Mastercard Identity Check Onboarding Guide for ACS Service Providers, Operators, Issuers, and Processors

15 October 2019

MSPTS

Contents

Chapter 1 Mastercard Identity Check Overview

Mastercard Identity Check™ is a global authentication program that utilizes the Mastercard authentication network in conjunction with the newly designed EMV® 3-D Secure protocol.

Introduction to Identity Check and EMV 3-D Secure

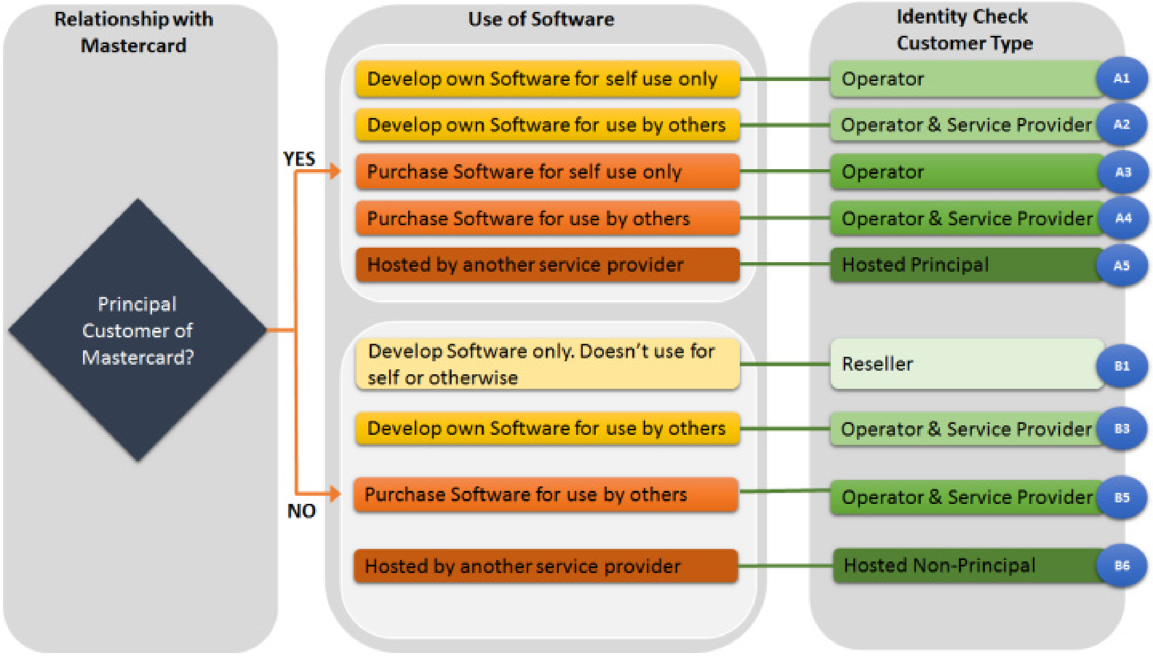
Mastercard Identity Check is a global authentication program that utilizes the Mastercard authentication network in conjunction with the EMV 3-D Secure® protocol. It is designed to help provide additional security for digital transactions and facilitate higher approval rates by improving the authentication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

The purpose of this guide is to assist 3-D Secure Service Providers, Operators, Issuers, and Processors through the onboarding processes of program registration, testing, and production readiness. For more specifics regarding the Mastercard Identity Check program, 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.

Figure 1.0 represents the decision tree to help determine the customer type and scenario.


Relationship with Mastercard
Use of Software
Identity Check Customer Type
Principal Customer of Mastercard?
YES
NO
Develop own Software for self use only
Develop own Software for use by others
Purchase Software for self use only
Purchase Software for use by others
Hosted by another service provider
Develop Software only. Doesn't use for self or otherwise
Develop own Software for use by others
Purchase Software for use by others
Hosted by another service provider
Operator
A1
Operator & Service Provider
A2
Operator
A3
Operator & Service Provider
A4
Hosted Principal
A5
Reseller
B1
Operator & Service Provider
B3
Operator & Service Provider
B5
Hosted Non-Principal
B6

The terms listed here relate to Mastercard Identity Check using EMV 3-D Secure onboarding for Principal Licensed Customers, 3-D Secure Service Provider, Operator, Reseller and Hosted Principal.

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.

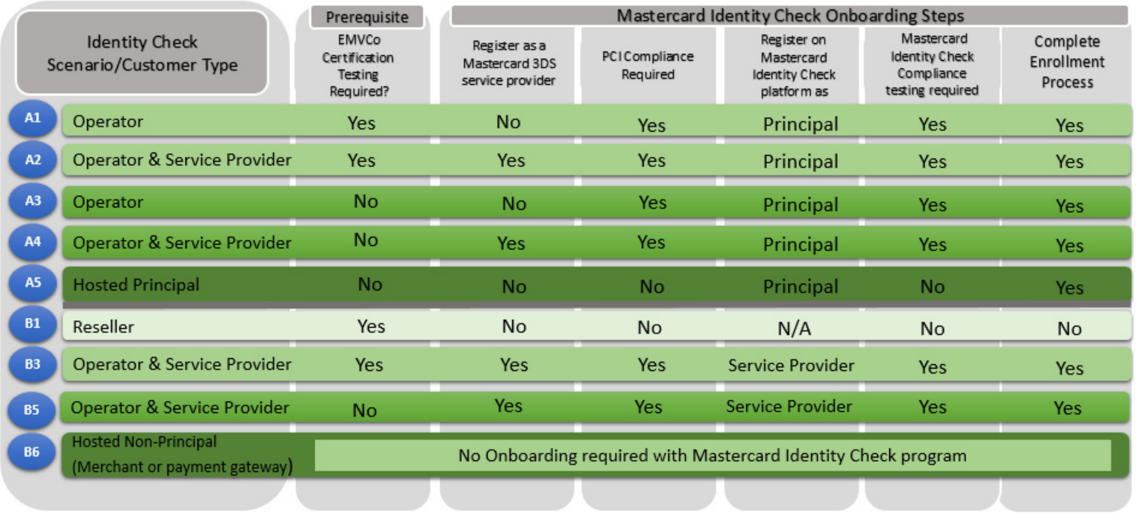
Hosted Principal—An acquirer, issuer, or processor that uses a service hosted by a third party ACS or 3DS Server solution.

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, there are five major steps for 3-D Secure onboarding with Mastercard for the support of Mastercard Identity Check utilizing EMV 3-DS.

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



	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
B3	Operator & Service Provider	Yes	Yes	Yes	Service Provider	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 and A3 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. EMVCo 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 ACS 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. It is specific for 3DS service providers and is used to manage 3DS PCI Compliance.

This registration will also enable service providers the ability to access Mastercard Connect and the testing platform for registration and testing. Once the Service Provider Registration is complete, a Company ID, a billable ICA number, and Operator ID is issued.

NOTE: A Mastercard host issuer/processor who operates software for its own use, whether developed in house or purchased (Customer Types A1 and A3) is exempt from 3-DS Secure Service Provider Registration and is governed by existing Mastercard PCI compliance rules.

3. Mastercard Identity Check Registration

Mastercard Identity Check registration enables the principal customers to accept the terms and conditions and declare the ability to support their customer's 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 registration is completed with the Company ID (CID) and billable ICA number for Mastercard Principal customers.

Principal customers are required to submit one registration per assigned CID supporting the Identity Check Program regardless of region, product, and BIN. Failure to register with the correct CID(s) will prevent directory server enrollment.

4. Mastercard Identity Check Compliance Testing

The Mastercard Identity Check Test Platform will support program registration for principal customers supporting the Mastercard Identity Check program.

It will also be used to register and test operators and service providers as defined by the Mastercard Identity Check Customers type. All entities requesting a connection with the Mastercard Identity Check directory server are required to register and complete compliance testing. As a result of successful compliance testing, a Letter of Compliance (LOC) will be issued.

5. Account Range Enrollment, Production Preparation, and Deployment

The Mastercard Identity Check Directory Server enrollment enables production loading of EMV 3-D Secure issuer account ranges with the associated ACS URL. Production certificates connectivity is unrelated to account range enrollment.

All Service Providers must register and complete testing, while Principal customers must register for the Identity Check program on the Mastercard Identity Check Testing Platform. These activities must complete prior to issuers enrolling their account ranges. Account ranges already loaded on the Mastercard SecureCode 1.0.2 Directory Server will not be automatically uploaded on to the Mastercard Identity Check Directory Server.

NOTE: Mastercard SecureCode 1.0.2 customers will continue to have the ability to add/delete and update changes to their account ranges using the SecureCode Directory Server Request Form.

Mastercard has developed Identity Solutions Services Management (ISSM), a self-service tool that will enable Mastercard Identity Check customers to manage their participation for key functions such as enrollment in an Identity Solution services and card range management.

ISSM will be available on the Mastercard Connect (MCC) at no cost to Identity Check customers. For more details regarding the tool, please refer to the Mastercard Identity Solutions Services Management User Guide.

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. Issuers and ACS providers must be prepared to process transactions upon completing directory server enrollment.

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
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

Acronym	Description
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
UCAF	Universal Cardholder Authentication Field in Mastercard Authorization

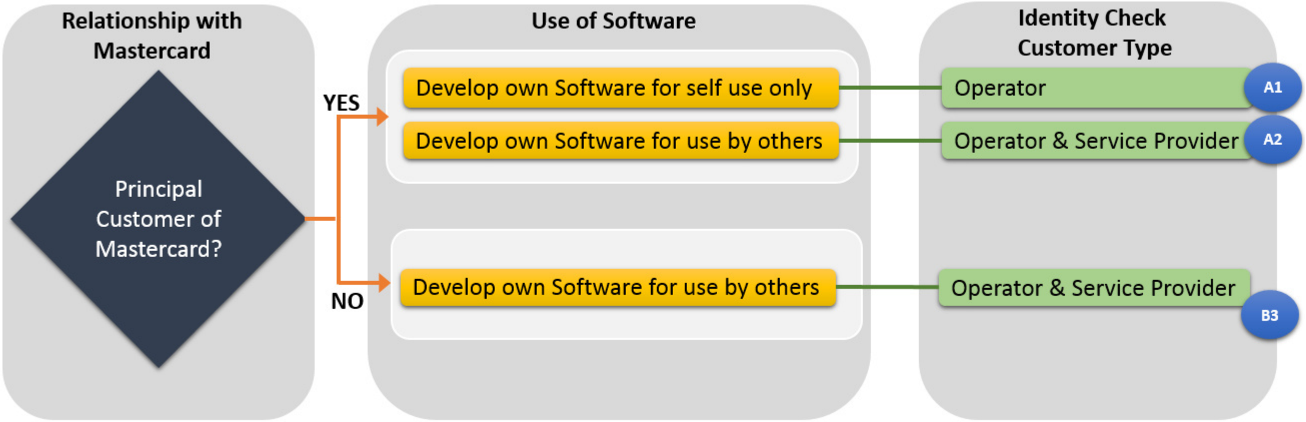
Chapter 2 Prerequisites

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

EMVCo Certification

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

EMVCo Certification is a prerequisite to starting the onboarding process with Mastercard Identity Check. The EMVCo Certification is a prerequisite step for the following Identity Check customer types and scenarios: A1, A2, and B3.


Relationship with Mastercard
Principal Customer of Mastercard?
YES
NO
Use of Software
Develop own Software for self use only
Develop own Software for use by others
Develop own Software for use by others
Identity Check Customer Type
Operator
A1
Operator & Service Provider
A2
Operator & Service Provider
B3

Prior to testing with Mastercard, the above parties must complete testing and approval of their software using the EMVCo Certification and receive their Letter of Approval and Reference Number.

EMV 3DS Approval Process

The EMV 3DS Approval Process consists of three phases: Pre-Compliance, Compliance, and Approval.

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, testing results are evaluated by EMVCo prior to moving to Compliance Testing.

Compliance

- This phase is designed to give operators and service providers the opportunity to run test cases and complete final testing.
- Final test results approved by EMVCo.

Approval

- Operators and Service Providers receive signed Letter of Approval and Reference Number from EMVCo.

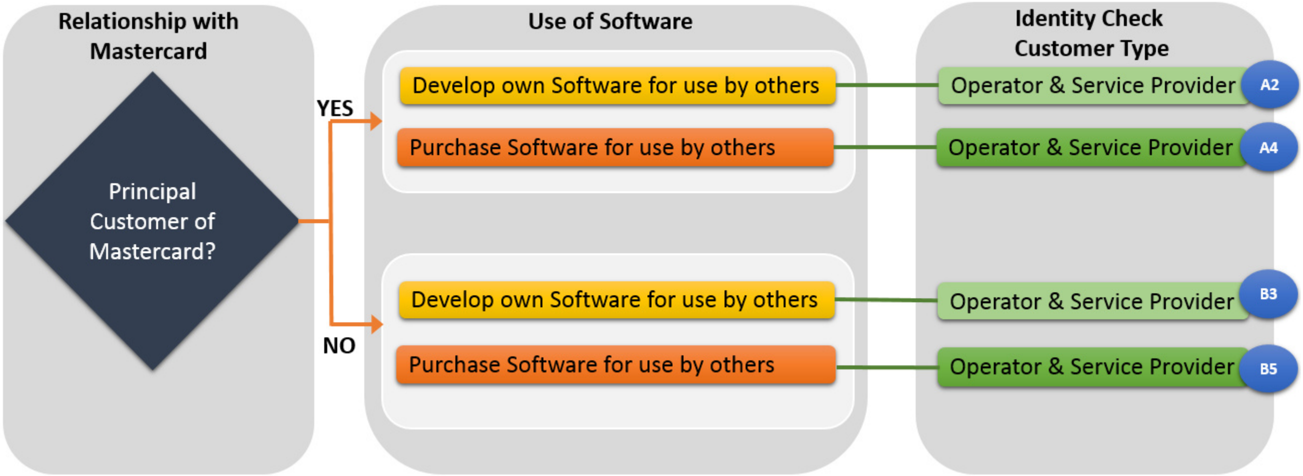
Useful EMVCo Links

- 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 Providers Customers Types

This section describes, in detail, the steps required to register as a Mastercard 3-D Secure service provider.

Registering as a Service Providers is a prerequisite to starting the onboarding process with Mastercard Identity Check for the following Identity Check customer types and scenarios: A2, A4, B3, and B5.


Relationship with Mastercard
Principal Customer of Mastercard?
YES
NO
Use of Software
Develop own Software for use by others
Purchase Software for use by others
Develop own Software for use by others
Purchase Software for use by others
Identity Check Customer Type
Operator & Service Provider
A2
Operator & Service Provider
A4
Operator & Service Provider
B3
Operator & Service Provider
B5

Background

In November 2017, PCI Security Standards Council (PCI SSC) released a new security standard called PCI 3DS Core Security Standard. This new 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 security standard, Mastercard must help ensure all 3-D Secure vendors adhere to its security requirements and rules which are managed using the Service Provider Program. The creation of this new classification will highlight which vendors must adhere to the PCI Core 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 (3-DSS) system that facilitates communication, using 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, using 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 (Sponsor) must 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 at 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:
   a. Company ID - will be used to log on to Mastercard Connect and request access to the Mastercard Identity Check Testing platform application.
   b. Operator ID - will be used to request both your testing and production certificates and will be also included in your EMV-3DS messages.

      NOTE: For Customer Types (A1 and A3) that do not require Service Provider Registration, email identity_solution_compliance@mastercard.com to request assignment of an Operator Id.

   c. 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.
4. The 3-D Secure Service Provider should complete form 1145b. The form will give the users access to Mastercard Connect and the Security Administration application. A SecurID 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, 3-D Secure Service Providers must submit an Attestation of Compliance (AOC) certificate to pcireports@Mastercard.com. The 3-D Secure Service Provider has 30 days to submit upon confirmation of registration. For additional information regarding PCI 3DS requirements, please visit: 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.

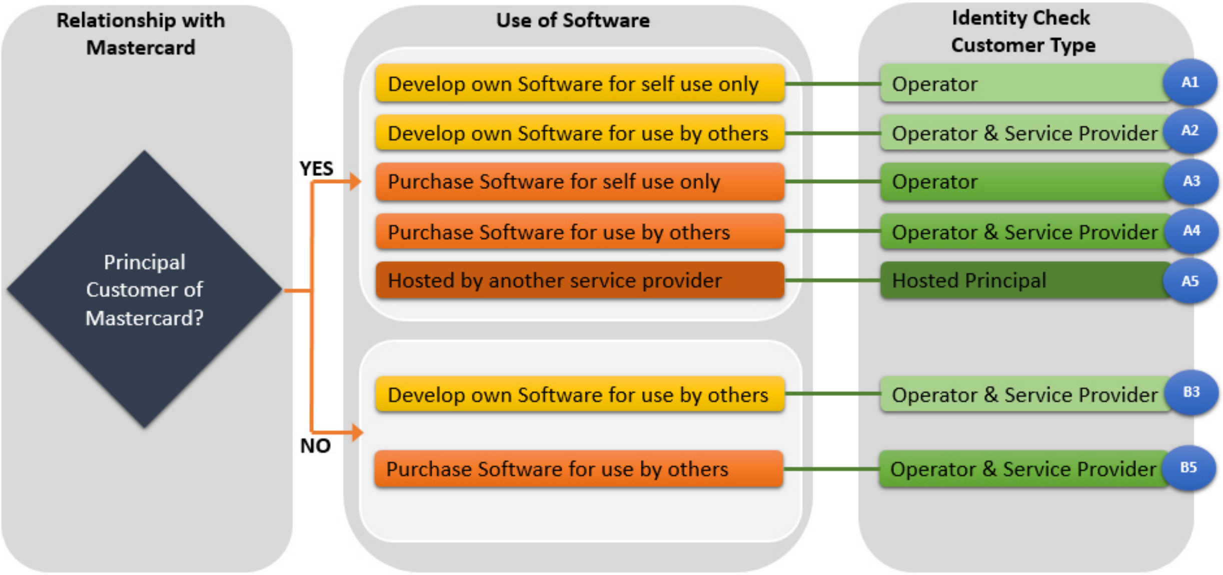
Chapter 3 Mastercard Identity Check Testing Platform Registration

This section describes the steps required to register on the Mastercard Identity Check Testing Platform.

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 is applicable for all Identity Check customer types and scenarios: A1-A5, B3, and B5.


Relationship with Mastercard
Principal Customer of Mastercard?
YES
NO
Use of Software
Develop own Software for self use only
Develop own Software for use by others
Purchase Software for self use only
Purchase Software for use by others
Hosted by another service provider
Develop own Software for use by others
Purchase Software for use by others
Identity Check Customer Type
Operator
A1
Operator & Service Provider
A2
Operator
A3
Operator & Service Provider
A4
Hosted Principal
A5
Operator & Service Provider
B3
Operator & Service Provider
B5

Request Access to Mastercard Connect

1. Sign up for Mastercard Connect at https://www.mastercardconnect.com. Review Appendix D 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. My Company Manager / Company Contact Management
3. Mastercard Identity Check Test Platform
4. Technical Resource Center

5. Identity Solutions Services Management (ISSM)

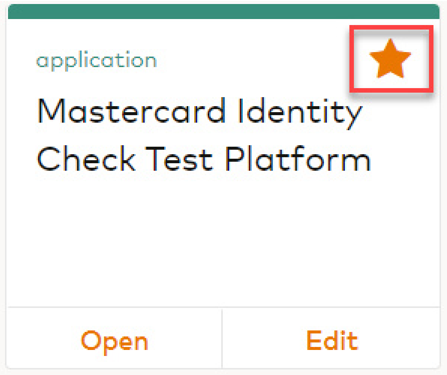
   NOTE: Identity Solutions Services Management is a tool designed for principal customers to enroll its ACS and Card Ranges on the directory server. Service Providers can receive access if a principal customer delegates access on its behalf.

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. Publications can be found on the Support page. No approval is for the Mastercard Identity Check Test Platform.

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.



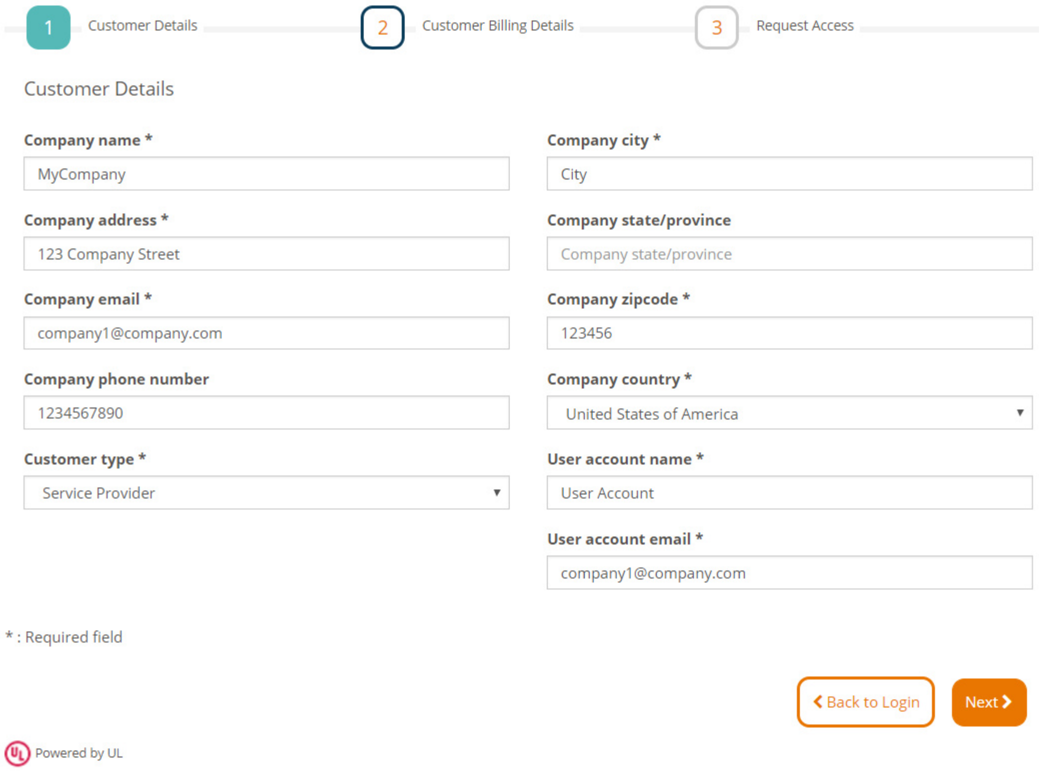
3. Review the related publications including the Mastercard Identity Check Program Guide to understand the specific processing and program requirements.
4. Open the Mastercard Identity Check Test Platform application and complete each of the following three sections. Reference the following table to 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
A5	Principal Customer	Mastercard Identity Check Program Registration Only

Customer Type	Customer Type	Registration Type
B3 and B5	Service Provider	Mastercard Identity Check Program Registration and Testing

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



Customer Details

Company name * MyCompany

Company address * 123 Company Street

Company email * company1@company.com

Company phone number 1234567890

Customer type * Service Provider

Company city * City

Company state/province Company state/province

Company zipcode * 123456

Company country * United States of America

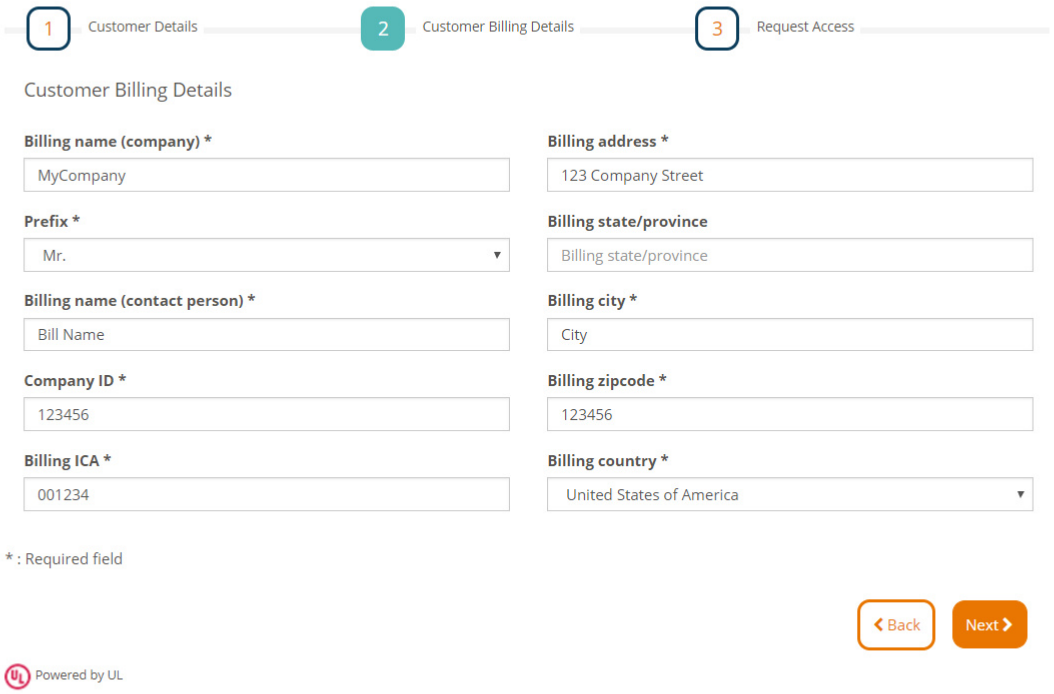
User account name * User Account

User account email * company1@company.com

* : Required field

b. **Customer Billing**—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** which can be found in the Mastercard 3-D Secure Service Providers Customers Types section above.
- Principal Customer will use the billing identifiers associated to their company.



Customer Billing Details

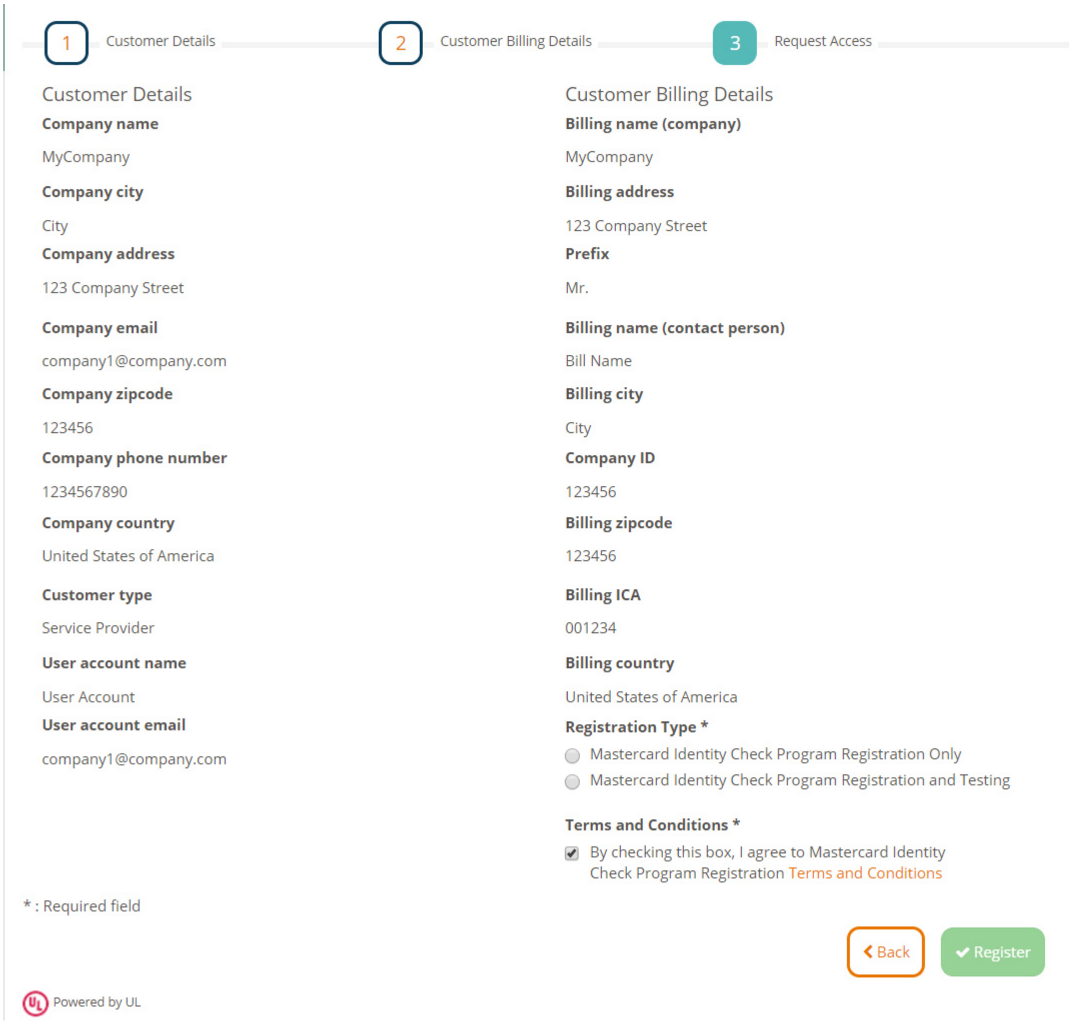
Billing name (company) *	Billing address *
MyCompany	123 Company Street
Prefix *	Billing state/province
Mr.	Billing state/province
Billing name (contact person) *	Billing city *
Bill Name	City
Company ID *	Billing zipcode *
123456	123456
Billing ICA *	Billing country *
001234	United States of America

* : Required field

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 card ranges on the directory server.



Customer Details

Company name
MyCompany

Company city
City

Company address
123 Company Street

Company email
company1@company.com

Company zipcode
123456

Company phone number
1234567890

Company country
United States of America

Customer type
Service Provider

User account name
User Account

User account email
company1@company.com

Customer Billing Details

Billing name (company)
MyCompany

Billing address
123 Company Street

Prefix
Mr.

Billing name (contact person)
Bill Name

Billing city
City

Company ID
123456

Billing zipcode
123456

Billing ICA
001234

Billing country
United States of America

Registration Type *
○ Mastercard Identity Check Program Registration Only
○ Mastercard Identity Check Program Registration and Testing

Terms and Conditions *
☑ By checking this box, I agree to Mastercard Identity Check Program Registration Terms and Conditions

* : Required field

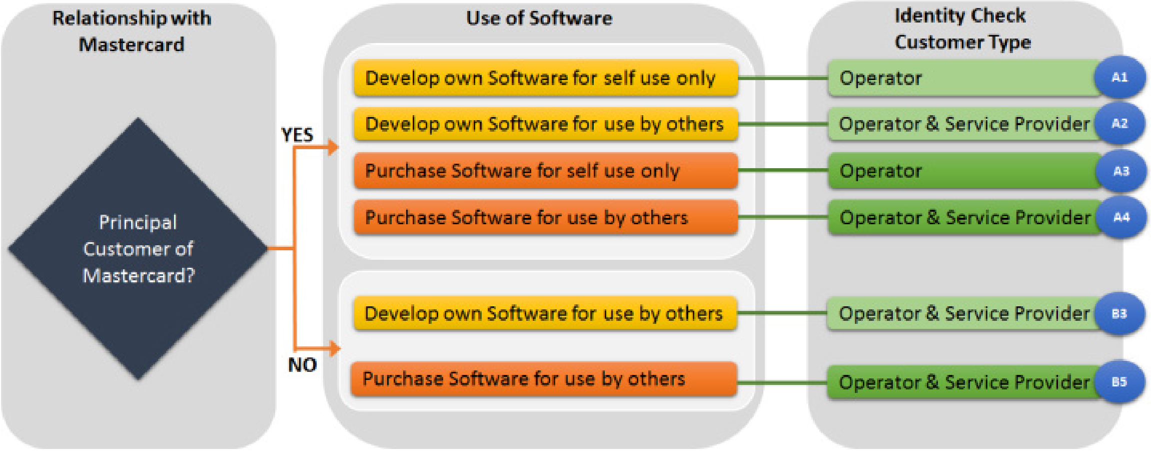
Chapter 4 Mastercard Identity Check Compliance Testing

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 ACS 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.

Mastercard Identity Check Testing

This section describes in detail the steps required complete testing 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.

This is applicable for the following Identity Check customer types and scenarios: A1-A4, B3, and B5.


Relationship with Mastercard
Principal Customer of Mastercard?
YES
NO
Use of Software
Develop own Software for self use only
Develop own Software for use by others
Purchase Software for self use only
Purchase Software for use by others
Develop own Software for use by others
Purchase Software for use by others
Identity Check Customer Type
Operator
A1
Operator & Service Provider
A2
Operator
A3
Operator & Service Provider
A4
Operator & Service Provider
B3
Operator & Service Provider
B5

NOTE: After a CIS Project Manager has been assigned and connectivity to the Mastercard Identity Check Test Platform has been established, the customer has 31 days to complete pre-compliance and compliance testing. Compliance testing fees are billed via MCBS Event ID 2VC8005. Completion is defined as all test cases executed and signed off by Mastercard. Customer implementation fees are separate from compliance testing fees and may vary by 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:
   - ACS TLS Server
   - ACS TLS Client
   - ACS Message Signing Certificate

   NOTE: One Message Signing certificate is required per Service Provider
2. Sign in to the Identity Check Testing Platform 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

NOTE: These are individual certificates. Mastercard does not issue combined/dual certificates.

Sandbox Connectivity

1. Use Sandbox Testing to establish connectivity of your ACS software to the Mastercard Identity Check Testing Platform.
2. After connectivity has been established, select the 'Move to Pre-Compliance' button

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 ACS Certificate ID. The ACS Certificate ID will be used to protect your Production CSR file.
3. After obtaining Pre-Compliance approval from CIS Project Manager, project will move automatically to Compliance Testing.
4. Complete the Letter of Compliance Form.
   - Contact Information
   - Business Contact
   - Security Contact
   - Certificate Contact
   - Click "Submit for LOC review" and await 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 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. CSR must be packaged into a password protected zip file. The password used to protect the zip file content must be the ACS certificate ID, which is located under Main Menu > Company Profile > Customer Details. Production CSR request should be sent to key_management@Mastercard.com. In order for KMS to receive clear certificate requests, we need to receive the request table completed together with the CSRs.

- ACS TLS Server
- ACS TLS Client
- ACS Message Signing Certificate

NOTE: One Message Signing certificate is required per Service Provider

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

Table 2: Certificate Forms & Details

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

Table 3: DN Requirements

ACS TLS Server	**ACS TLS Client**	**ACS Message Signing**
CN: [Domain Name] OR [public IP]	CN: [Domain Name] OR [public IP]	CN: [Free text]
PROD OU: ACSS-[Operator ID]	PROD OU: ACSC-[Operator ID]	PROD OU: ACSMS-[Operator ID]-[Optional Free Text]
MTF OU: ACSS-MTF-[Operator ID]	MTF OU: ACSC-MTF-[Operator ID]	MTF OU: ACSMS-MTF-[Operator ID]-[Optional Free Text]
O: [Operator registered company name]	O: [Operator registered company name]	O: [Operator registered company name]
ST: <State optional>	ST: <State optional>	ST: <State optional>
L: <Local optional>	L: <Local optional>	L: <Local optional>

ACS TLS Server	ACS TLS Client	ACS Message Signing
C: [valid 2 character ISO country code]	C: [valid 2 character ISO country code]	C: [valid 2 character ISO country code]

NOTE: The Mastercard-assigned Operator ID is provided once the service provider 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. The ACS must requests all certificates. If an issuer requests its own message signing cert, the ACS must uniquely identify the issuer in the in the [Optional Free Text] field.

Appendix A Identity Check Onboarding Documentation

This appendix contains documentation needed for Identity Check onboarding.

Onboarding Checklist

Complete	Task / Requirement	ACS Providers	Issuer / Processor	CIS	Reference
□	Choose a Mastercard Identity Check ACS providers		X		Compliant vendor service provider
□	Review the Mastercard Identity Check Program Guide		X		Mastercard Connect/ Publications
□	Open project with your ACS provider and select a Mastercard Identity Check compliant solution		X		
□	Review Mastercard Identity Check branding requirements	X	X		Branding Guidelines
□	Begin 3-D Secure Service Provider program. Request sponsor (issuer) to complete registration on behalf of 3-D Secure Service Provider	X	X		Mastercard Connect/My Company Manager
□	Receive 3-D Secure Service Provider Company ID (CID) assigned by Mastercard Franchise and sent to Sponsor	X			3-D Secure Service Provide need to request CID from Sponsor. CID is needed to access Mastercard Connect
□	Receive ACS Operator Id assigned by Identity Solutions Compliance. Receive ICA number for billing, if applicable.	X			
□	Complete form1145b to assign Security Administrators to manage the access for the 3-D Secure Service Provider	X			online_provisioning@mastercard.com

Complete	Task / Requirement	ACS Providers	Issuer / Processor	CIS	Reference
□	Sign up for Mastercard Connect using assigned 3-D Secure Service Provider CID.	X			Mastercard Connect
□	Review the PCI 3DS Core Security Standard Specification and related documents,then begin assessment process	X			PCI Security Standards Organization
□	Provide appropriate 3DS PCI materials to the Mastercard Standards Team as required by the 3-D Secure Service Provider Program	X			PCI Security Standards Organization Document Library
□	Complete applicable certification testing with EMVCo and receive Letter of Approval and Reference ID	X			https://www.emvco.com EMVCo certification can be done concurrently with the Service Providers steps above
□	Request/verify access to Mastercard Connect and the following applications: • Mastercard Identity Check Test Platform • Publications • My Company Manager - Company Contact Management • Technical Resource Center • Identity Solutions Services Management	X	X		Mastercard Connect Access to Mastercard Identity Check Testing Platform may take a few days
□	Review the Mastercard Identity Check Onboarding Guide	X	X		Mastercard Connect/ Publications

Complete	Task / Requirement	ACS Providers	Issuer / Processor	CIS	Reference
□	Sign in to Mastercard Connect and access the Mastercard Identity Check Testing Platform	X	X		Mastercard Connect**/** Mastercard Identity Check Testing Platform
□	**Register for the Mastercard Identity Check program under:** 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 are required		X		Mastercard Connect/ Mastercard Identity Check Testing Platform

Complete	Task / Requirement	ACS Providers	Issuer / Processor	CIS	Reference
□	**Register and test for the Mastercard Identity Check program under:** 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		X	
□	Mastercard to assign a CIS project manager	X		X	
□	With CIS assistance, create and submit testing Certificate Signing Request (CSR). Required certificates • ACS TLS Server • ACS TLS Client • ACS Message Signing	X		X	Testing CSR does not need to be password protected.
□	Install testing certificates	X			

Complete	Task / Requirement	ACS Providers	Issuer / Processor	CIS	Reference
□	Sign in to Mastercard Identity Check Testing Platform with your assigned Users 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
□	**Sandbox** Establish connectivity to the Mastercard Identity Check Platform using the 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 moved to "Compliance Testing"	X			Mastercard Identity Check Testing Platform
□	Generate SPA2 IAV	X	X		Mastercard Connect/ Publications/SPA2 for EMV 3DS Identity Check

Complete	Task / Requirement	ACS Providers	Issuer / Processor	CIS	Reference
□	Under **Main Menu > Company Profile > Customer Details** 3- D Secure Service Provider administrator needs to populate the ACS Certificate ID. Certificate ID is required to request certificates	X			Mastercard Identity Check Testing Platform
□	**Complete Letter of Compliance enrollment form:** • Contact Information • Business Contact • Security Contact • Certificate Contact Click "Submit for LOC review" button and await approval from CIS	X		X	Mastercard Identity Check Testing Platform
□	**Compliance Testing** Execute all test cases and await approval from your assigned CIS project manager	X		X	Mastercard Identity Check Testing Platform
□	Receive Mastercard Letter of Compliance	X		X	Provided by Mastercard
□	Update EMV-3DS messages to include the Mastercard assigned Operator ID	X			Provided by Mastercard

Complete	Task / Requirement	ACS Providers	Issuer / Processor	CIS	Reference
□	Create and submit Production Certificate Signing Request (CSR). The password used to protect the zip file must be the ACS certificate ID. Required Certificates: • ACS TLS Server • ACS TLS Client • ACS Message Signing	X			key_management@mastercard.com
□	Establish connectivity to the Production Directory Server	X			
□	Complete all end to end back office testing and implementations	X	X		
□	Coordinate live dates among all participants	X	X		
□	Enroll account ranges and ACS URL on the Identity Directory Server	X	X		Enrollment occurs through the ISSM Application
□	Maintain Smart Authentication Stand-In enrollment through Qualtrics survey	X	X		https://mastercard.az1.qualtrics.com/jfe/form/SV_41tJYjsidIllxC5
□	Monitor Production Transactions	X	X		

Access to Mastercard Connect

Results

Click Mastercard Connect Sign Up Guide to open the file.

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

Appendix B Production Procedures

The Production Procedures section includes the Company Contact Management application update and 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

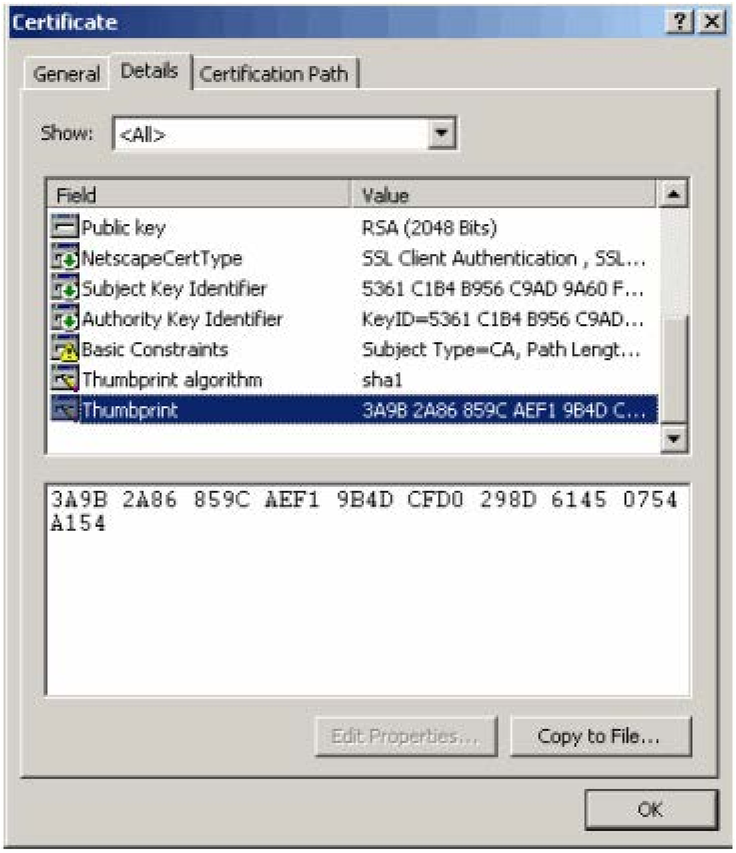
Within a Windows environment, double click on any individual Privacy Enhanced Mail (PEM) or Distinguished Encoding Rules (DER) encoded certificate file, and then click the Details tab from the resulting window.

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).



Show: <All>

Field	Value
Public key	RSA (2048 Bits)
NetscapeCertType	SSL Client Authentication , SSL...
Subject Key Identifier	5361 C1B4 B956 C9AD 9A60 F...
Authority Key Identifier	KeyID=5361 C1B4 B956 C9AD...
Basic Constraints	Subject Type=CA, Path Lengt...
Thumbprint algorithm	sha1
Thumbprint	3A9B 2A86 859C AEF1 9B4D C...

```
3A9B 2A86 859C AEF1 9B4D CFD0 298D 6145 0754
A154
```

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
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

Subject Name	
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
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.

Account Range Enrollment on Mastercard Identity Check Directory Server for Customers

This is applicable for the following Identity Check customer types and scenarios: A1-A5, B3, and B5.

Customers have the ability to add, update, and delete their card ranges in the Identity Solutions Services Management (ISSM) application found on Mastercard Connect. Refer to the Mastercard Identity Solutions Services Management User Guide for more detailed instructions on account range enrollment and other onboarding activities. 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 account ranges on the Directory Server. Failure to do so will prevent card range enrollment.

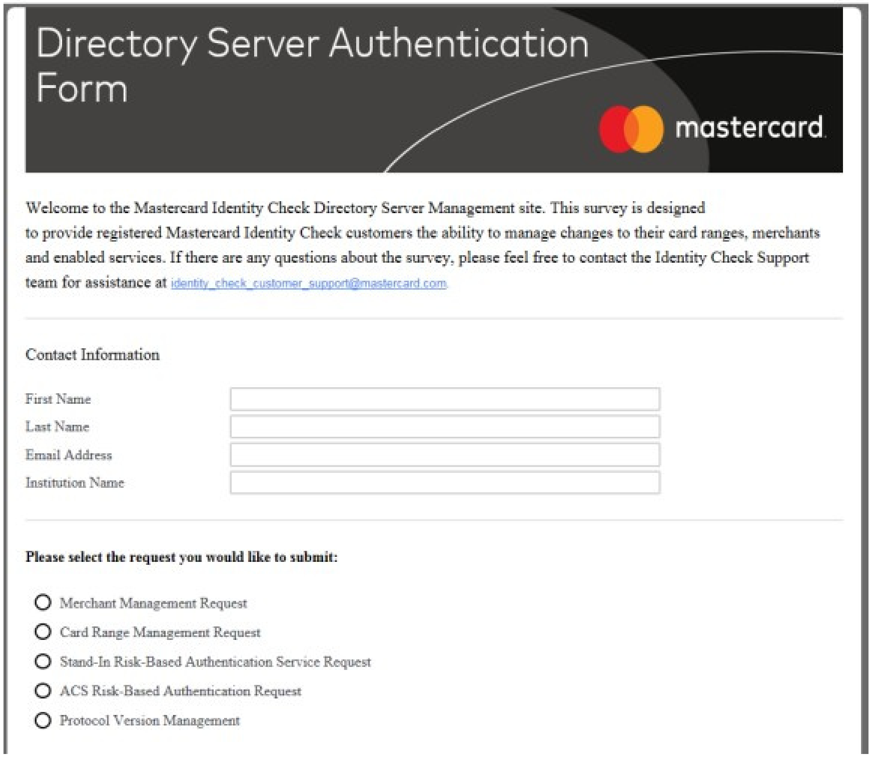
NOTE: Mastercard Identity Check Directory Server account card range enrollment is separate from the Mastercard SecureCode 3DS1.0.2.

Mastercard Identity Check Smart Authentication Stand-In Management

Issuers have the ability to maintain their Smart Authentication Stand-In participation (opt-out/ opt-in). The ability to opt-out of Smart Authentication Stand-In is only available for issuers in select countries. Issuers in the Asia Pacific, Latin America, Middle-East Africa, and North America regions are not able to opt-out. The maintenance of these parameters can be performed the following Qualtrics link: https:// mastercard.az1.qualtrics.com/jfe/form/SV_41tJYjsidIIlxC5. For more information on Smart Authentication Stand-In participation, contact IDC_Customer_Support@mastercard.com

Use the steps below to complete and submit Smart Authentication Stand-In Forms.

1. Complete the Contact information section and select Smart Authentication Stand-In Request.



Directory Server Authentication Form

Welcome to the Mastercard Identity Check Directory Server Management site. This survey is designed to provide registered Mastercard Identity Check customers the ability to manage changes to their card ranges, merchants and enabled services. If there are any questions about the survey, please feel free to contact the Identity Check Support team for assistance at identity_check_customer_support@mastercard.com

Contact Information

First Name

Last Name

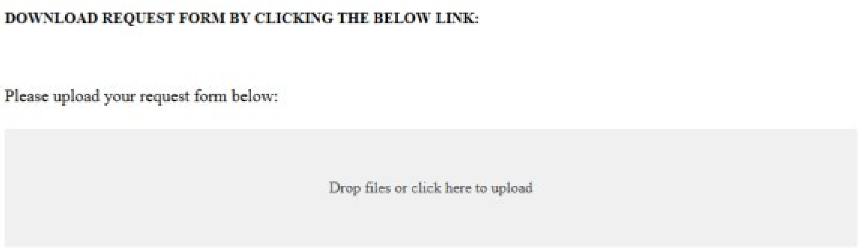
Email Address

Institution Name

Please select the request you would like to submit:

○ Merchant Management Request
○ Card Range Management Request
○ Stand-In Risk-Based Authentication Service Request
○ ACS Risk-Based Authentication Request
○ Protocol Version Management

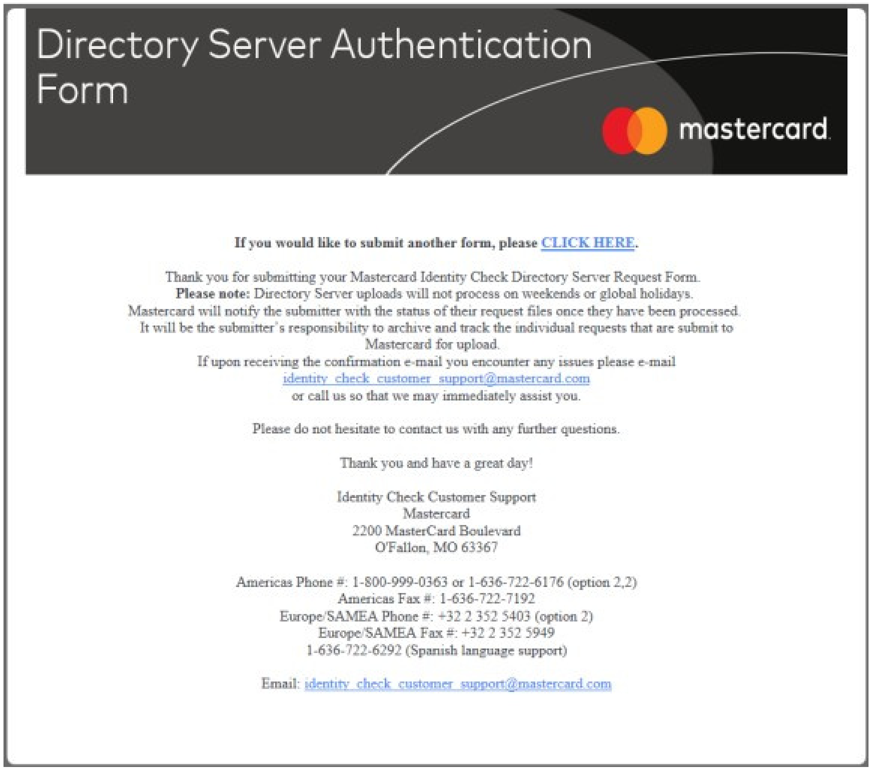
2. Click “Next” This will take you to the home page of the process selected above. The home page contains additional instructions, a link to download the current form version and the upload link to process the request form.
3. Fill the form out and save the file. Additional Instructions for completing the form are located on the first tab of the form. We do not require a specific file name, please name the file as you or your company desires. Please do not password protect or zip files, unless required by your organization.
4. Save the file to your desired location.
5. Click Browse to upload your request form. This is located near the bottom of the process.



DOWNLOAD REQUEST FORM BY CLICKING THE BELOW LINK:

Please upload your request form below:

6. Click Next
7. Once uploaded you will receive the below confirmation screen. Mastercard will process the uploaded files and email confirmation when upload is complete.



Directory Server Authentication Form

If you would like to submit another form, please CLICK HERE.

Thank you for submitting your Mastercard Identity Check Directory Server Request Form.
Please note: Directory Server uploads will not process on weekends or global holidays.
Mastercard will notify the submitter with the status of their request files once they have been processed.
It will be the submitter's responsibility to archive and track the individual requests that are submit to Mastercard for upload.
If upon receiving the confirmation e-mail you encounter any issues please e-mail
identity_check_customer_support@mastercard.com
or call us so that we may immediately assist you.

Please do not hesitate to contact us with any further questions.

Thank you and have a great day!

Identity Check Customer Support
Mastercard
2200 MasterCard Boulevard
O'Fallon, MO 63367

Americas Phone #: 1-800-999-0363 or 1-636-722-6176 (option 2,2)
Americas Fax #: 1-636-722-7192
Europe/SAMEA Phone #: +32 2 352 5403 (option 2)
Europe/SAMEA Fax #: +32 2 352 5949
1-636-722-6292 (Spanish language support)

Email: identity_check_customer_support@mastercard.com

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

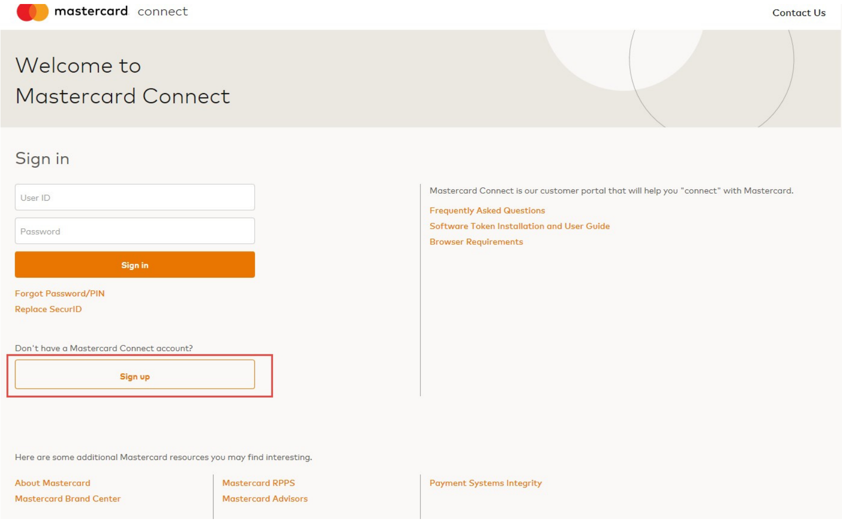
1. Uploads to the directory server through ISSM occur in real-time upon submission by user.
2. Submitters receive confirmation notification from application once the upload request has been successfully submitted.

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.



mastercard connect

Contact Us

Welcome to
Mastercard Connect

Sign in

User ID

Password

Sign in

Forgot Password/PIN
Replace SecurID

Don't have a Mastercard Connect account?

Sign up

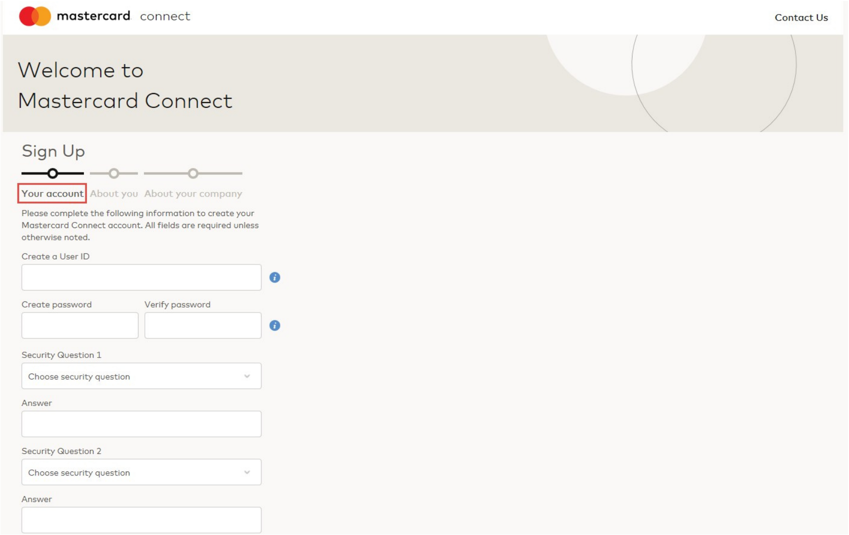
Mastercard Connect is our customer portal that will help you "connect" with Mastercard.

Frequently Asked Questions
Software Token Installation and User Guide
Browser Requirements

Here are some additional Mastercard resources you may find interesting.

About Mastercard
Mastercard Brand Center
Mastercard RPPS
Mastercard Advisors
Payment Systems Integrity

Step 1: Sign Up - Your Account



mastercard connect

Contact Us

Welcome to
Mastercard Connect

Sign Up

Your account About you About your company

Please complete the following information to create your Mastercard Connect account. All fields are required unless otherwise noted.

Create a User ID

Create password Verify password

Security Question 1

Choose security question

Answer

Security Question 2

Choose security question

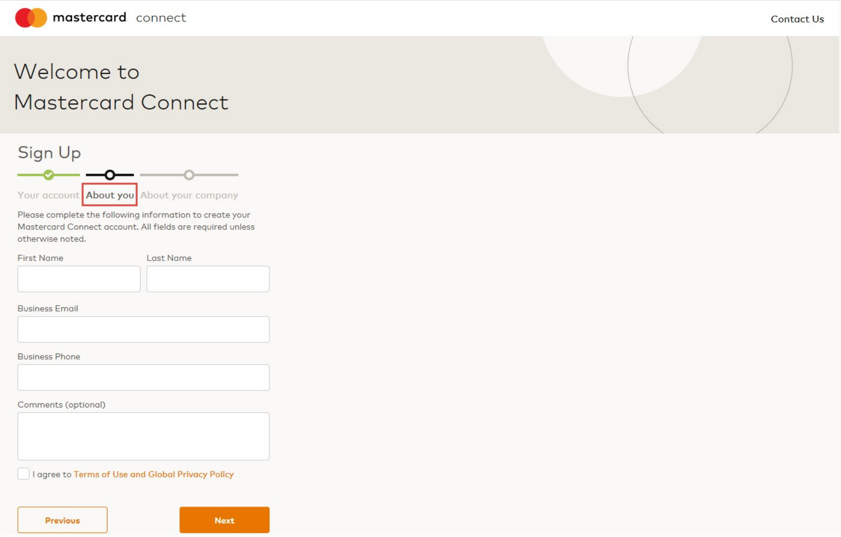
Answer

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

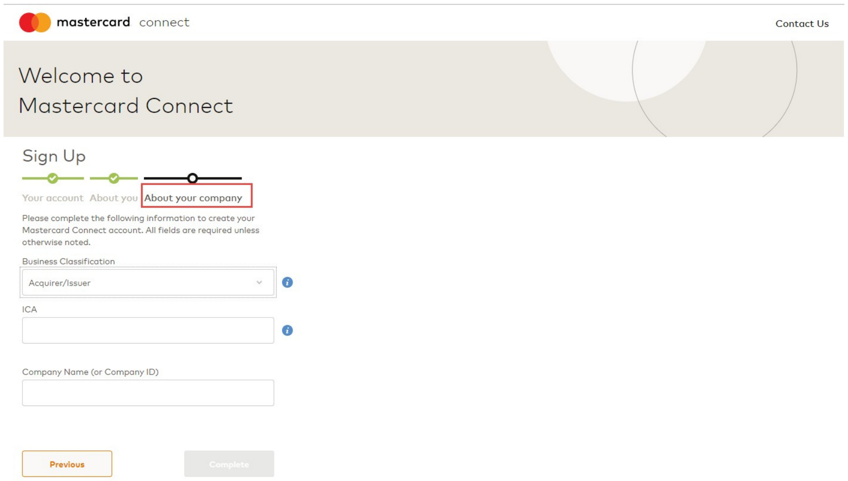


Please complete the following information to create your Mastercard Connect account. All fields are required unless otherwise noted.

□ I agree to Terms of Use and Global Privacy Policy

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



Welcome to
Mastercard Connect

Sign Up

Please complete the following information to create your Mastercard Connect account. All fields are required unless otherwise noted.

Business Classification: Acquirer/Issuer

ICA:

Company Name (or Company ID):

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 Company 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 Customer Operations Services team or the Mastercard Law Department for the registration status of particular product, program, or service names outside the United States.

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

Disclaimer

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 screen available on Mastercard Connect™. Go to Publications Support for centralized information.