Key Performance Indicator
LOA	Letter of Approval (issued by EMVCo)
LOC	Letter of Compliance (issued by Mastercard)
PCI SSC	Payment Card Industry Data Security Standards Council
SDK Reference Number	Reference number assigned by EMVCo
SHA2	Secure Hash Algorithm 2
SPA2	Mastercard AAV (UCAF) algorithm for support of Identity Check and EMV 3-D Secure
SUT	System Under Test
TLS	Transport Layer Security

Acronym	Description
UCAF	Universal Cardholder Authentication Field in Mastercard Authorization

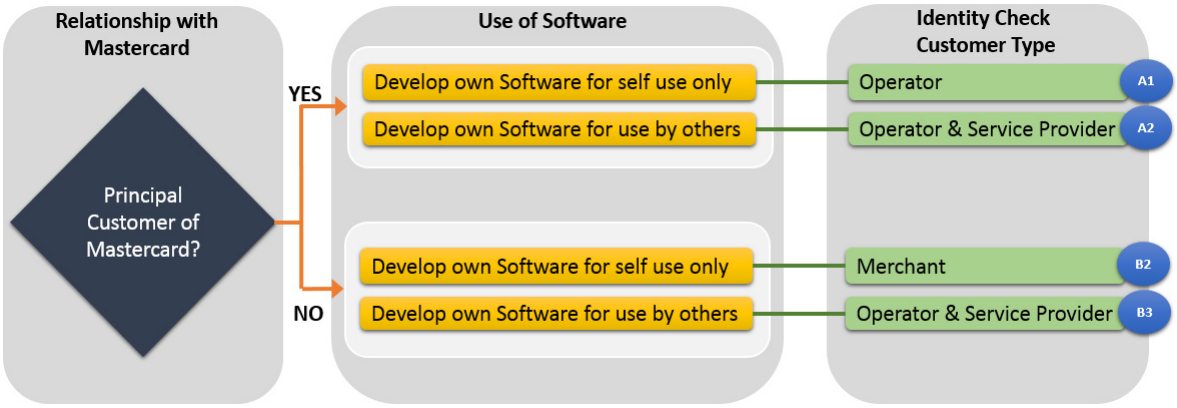
Chapter 2 Prerequisites

This section provides an overview of the EMVCo certification and Mastercard 3-D Secure Service Provider registration.

EMVCo Certification

This section provides an overview of the steps required to obtain EMVCo certification.

The EMVCo Certification is a prerequisite step for the following Identity Check customers types and scenarios: A1, A2, B2, and B3.



Prior to testing with Mastercard, the customer types listed above must complete Testing and Approval of their software through the EMVCo Certification process and receive their Letter of Approval and applicable Reference Number.

EMV 3DS Approval Process

The EMVCo Approval Process consists of three phases: Pre-Compliance, Compliance, and Approval.

1. **Pre-Compliance**
   - This phase is designed to give operators and service providers the opportunity to run test cases and evaluate their products.
   - At the end of this phase, test results are evaluated by EMVCo prior to moving to Compliance Testing.
2. **Compliance**
   - This phase is designed to give operators and service providers the opportunity to run test cases and complete final testing.
   - Final test results are approved by EMVCo.
3. **Approval**
   - Operators and Service Providers receive the signed Letter of Approval and Reference Number from EMVCo.

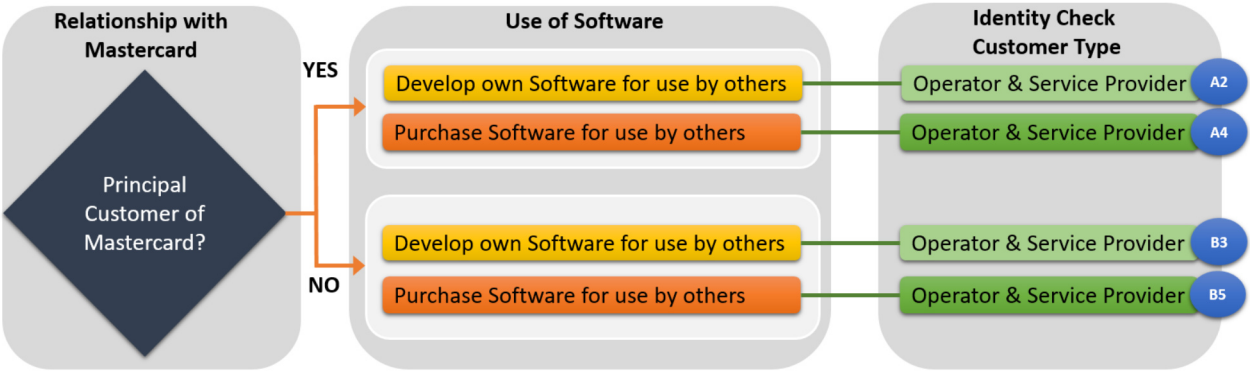
Useful EMVCo Links

- EMVCo 3-D Secure Protocol and Core Functions Specification: www.emvco.com
- EMV 3-D Secure specification questions: 3DS_admin@emvco.com
- EMVCo 3DS compliant software: https://www.emvco.com/emv-technologies/3d-secure/

Mastercard 3-D Secure Service Provider Program Customer Type

This section describes the steps required to register as a Mastercard 3-D Secure Service Provider.

Registering as a service provider is a pre-requisite step to starting the onboarding process with Mastercard Identity Check for the following Identity Check customers types and scenarios: A2, A4, B3, and B5.



Background

In November 2017, PCI Security Standards Council (PCI SSC) released a new security standard called PCI 3DS Core Security Standard. This security standard supports EMVCo's EMV® 3- D Secure (3DS) Protocol and Core Functions Specification which is to be adopted globally across all payment networks in 2018. With the release of this new Security Standard, Mastercard must help ensure all 3-D Secure vendors adhere to security requirements and rules which are managed through the Service Provider Program. The creation of this new classification highlights which vendors must adhere to the PCI 3DSCore Security Standard.

3-D Secure Service Provider

Mastercard established a new service provider category 3-D Secure Service Provider. A 3-D Secure Service Provider is an entity that operates as follows:

- Controls a 3-D Secure Server system that facilitates communication (through the EMV® 3-D Secure specification) to initiate cardholder authentication under the Mastercard Identity Check Program rules.
- Manages an Access Control Server (ACS) system that verifies (through the EMV® 3-D Secure specification) whether authentication is available for a card number and device type, and authenticates specific cardholders under the Mastercard Identify Check Program rules.

3-D Secure Service Provider Registration

Each principal customer that supports transactions by means of a 3-D Secure Program must register the 3-D Secure Service Provider as required by the Mastercard Standards. Principal

customers should register the 3-D Secure Service Provider on behalf of their affiliate customers.

Registration requirements are as follows:

1. Principal customer (sponsor) must register 3-D Secure Service Provider in My Company Manager application on Mastercard Connect. For more information refer to the user guide:
   https://www.mastercardconnect.com/business/public/content/dam/b2b/mcc/guides/Service_Provider_Registration_Step_by_Step.pdf

   Additional resources for Service Provider maintenance activities can be found https://www.mastercardconnect.com/business/secured/en-us/cmscommon/home/support/myapps.html#/mycompanymanagerapp

   NOTE: If the service provider profile does NOT exist a new registration will need to occur. It takes 48 hours for the new service provider to become active. Once the service provider is in the system, the registration can occur.
2. The Identity Solutions Compliance team will confirm back to Service Provider of completed registration and provide next steps.
3. Service Provider will be assigned the following:
   - Company ID - will be used to log on to Mastercard Connect and request access to the Mastercard Identity Check Testing platform application.
   - Operator ID - will be used to request both your testing and production certificates and will be also included in your EMV-3DS messages.
   - 3DS Requestor ID Prefix – for more information regarding this value, refer to the Mastercard Identity Check Program Guide.
   - 3DS Service Provider will be assigned a billable ICA number prior to opening a compliance project. This will be sent via email to the Service Provider.

   NOTE: For Customer Types that do not require Service Provider registration (A1, A3, B2, and B4), contact identity_solutions_compliance@mastercard.com to request to be assigned an Operator Id and 3DS Requestor ID Prefix.
4. The 3-D Secure Service Provider should complete form 1145b. The form will give users access to Mastercard Connect and the Security Administrator application. A SecureID soft token will be emailed to the users. The Security Administrators will be responsible for managing the users from their company.
5. Upon approval of the service provider registration, all 3-D Secure Service Providers must submit an Attestation of Compliance (AOC) certificate to pcireports@masterard.com. The 3-D Secure Service Provider has 30 days to submit upon confirmation of registration. For additional information regarding PCI 3DS requirements, refer to https://www.pcisecuritystandards.org/

NOTE: If you are currently registered as a service provider under another program, you are also required to register as a 3-D Secure Service Provider following all steps listed above. Principal Customer (Sponsor) may be subject to a registration fee.

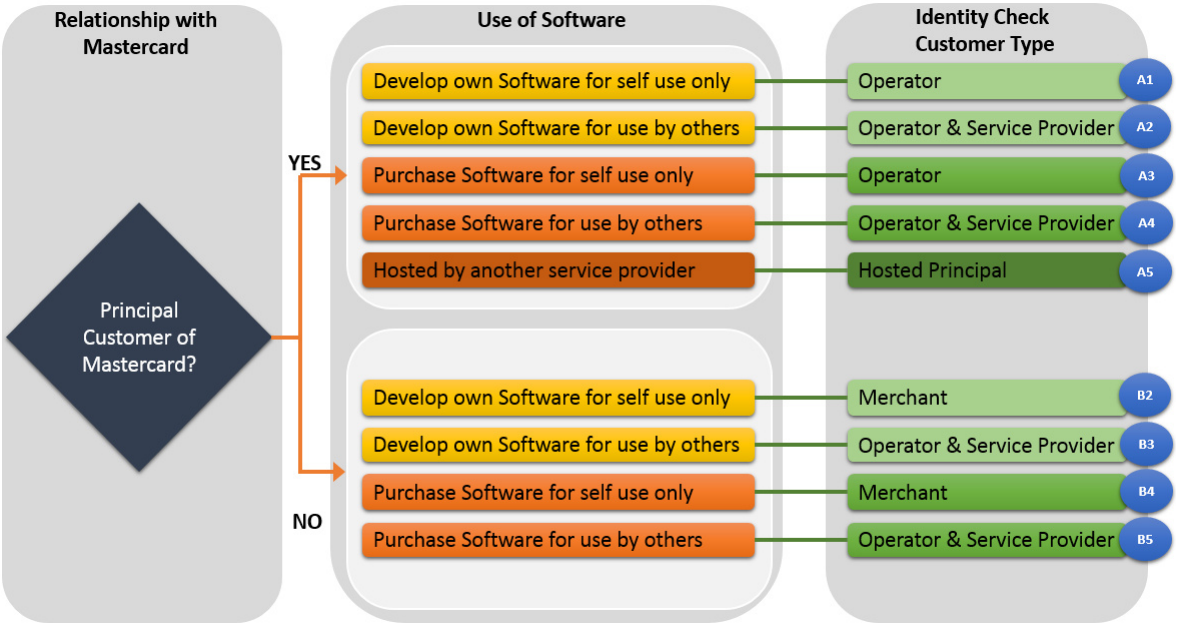
Chapter 3 Mastercard Identity Check Program Registration

This section describes the registration process for customer types A1-B5.

Mastercard Connect Access and Mastercard Identity Check Test Platform Registration

This section describes in detail the steps required to request access to Mastercard Connect and to register on Mastercard Identity Check Testing Platform.

This step is applicable to all Identity Check customer types and scenarios: A1-A5 and B2-B5.



Request access to Mastercard Connect

Request access to Mastercard Connect through https://www.mastercardconnect.com.

Review Access to Mastercard Connect for further information on Mastercard Connect sign up process.

1. Sign in to the Mastercard Connect (https://www.mastercardconnect.com). Review Mastercard Connect Sign Up Guide for further information on Mastercard Connect Registration details.
2. On page three of the sign up process, select the Business Classification of Processor then enter your Company Name or Company ID.
3. You will receive an on screen confirmation number. You will also receive an email indicating that your order was sent to your Security Administrator for approval. Once the order is approved, you will receive an email notification that your account is ready for use.

Required Applications

Once the Mastercard Connect account is ready for use, it is recommended that each user requests access to the following applications in the Mastercard Connect Store.

1. Publications
2. Mastercard Identity Check Test Platform
3. My Company Manager / Company Contact Management
4. Technical Resource Center
5. Identity Solutions Services Management (ISSM)

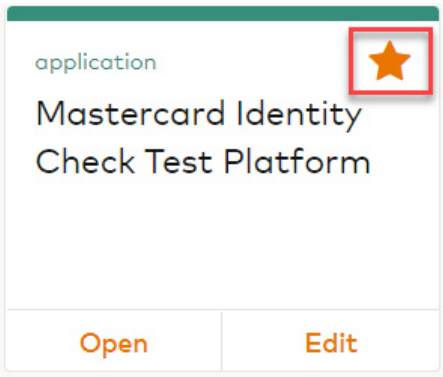
NOTE: Identity Solutions Services Management is a tool designed for principal customers (acquirers) to enroll its merchant ids and acquiring bins on the directory server. Service Providers can receive access if a principal customer delegates access on its behalf.

After all approvals have taken place, the applications will be available under My Items. The Mastercard Identity Check Test Platform does not require approvals and will be found under My Items after checkout. The Publications page can be found on the Support page.

Accessing the Mastercard Identity Check Testing Platform

1. Sign in to Mastercard Connect using your User ID and Password
2. Launch the Mastercard Identity Check Test Platform

NOTE: The application can be found under the 'My Items' section on MC Connect. Users have the ability add applications to the MC Connect Home page by clicking the star icon in the top right of the application.



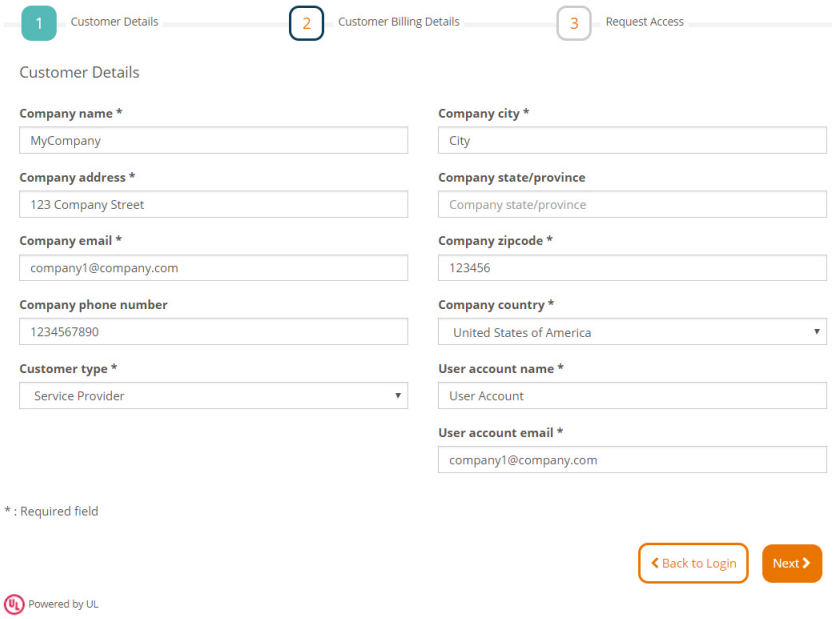
3. Review the related publications including the Mastercard Identity Check Program Guide to understand the specific processing and program requirements.
4. Open the Mastercard Identity Check Test Platform application and complete each of the following three sections. Reference the following table to assist users with registration:

Table 1: Customer Type Registration

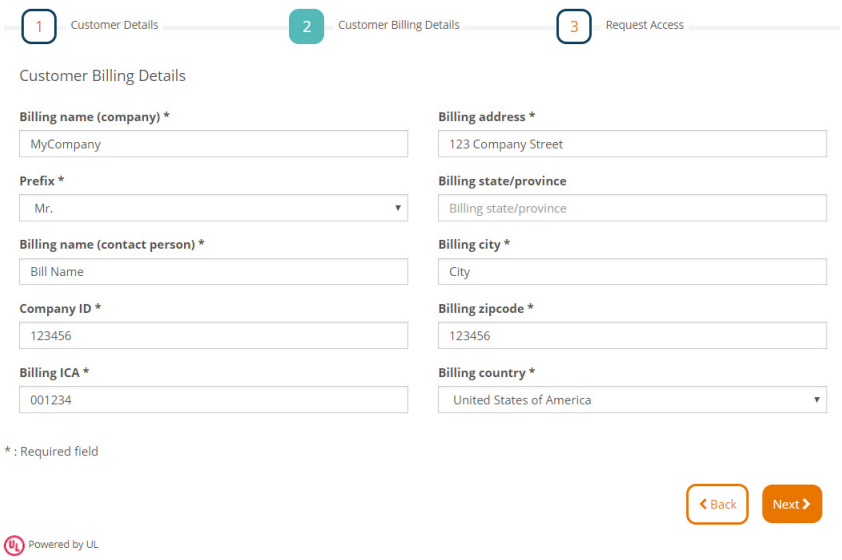
Customer Type	Customer Type:	Registration Type:
A1, A2, A3, and A4	Principal Customer	Mastercard Identity Check Program Registration and Testing

Customer Type	Customer Type:	Registration Type:
A5	Principal Customer	Mastercard Identity Check Program Registration Only
B2 and B4	Merchant	Mastercard Identity Check Program Registration and Testing
B3 and B5	Service Provider	Mastercard Identity Check Program Registration and Testing

a. **Customers Details**—fill in applicable company information and select Customer Type based on the Customer Type Registration table above.



b. **Customer Billing Details**—complete billing details that are registered with Mastercard.
   - Service Providers will be provided with applicable billing details at the completion of **3-D Secure Service Provider Registration** located in the Mastercard 3-D Secure Service Provider Program Customer Type section above.
   - Principal Customer will use the billing identifiers associated to their company



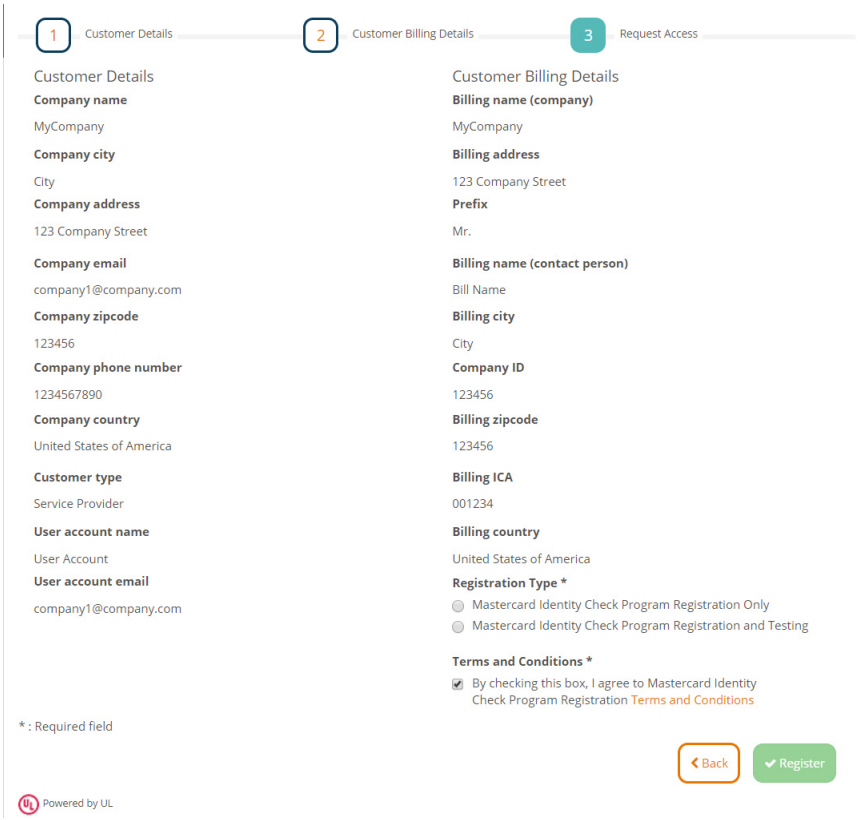
c. **Request Access**—Review and confirm registration information
   - Select Registration Type based off customer type shown in the Customer Type Registration table.
     - When registration type is Mastercard Identity Check Program Registration only, a confirmation message appears indicating no further action is required
     - When registration type is Mastercard Identity Check Program Registration and Testing, a temporary test platform User ID/Temporary password is assigned
   - Review and Accept Terms and Conditions.
   - Select Register button at the end of the Screen.

A confirmation message will be displayed that no further actions is required.

Example: "Thank you for your registration. If this was a registration only request, no further action required. If this is a registration and testing request, expect further correspondence from your assigned Customer Implementation Support Project Manager."

- If Registration and Testing was selected, Mastercard Customer Implementation Services (CIS) team will be in contact regarding user id, temporary password, and project kick off.
- If Registration Only was selected, no further action is needed. Users will not receive access to the test platform, log in credentials will not be provided, and no email notification will be sent to user.

NOTE: Program Registration is completed at the Company ID level. Principal customers are required to submit one registration per assigned CID supporting the Identity Check Program regardless of region, product, and BIN prior to enrolling merchants or card ranges on the Directory Server.



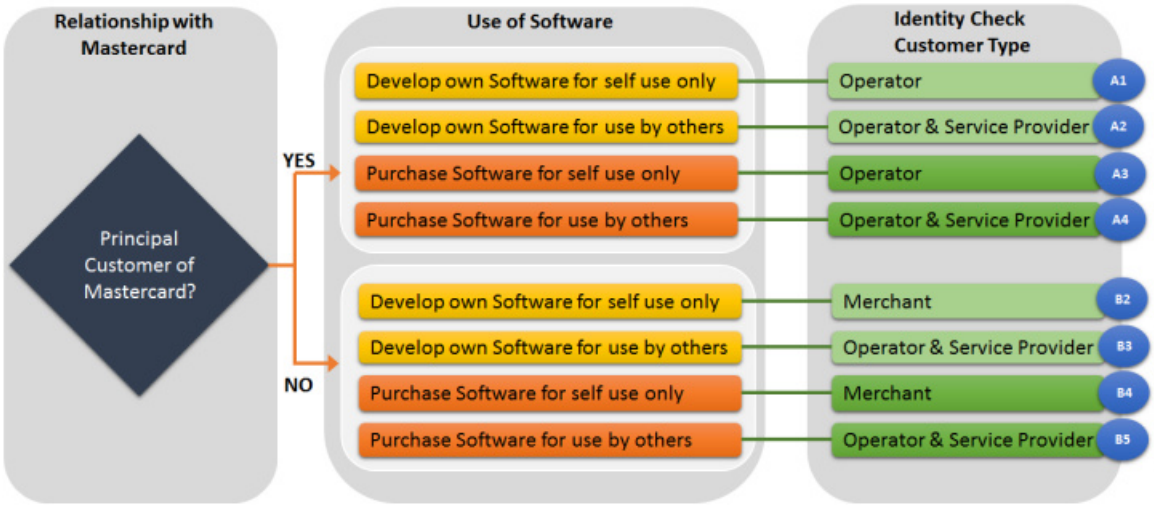
Chapter 4 Mastercard Identity Check Platform Compliance Testing

Testing on the Mastercard Identity Check platform enables EMVCo tested and approved components to test compliance with Mastercard Identity Check program processing rules. The testing platform allows the 3DS server to create a testing request and perform sandbox testing, pre-compliance testing, and final compliance testing. Successfully completed testing results in a Letter of Compliance and a 3DS Server Operator ID.

Mastercard Identity Check Testing

This section describes in detail the steps required complete testing certification with Mastercard Identity Check Test Platform. Refer to the Mastercard Identity Check Test Platform User Guide for more detailed information on using the test platform.

The section is applicable to the following Identity Check customer type and scenarios: A1-A4 and B2-B5.



NOTE: The testing window for the Mastercard Identity Check Test platform is 31 days to complete pre-compliance and compliance testing. The 31 day window begins when CIS contacts the customer with the platform credentials. If testing is not complete in 31 days, an additional testing window of 31 days may be assessed. Compliance testing fees are billed using MCBS event 2VC8005. Completion is defined as all test cases executed and signed off by Mastercard and a Letter of Compliance (LOC) is generated. Customer implementation fees are separate from compliance fees and may vary per region.

Testing Certificate Setup

1. Create and submit testing Certificate Signing Request (CSR) and send to your assigned CIS Project Manager. An example of the CSR form and details can be found in the *Certificate Forms and Details* section. Certificate ID protection is not required for testing certificates. The following certificates are required:
   - 3DS Requestor TLS Server
   - 3DS Requestor TLS Client

   NOTE: These are individual certificates. Mastercard does not issue combined/dual certificates.
2. Sign in to the Identity Check Test platform application using your ID/temporary password and create a new password.
3. Install the test certificates provided by Mastercard.

4. Set up a project and accept testing Terms and Conditions on the Mastercard Test Platform.

Sandbox Connectivity

1. Use Sandbox Testing to connect your 3DS Server software to the Mastercard Identity Check Testing Platform.
2. To establish connectivity to the Mastercard Identity Check Test Platform, the 3DS Server will be required to code to proprietary API messages to fully connect to the test platform. These proprietary API messages help simulate the message flow within the 3DS Requestor Environment.

   NOTE: These proprietary API messages are the same messages that are used during the EMVCo testing. Minor modification may be required to connect to the Mastercard environment. Refer to the *Mastercard Identity Check Test Platform User Guide Appendix A* for more information.

3. After Connectivity has been established, select Move to Pre-Compliance.

Pre-Compliance Testing

The pre-compliance testing area allows you to manually run and re-run test cases as needed.

1. Pre-Compliance Testing.
   – Manually run and rerun test cases as needed
   – Pass all automated and manual test cases
   – Submit test cases for review and await approval from CIS project manager before you move to Compliance Testing
2. Under Main Menu > Company Profile > Customer Details, the Principal Customer administrator needs to populate the 3DS Server Certificate ID. The 3DS Server Certificate ID will be used to protect your Production CSR file.
3. Obtain Pre-Compliance approval from CIS Project Manager. The project automatically moves to Compliance Testing.
4. Complete Letter of Compliance Form.
   – Contact Information
   – Business Contact
   – Security Contact
   – Certificate Contact
   – Click Submit for LOC review and wait for approval from CIS Project Manager

Compliance Testing

1. Execute all test cases. If one test case fails, the compliance test will be required again.
2. Complete a Mastercard Survey
3. Obtain your Mastercard 3DS Operator ID and Letter of Compliance

Production Certificate Set Up

Additional information on how to create a CSR can be found in Appendix B of this guide.

1. Create and submit a Certificate Signing Request (CSR) to request access to Production. Copy the CSR to a password protected zip file. The password to protect the zip file content must be the 3DS Server Certificate ID. To locate the 3DS Server Certificate ID, on the Main Menu, select Company Profile, then click Customer Details. Send the password protected zip file to key_management@mastercard.com. The following certificates are required:
   – 3DS Requestor TLS Server
   – 3DS Requestor TLS Client

   In order for KMS to receive clear certificate requests, 3DS Servers must review and complete the request tables and provide the CSRs.

   Additional information on how to create a CSR can be found in Appendix B, Production Procedures.

Table 2: Certificate Forms and Details

Identity Check 3DS 2.0 – SHA2 – Certificate request	
Environment	Test / Prod
CSR file/attachment name (optional)	-
Operator ID	-
Certificate type	• 3DS Server TLS Server • 3DS Server TLS Client
Certificate renewal because expiration	Yes / No
Expiring Certificate serial number	-
Expiring Certificate DN	-

Table 3: DN Requirements

3DS Server TLS Server	**3DS Server TLS Client**
CN: [Domain Name] OR [public IP]	CN: [Domain Name] OR [public IP]
PROD OU: 3DSS-[Operator ID]	PROD OU:3DSC-[Operator ID]
MTF OU: 3DSS-MTF-[Operator ID]	MTF OU:3DSC-MTF-[Operator ID]
O: [Operator registered company name]	O: [Operator registered company name]
ST: <State optional>	ST: <State optional>

3DS Server TLS Server	3DS Server TLS Client
L: <Local optional>	L: <Local optional>
C: [valid 2 character ISO country code]	C: [valid 2 character ISO country code]

NOTE: The Mastercard-assigned Operator ID is provided once service prover registration is complete and should be included in the OU attribute. The format of the Mastercard-assigned Operator ID: (Component Type - 3 char alpha fixed)-(Version - 4 char alpha numeric fixed)-(Client Name – variable up to 17 varchar)-(Serial number 5 digits numeric fixed). For example: SVR-V210- ACME_INC-12345.

Appendix A Identity Check Onboarding Documentation

This appendix contains documentation needed for Identity Check onboarding.

Onboarding Checklist

	Task / Requirement	Acquirer	3DS Server	Merchant	SDK	Reference
□	Choose a Mastercard Identity Check compliant 3DS server service provider	X		X		Compliant Vendor service provider
□	Review the Mastercard Identity Check Program Guide	X	X	X		Mastercard Connect/Publications
□	Open a project with 3DS server operator	X		X		
□	Coordinate merchant onboarding with 3DS Server and Acquirer for Mastercard Identity Check	X	X	X		
□	Review Mastercard Identity Check branding requirements	X	X	X		Branding Guidelines
□	Begin registration as a Mastercard 3-D Secure Service Provider – Request your sponsor (issuer or acquirer) to complete registration on behalf of 3DS Server	X	X			Mastercard Connect/My Company Manager

	Task / Requirement	Acquirer	3DS Server	Merchant	SDK	Reference
□	Receive 3-D Secure Service Provider Company ID (CID) assigned by Mastercard franchise and sent to Sponsor	X	X			3DS server operator should request the CID from their Sponsor
□	Receive 3-D Secure Service Provider Mastercard assigned 3DS Server Operator ID, 3DS Requestor ID prefix, and an ICA number for billing, if applicable		X			
□	Complete form 1145b to assign Security Administrators to manage the access for the 3-D Secure Service Provider		X			online_provisioning@mastercard.com
□	Sign up for Mastercard Connect using assigned 3DS Service Provider CID		X			Mastercard Connect
□	Review the PCI 3DS Core Security Standard Specification and related documents, and begin assessment process		X		X	PCI Security Standards Operation

	Task / Requirement	Acquirer	3DS Server	Merchant	SDK	Reference
□	Provide appropriate PCI 3DS materials to the Mastercard Standards Team as required by the 3DS Service Provider Program		X			PCI Security Standards Organization Document Library
□	Complete applicable testing with EMVCo and receive Letter of Approval and Reference ID		X		X	https://www.emvco.com
□	Request access/ verify access to the following: • Mastercard Identity Check Testing Platform application • Publications • My Company Manager / Company Contact Management • Identity Solutions Services Management (ISSM) application	X	X			Mastercard Connect/Store **NOTE: ISSM access is designed for principal customers (acquirers) only. Access may be delegated to service providers at the discretion of the acquirer.**
□	Review the Mastercard Onboarding Guides	X	X			Mastercard Connect/Publications
□	Register the SDK and request Mastercard Public Key				X	https://developer.mastercard.com

	Task / Requirement	Acquirer	3DS Server	Merchant	SDK	Reference
□	Register for the Merchant Enrollment API, if applicable	X	X			https://developer.mastercard.com/product/identity-check
□	Ensure transactions are TLS 1.2 or greater		X			
□	Sign in to Mastercard Connect, and access the Mastercard Identity Check Testing Platform	X	X			Mastercard Identity Check Testing Platform

	Task / Requirement	Acquirer	3DS Server	Merchant	SDK	Reference
□	Register for Mastercard Identity Check. Customer Details • Select customer type "Principle Customers" Customer Billing Details Request Access • Select appropriate registration type Accept Terms and Conditions Select "Register" button at the end of the screen • Confirmation message will be displayed that no further actions is required	X				Mastercard Identity Check Testing Platform

	Task / Requirement	Acquirer	3DS Server	Merchant	SDK	Reference
□	Register and test for Mastercard Identity Check Customer Details • Select customer type "Service Provider" Customer Billing Details Request Access • Select Mastercard Identity Check Program Registration and Testing Accept Terms and Conditions Select "Register" button at the end of the screen		X			Mastercard Identity Check Testing Platform
□	Receive a Mastercard Identity Check Testing Platform user ID and temporary password		X			Provided by Mastercard
□	Mastercard will assign a CIS project manager					Provided by Mastercard

	Task / Requirement	Acquirer	3DS Server	Merchant	SDK	Reference
□	Create and submit testing Certificate Signing Request (CSR) according to specifications. Required Certificates: 3DS Server TLS Client 3DS Server TLS Server One set required per 3DS server connecting to DS. All certificates will be SHA2.		X			Submit to Customer Implementation Service (CIS) project manager. Test CSR does not need password protection.
□	Install testing certificates		X			Provided by Mastercard
□	Develop toward proprietary API messages for Test Platform connectivity		X			Identity Check Test Platform User Guide, Appendix A
□	Sign in to Mastercard Identity Check Testing Platform with the User ID and Temporary Password, and create a new password		X			Mastercard Identity Check Testing Platform
□	Set up a project and accept testing Terms and Conditions		X			Mastercard Identity Check Testing Platform

	Task / Requirement	Acquirer	3DS Server	Merchant	SDK	Reference
□	**Sandbox** Establish connectivity to the Mastercard Identity Check Platform testing certificates. Click on "Move to Pre-Compliance"		X			Mastercard Identity Check Testing Platform
□	Pre-compliance • Remove all bugs • Pass all automated and manual test cases • Submit test cases for review and await approval from your assigned CIS project manager Once approval is received project will automatically be set to "Compliance Testing"		X			Mastercard Identity Check Testing Platform

	Task / Requirement	Acquirer	3DS Server	Merchant	SDK	Reference
□	Under Main Menu>Company Profile>Customer Details 3Ds Service provider administrator needs to populate the 3DSS Certificate ID. Certificate ID is required to request certificates		X			3DS service provider administrator
□	Complete Letter of Compliance enrollment form: • Contact Information • Business Contact • Security Contact • Certificate Contact		X			Mastercard Identity Check Testing Platform Click "Submit for LOC review" button and await approval from CIS
□	Compliance testing Execute all test cases without error		X			Mastercard Connect/Mastercard Identity Check Testing Platform
□	Receive Mastercard Letter of Compliance		X			Provided by Mastercard
□	Update EMV-3DS messages to include the Mastercard assigned 3DS Server Operator ID		X			Provided by Mastercard

	Task / Requirement	Acquirer	3DS Server	Merchant	SDK	Reference
□	Create and submit Production Certificate Signing Request (CSR). Required certificates: 3DS Server TLS Client 3DS Server TLS Server One set required per 3DS server connecting to DS.		X			key_management@mastercard.com
□	Establish connectivity to the production directory server		X			
□	Complete all end to end back office testing	X	X	X	X	
□	Coordinate live dates among all participants	X	X	X	X	
□	Enroll merchant IDs/acquiring BINs on the Identity Check directory server	X				Enrollment occurs through the ISSM Application
□	Monitor Production Transactions	X	X	X		All participants

Access to Mastercard Connect

Results

Click Mastercard Connect Sign Up Guide to open the file.

Identity Check Insights

Mastercard has defined a custom payment message category called Identity Check Insights, formerly called Data Only, that allows the merchant the flexibility to share data through the EMV® 3DS rails to influence an issuer's decision to approve a transaction without requesting authentication and thus with no risk of cardholder challenge and added latency.

An Identity Check Insights message is identified by the value in the "Message Category" field defined by Mastercard. A normal authentication request is represented by message category 01 (payment) or 02 (non-payment), an Identity Check Insights (without authentication) is requested using Mastercard message category value of 80. For more information, refer to the Mastercard Identity Check Program Guide.

Identity Check Onboarding for Identity Check Insights will follow the same pre-requisites that have been described in this onboarding guide.

NOTE: Since this is a Mastercard defined solution, Identity Check Insights is not tested during Approvals Testing through EMVCo. Support of Identity Check Insights is optional for each merchant and is not part of the Mastercard compliance testing.

Public Key Management for Software Development Kit (SDK)

SDK Operators are required to register and install the Mastercard Public Key.

SDK Operators are required to register and install the Mastercard Identity Check- DS Public Certificate. Mastercard will utilize the registration information for communication with the SDK. Communications could be notification of a broadcast message relating to a key compromise, failures on the SDK, SDK reference number and key id, or information on the latest version of keys as seen by the Mastercard Authentication network.

The Mastercard Directory Server Public Key can be obtained from the Mastercard Developers site which is located at https://developer.mastercard.com/product/identity-check. An SDK will be required to request access to the developer site and the API, before being able to access the public certificate.

1. On the developer zone API page, select the product Mastercard Identity Check-DS Public Cert
2. Select View Documentation
3. Complete the registration process to receive a User ID and password for the developer zone
4. Complete the SDK Vendor information access form by providing the following information:
   - SDK First Name
   - Last Name
   - Email of the person and entity requesting the public key
   - EMVCo reference number

   – Select Request Access when the above information is complete
5. A request confirmation screen will be displayed and an email will be received when access is granted.

Once access is granted to the page, the user is able to download the directory server public key directly from the Identity Check page. The DS CA certificate can be obtained by emailing identity_solutions_compliance@mastercard.com. The user that registered within the API page must be the user who requests the DS root certificate.

Merchant Enrollment API

The Merchant Enrollment API enables acquirers and their service providers to manage merchant participation in Mastercard Identity Check on EMV 3DS (3DS2).

Acquirers and service providers can add/delete merchants directly in Mastercard Identity Solutions Services Management (ISSM) by sending the enrollment data through an API.

Access to the Merchant Enrollment API can be requested through the Mastercard Developers site which is located at https://developer.mastercard.com/product/identity-check.

1. Once on the developer zone API page, select the ISSM Merchant Enrollment API card.
2. Select View Documentation.
3. Complete the access request form to request access to the Merchant Enrollment API.
4. A request confirmation screen will be displayed and an email will be received when access is generated.
5. Once Access is granted, instructions will be made available on the documentation page to create a project and utilize the API.

Appendix B Production Procedures

The Production Procedures section includes the Company Contact Management application update and steps for requesting Production Certificates.

Company Contact Management

The Company Contact Management application is a global repository of contacts that allows Mastercard customers to view contact information for other companies and to find their portfolio information. It is also used to notify contacts of any planned service disruptions or platform detected service events. Mastercard Identity Check participants should ensure appropriate contacts are included in this application to ensure delivery of Mastercard Identity Check notifications.

About this task

For more information on this application, refer to the Company Contact Management Application User Guide found on Mastercard Connect.

Contact Type: Identity Check

Production Certificates

This section contains the steps for requesting Production Certificates.

Mastercard Certificate Authority Request Procedures

This chapter contains instructions for various tasks involving the certificate authority requests.

Functions of End-Entity Certificates

A Mastercard implementation of the EMV 3-D Secure program requires Mastercard hierarchy end-entity certificates to be used for the following functions.

3-D Server

- 3 DS Server Transport Layer Security (TLS 1.2 or greater) Client certificate for communications between the 3 DS Server and the Mastercard Directory Server
- 3 DS Server Transport Layer Security (TLS 1.2 or greater) Server certificate for communications between the Mastercard Directory Server and 3 DS Server.

ACS

- Access Control Server (ACS) TLS Server certificate for communications between the Mastercard Directory and the Issuer Access Control Server (ACS)
- ACS TLS Client certificate for communications between the issuer ACS and Mastercard Directory
- Issuer ACS digital signature certificate for signing ACS Signed content

SDK

- Encryption certificate with DS public key to encrypt device information

- Directory Server root certificate to validate certificate chain in ACS signed content.

Request an End-Entity Certificate

To request and receive an end-entity certificate from the Mastercard Identity Check Certificate Authority (CA), follow these steps.

About this task

NOTE: Failure to follow these instructions may result in a processing delay or rejection of a certificate request.

Procedure

1. Create the certificate request.
2. Package the certificate request.
3. Transmit the certificate request.
4. Receive the certificates.
5. Validate and install the certificate chain and CA certificates.

   Mastercard will make every attempt to process each certificate request within four business days of receipt.

   Each of the following sections details the process flow for each specific type of certificate request.

   NOTE: Mastercard requires that all customers participating in the Mastercard Identity Check program work through their 3-DS Server or Access Control Server (ACS) vendor-support process to understand how to create certificate requests and how to install certificates.

   IMPORTANT:

   Certificates are issued/renewed at the request of customers participating in the Mastercard Identity Check program. These customers:

   - **Are responsible for renewal decisions and are free to plan the replacement of expiring certificates at their convenience.**
   - **Must anticipate the expiration date and plan the replacement in taking into account systems implementation windows, staff workload, and Public Key Infrastructure (PKI) service time to deliver.**

Request a 3-DS Server Client and Server TLS Certificate

These end-entity Transport Layer Security (TLS) Client and Server certificates are used by the 3-DS Server to establish communication with the Mastercard Directory.

About this task

NOTE: Failure to follow these instructions may result in a processing delay or rejection of a certificate request.

Procedure

1. Create a separate PKCS#10 certificate request for each certificate being requested. All PKCS#10 requests must comply with the Mastercard guidelines for key size and subject name contents. Any deviation will result in the request being rejected. Any requested validity period greater than what is allowed will be automatically truncated. Any other options added to the request but not defined by our certificate policy also may be truncated or discarded.

   The PKCS#10 request file should be Base64 encoded. Mastercard requires that the PKCS#10 file be named as follows: "3-DSServer-TLS-Client-OperatorID-dateDDMMYY" for client certificate and "3-DSServer-TLS-Server-OperatorID-dateDDMMYY" for server certificate. For example, a request to be sent on 1 April 2020 in which Operator ID (OperatorID) is equal to SVR-V201-AZ-25258, would appear as "3-DSServer-TLS-Client-SVR-V201-AZ-25258-01042020" for client certificate.

   The following table highlights the relevant certificate profile information. To avoid XML parser errors, avoid the use of the characters **&** and **<**.

Validity	Determined by the certificate authority (CA)—may be up through the expiration date of the Root and Acquirer subordinate CA certificates.	
Key Size	Minimum 2048 bit	
Subject alternative name (Only for server certificate)	DNS name. Example www.3DSServer.com. Up to five DNS names are allowed. At least one DNS name must match common name	
Common Name (CN)	The common name must be populated with one of the following characteristics of the site that will utilize the certificate [Domain Name] OR [public IP].	
	Domain Name	For example, www.3DSServer.com
Organizational Unit (OU)	Unique identification of the party is required within the OU field of the certificate. 1. 3DSS-[Operator ID] for TLS Server Certificate 2. 3DSC-[Operator ID] for TLS Client Certificate.	
Organizational Name (O)	Operator registered company name	

Country (C)	Country where processor is located. This should be the ISO 3166 2 character country code (for example, U.S.)

2. Prior to sending the PKCS#10 certificate request(s) for processing, each request must be packaged into a password protected zip file. It is acceptable to send multiple PKCS#10 requests in a single zip file as long as they are for the same Mastercard member institution. Otherwise, a separate zip file is required.

   The password used to protect the zip file contents must be the same as the certificate validation password provided during the registration for Mastercard Identity Check. In the case of a forgotten password, please contact customer support. Mastercard will not distribute the password.
3. Each PKCS#10 certificate request must be sent to the Mastercard CA for processing. All requests must be received by Mastercard at key_management@Mastercard.com. At least one registered contact must be copied in the email request.

   The e-mail request must contain the following information:

   – Password protected zip file containing PKCS#10. If the zip file contains multiple requests, the following information is required for each request.
   – In the body of the e-mail:
     – Associated certificate distinguished name(s) for each certificate request contained in the zip file—including the common name (CN), organizational unit (OU), organization (O), and country (C).
     – Associated certificate usage for each certificate request contained in the zip file— 3-DS Server TLS client certificate

   Mastercard will reject any certificate request messages that contain either the accompanying private key or associated certificate validation password. Inclusion of the certificate validation password will also require establishment of a new password prior to proceeding with any certificate request processing.

   By default, all certificates will be returned in Privacy Enhanced Mail (PEM), PKCS#7, and Distinguished Encoding Rules (DER) formats. Consult your vendor regarding the appropriate format for your application.

   For security reasons, Mastercard may contact the individuals authorized to submit certificate requests, as identified on the program enrollment forms, to confirm the validity of a certificate request.
4. The end-entity and CA certificates will be returned to the certificate requestor. The response will contain the following attachments:
   – End-entity certificate in PEM, PKCS#7, and DER formats.
   – Mastercard hierarchy root and subordinate CA certificate(s) in PEM, PKCS#7, and DER formats.
5. Mastercard strongly encourages the key management contacts to validate the end-entity certificates before loading them into the application. Additionally, all active Mastercard Identity Check Root and subordinate CA certificate(s) should be validated before making any additions to the application trusted certificate store. Refer to both the Mastercard

Identity Check Root Certificates section and Certificate Validation section for more information.

Request an Access Control Server (ACS) TLS Server, Client, and Digital Signing Certificate

These end-entity certificates are used to secure communication between the ACS and the Mastercard Directory server, and to perform digital signatures for ACS Signed Content.

About this task

NOTE: Failure to follow these instructions may result in a processing delay or rejection of a certificate request.

Procedure

1. Create a separate PKCS#10 certificate request for each certificate being requested. All PKCS#10 requests must comply with the Mastercard guidelines for key size and subject name contents. Any deviation will result in the request being rejected. Any requested validity period greater than what is allowed will be automatically truncated. Any other options added to the request but not defined by our certificate policy also may be truncated or discarded.

   Issuer ACS TLS Client and Server Certificates

   The PKCS#10 request file should be Base64 encoded. Mastercard requires the following naming convention for the PKCS10 file – "ACS-TLS-Client-OperatorID-dateDDMMYY" for client certificate and "ACS-TLS-Server-OperatorID-dateDDMMYY" for server certificate. For example, a request to be sent on 1 April 2020, in which operator ID (OperatorID) is equal to ACS-V210-MYACS-94909, would appear as "ACS-TLS--Server-ACS-V210-MYACS-94909-01042020" OR, for client: ACS-TLS-Client-ACS-V201-MYACS-94909-01042020.

   The following table highlights the relevant certificate profile information. To avoid XML parser errors, avoid the use of the characters **&** and **<**.

Validity	Assigned by the CA—may be up through the validity of the root and issuer subordinate CA certificates	
Key Size	Minimum 2048 bit	
Subject Name		
Common Name (CN)	The common name must be populated with one of the following characteristics of the site that will utilize the certificate [Domain Name] OR [public IP].	
	Domain Name	For example, www.ACSName.com

Subject alternative name (only for server certificate)	DNS name. Example www.ACSName.com. Up to five DNS names are allowed. At least one DNS name must match common name
Organizational Unit (OU)	Unique identification of the party is required within the OU field of the certificate. 1. Prod OU: ACSMS [Operator ID] for TLS ACS Server Certificate 2. ACSC-[Operator ID] for TLS ACS Client Certificate
Organizational Name (O)	Name of the ACS service provider or processor (if applicable). The name provided in this field must match the name as indicated in the enrollment forms.
Country (C)	Country where the processor is located. This should be the ISO 3166 2 character country code (for example, U.S.)

ACS Digital Signing Certificate

The PKCS#10 request file should be Base64 encoded. Mastercard requires the following naming convention for the PKCS10 file – "ACS-Signing-OperatorID-OptionalFreeText-dateDDMMYY". For example, a request to be sent on 1 April 2018, in which OperatorId-OptionalFreeText is equal to ACS-V201-MYACS-94909-OptionalFreeText, would appear as "ACS-Signing-ACS-V201-MYACS-94909-OptionalFreeText."

NOTE: If multiple signing certificate will be issued, the ACS must uniquely identify each individual signing certificate. It is recommended that ACS indicates the issuer name in the Optional Free Text field if issuing individual signing certs to each issuer. Otherwise, the ACS providers are able to designate its own value.

The following table highlights the relevant certificate profile information.

Validity	2 years
Key Size	Minimum 2048 bit
Subject Name	
Common Name (CN)	The common name must be populated with a unique identifier determined by the issuer.
Organizational Unit (OU)	Unique identification of the party is required within the OU field of the certificate. ACSMS-Operator ID-[Optional Free Text]
Organizational Name (O)	Name of the issuer. The name provided in this field must match the name as indicated in the associated issuer enrollment forms.
Country (C)	Country where the issuer or issuer processor is located. This should be the ISO 3166 2 character country code (for example, U.S.)

2. Prior to sending the PKCS#10 certificate request(s) for processing, each request must be packaged into a password protected zip file. It is acceptable to send multiple PKCS#10 requests in a single zip file as long as they are for the same Mastercard customer institution. Otherwise, a separate zip file will be required.

   The password used to protect the zip file contents must be the same as the certificate validation password provided on the Mastercard Identity Check program enrollment forms or as registered in the Mastercard Identity Check testing platform. In the case of a forgotten password, an updated enrollment form is required. Mastercard will not distribute the password.
3. Each PKCS#10 certificate request must be sent to the Mastercard Certificate Authority for processing. All requests must be received by Mastercard at key_management@Mastercard.com from authorized individuals as identified on the program enrollment forms.

   The e-mail request must contain the following information:

   – Password-protected zip file containing PKCS#10. If the zip file contains multiple requests, the following information is required for each request.
   – In the body of the e-mail message:
     – Associated certificate distinguished name(s)—including the common name (CN), organizational unit (OU), organization (O) and country (C).
     – Associated certificate usage—ACS TLS Client, Server certificate or ACS digital signing certificate.

   WARNING: The password must NOT be sent along with the e-mail. Inclusion of the password in the e-mail will result in the password being invalidated. A new password will need to be established prior to proceeding with any certificate request processing.

   Mastercard will reject any certificate request message that contains either the accompanying private key or associated certificate validation password. Inclusion of the certificate validation password will also require establishment of a new password prior to proceeding with any certificate request processing.

   By default, all certificates will be returned in Privacy Enhanced Mail (PEM), PKCS#7, and Distinguished Encoding Rules (DER) formats. Consult your vendor regarding the appropriate format for your application.

   For security reasons, Mastercard may contact the individuals authorized to submit certificate requests to confirm the validity of a certificate request.
4. The end-entity and CA certificates will be returned to the certificate requestor. The response will contain the following attachments:
   – End-entity certificate in PEM, PKCS#7, and DER formats.
   – Mastercard hierarchy Root and subordinate CA certificate(s) in PEM, PKCS#7, and DER formats.
5. Mastercard **strongly** encourages the key management contacts to validate the end-entity certificates before loading them into the application. Additionally, all active Mastercard Identity Check Root and subordinate CA certificate(s) should be validated before making

any additions to the application trusted certificate store. Refer to both the Mastercard Identity Check Root Certificate section and Certificate Validation section for more information.

SDK Encryption Certificate

SDK vendor can download the SDK encryption certificate and subordinate CA certificate from Mastercard developer zone: https://developer.mastercard.com/product/identity-check.

Certificate Validation

This section contains details about the validation of root and subordinate certificates.

Process of Validating Certificates

Mastercard provides certificates that are industry-standard, X.509 version 3 format. Each of the certificates contains several unique, identifying characteristics that can be used for validation.

Mastercard strongly encourages all implementations to validate all Root and subordinate certificates before adding them to the application trusted certificate store. This validation is done by confirming the contents of several key fields within the certificate received from Mastercard. Root and subordinate certificate authorities (CAs) values are provided in Mastercard Identity Check Production Certificate Authority (CA) Hierarchy.

These fields include the following:

Subject Name:	The name of the entity to which the certificate refers. That is, this certificate certifies the public key of the subject who holds the corresponding private key.
Serial Number:	An integer value associated with the certificate, unique within the issuing CA, and assigned by the CA to each certificate.
Thumbprint:	Hash of the entire certificate

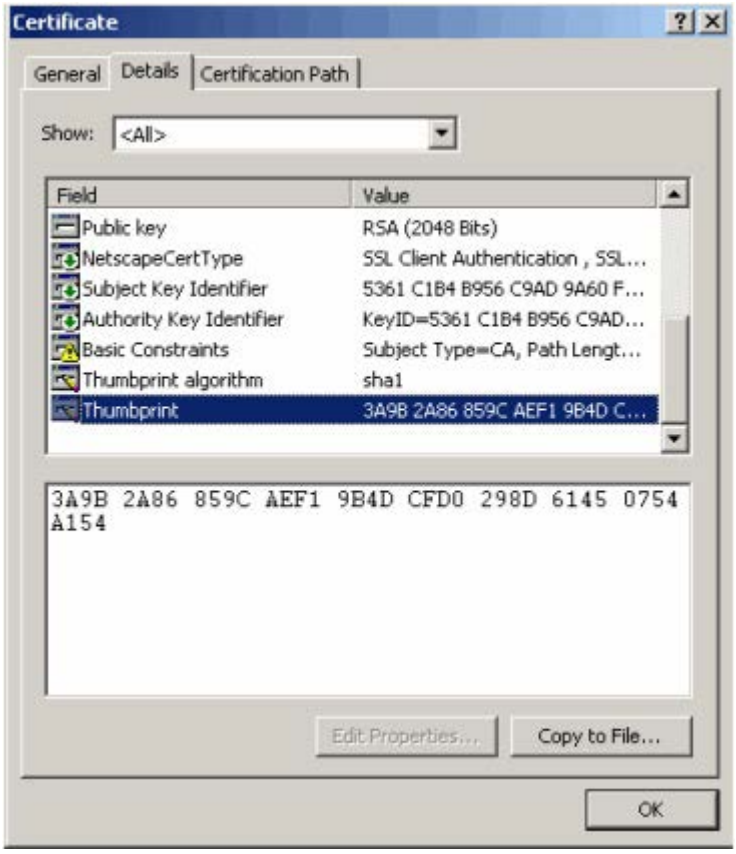
Within a Windows environment, double click on any individual Privacy Enhanced Mail (PEM) or Distinguished Encoding Rules (DER) encoded certificate file, and then click the Details tab from the resulting window.

In addition to above validation, connecting system should validate the following while establishing TLS connection.

ACS shall validate whole certificate chain while communicating with DS (Validate that DS present the client/ Server signed by Directory Server issuer subordinate CA.

3DS Server shall validate whole certificate chain while connecting communicating with DS (Validate that DS present the Client/ Server certificate signed by Directory Server acquirer subordinate CA).

SDK shall validate whole certificate chain after downloading from Mastercard (Validate that SDK encryption certificate signed by Directory Server acquirer subordinate CA) and validate that certificate CN=3ds2.directory.mastercard.com).



PKCS#7 files can be viewed in a similar fashion. This will result in a directory structure being displayed that shows each certificate in the file. These certificates can then be viewed in the same way as described above.

To check the value, click the corresponding fieldname in the left column. The complete contents of the field will display in the lower box.

Mastercard Identity Check Production Certificate Authority (CA) Hierarchy

Details of the Mastercard Identity Check Production CA Hierarchy— including the root CA, acquirer subordinate CA, and issuer subordinate—are described as follows:

Root CA Certificate

The Mastercard production Root CA is signing both acquirer and issuer subordinate certificates.

Subject Name	
Common Name (CN)	PRD Mastercard Identity Check Root CA
Organizational Unit (OU)	Mastercard Identity Check Gen 3
Organization (O)	Mastercard

Subject Name	
Country (C)	US
Serial Number	16 c8 f2 22 ea a1 c3 cd 30 34 c8 d7 53 8e e5 7e
Thumbprint	46 e7 f5 0d 04 91 4e d2 5d 78 e0 fb f0 3c 59 6b b8 ea 69 d7
Validity	Until Monday, July 15, 2030 9:10:00 AM

Acquirer Subordinate CA Certificate

The acquirer subordinate CA is used to sign all end-entity TLS client and server certificates used by the 3-DS Server to establish communication with the Mastercard Directory. Additionally, SDK Encryption Certifications should be signed by Issuer Subordinate CA.

Subject Name	
Common Name (CN)	PRD Mastercard 3DS2 Acquirer Sub CA
Organizational Unit (OU)	Mastercard Identity Check Gen 3
Organization (O)	Mastercard
Country (C)	US
Serial Number	6a 7e 21 42 35 0c 70 16 0a 4d 50 f4 15 5e ca 11
Thumbprint	4ade 8187 bb87 e2df 6aa0 e564 e374 b4dc 71b7 2972
Validity	Until Wednesday, July 15, 2026 8:00:00 AM

Issuer Subordinate CA Certificate

The issuer subordinate CA is used to sign all end-entity TLS client and server certificates used to establish communication between the issuer Access Control Server (ACS) and the Mastercard Directory. Additionally, this subordinate CA is also used to sign all ACS digital signing certificates.

Subject Name	
Common Name (CN)	PRD Mastercard 3DS2 Issuer Sub CA
Organizational Unit (OU)	Mastercard Identity Check Gen
Organization (O)	Mastercard
Country (C)	US
Serial Number	09 65 c0 82 25 bf c5 0b ba 59 01 a2 d2 51 f1 29
Thumbprint	f385 2f4f 1dee 3cd0 2ee8 1bf3 424d 6e2c 2606 a774

Subject Name	
Validity	Until Thursday, March 28, 2013 5:35:54 PM GMT

Appendix C Mastercard Identity Check Onboarding Quick Reference Using EMV 3DS

This appendix a quick reference checklist.

Mastercard Identity Check Directory Server Enrollment

The Mastercard Identity Check directory server, maintains the relationship of the acquiring company ID, acquiring BIN, and merchant ID.

The merchant acquirer is responsible for the processing of the authorization and clearing data as well as receipt of the directory server billing, where applicable. Therefore, directory server maintenance should only be performed by the merchant acquirer, unless explicit permission is provided to the 3DS operator or service provider. Maintenance and enrollment can be performed using the Identity Solutions Service Management (ISSM) application found on MC Connect. Refer to the Mastercard Identity Solutions Services Management User Guide for more detailed instructions on account range enrollment and other onboarding activities.

NOTE: Identity Check Program Registration for all applicable Company Ids (CID) is a prerequisite for directory server enrollment.

Scaling Merchant Enrollments

Mastercard has defined three enrollment process options for acquirers that is designed to help scale the amount of merchant ids (MID) that need to be enrolled on the directory server.

There may be scenarios for large merchants where there is a large amount of merchant ids that are utilized and maintained through their acquirer(s) and the approaches below are designed to provide flexibility on the directory server enrollment and subsequent maintenance overtime, while maintaining a level of traceability for each merchant.

- Option 1—Bulk upload via ISSM (available today for up to 1500 records per file)
- Option 2—Merchant Enrollment API, see Appendix A, Merchant Enrollment API
- Option 3—Register one Acquirer BIN/MID for each country where a given merchant operates
  - Merchants use the same MID/BIN for their authentication requests
  - Underlying merchant identified in the authentication message using the Merchant Name in addition to the Requestor ID

  NOTE:

  - **Must establish relationship with acquirer who owns BIN (if not already in place), 3DS network fees may be passed on by acquirer to the registered MID**
  - **PSP/Operator would need to send correct Requestor ID/Merchant Name for each merchant**
  - **MID in Authentication will NOT match Authorization**
  - **Acquirer TRA flag will be set to 'NO' in ISSM as unable to identify individual merchants (indicates to the Issuer if TRA exemption can be used by merchant)**
  - **Merchants will not be eligible for white listing unless registered individually**

Additional Notes

1. The SecureCode 1.0.2 directory server and Identity Check 2.0 directory server are separate servers and have separate enrollment processes.
2. Acquiring BINs /Merchant IDs loaded on the Mastercard SecureCode 1.0.2 directory server will not be automatically uploaded on to the Mastercard Identity Check directory server.
3. All registrations and testing for the Mastercard Identity Check Testing Platform must be complete prior to enrolling acquiring BINs/Merchant IDs to the Mastercard Identity Check directory server. The Mastercard Company ID and Primary ICA number are required to add, delete, and update. Refer to the My Company Manager application found on Mastercard Connect to find the Company Id and Primary ICA number.
4. Once account ranges are loaded onto through ISSM, they become effective on the directory server. Issuers and ACS providers must be prepared to process transactions upon completing directory server enrollment.
5. Issuers may delegate access to ISSM for card range enrollment activities to its service provider(s) or process(es) through the Business Administration (Register & Provision a Company) application on Mastercard Connect.
6. BINs that start with the following digits are only included in ISSM: 51, 52, 53, 54, 55, 6390, 67 and 2 series BINs starting from 222100 to 272099. If the BIN range falls outside of those digits, contact IDC_Customer_Support@mastercard to get the bins loaded to allow for ISSM enrollment.
7. Card Ranges enrolled on the directory server must match the length of the card numbers issued from that range. For example, if the card numbers issued from a given range are 16 digits, the card range enrolled must be a 16 digit range. Any range enrolled less than the issued card length may result in transactions routing to the Smart Authentication Stand-In Service, Attempts processing, or general enrollment errors.

Timeframes for Loading Data

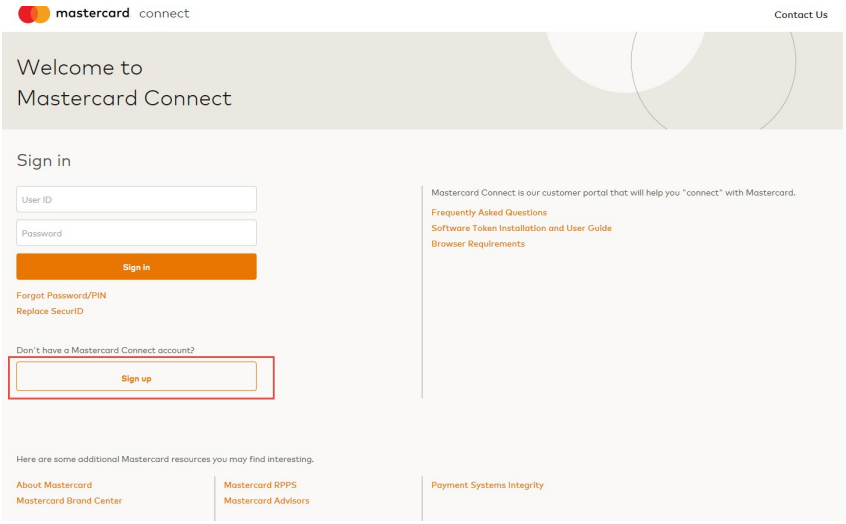
1. Uploads to the directory server through ISSM occur in real-time upon submission by user.
2. Submitters receive confirmation notification from application once the upload request has been successfully submitted.

Appendix D Mastercard Connect Sign Up Guide

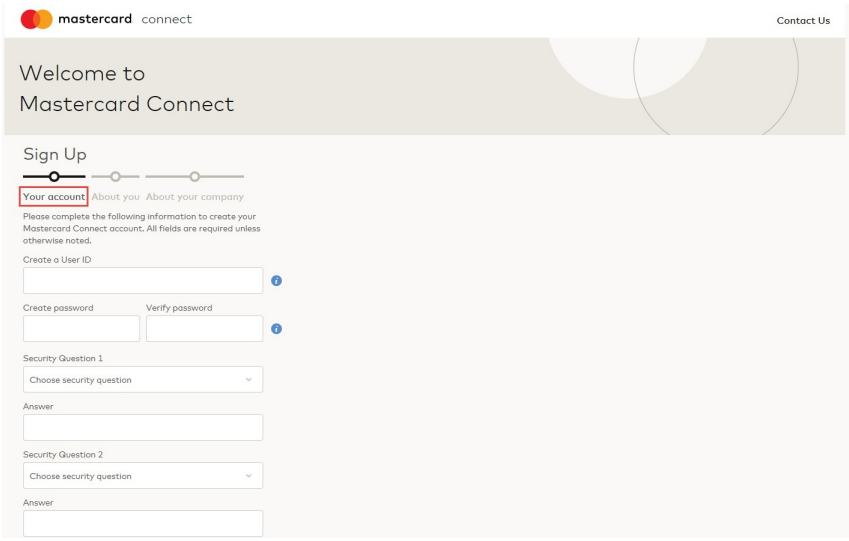
This appendix describes the procedures to sign up for Mastercard Connect.

New User Sign Up

New users can sign up for Mastercard Connect by clicking the 'Sign Up' link in the left hand section on the Sign in page. The 3-step Sign up process will create your Mastercard Connect account.



Step 1: Sign Up - Your Account

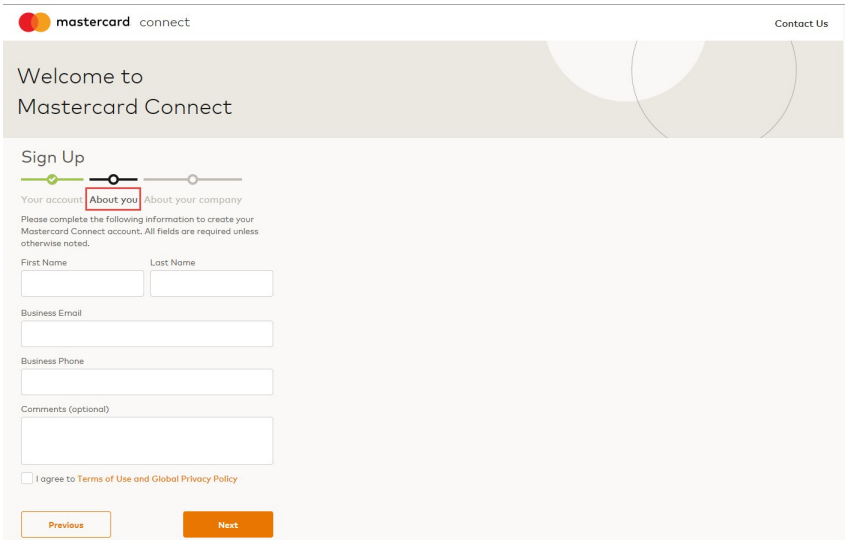


1. Create a User ID. Your User ID must meet the following requirements:
   a. Begin with a letter.
   b. 6 to 30 characters in length.
   c. A-Z, a-z, _, @, and - can be used.
   d. No spaces or commas can be used.
2. Create and verify your password. Your password must meet the following requirements:

a. Minimum of one alphabetic character.
b. Minimum of one non-alphabetic character such as 0-9,!,@,$...
c. Maximum of 2 repeated characters.
d. Minimum length of 8 characters
e. Password cannot match the User ID.

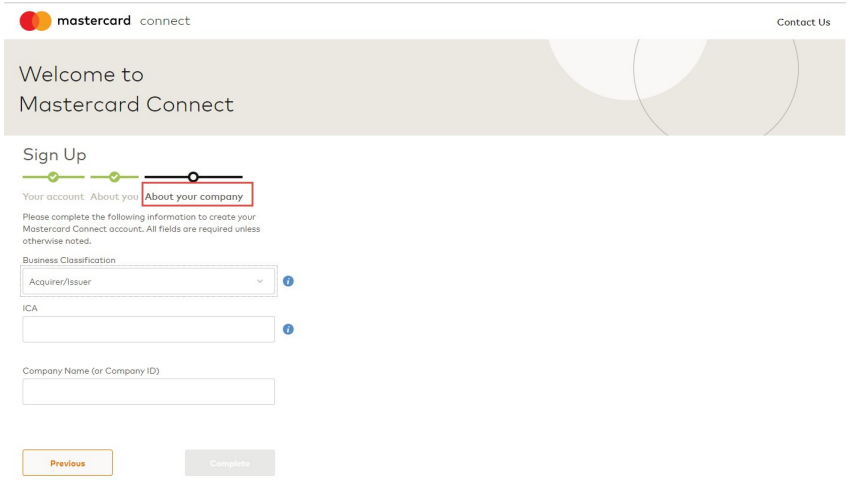
3. Select 2 Security Questions and Answers.

Step 2: Sign Up - About You



1. Enter First and Last Name
2. Enter your Business Email. This email will be used to send notifications to you.
3. Enter your Business Phone Number.
4. The Comments section is optional and can be used to send a message to your Security Administrator.
5. You must agree to the Terms of Use and the Global privacy policy or you will not be able to create a Mastercard Connect account.

Step 3: Sign Up - About your company



1. Select the business classification from the drop down list that best describes your company.
2. Enter the ICA number assigned to you by Mastercard, if applicable. An ICA is a 3 to 8 digit identifier.
3. Enter you Company name or the 6 digit Customer ID (CID) assigned to you by Mastercard.
4. Select Complete.

Notices

Following are policies pertaining to proprietary rights, trademarks, translations, and details about the availability of additional information online.

Proprietary Rights

The information contained in this document is proprietary and confidential to Mastercard International Incorporated, one or more of its affiliated entities (collectively "Mastercard"), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of Mastercard.

Trademarks

Trademark notices and symbols used in this document reflect the registration status of Mastercard trademarks in the United States. Please consult with the Global Customer Service team or the Mastercard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

Disclaimer

Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, Mastercard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not Mastercard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, Mastercard specifically disclaims all representations and warranties that any practice or implementation of this document will not infringe any third party patents, copyrights, trade secrets or other rights.

Translation

A translation of any Mastercard manual, bulletin, release, or other Mastercard document into a language other than English is intended solely as a convenience to Mastercard customers. Mastercard provides any translated document to its customers "AS IS" and makes no representations or warranties of any kind with respect to the translated document, including, but not limited to, its accuracy or reliability. In no event shall Mastercard be liable for any damages resulting from reliance on any translated document. The English version of any Mastercard document will take precedence over any translated version in any legal proceeding.

Information Available Online

Mastercard provides details about the standards used for this document—including times expressed, language use, and contact information—on the Publications Support page available on Mastercard Connect™. Go to Publications Support for centralized information.