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

1 February 2022

MIPTS

Contents

Summary of changes, 1 February 2022

This summary reflects changes effective since the last publication of this manual.

Description of change	Where to look
Minor editorial, grammatical, and typographical fixes, and formatting changes	Throughout
Chapter 1	
Replace figure and update title	Intended audience
Update hosted principal definition	Customer type definitions
• Make minor updates • Replace figure	Scope
Chapter 2	
• Replace title • Update summary	Onboarding requirements for operators and service providers
• Replace figure and figure title • Add new note to "Background" subsection	Mastercard 3-D Secure service provider onboarding
Make minor updates to opening paragraphs; replace image Make minor updates to "Request access to Mastercard Connect" subsection Make minor updates to "Required applications" subsection; reorder applications Make major updates (section rewrite) to "Accessing Identity Solutions Services Test Platform" subsection	Mastercard Connect access and Mastercard Identity Check registration
• Make major updates • Add new images	Register for Identity Check in ISST
• Add new subsection, "CIS project initiation request" • Make minor updates to Compliance test subsection	Mastercard Identity Check compliance testing
Make minor updates	Mastercard Identity Check compliance renewal

Description of change	Where to look
Add new section	Mastercard Identity Check functional testing
Move from appendix A	Company Contact Management
Chapter 3	
Add new sections	Hosted principal Identity Check onboarding Required applications 3-D Secure service provider registration Access Identity Solutions Services Test Platform Register for Identity Check in the Mastercard ISST Functional testing
Move from appendix A	Merchant Enrollment API Company Contact Management
Move from appendix C	Mastercard Identity Check Directory Server enrollment Additional notes Scaling merchant enrollments
Chapter 4	
Remove	
Appendix A	
Make major updates	Onboarding checklist Renewal checklist
Appendix B	
• Update title • Remove contact management-related text	Certificate procedures
Appendix C	
Remove	
Appendix D	
Rename to appendix C	Mastercard Connect sign-up guide

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 using the Mastercard authentication network.

Introduction to Identity Check and EMV 3-D Secure

Mastercard Identity Check is a global authentication program that uses the Mastercard authentication network with the EMV 3-D Secure Protocol.

Mastercard® Identity Check™ and EMV® 3-D Secure are designed to help provide more security for digital transactions and to enable higher approval rates by improving the authentication experience for issuers and cardholders for the e-commerce protocol.

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.

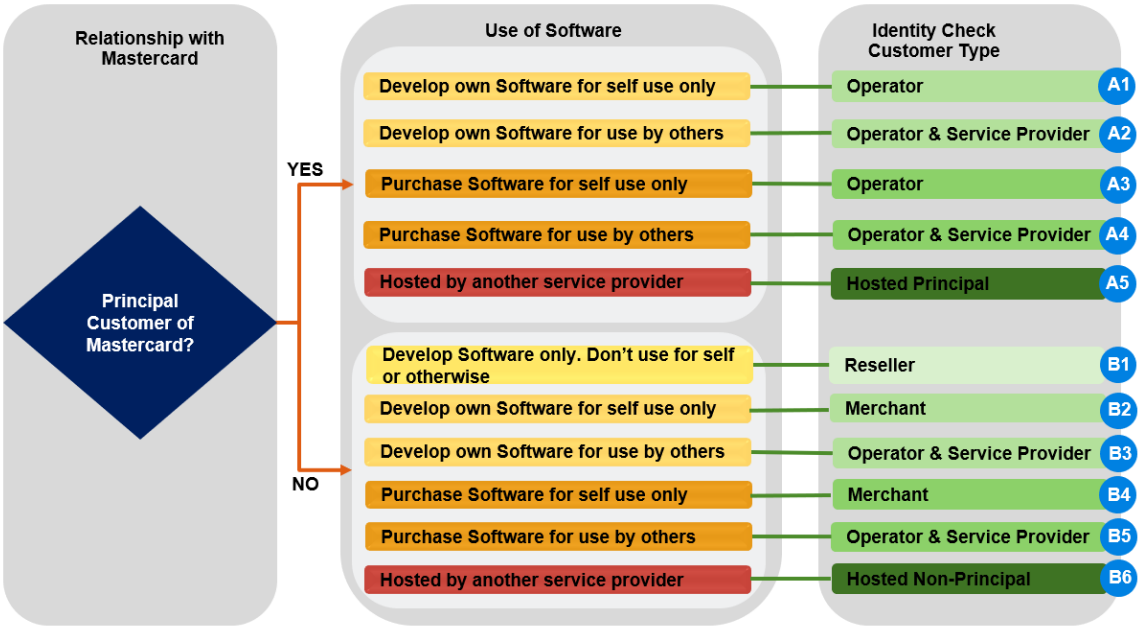
For more information about the Mastercard Identity Check program, refer to the *Mastercard Identity Check Program Guide*, which is available from Mastercard Connect™ Technical Resource Center.

Intended audience

To help identify the steps required to onboard with Mastercard Identity Check, customers must determine their Identity Check customer type and associated scenario before reading this onboarding guide.

This figure represents the decision tree to help you determine your customer type and scenario.

Figure 1: Mastercard Identity Check customer types and associated scenarios



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

Customer type definitions

The definitions in this section relate to Mastercard Identity Check onboarding for acquirers, merchants, and 3-D Secure (3DS) service providers.

Table 1: Customer types

Customer type	Description
Principal licensed customer of Mastercard	A customer licensed by Mastercard to offer branded products and services.
Mastercard 3DS service provider	This is a category within the Mastercard service provider program. An entity that hosts 3DS authentication solutions for Mastercard principal customers and their merchants. Noncustomers that provide authentication services, such as Identity Check, using EMV 3-D Secure are required to register in the program.

Customer type	Description
Acquirer	The Mastercard principal customer that provides the authorization, clearing functions, or both for their merchants using Mastercard Identity Check and EMV 3DS.
Merchant	A 3DS requestor using authentication services from a 3DS Server. The 3DS requestor may use a 3DS Software Development Kit (SDK).
Reseller	An 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 Access Control Server (ACS) or 3DS Server solution.
ACS operator	A customer that operates ACS software, that bought the ACS software from a reseller and wants to connect to the Mastercard Identity Check Directory Server.

Scope

3-D Secure onboarding with Mastercard for the support of Mastercard Identity Check using EMV 3DS is made up of five major steps. This guide explains these steps.

The steps vary depending on the relationship with Mastercard, usage of software, and the customer type. Each step has multiple activities and prerequisites, as illustrated in this figure. A checklist of steps is provided in the "Onboarding checklist" section of appendix A.

Figure 2: Prerequisites and onboarding steps by scenario and customer type

	Identity Check Scenario/Customer Type	Prerequisite: EMVCo Approvals Testing Required	Mastercard Identity Check Onboarding Steps: Register as a Mastercard 3DS Service Provider	PCI Compliance Required	ISST Platform Access Role	Identity Check Compliance Testing Required	Complete ISSM Enrollment Process
A1	Operator	Yes	No	Yes	Principal Customer – Operator 3DSS*	Yes	Yes
A2	Operator & Service Provider	Yes	Yes	Yes	Principal Customer – Operator 3DSS*	Yes	Yes
A3	Operator	No	No	Yes	Principal Customer – Operator 3DSS*	Yes	Yes
A4	Operator & Service Provider	No	Yes	Yes	Principal Customer – Operator 3DSS*	Yes	Yes
A5	Hosted Principal	No	No	No	Acquirer *	No	Yes
B1	Reseller	Yes	No	No	Service Provider – 3DSS*	No	No
B2	Merchant	Yes	No	Yes	Merchant Operator 3DSS*	Yes	Yes
B3	Operator & Service Provider	Yes	Yes	Yes	Service Provider – 3DSS*	Yes	Yes
B4	Merchant	No	No	No	Merchant Operator 3DSS*	Yes	Yes
B5	Operator & Service Provider	No	Yes	Yes	Service Provider – 3DSS*	Yes	Yes
B6	Hosted Non-Principal (Merchant or payment gateway)	No onboarding required with the Identity Check program			Merchant/PSP/Wallet*		

* **ISST has Admin and Tester/Read Only roles available for users to select.** Admin roles allow users to complete registration, perform testing functions, and perform ISSM functions (if applicable based off customer type).

NOTE: A1, A3, and B2 must be PCI-compliant but do not require proof. A2, A4, B3, and B5 have 30 days to submit their Attestation of Compliance (AOC) to Mastercard.

1. EMV 3-D Secure compliance testing and approvals

Although EMV 3-D testing and approvals are requirements of EMV[1]Co, often they are also a prerequisite to entry onto the Mastercard Identity Check Program. Successful EMVCo testing results in a Letter of Approval (LOA) 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 Identity Solutions Services Test Platform (ISST) for registration and testing. Once the service provider registration is completed, a company ID (CID), operator ID, billable ICA number, and 3DS requestor ID prefix are issued.

NOTE: The only exception to this rule is if a Mastercard acquiring customer operates the software (customer types A1 and A3). These customers are governed under the Mastercard Payment Card Industry (PCI) Compliance rules.

[1] EMV is a registered trademark of EMVCo LLC in the United States and other countries. For more information, visit http://www.emvco.com.

NOTE: The 3DS Server must use the 3DS requestor ID prefix as a traceability mechanism to identify the Payment Service Provider (PSP) at the merchant level. For more information, refer to the "Mastercard Identity Check required data elements" section in chapter 4 of the *Mastercard Identity Check Program Guide*.

3. Mastercard Identity Check registration

Mastercard Identity Check registration enables all customer types to accept the terms and conditions and declare their ability to support their merchant participation. This step includes requesting Mastercard Connect access along with getting access to the applications needed to support the Identity Check Program.

Program registration is completed through the ISST application on Mastercard Connect. Customers must request this access through the Mastercard Connect Store before completing program registration. Mastercard Identity Check program registration is completed with the customer'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 Mastercard Identity Check Directory Server.

4. Mastercard Identity Check compliance testing

The ISST application is used to test operators, service providers, and merchants, as defined by the Mastercard Identity Check customer types. All entities requesting a connection to the Mastercard Identity Check Directory Server are required to register and complete compliance testing. A Letter of Compliance (LOC) is issued when compliance testing is successfully completed.

NOTE: 3DS merchants, operators, and service providers connecting to ISST for compliance testing must support proprietary application programming interfaces (APIs) to establish full connection to the test platform. For more information, refer to the Docs section in the ISST Test Platform module.

5. Enrollment, production preparation, and deployment

Mastercard Identity Check Directory Server enrollment enables production loading of acquiring Bank Identification Numbers (BINs) with merchant IDs (MIDs). Production certificate connectivity is unrelated to merchant enrollment, and steps 1 through 4 must be completed before 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.

Contacts and related reference materials

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

Customer Technical Services

Customers can reach Mastercard Global Customer Technical Support (CTS) for support through the means listed in this section.

- Phone:
  - 800-999-0363 (Inside U.S.)
  - 636-722-6176 (Outside U.S.)
  - 636-722-6292 (Spanish Language Support)
- Fax: 636-722-7192
- Email: Digital.Identity.Solutions.Support@mastercard.com

Mailboxes

For questions about the Identity Check program compliance:
Identity_Solutions_Compliance@mastercard.com

Related Mastercard publications

- *Test Platform User Guide* - Under Docs in the Identity Solutions Services Test Platform module
- *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"
- *KMS Portal User Guide* - In the Key Management application on Mastercard Connect
- *Mastercard Identity Check Compliance Program-Access Control Server (ACS) Software*
- *Mastercard Identity Check Onboarding Guide for ACS Service Providers, Operators, Issuers, and Processors*
- *Mastercard Identity Check Compliance Program-3DS Server (3DSS) Software*
- *Data Integrity Monitoring Program*
- *Mastercard Service Provider Registration Guide*
- AN 3391 *Mastercard Customer Roadmap to Transition from 3DS 1.0 to EMV 3DS (2.0)*
- *Mastercard Standards for Trusted Merchant Listing User Guide Version*

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.

Table 2: Acronyms

Acronym	Description
3DS	Three Domain Secure
3DS SDK	3-D Secure Software Development Kit
3DS Server	The system that enables 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
API	Application Programming Interface
AOC	Attestation of Compliance
BIN	Bank Identification Number
CA	Certificate Authority

Acronym	Description
CID	Company ID
C&I	Cyber and Intelligence Solutions
CIS	Customer Implementation Services
CSR	Certificate Signing Request
CTS	Customer Technical Services
DER	Distinguished Encoding Rules
DNS	Domain Name Server
DS	Mastercard Identity Check Directory Server
EMVCo	EMVCo, LLC is a technical body that enables the worldwide interoperability and acceptance of secure payment transactions by managing and evolving the EMV specifications and related testing processes. EMVCo is the governing body for the EMV 3-D Secure Protocol.
EMV 3-D Secure	Specification published by EMVCo (3DS 2.0)
GIS	Global Information Security
IAV	Issuer Authentication Value
IDC	Mastercard Identity Check
ISSM	Identity Solutions Services Management
ISST	Identity Solutions Services Test Platform
KMS	Key Management Services
KPI	Key Performance Indicator
LOA	Letter of Approval (issued by EMVCo)
LOC	Letter of Compliance (issued by Mastercard)
MID	Merchant ID
MTF	Mastercard Test Facility
PCI	Payment Card Industry
PCI SSC	Payment Card Industry Data Security Standards Council
PEM	Privacy Enhanced Mail
PSP	Payment Service Provider
SDK	Software Development Kit
SDK Reference Number	Reference number assigned by EMVCo

Acronym	Description
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
TRA	Transaction Risk Analysis
UCAF	Universal Cardholder Authentication Field in Mastercard Authorization

Chapter 2 Onboarding requirements for operators and service providers

This chapter provides an overview of the steps required for 3-D Secure (3DS) operators and service providers to onboard to the Identity Check Program.

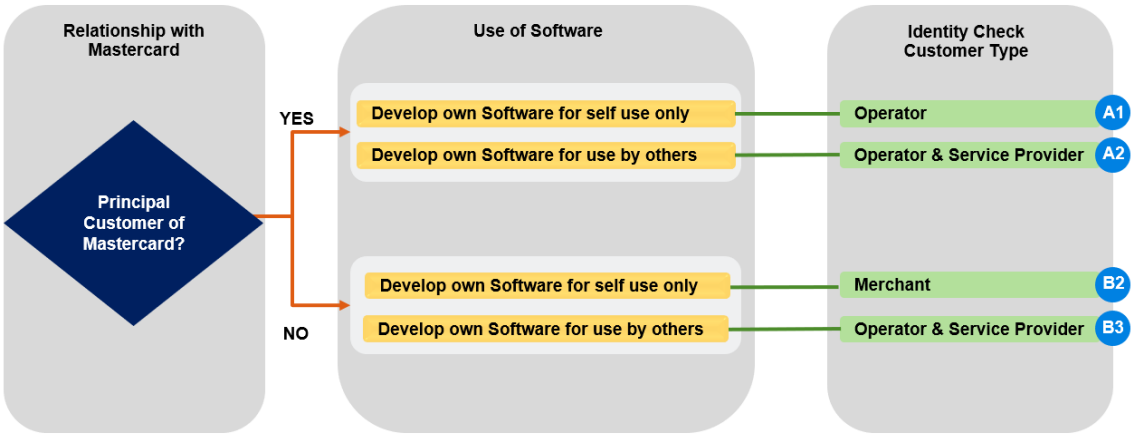
EMVCo approvals

This section provides an overview of the steps required to obtain an EMVCo Letter of Approval (LOA).

Completion of the EMV®Co approvals process is a prerequisite to starting the onboarding process with Mastercard® Identity Check™.

These Identity Check customer types and scenarios, which are shown in this figure, must complete the EMVCo approvals process: A1, A2, B2, and B3.

Figure 3: Identity Check customer types for EMVCo approvals



The "EMV 3DS approval process" section outlines the EMVCo approvals process. For more information, go to the EMVCo website at http://www.emvco.com.

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 allow operators and service providers to run test cases and evaluate their products.
   - At the end of this phase, test results are evaluated by EMVCo before moving to compliance testing.
2. Compliance
   - This phase is designed to allow operators and service providers to run test cases and complete final testing.
   - Final test results are approved by EMVCo.
3. Approval
   - Operators and service providers receive the signed LOA and reference number from EMVCo.

Useful EMVCo links

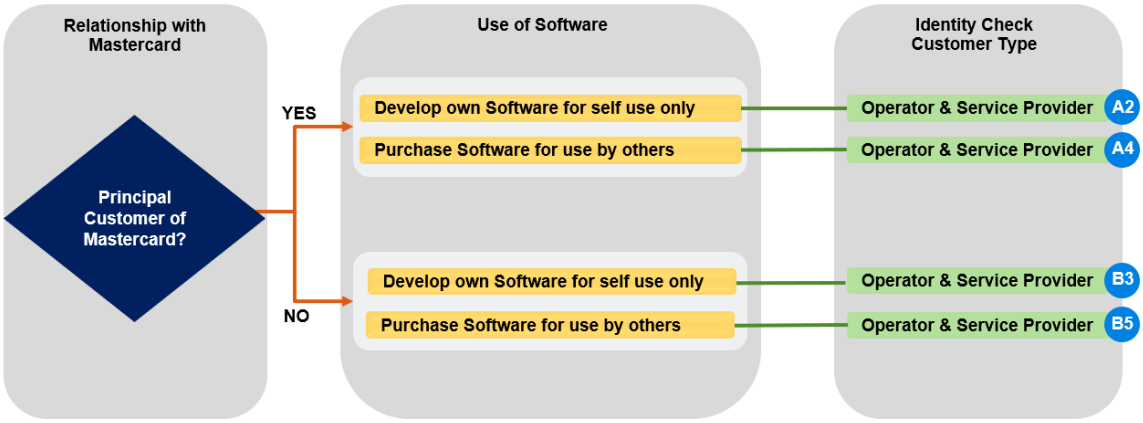
- EMVCo 3-D Secure Protocol and Core Functions Specification: www.emvco.com
- EMV 3-D Secure specification questions: 3DS_admin@emvco.com
- EMVCo 3-D Secure (3DS) compliant software: https://www.emvco.com/emv-technologies/3d-secure/

Mastercard 3-D Secure service provider onboarding

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

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

Figure 4: Mastercard 3-D Secure service provider registration



NOTE: A1, A3, and B2 must be PCI-compliant but do not require proof. A2, A4, B3, and B5 have 30 days to submit their Attestation of Compliance (AOC) to Mastercard.

3-D Secure Service Provider

With the release of the PCI 3DS Core Security Standard, Mastercard must help ensure that all 3-D Secure vendors adhere to security requirements and rules, which are managed through the Service Provider Program. The creation of the service provider classification highlights which vendors must adhere to the Payment Card Industry (PCI) 3DS Core Security Standard.

A 3-D Secure service provider is an entity that

- controls a 3-D Secure server system that enables 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 Identity Check Program rules.

3-D Secure service provider registration

Each principal customer that supports transactions through 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.

Completion of service provider registration uses this process:

1. The principal customer (sponsor) must register the 3-D Secure service provider in the My Company Manager application on Mastercard Connect™. For more information, refer to the *Mastercard Service Provider Registration Guide* on Mastercard Connect.

   NOTE: If the service provider profile does *not* exist, a new registration is needed. Forty-eight hours are required 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 confirms to the service provider that registration is complete and will provide form 1145b, Mastercard Connect Access, and any remaining steps.
3. The service provider is assigned these:
   - Company ID (CID), which will be used to log on to Mastercard Connect and request access to Identity Solutions Services Test Platform (ISST).
   - Operator ID, which will be used to request both testing and production certificates and will also be included in EMV-3DS messages.
   - 3DS requestor ID prefix. For more information about this value, refer to the *Mastercard Identity Check Program Guide*.
   - A billable ICA number, which will be assigned to the service provider before opening a compliance project. The number will be sent by email.

   NOTE: Customer types that do not require service provider registration (A1, A3, B2, and B4) should send an email to identity_solutions_compliance@mastercard.com to request assignment of an operator ID and a 3DS requestor ID prefix.

4. The 3-D Secure service provider must complete form 1145b. The form gives 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 AOC certificate to pcireports@mastercard.com. The 3-D Secure service provider has 30 days to submit upon confirmation of

registration. For more information about PCI 3DS requirements, go to https://www.pcisecuritystandards.org/.

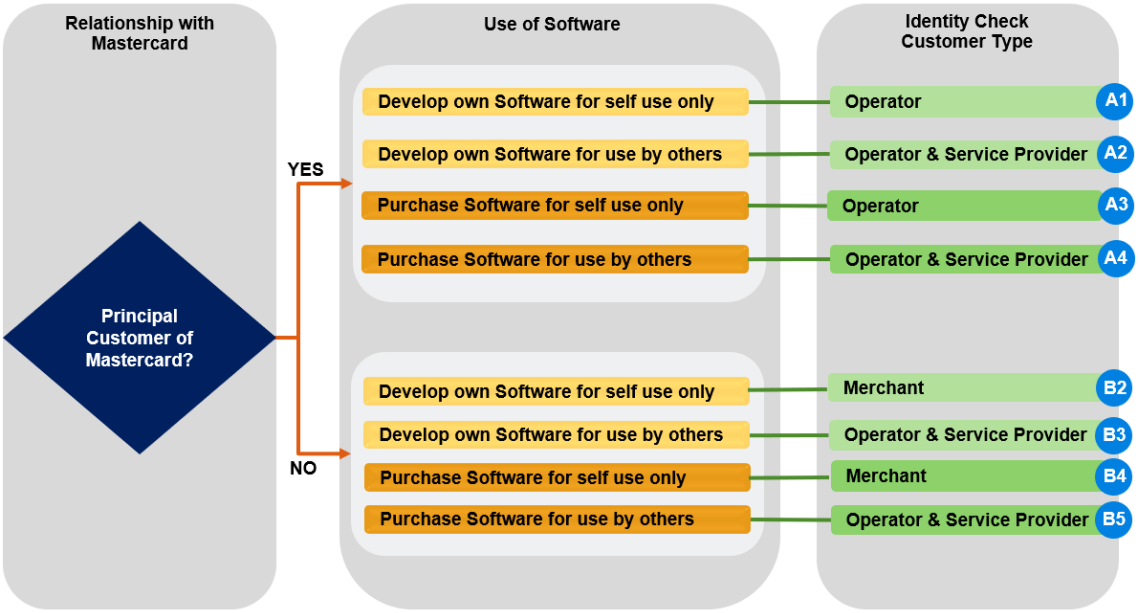
NOTE: If a customer is currently registered as a service provider under another program, it is also required to register as a 3-D Secure service provider. A principal customer (sponsor) may be subject to a registration fee.

Mastercard Connect access and Mastercard Identity Check registration

This section describes the steps required to request access to Mastercard Connect and to register on ISST.

The steps outlined in this section apply to these Identity Check customer types: A1 through A4 and B2 through B5.

Figure 5: Applicable customer types for Mastercard Connect access and Identity Check registration



Request access to Mastercard Connect

This section outlines the steps for requesting access to Mastercard Connect.

Procedure

1. Sign in to Mastercard Connect at https://www.mastercardconnect.com.
   For more information on Mastercard Connect registration, refer to the "Sign up a new user" section in appendix C.

2. On page three of the sign-up process, select the Business Classification of Processor and then enter your company name or CID.

   You will receive an onscreen 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, Mastercard recommends that each user requests access to the applications listed in this section. The applications are available from the Mastercard Connect Store.

- Identity Solutions Services Test Platform (ISST)

  NOTE: For access designations based on customer type, refer to the table in the "Accessing Identity Solutions Services Test Platform" section.

- Company Contact Management in My Company Manager
- Technical Resource Center
- Identity Solutions Services Management (ISSM)

  NOTE: ISSM is a tool for principal customers (acquirers) to enroll their merchant IDs (MIDs) and acquiring Bank Identification Numbers (BINs) on the Mastercard Directory Server. A service provider can receive access if a principal customer delegates access on its behalf.

- Key Management Portal

After all approvals have been granted, the applications are available under My Items.

Accessing Identity Solutions Services Test Platform

Identity Solutions Services Test Platform (ISST) is a centralized program management and testing application for parties that participate in Identity Check and its supporting authentication network services.

ISST supports these capabilities for operators and service providers that participate in the Identity Check Program:

- Identity Check Program registration
- Identity Check compliance testing
- Identity Check functional testing

Users requiring access to ISST must request access through the Mastercard Connect Store checkout process, and the company's security administrator must approve the order before full access is granted. This table outlines the role definitions based on customer type.

Table 3: Access designation based on customer type

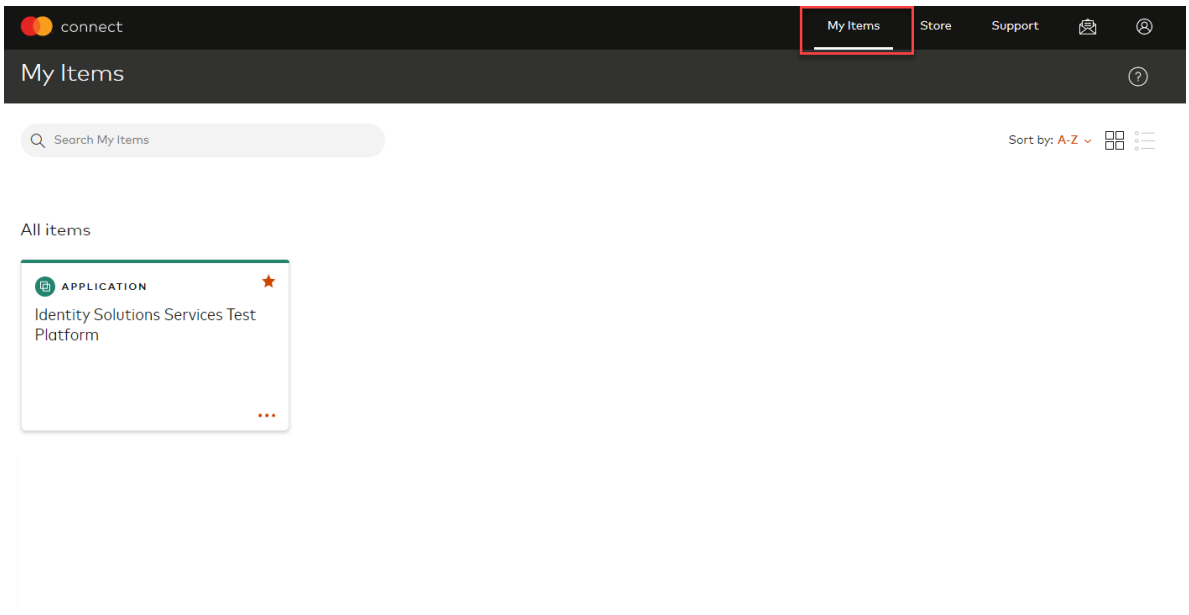
Customer scenario	Customer type	Role selection
A1, A2, A3, and A4	Principal customer	Principal Customer - Operator 3DSS - Admin or Principal Customer - Operator 3DSS - Tester
B2 and B4	Merchant	Merchant - Operator - 3DSS or Merchant Operator 3DSS - Tester
B3 and B5	Service provider	Service Provider - 3DDS - Admin or Service Provider - 3DSS - Tester

An Admin role allows users to register for any required program along with full access to the test platform. A Tester role allows read-only access to view its company's registered programs but will receive full access to the test platform.

NOTE: There is no charge to order ISST, but companies may incur fees related to compliance or functional testing.

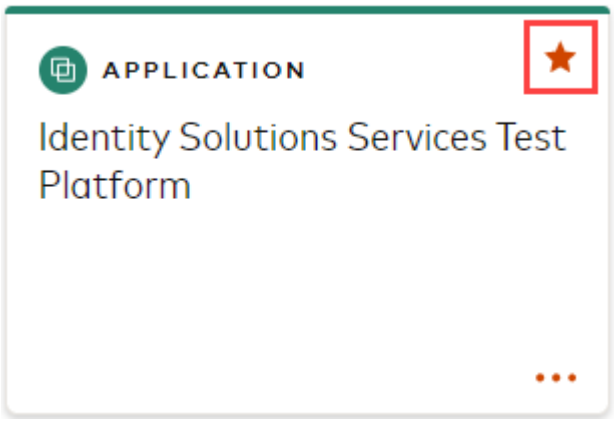
Once access has been granted, users can access the ISST application through My Items on Mastercard Connect.

Figure 6: Accessing the ISST application through My Items on Mastercard Connect



Users can also add applications to the Mastercard Connect homepage by clicking the star icon in the top-right corner of the application.

Figure 7: Adding an application to the Mastercard Connect homepage



Register for Identity Check in ISST

To participate in the Identity Check Program, all customer types must register and accept the terms and conditions of the program.

About this task

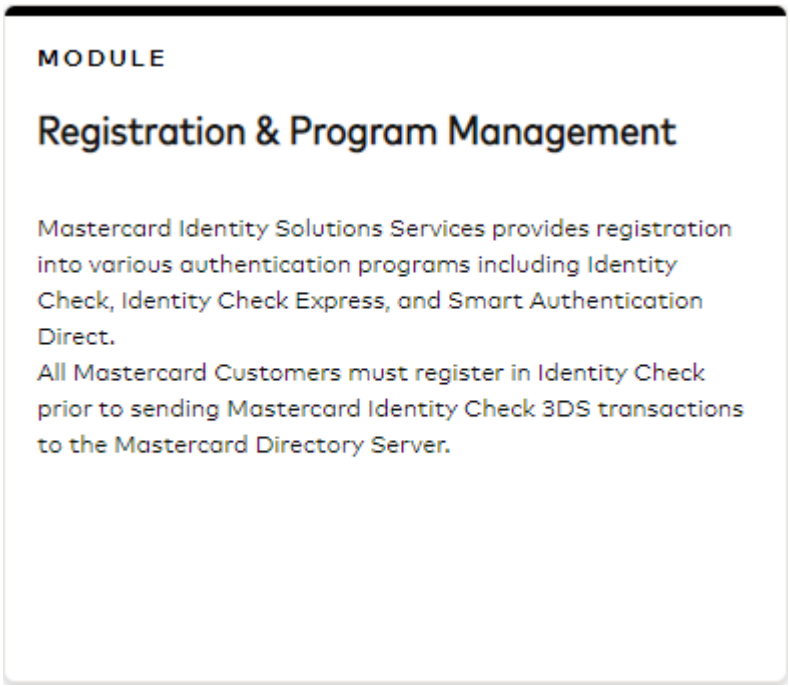
Identity Check registration is a one-time registration that is completed when an operator or service provider onboards for the first time. An administrator user

must complete registration functions in the ISST application by following these steps.

Procedure

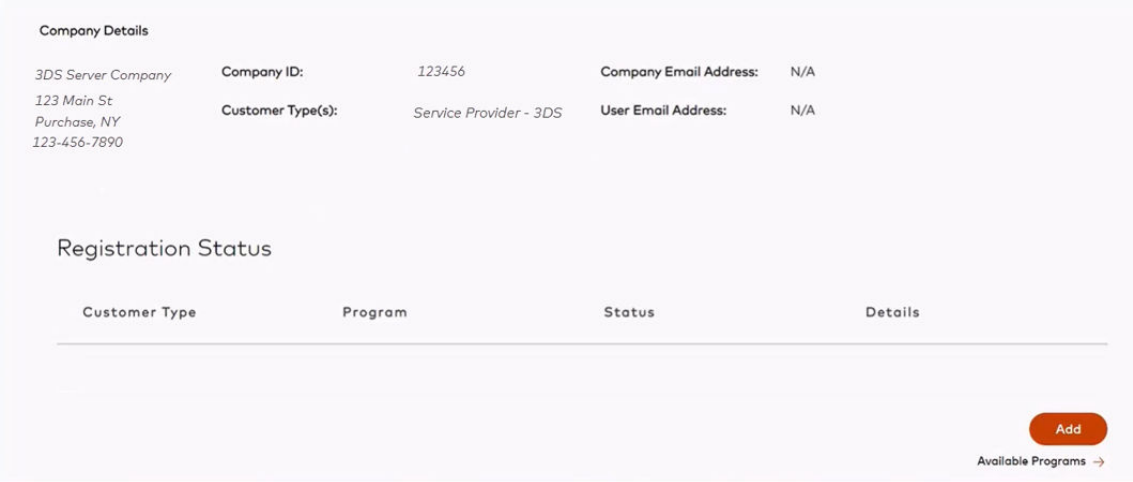
1. In the ISST application, open the Registration & Program Management Module by selecting the module box.

Figure 8: Registration & Program Management module



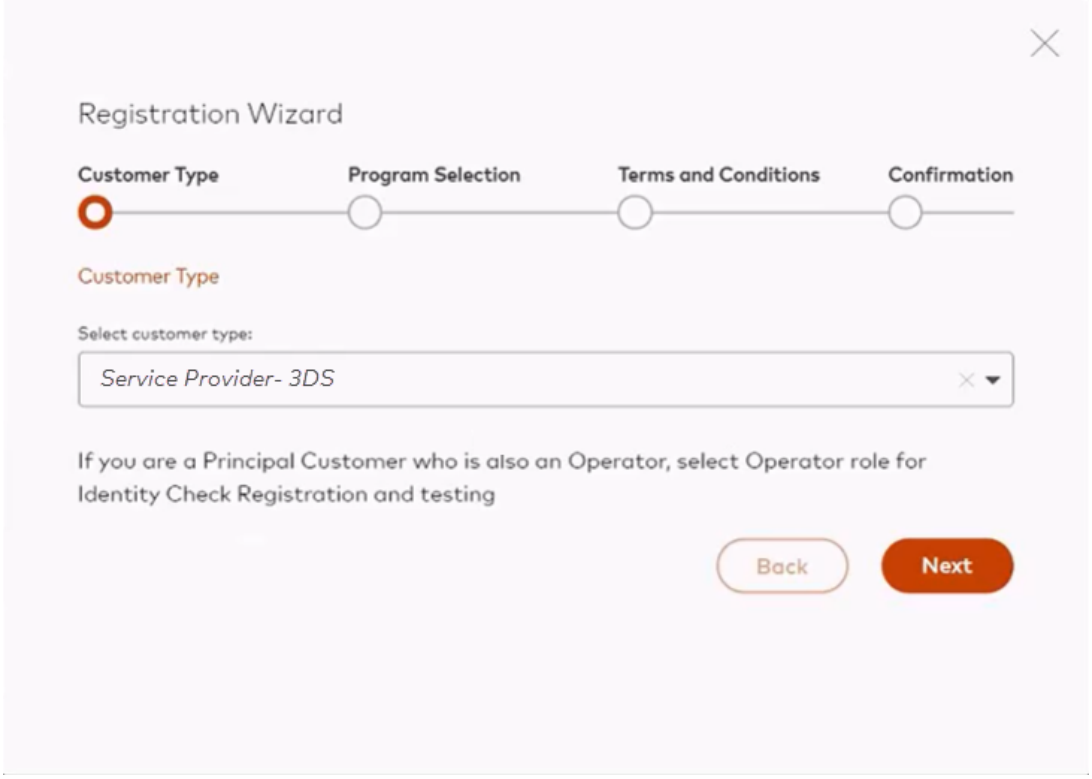
- Within the Registration & Program Management module, the **Company Details** section is pre-populated based on the user's Mastercard Connect profile.
- The **Registration Status** section lists all active registrations for the company displayed.
- **Available Programs** on the bottom-right of the screen displays all programs available for registration based on the company and customer type that was selected when access was requested to ISST in the Mastercard Connect Store.

Figure 9: Company details and registration status



2. Register for a program.
   a. On the bottom-right corner of the **Company Details** screen, click **Add**.
   b. On the **Customer Type** screen, select the customer type for the registration request.

      Figure 10: Selecting the customer type

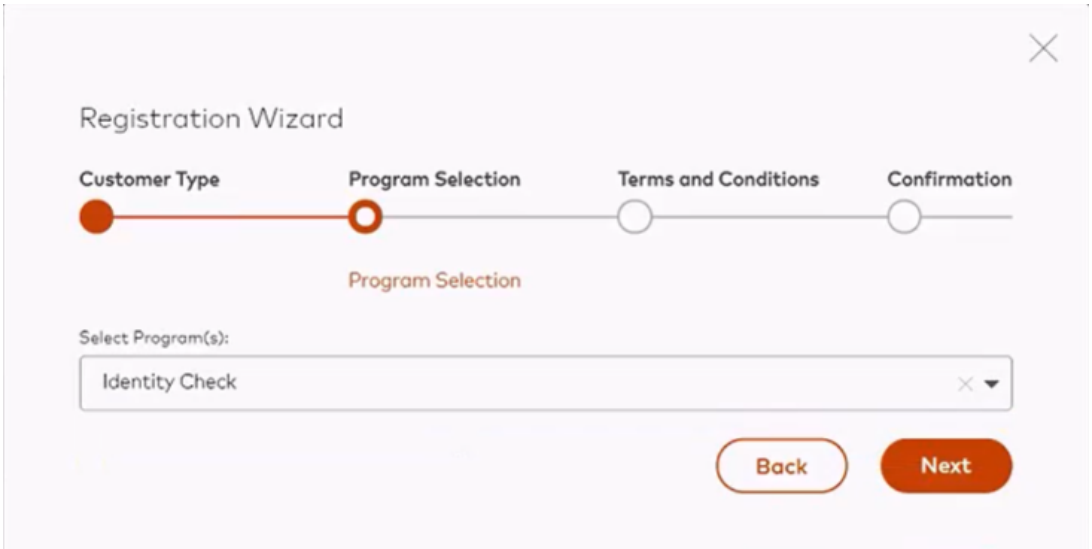


   c. Click **Next**.

The **Program Selection** screen displays a list of available programs for registration.

d. Select registration type Identity Check.

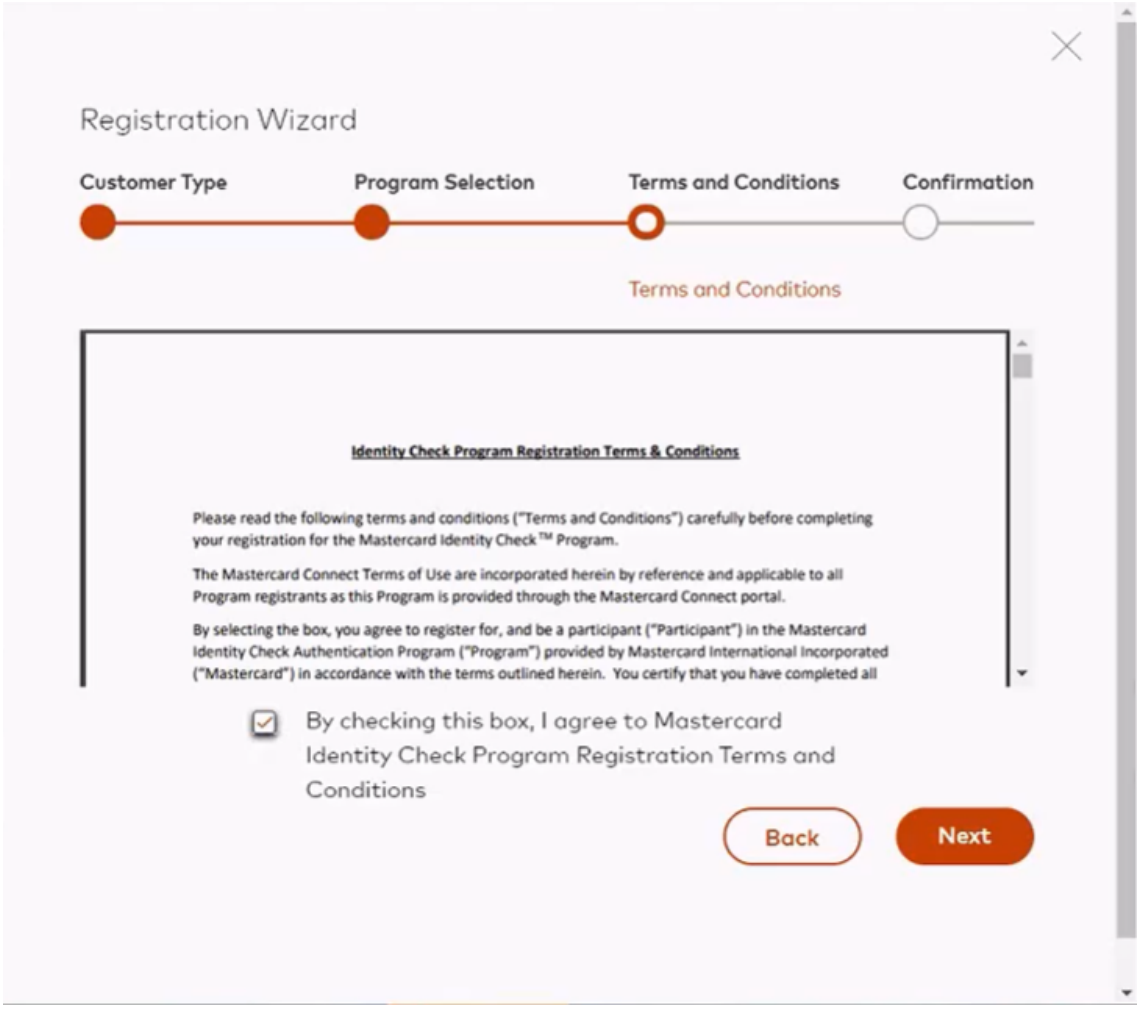
Figure 11: Selecting the Identity Check registration type



If no selections are displayed, refer to the **Registration Status** section to determine if registration has already been completed.

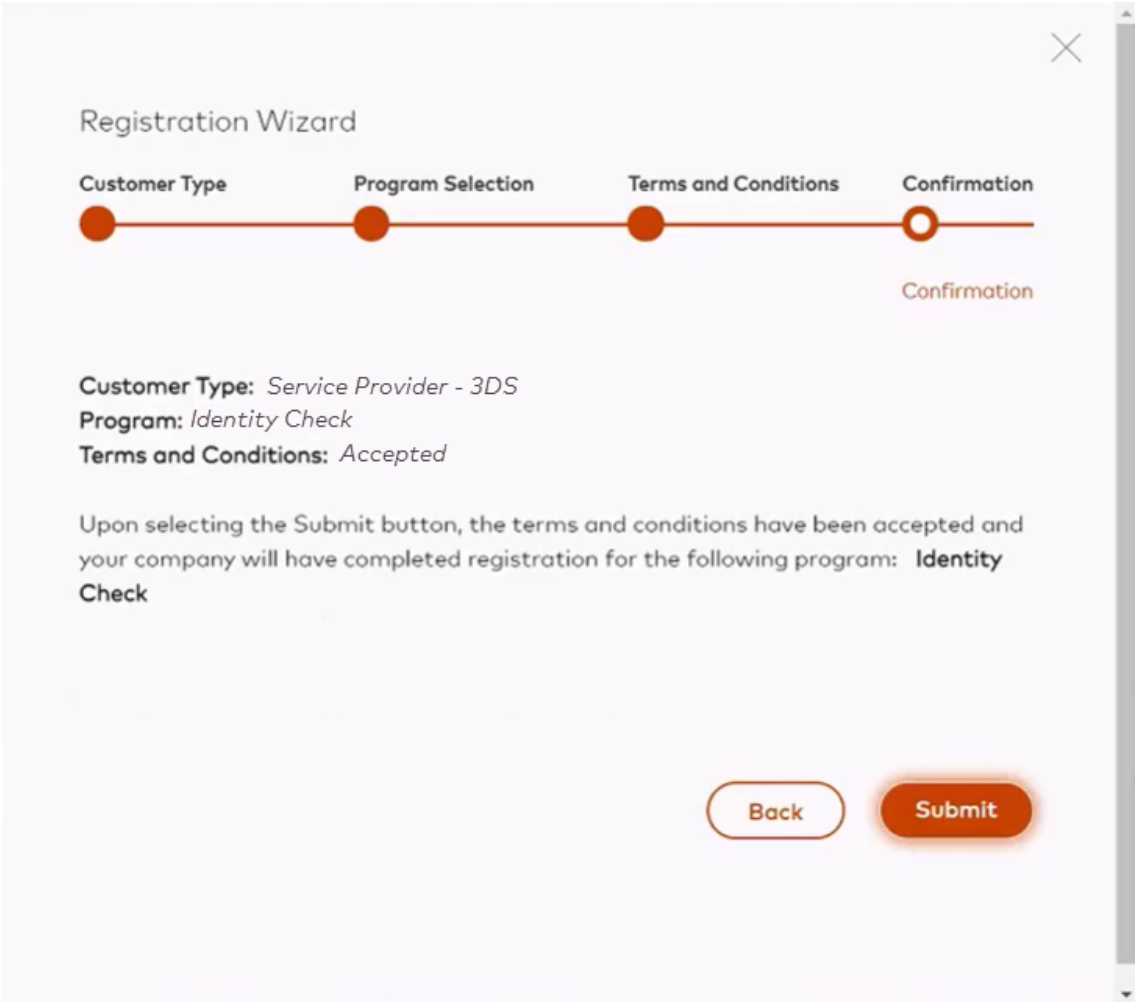
3. Click **Next**.
4. On the **Terms and Conditions** screen, review the terms and conditions and then check the box to agree to them.

Figure 12: Agreeing to the terms and conditions



5. Click **Next**.
   The **Confirmation** screen displays a summary of the registration request.
6. Click **Submit**.

Figure 13: Completing the registration request



Results

- Once the registration has been submitted, it is effective immediately. The user will receive a confirmation email of the successful registration.
- The user can proceed with compliance testing. For more details, refer to the "Mastercard Identity Check compliance testing" section.

NOTE: Operators and service providers do not need to submit a new registration for each EMVCo version. For operators and service providers renewing Identity Check compliance or upgrading to a new version, refer to the "Renew Mastercard Identity Check compliance" section.

Mastercard Identity Check compliance testing

This section outlines the steps required to onboard and complete compliance testing within the ISST application on Mastercard Connect.

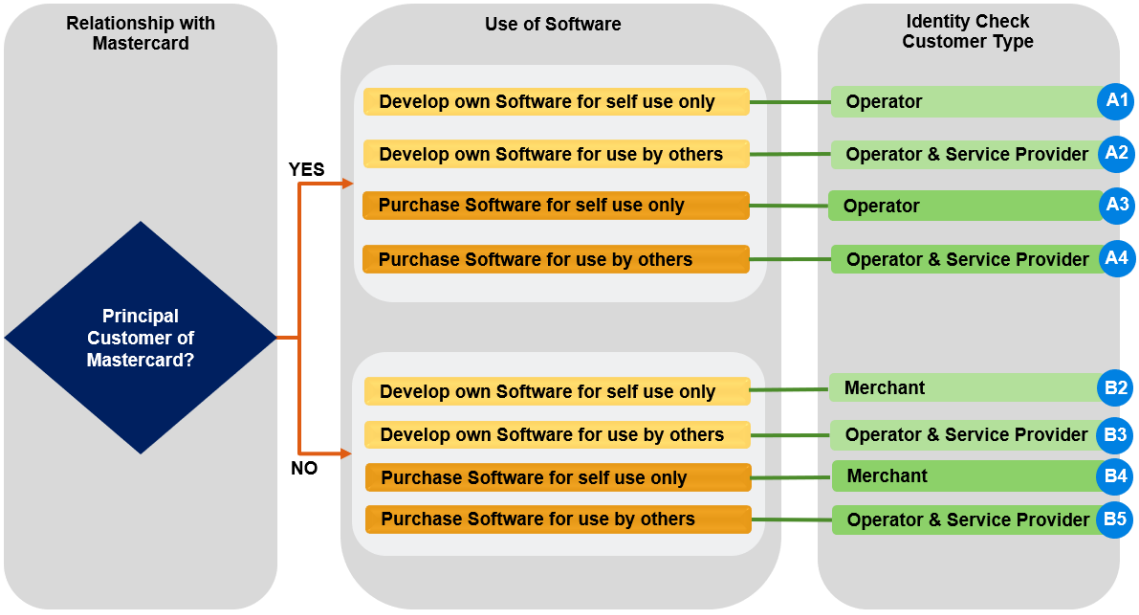
Testing on the ISST enables EMVCo tested and approved components to test compliance with Mastercard Identity Check program-processing rules. Operators and service providers operating EMV 3DS software within the Identity Check Program are required to complete compliance testing every 2 years, as defined in the *Mastercard Identity Check Compliance Program - 3DS Server (3DSS) Software* guide.

The test platform allows the 3DS server to create a testing project and test its software against the Identity Check Compliance Test Plan. Successful completion of the compliance-testing results in a Letter of Compliance (LOC).

This section describes the steps required to complete testing with ISST. For more detailed information on using the test platform, refer to the Docs section in the application.

Compliance testing is required for these Identity Check customer types: A1 through A4 and B2 through B5.

Figure 14: Identity Check customer types required to complete compliance testing



Initiate a CIS project

To initiate a project with the Customer Implementation Services (CIS) team, follow the steps in this section.

Procedure

1. Send an email to Identity_Check_Mandate_Testing@mastercard.com.
2. Provide this information:
   - Company name, as listed in ISST
   - CID
   - Billable ICA number
   - EMVCo LOA
   - Mastercard operator ID

   For Customer types (A1 and A3) that do not require service provider registration, send an email to identity_solutions_compliance@mastercard.com to request assignment of an operator ID.

   NOTE: After a CIS project manager has been assigned and connectivity to ISST has been established, the customer has 31 days to complete compliance testing. Compliance testing fees are billed using MCBS Event ID 2VC8005 or 2VC8015. Fees vary by region. Completion is defined as all test cases executed and signed off by Mastercard. Customer implementation fees are separate from compliance-testing fees and also vary by region.

Set up testing certificates

This section describes the process by which a 3DS Server sets up testing certificates that are required to connect to the directory server and ISST.

Procedure

1. Create and submit a test Certificate Signing Request (CSR) through the Key Management Portal.

   An example of the CSR form and details is in the "Certificate forms and details" table in the "Set up production certificates" section. These certificates are required:

   - 3DS Requestor TLS Server
   - 3DS Requestor TLS Client

   NOTE: These are individual certificates. Mastercard does not issue combined or dual certificates.
2. Install the test certificates provided by Mastercard.
3. Set up a project.

Complete Identity Check compliance testing

The steps in this section summarize what is required to complete Identity Check compliance testing.

About this task

For more detailed instructions on how to use the ISST, refer to the user guide under the Docs section in the test platform.

To connect to the compliance test platform to complete the compliance test cases, the 3DS Server must open a project within the test platform.

To establish connectivity to ISST, the 3DS Server must code to proprietary application programming interface (API) messages to fully connect to the test platform. These proprietary API messages help simulate the message flow within the 3DS requestor environment. For more information, refer to the System Under Test (SUT) configuration tab within the test platform.

After connectivity has been established, all test cases can be completed.

Procedure

1. Run and rerun test cases as needed.
2. Complete all manual test cases.
3. Validate that all test cases meet pass criteria or request an exception.
4. Click **Submit for Review** and wait for approval from the CIS project manager.
5. Once the project is approved, complete the LOC form.

   This information will be used to create the LOC notice once the project is completed:

   - Contact information
   - Technical contact
   - Contact address
   - Product
6. To close the project, click **Submit**.

Results

Once the project is closed in ISST, the LOC will be created and emailed to the contact listed on the LOC. The LOC is valid for 2 years, and the approved software will be listed on the Mastercard Identity Check vendor list at www.mastercard.us/en-us/business/overview/safety-and-security/identity-check/identity-check-vendors.html.

Set up production certificates

Production certificates are required for operators and service providers to establish connectivity to the production environment.

Procedure

Create and submit a CSR in the Key Management Portal.

For the Key Management Portal to process the CSR, the 3DS Server must upload the CSR to the Key Management Portal in the correct format. An example of the CSR form and CSR details is in the "Certificate forms and details" table.

These certificates are required:

- 3DS Requestor TLS Server
- 3DS Requestor TLS Client

For the Key Management Portal to process the CSR, 3DS Servers must review and complete the request tables and upload the CSRs to the Key Management Portal in the correct format.

For more information on how to create a CSR, refer to appendix B.

These two tables outline the requirements that 3DS Server providers must meet when generating certificate requests through the Key Management Portal.

Table 4: Certificate forms and details

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

Table 5: DN requirements

3DS Server TLS Server	**3DS Server TLS Client**
CN: [Domain Name] OR [public IP]	CN: [Domain Name] OR [public IP]

3DS Server TLS Server	3DS Server TLS Client
PROD OU: 3DSS-[Operator ID]-[Free Text]	PROD OU:3DSC-[Operator ID]-[Free Text]
MTF OU: 3DSS-MTF-[Operator ID]-[Free Text]	MTF OU:3DSC-MTF-[Operator ID]-[Free Text]
O: [Operator registered company name]	O: [Operator registered company name]
ST: <State optional>	ST: <State optional>
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 the service provider registration is completed and should be included in the OU attribute.

The format of the Mastercard assigned Operator ID is (Component Type - 3 char alpha fixed)-(Version - 4 char alpha numeric fixed)-(Client Name - variable up to 17 varchar)-(Serial number five digits numeric fixed), for example, SVR-V210- ACME_INC-12345.

Mastercard Identity Check compliance renewal

The Mastercard Identity Check Program requires that all 3DS service providers and operators renew their Identity Check compliance every 2 years.

The current renewal date for all active service providers and operators is located on the LOC.

To initiate a project with the CIS team, perform these steps:

1. Open a compliance project by sending an email to Identity_Check_Mandate_Testing@mastercard.com
2. Provide this information:
   - Company name, as listed in ISST
   - CID
   - Billable ICA number
   - EMVCo LOA reference number
   - Mastercard operator ID

The compliance renewal testing process follows the same steps as outlined in the "Mastercard Identity Check compliance testing" section. A renewal checklist for compliance testing is in appendix A. This checklist contains all the required steps to complete a compliance renewal project. The checklist does not contain renewal processes that are outside of the compliance process.

Examples of renewal processes outside of the compliance testing process include

- PCI renewals,
- certificate renewals, and
- service provider registration renewals.

The Test Platform will be upgraded to support

- all active EMV 3DS protocol versions to allow existing service providers and operators to renew their Identity Check compliance and
- other Identity Check-defined use cases allowed by the EMV 3DS specification.

NOTE: Service providers and operators must complete Identity Check compliance testing based on the EMVCo LOA version number. For example, if coming in with a 2.2 LOA, the software must test against the 2.2 Identity Check Test Plan.

For operators and service providers onboarding to the Identity Check Program for the first time, refer to chapter 2, "Identity Check operator and service provider onboarding requirements."

Mastercard Identity Check functional testing

ISST offers 3DS Server operators and service providers the ability to perform authentication testing in the Mastercard Test Facility (MTF) against the MTF Directory Server.

Functional testing is an optional offering that enables parties to perform testing beyond the use cases available for compliance testing.

For a 3DS Server to participate in functional testing, these actions must occur:

1. Identity Check Program Registration must be completed.

   NOTE: The ISST application is not accessible for a user until a registration for its CID has been submitted.

2. The 3DS Server must have completed compliance testing and have a valid LOC from Mastercard.

   NOTE: Operators and service providers can only test against the EMVCo versions for which their 3DS Server has listed on their current LOC.

3. 3DS Servers must have their own test merchant integrated into ISST.
4. Acquirers must complete enrollment of the MIDs and acquirer BINs through the Sandbox Identity Solutions Services Management application, which is part of the ISST application. For more instructions on enrollment activities, refer to the *Identity Solutions Services Management User Guide*.

For more instructions on using the functional test platform, refer to the Docs section in the Test Platform.

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.

The application is also used to notify contacts of any planned service disruptions or platform-detected service events. Mastercard Identity Check participants must include appropriate contacts in this application to ensure delivery of Mastercard Identity Check notifications.

For more information on this application, refer to the *Company Contact Management Application User Guide*, which is available on Mastercard Connect.

The contact type is Identity Check.

Chapter 3 Identity Check principal customer onboarding requirements

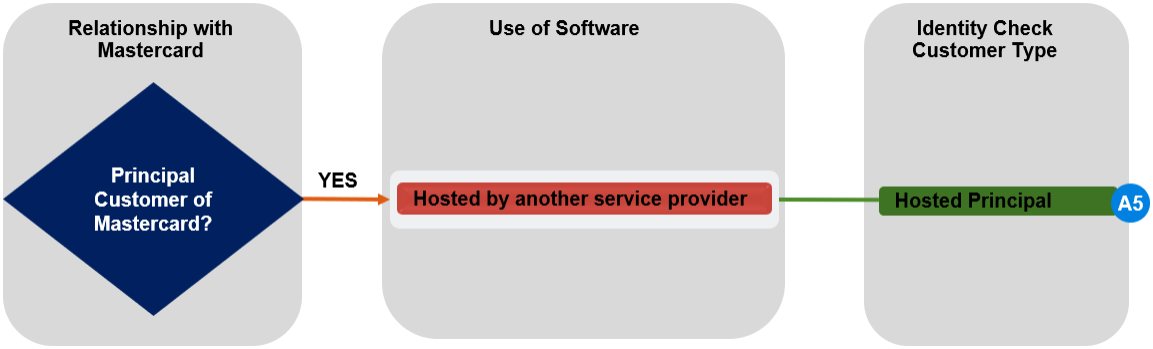
This chapter provides an overview of the steps required for 3-D principal customers to onboard to the Identity Check Program.

Hosted principal Identity Check onboarding

This section describes the steps required to onboard as a Mastercard 3-D Secure principal customer.

Registering as a principal customer is a prerequisite to starting the onboarding process with Mastercard® Identity Check™ for the A5 Identity Check customer type and scenario.

Figure 15: Registering as a principal customer to Identity Check



Required applications

Principal customers must have access to Mastercard Connect to support the Identity Check Program. Mastercard recommends that each user requests access to the applications listed in this section.

These applications are available from the Mastercard Connect™ Store:

- Identity Solutions Services Test Platform (ISST)
- Company Contact Management within My Company Manager
- Technical Resource Center
- Identity Solutions Services Management (ISSM)

NOTE: ISSM is a tool for principal customers (acquirers) to enroll their merchant IDs (MIDs) and acquiring Bank Identification Numbers (BINs) on the directory server. A service provider can receive access if a principal customer delegates access on its behalf.

After all approvals have been given, the applications are available under My Items.

3-D Secure service provider registration

Each principal customer that supports transactions through a 3-D Secure Program must register the 3-D Secure service provider as required by the Mastercard Standards.

Principal customers (sponsors) must register the 3-D Secure service provider on behalf of their affiliate customers.

These are the registration requirements:

The principal customer (sponsor) must register the 3-D Secure service provider in the My Company Manager application on Mastercard Connect. For more information, refer to the *Mastercard Service Provider Registration Guide*.

NOTE: If the service provider profile does *not* exist, a new registration must occur. Forty-eight hours are required for the new service provider to become active. Once the service provider is in the system, the registration can occur.

If the principal customer is onboarding a 3-D Secure service provider for the first time, refer to the "3-D Secure service provider registration" section in chapter 2.

Access Identity Solutions Services Test Platform

The Identity Solutions Services Test Platform (ISST) application is a centralized program management and testing application for customers that participate in Identity Check and its supporting authentication network services.

About this task

The ISST application supports these capabilities for hosted principal customers (customer type A5) that participate in the Identity Check Program:

- Identity Check Program Registration
- Identity Check Functional Testing

A program registration with a valid company ID (CID) is required to gain access and complete any functional testing or production enrollment. Principal customers must also ensure that their service provider has completed Identity Check compliance testing requirements.

Users requiring access to ISST must request access through the Mastercard Connect Store checkout process, and the company's security administrator must approve the order before full access is granted.

This table outlines the role definition based on customer type.

Table 6: Access designation based on customer type

Customer scenario	Customer type	Role selection
A5	Principal Customer	Acquirer Administration or Acquirer Readonly

An Admin role allows users to register for any required program along with full access to the test platform. A Tester role allows read-only access to view its registered programs but will receive full access to the test platform.

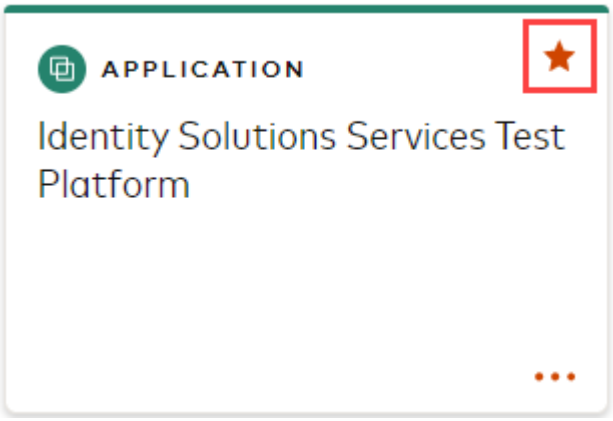
Once access to ISST has been granted, users can access the application by following these steps:

Procedure

1. Sign in to Mastercard Connect using your user ID and password.
2. Launch the Identity Solutions Services Test Platform application.

   NOTE: The application is under My Items on Mastercard Connect. Users can add applications to the Mastercard Connect homepage by clicking the star icon in the top-right corner of the application.

   Figure 16: Adding the ISST application to My Items



3. Review the related publications, including the *Mastercard Identity Check Program Guide*, to understand the specific processing and program requirements.
4. Open the Identity Solutions Services Test Platform application and complete registration and merchant enrollment.

Register for Identity Check in the Mastercard ISST

To participate in the Identity Check Program, all customer types must register and accept the terms and condition of the program.

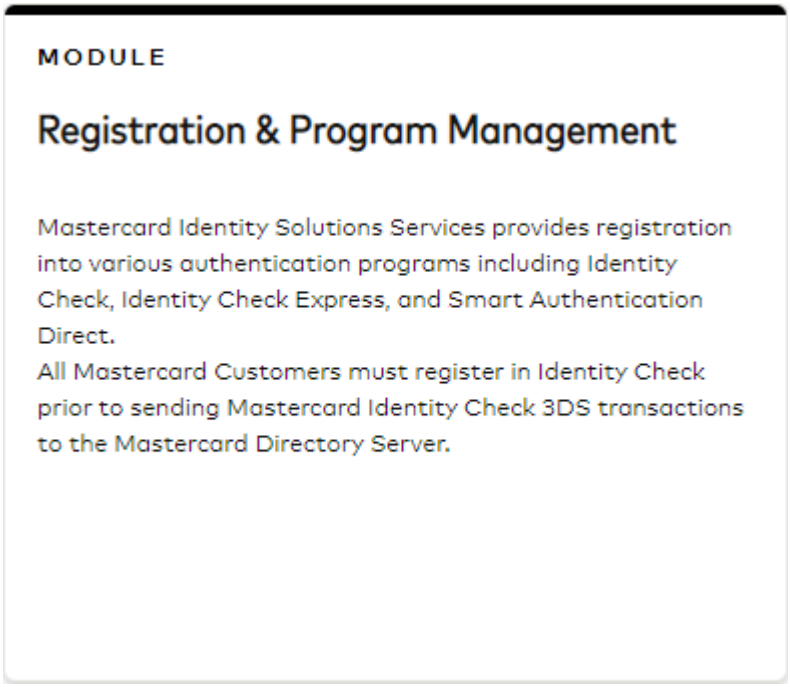
About this task

Identity Check registration is a one-time registration that is completed when a principal customer onboards for the first time. An administrator user must complete registration functions in the ISST application by following these steps:

Procedure

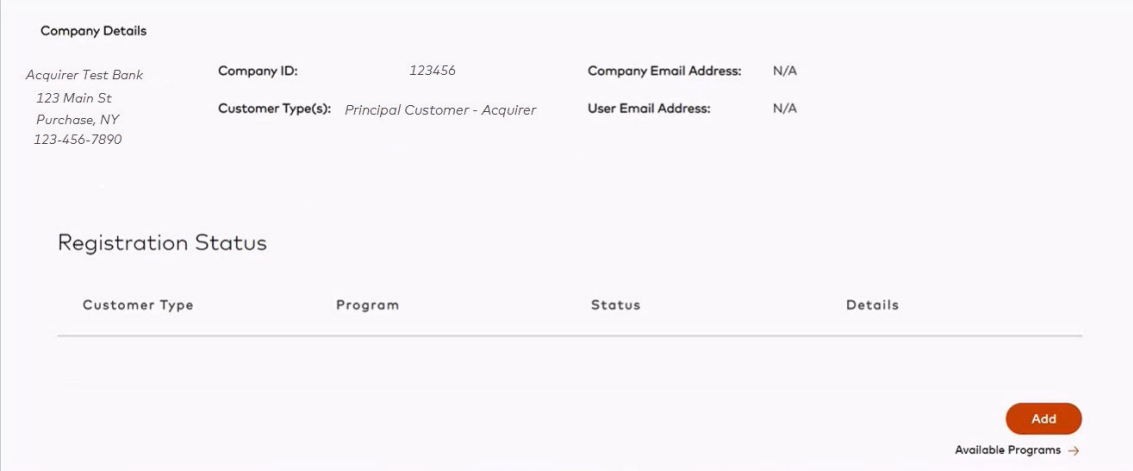
1. In the ISST application, open the Registration & Program Management Module by selecting the module box.

Figure 17: Registration & Program Management module



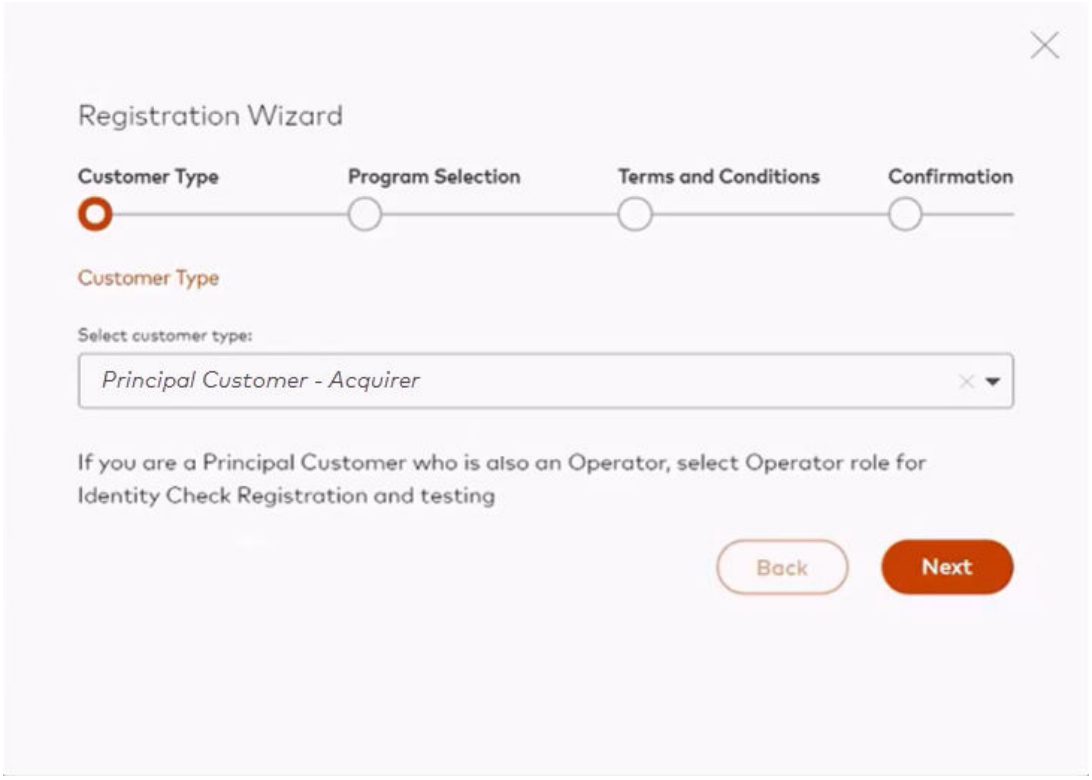
   - Within the Registration & Program Management module, the **Company Details** section is pre-populated based on the user's Mastercard Connect profile.
   - The **Registration Status** section lists all active registrations for the company displayed.
   - **Available Programs** on the bottom-right of the screen is link that will display all programs available for registration based on the company and customer type that was selected in the Mastercard Connect Store.

Figure 18: Company details and registration status



2. Register for a program.
   a. In the bottom-right corner of the **Company Details** screen, click **Add**.
   b. On the **Customer Type** screen, select the customer type for the registration request.

      Figure 19: Selecting the customer type

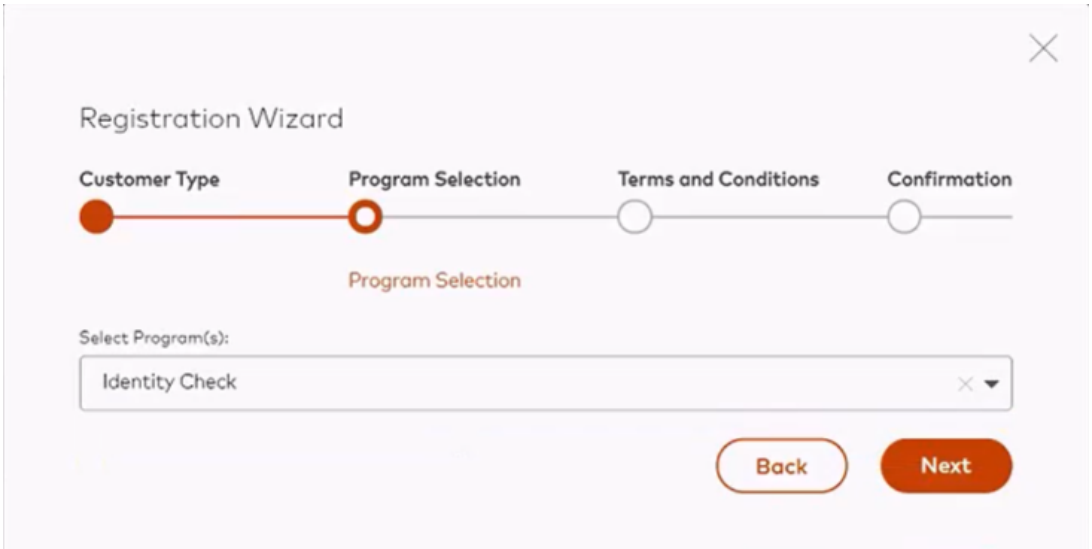


   c. Click **Next**.

The **Program Selection** screen displays a list of available programs for registration.

d. Select registration type Identity Check.

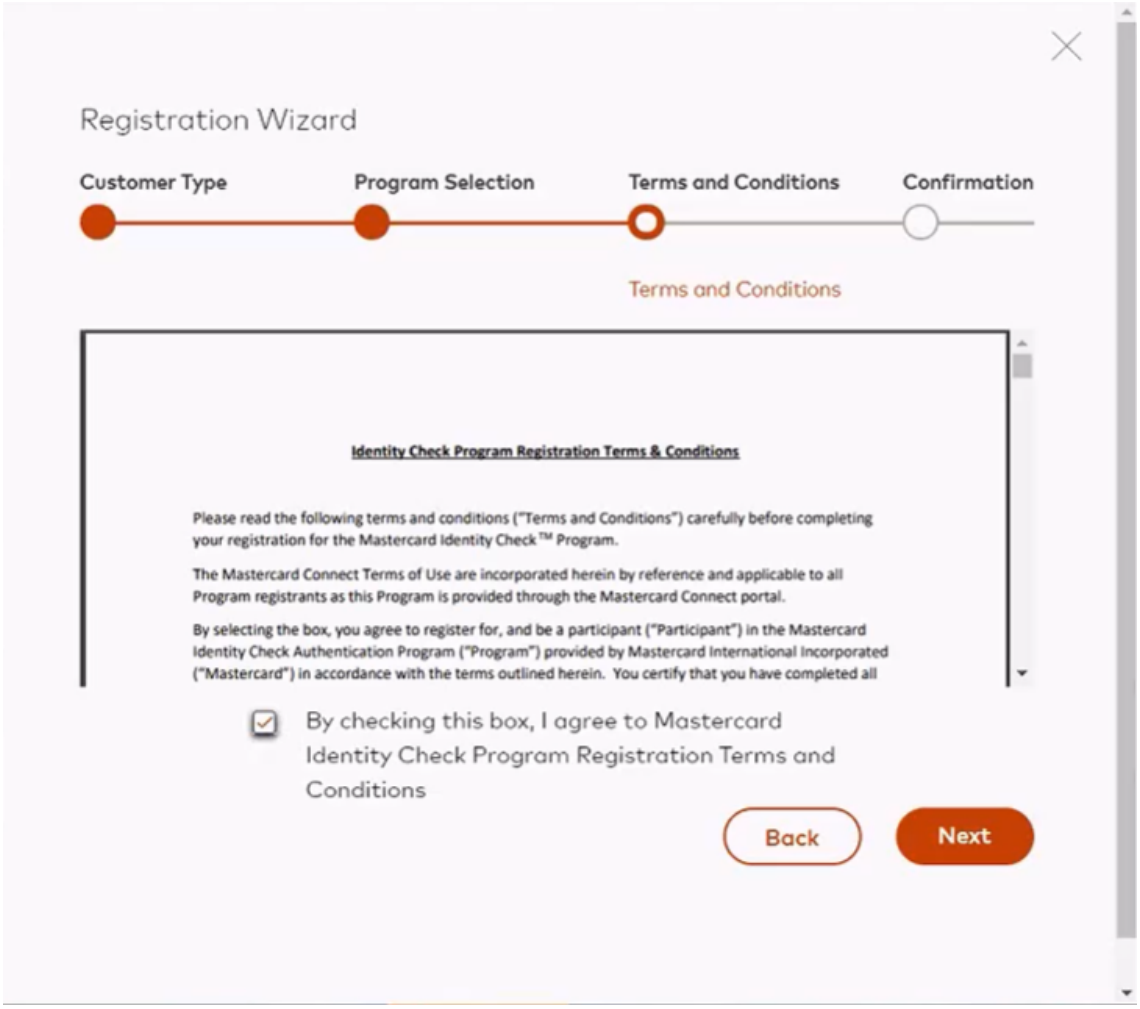
Figure 20: Selecting the Identity Check registration type



If no selections are displayed, refer to the **Registration Status** section to determine if registration has already been completed.

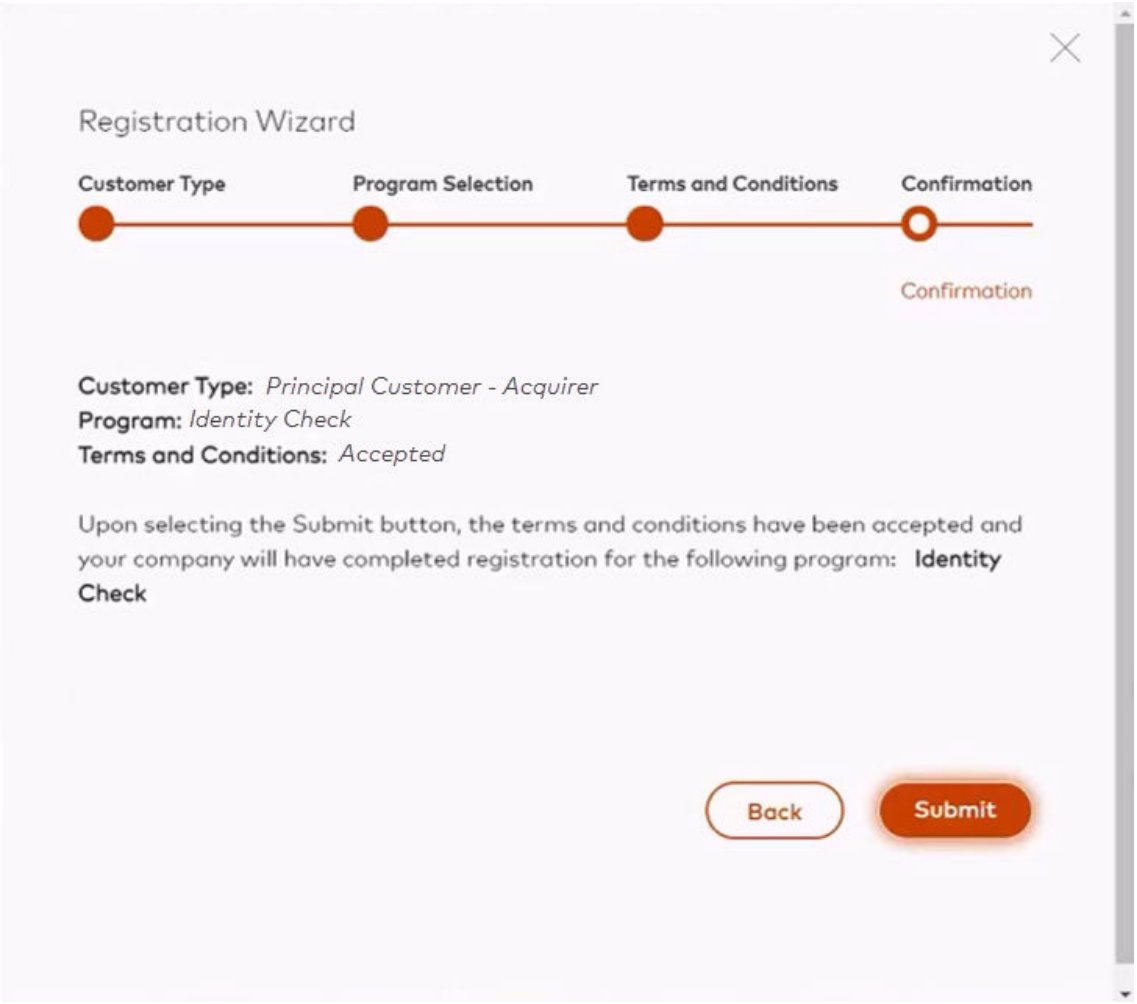
3. Click **Next**.
4. On the **Terms and Conditions** screen, review the terms and conditions and then check the box to agree to them.

Figure 21: Agreeing to the terms and conditions of the program



5. Click **Next**.
   The **Confirmation** screen displays a summary of the registration request.
6. Click **Submit**.

Figure 22: Completing the registration request



Results

- Once the registration has been submitted, it is effective immediately. The user will receive a confirmation email of the successful registration.
- The user can proceed with the next onboarding steps.

Functional testing

ISST offers merchants, acquirers, or both the ability to perform authentication testing in the Mastercard Test Facility (MTF) against the MTF Directory Server.

For an acquirer or merchant to participate in functional testing, these actions must occur:

1. Identity Check Program Registration must be completed.

NOTE: The ISST application is not accessible to a user until a registration for that company's company ID (CID) has been submitted.

2. The 3-D Secure (3DS) Server must have completed compliance testing and have a valid Letter of Compliance (LOC) from Mastercard.

   NOTE: Acquirers can only test against EMV®Co versions for which their 3DS Server has listed on their current LOC.

3. 3DS Servers must have their own test merchant integrated into ISST.
4. Acquirers must complete enrollment of the MIDs and acquirer BINs through the Sandbox Identity Solutions Services Management application, which is part of the ISST application. For more instructions on enrollment activities, refer to the *Identity Solutions Services Management User Guide*.

For more instructions on using the Functional Test Platform, refer to the Docs section in the ISST application.

Mastercard Identity Check Directory Server enrollment

This section outlines the steps required for merchant enrollment on the Mastercard Directory Server.

Customers can add, update, and delete their MID and acquirer BINs in the ISSM application, which is available on Mastercard Connect, or through the Merchant Enrollment Application Programming Interface (API) from Mastercard Developers.

The merchant acquirer is responsible for the processing of the authorization and clearing data and for receipt of the directory server billing, where applicable. Maintenance and enrollment can be performed using the ISSM application.

For more detailed instructions on account range enrollment and other onboarding activities, refer to the *Mastercard Identity Solutions Services Management User Guide*.

NOTE: Identity Check program registration for all applicable CIDs is a prerequisite for directory server enrollment.

Merchant Enrollment API

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

About this task

Acquirers and service providers can add or delete merchants directly in ISSM by sending the enrollment data through an API.

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

Procedure

1. On the Developer Zone API page, select the **Mastercard Identity Check API** page.
   Under **Resources**, the **Merchant Enrollment** page is displayed.
2. Click **View Documentation**.
3. Follow the instructions on the **Documentation** page for creating a project and using the API.

Additional notes

The items listed in this section must be considered when enrolling on the Mastercard Directory Server.

- The SecureCode™ 1.0.2 Directory Server and Identity Check 2.0 Directory Server are separate servers and have separate enrollment processes.
- Acquiring BINs and MIDs loaded on the Mastercard SecureCode 1.0.2 Directory Server are not automatically uploaded onto the Mastercard Identity Check Directory Server. Refer to AN 3391 for decommission activities related to SecureCode 1.0.2 enrollment.
- All registrations and testing for ISST must be completed before enrolling acquiring BINs and MIDs to the Mastercard Identity Check Directory Server.
- Merchants, acquirers, or both must communicate to the 3DS operator or service provider when the merchant enrollments are completed. Transactions that are authenticated before enrollment will result in an error.
- Acquirers may delegate access to ISSM for merchant enrollment activities to their service providers or processes through the Business Administration (Register & Provision a Company) application on Mastercard Connect.
- BINs that start with these 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 is outside of those digits, contact Digital.Identity.Solutions.Support@mastercard.com to have the BINs loaded to allow for ISSM enrollment.

Scaling merchant enrollments

Mastercard has defined three enrollment process options for acquirers to help scale the number of MIDs that must be enrolled on the directory server.

There may be scenarios for large merchants where many MIDs are used and maintained through their acquirers. These three options are designed to provide

flexibility on directory server enrollment and subsequent maintenance over time while maintaining a level of traceability for each merchant:

- Option 1 - Bulk upload through ISSM (currently available for up to 1,500 records for each file).
- Option 2 - Merchant Enrollment API. Refer to the "Merchant Enrollment API" section.
- Option 3 - Register one acquirer BIN or MID for each country where a given merchant operates.
  - Merchants use the same BIN or MID for their authentication requests.
  - Underlying merchants are identified in the authentication message using the merchant name and the requestor ID.

NOTE:

- **Merchants must establish a relationship with the acquirer who owns the BIN if the BIN is not already in place. 3DS network fees may be passed on by the acquirer to the registered MID.**
- **The Payment Service Provider (PSP) or operator must send the correct requestor ID and merchant name for each merchant.**
- **The MID in authentication will *not* match authorization.**
- **The acquirer Transaction Risk Analysis (TRA) flag will be set to NO if ISSM is unable to identify individual merchants, which indicates to the issuer if a TRA exemption can be used by the merchant.**
- **Merchants will not be eligible for trusted merchant listing unless registered individually. For additional information, refer to the *Mastercard Standards for Trusted Merchant Listing User Guide Version*.**

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.

The application is also used to notify contacts of any planned service disruptions or platform-detected service events. Mastercard Identity Check participants must include appropriate contacts in this application to ensure delivery of Mastercard Identity Check notifications.

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

The contact type is Identity Check.

Appendix A Identity Check onboarding documentation

This appendix contains documentation needed for Identity Check onboarding.

Onboarding checklist

The table in this section outlines the onboarding requirements for an acquirer, 3DS Server, merchant, or SDK that is onboarding to Identity Check for the first time.

Table 7: Onboarding checklist

Row no.	Task/requirement	Acquirer	3DS Server	Merchant	SDK	Reference
1	Choose a Mastercard® Identity Check™ compliant 3-D Secure (3DS) Server service provider.	X		X		Compliant Vendor service provider
2	Review the *Mastercard Identity Check Program Guide*.	X	X	X		Mastercard Connect/ Technical Resource Center
3	Open a project with 3DS Server operator.	X		X		
4	Coordinate merchant onboarding with 3DS Server and acquirer for Mastercard Identity Check.	X	X	X		
5	Review Mastercard Identity Check branding requirements.	X	X	X		Branding Guidelines
6	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

Row no.	Task/requirement	Acquirer	3DS Server	Merchant	SDK	Reference
7	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.
8	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			
9	Complete form 1145b to assign security administrators to manage the access for the 3-D Secure service provider.		X			online_provisioning@mastercard.com
10	Sign up for Mastercard Connect™ using assigned 3DS service provider CID.		X			Mastercard Connect
11	Review the Payment Card Industry (PCI) 3DS Core Security Standard Specification and related documents and begin assessment process.		X		X	PCI Security Standards Operation

Row no.	Task/requirement	Acquirer	3DS Server	Merchant	SDK	Reference
12	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
13	Complete applicable testing with EMV®Co and receive Letter of Approval (LOA) and reference ID.		X		X	https://www.emvco.com
14	Request and verify access to these: • Identity Solutions Services Test Platform (ISST) • Technical Resource Center • My Company Manager / Company Contact Management • Key Management Portal • 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.**
15	Review the Mastercard onboarding guides.	X	X			Mastercard Connect/ Technical Resource Center
16	Register the Software Development Kit (SDK) and request Mastercard Public Key.				X	https://developer.mastercard.com

Row no.	Task/requirement	Acquirer	3DS Server	Merchant	SDK	Reference
17	Register for the Merchant Enrollment Application Programming Interface (API), if applicable.	X	X			https://developer.mastercard.com/product/identity-check
18	Ensure that transactions are Transport Layer Security (TLS) 1.2 or greater.		X			
19	Sign in to Mastercard Connect and access ISST.	X	X			Mastercard Connect/ ISST
20	Register for Mastercard Identity Check.	X	X			Mastercard Connect/ ISST
21	Request a project with Customer Implementation Services (CIS) to complete compliance testing.					Identity_Check_Mandate_Testing@mastercard.com
22	Create and submit testing Certificate Signing Request (CSR) according to specifications. Required Certificates: 3DS Server TLS Client 3DS Server TLS Server One set required 3DS for each server connecting to directory server. All certificates must be Secure Hash Algorithm 2 (SHA2).		X			Mastercard Connect/Key Management Portal

Row no.	Task/requirement	Acquirer	3DS Server	Merchant	SDK	Reference
23	Install testing certificates.		X			Provided by Mastercard
24	Develop toward proprietary API messages for Test Platform connectivity.		X			ISST/System Under Test (SUT) Configuration screen
25	Launch the ISST application on Mastercard Connect.		X			Mastercard Connect/ ISST
26	Complete compliance testing: Set up a project, execute all test cases, and await approval from your assigned CIS project manager.		X			Mastercard Connect/ ISST
27	Complete Letter of Compliance (LOC) enrollment form.		X			ISST
28	Receive Mastercard LOC.		X			Provided by Mastercard
29	Update EMV-3DS messages to include the Mastercard assigned 3DS server operator ID.		X			Provided by Mastercard
30	Create and submit production CSR. Required certificates: 3DS Server TLS Client 3DS Server TLS Server One set required for each 3DS Server connecting to directory server.		X			Mastercard Connect/Key Management Portal

Row no.	Task/requirement	Acquirer	3DS Server	Merchant	SDK	Reference
31	Establish connectivity to the Production Directory Server.		X			
32	Complete all end-to-end back-office testing.	X	X	X	X	
33	Coordinate live dates among all participants.	X	X	X	X	
34	Enroll merchant IDs (MIDs) and acquiring Bank Identification Numbers (BINs) on the Identity Check Directory Server.	X				Enrollment occurs through the ISSM application.
35	Monitor production transactions.	X	X	X		All participants

Renewal checklist

This checklist is to ensure that all tasks and requirements are completed for renewals or upgrading to a new protocol version.

Table 8: Renewal checklist

Row no.	Task/requirement	Acquirer	3DS Server	Merchant	SDK	CIS	Resource
1	Review the *Mastercard Identity Check Program Guide*.	X	X				Mastercard Connect/ Technical Resource Center

Row no.	Task/requirement	Acquirer	3DS Server	Merchant	SDK	CIS	Resource
2	Open a project with 3DS Server operator and ensure that all Identity Check supported versions are enabled by the 3DS Server.	X		X			
3	Complete applicable testing with EMVCo and receive LOA and reference ID number.		X				https://www.emvco.com
4	Review the *Mastercard Identity Check Onboarding Guide*.	X	X				Mastercard Connect/ Technical Resource Center
5	Register the SDK and download Mastercard Public Key, if applicable. **NOTE: Certificates will not vary between versions, but updated public certificates may need to be downloaded in the event of expiration.**		X		X		https://developer.mastercard.com/
6	Register for the Merchant Enrollment API, if applicable.	X	X				https://developer.mastercard.com/product/identity-check

Row no.	Task/requirement	Acquirer	3DS Server	Merchant	SDK	CIS	Resource
7	Open project with CIS to initiate compliance project.		X				Identity_Check_Mandate_Testing@mastercard.com
8	Launch the ISST application on Mastercard Connect.		X				Mastercard Connect/ISST
9	Compliance testing: Open a project and execute all test cases and await approval from your assigned CIS project manager.		X			X	
10	Complete LOC enrollment form.		X			X	Mastercard Connect/ISST
11	Receive Mastercard LOC.		X				Provided by Mastercard
12	Update EMV-3DS messages to include latest version references.		X	X			
13	Complete all end-to-end back-office testing and implementations for latest version.	X	X	X	X		
14	Coordinate live dates among all participants.	X	X	X	X		

Row no.	Task/requirement	Acquirer	3DS Server	Merchant	SDK	CIS	Resource
15	Enroll MIDs and acquiring BINs on the Identity Check Directory Server.	X					Enrollment occurs through the ISSM application enrollment once across versions. If enrollment is present for version 2.1 configuration, no additional action is required within ISSM to enroll merchants for version 2.2.
16	Monitor production transactions.	X	X				

Identity Check Insights

Mastercard has defined a custom payment message category called Identity Check Insights.

This category allows merchants the flexibility to share data through the EMV 3DS rails to influence an issuer's decision to approve a transaction without requesting authentication, 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), and an Identity Check Insights request (without authentication) is represented by message category 80. For more information, refer to the *Mastercard Identity Check Program Guide*.

Identity Check onboarding for Identity Check Insights follows the same prerequisites that are described in this onboarding guide.

NOTE: Because 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, but Mastercard requires all 3DS servers to support this message category as part of compliance testing.

Appendix B Certificate procedures

This appendix includes the steps for requesting production certificates.

Mastercard certificate authority request procedures

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

Functions of end-entity certificates

A Mastercard implementation of the EMV 3-D Secure (3DS) program requires Mastercard hierarchy end-entity certificates to be used for the functions that are listed in this section.

3-D Server

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

ACS

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

SDK

- Encryption certificate with the directory server public key to encrypt device information
- Directory server root certificate to validate the 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 the steps in this section.

About this task

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

Procedure

1. Create the certificate request.

2. Upload the certificate request through the Key Management Portal.
3. Download the certificates from the Key Management Portal.
4. Validate and install the certificate chain and CA certificates.

Results

Mastercard tries to process each certificate request within 4 business days of receipt.

These sections detail the process flow for each type of certificate request:

- Request a 3DS Server Client and Server TLS certificate
- Request an ACS TLS Server, Client, and Digital Signing certificate

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

IMPORTANT:

Certificates are issued and 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 and**
- **must anticipate the expiration date and plan the replacement in considering systems implementation windows, staff workload, and Public Key Infrastructure (PKI) service time to deliver.**

Request a 3DS Server Client and Server TLS certificate

The end-entity TLS Client and Server certificates are used by the 3DS Server to establish communication with the Mastercard Directory Server.

About this task

This task describes the process that a 3DS Server must complete to perform a certificate exchange so the 3DS Server can establish connectivity with the Mastercard Directory Server.

IMPORTANT: 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 Mastercard 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

- `3-DSServer-TLS-Client-OperatorID-dateDDMMYYYY` for client certificate and
- `3-DSServer-TLS-Server-OperatorID-dateDDMMYYYY` 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 is `3-DSServer-TLS-Client-SVR-V201-AZ-25258-01042020` for client certificate.

This table highlights the relevant certificate profile information. To avoid XML parser errors, do not use the characters "&" and "<."

Table 9: Relevant certificate profile information

Subject name	Description
Validity	Determined by the 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)	Domain Name Server (DNS) name, for example www.3dsservername.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 these characteristics of the site that will use the certificate [Domain Name] OR [public IP]. Domain Name, for example, www.3dsservername.com.
Organizational Unit (OU)	Unique identification of the party is required within the OU field of the certificate. – 3DSC-[Operator ID]-[Optional Free Text] for TLS client certificate – 3DSS-[Operator ID]-[Optional Free Text] for TLS server certificate
Organizational Name (O)	Operator registered company name.

Subject name	Description
Country (C)	Country where processor is located. This should be the ISO 3166 two-character country code (for example, U.S.).

2. Send each PKCS#10 certificate request to the Mastercard CA for processing.

   All requests must be uploaded through the Key Management Portal application on Mastercard Connect for processing. At least two security officers must be registered within the portal. For more information, refer to the *Key Management User Guide* in the application.

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

   For security reasons, Mastercard may contact the individuals authorized to submit certificate requests, as identified on the Key Management Portal, to confirm the validity of a certificate request.

Results

The end-entity and CA certificates are returned to the certificate requestor. The response contains these attachments:

- End-entity certificate in PEM, PKCS#7, and DER formats
- Mastercard hierarchy root and subordinate CA certificates in PEM, PKCS#7, and DER formats

Mastercard strongly encourages the key management contacts to validate the end-entity certificates before loading them into the application. Also, all active Mastercard Identity Check root and subordinate CA certificates should be validated before making any additions to the application-trusted certificate store. For more information, refer to the "Certificate validation" section.

Request an ACS TLS Server, Client, and Digital Signing certificate

ACS TLS server, client, and digital signing certificates are end-entity certificates that 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

This task describes the process that an ACS must take to perform a certificate exchange so it can establish connectivity with the Mastercard Directory Server.

IMPORTANT: 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 Mastercard certificate policy also may be truncated or discarded.

   ACS TLS Client and Server certificates

   The PKCS#10 request file should be Base64 encoded. Mastercard requires these naming conventions for the PKCS10 file:

   – `ACS-TLS-Client-OperatorID-dateDDMMYYYY` for client certificate
   – `ACS-TLS-Server-OperatorID-dateDDMMYYYY` 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 is

   – `ACS-TLS-Client-ACS-V201-MYACS-94909-01042020` for client certificate and
   – `ACS-TLS-Server-ACS-V210-MYACS-94909-01042020` for server certificate.

   This table highlights the relevant certificate profile information. To avoid XML parser errors, do not use the characters "&" and "<."

Table 10: ACS TLS - Certificate profile information

Subject name	Description
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 these characteristics of the site that will use the certificate [Domain Name] OR [public IP]. Domain Name, for example, www.ACSName.com
Subject alternative name (only for server certificate)	Domain Name Server (DNS) name, for example www.ACSName.com. Up to five DNS names are allowed. At least one DNS name must match Common Name.

Subject name	Description
Organizational Unit (OU)	Unique identification of the party is required within the OU field of the certificate. – Prod OU: ACSS-[Operator ID]-[Optional Free Text] for TLS ACS Server Certificate – ACSC-[Operator ID]-[Optional Free Text] 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 two-character country code (for example, U.S.).

ACS Digital Signing certificate

The PKCS#10 request file should be Base64 encoded. Mastercard requires this naming convention for the PKCS10 file:

`ACS-Signing-OperatorID-OptionalFreeText-dateDDMMYYYY`.

For example, a request to be sent on 1 April 2020 in which OperatorId-OptionalFreeText is equal to ACS-V201-MYACS-94909-OptionalFreeText is `ACS-Signing-ACS-V201-MYACS-94909-OptionalFreeText-01042020`.

NOTE: If multiple signing certificates will be issued, the ACS must uniquely identify each signing certificate. Mastercard recommends that the ACS indicates the issuer name in the "Optional Free Text" field of the issuing individual signing certificates to each issuer. Otherwise, the ACS providers are able to designate their own value.

This table highlights the relevant certificate profile information.

Table 11: ACS - Certificate profile information

Subject name	Description
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.

Subject name	Description
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 two-character country code (for example, U.S.).

2. Send each PKCS#10 certificate request to the Mastercard CA for processing.

   All requests must be uploaded through the Key Management Portal application found on Mastercard Connect. At least two security officers must be registered within the portal. For more information, refer to the *Key Management User Guide* in the application.

   By default, all certificates will be returned in PEM, PKCS#7, and DER formats. Consult your vendor about 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.

Results

The end-entity and CA certificates are returned to the certificate requestor. The response contains these attachments:

- End-entity certificate in PEM, PKCS#7, and DER formats
- Mastercard hierarchy root and subordinate CA certificates in PEM, PKCS#7, and DER formats

Mastercard strongly encourages the key management contacts to validate the end-entity certificates before loading them into the application. Also, all active Mastercard Identity Check root and subordinate CA certificates should be validated before making any additions to the application-trusted certificate store. For more information, refer to the "Mastercard Identity Check root certificate" and "Certificate validation" sections.

SDK encryption certificate

Software Development Kit (SDK) vendors can download the SDK encryption certificate and subordinate CA certificate from the Mastercard Developer Zone.

The Mastercard Developer Zone is located at https://developer.mastercard.com/product/identity-check.

Certificate validation

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

Validating certificates

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

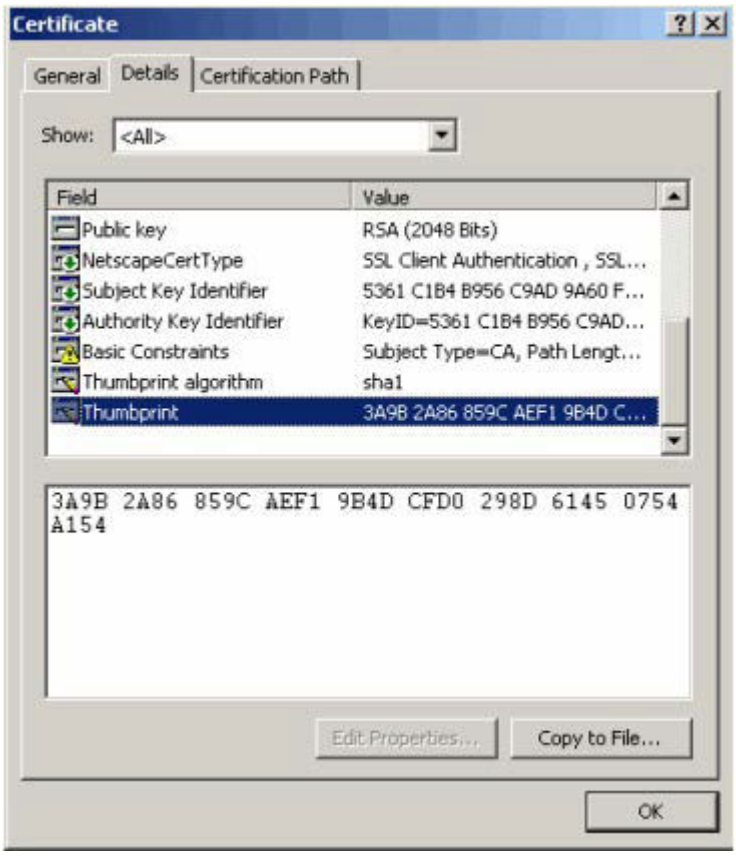
Mastercard strongly encourages all implementations to validate all root and subordinate certificates before adding them to the application-trusted certificate store. This validation is done by confirming the contents of several key fields within the certificate received from Mastercard. Root and subordinate certificate authorities values are provided in the Mastercard Identity Check production CA hierarchy.

These fields include these:

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 any PEM or DER encoded certificate file and then click the **Details** tab on the resulting window.

Figure 23: Example certificate file details



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 PEM or DER encoded certificate files.

To check the value, click the corresponding field name in the left column. The complete contents of the field are displayed in the lower box.

In addition to this validation, the connecting system should validate these certificates while establishing the TLS connection:

- The ACS must validate the whole certificate chain while communicating with the directory server, that is, validate that the directory server presents the client/server signed by the directory server issuer-subordinate CA.
- The 3DS Server must validate the whole certificate chain while communicating with the directory server, that is, validate that the directory server presents the client/server certificate signed by the directory server acquirer-subordinate CA.
- The SDK must validate the whole certificate chain after downloading it from Mastercard, that is, validate that the SDK encryption certificate is signed by the directory server acquirer-subordinate CA and validate that certificate Common Name (CN) = 3ds2.directory.mastercard.com.

Mastercard Identity Check production CA hierarchy

Details of the Mastercard Identity Check production CA hierarchy, including the root CA, acquirer-subordinate CA, and issuer-subordinate CA, are described in this section.

Root CA certificate

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

Table 12: Production CA

Subject name	Value
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 3DS Server to establish communication with the Mastercard Directory Server. Also, SDK encryption certificate should be signed by the issuer-subordinate CA.

Table 13: SDK encryption certificate

Subject name	Value
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	Value
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 ACS and the Mastercard Directory Server. Also, this subordinate CA is used to sign all ACS digital signing certificates.

Table 14: Issuer-subordinate CA

Subject name	Value
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, 2031 5:35:54 PM GMT

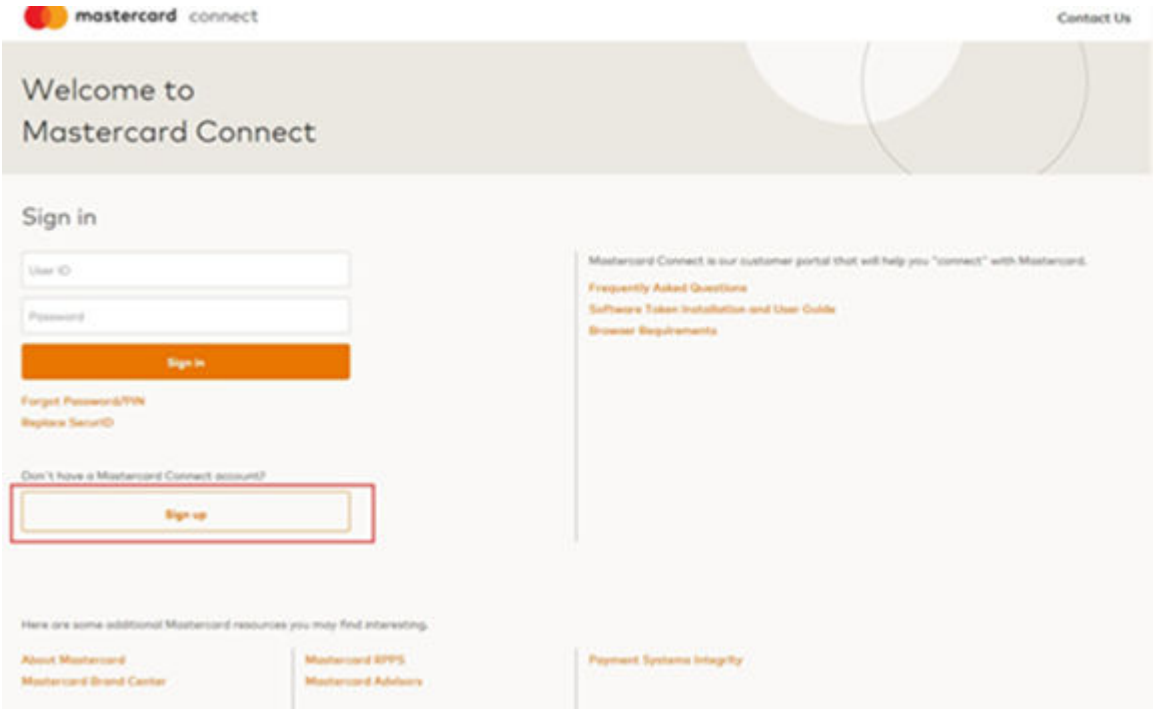
Appendix C Mastercard Connect sign-up guide

This appendix explains how to sign up for Mastercard Connect.

Sign up a new user

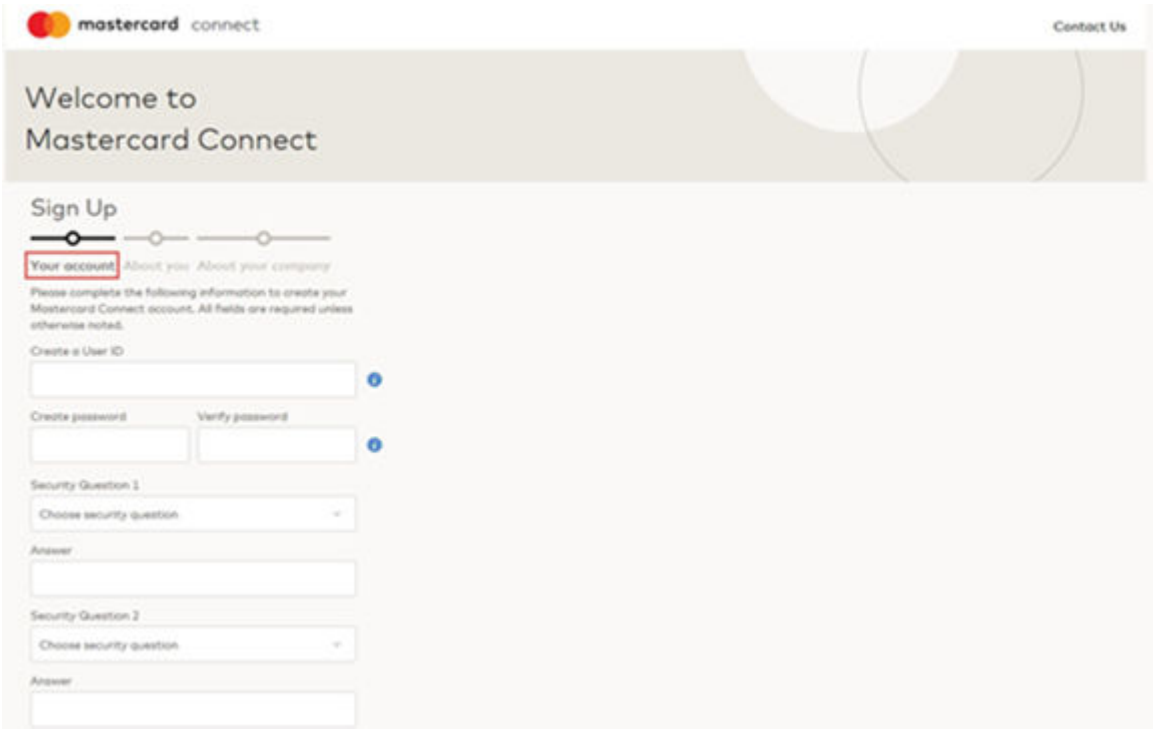
New users can begin the sign-up process for Mastercard Connect by clicking the Sign Up link on the Sign in page in Mastercard Connect. The three-step process creates a Mastercard Connect account.

Figure 24: Mastercard Connect Sign in page



Step 1: Sign Up - Your account

Figure 25: Your account section



1. Create a user ID.

   Your user ID must meet these requirements:

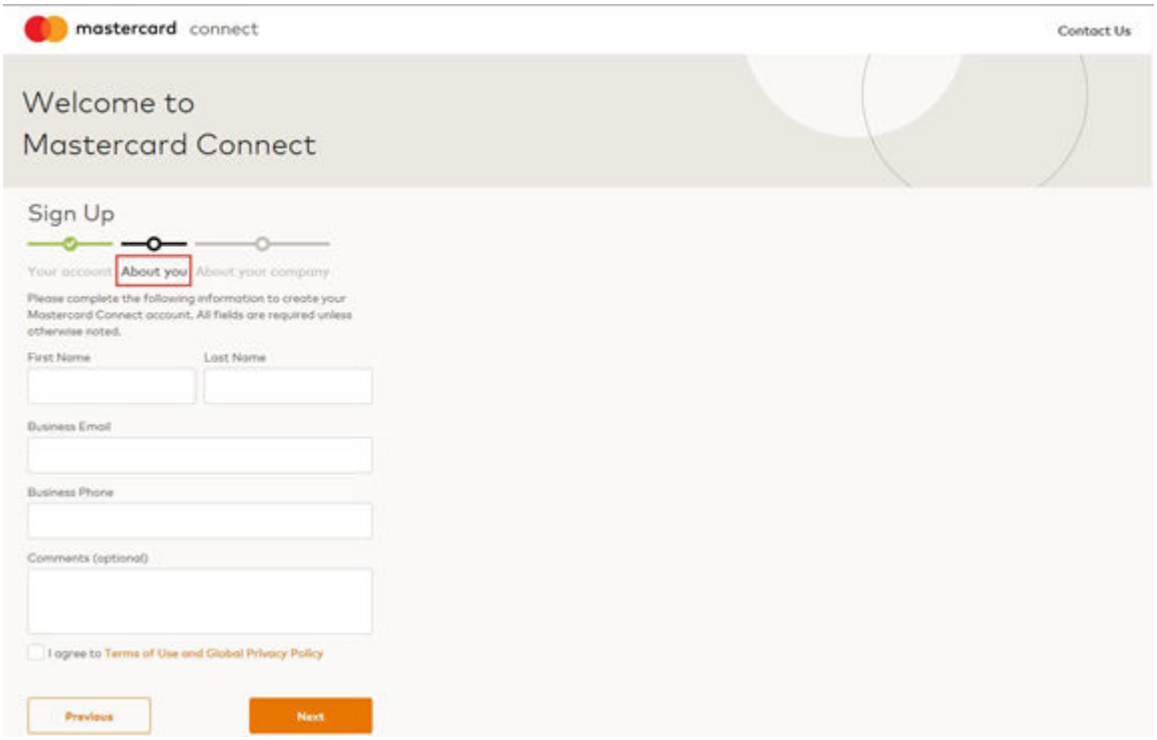
   a. Begin with a letter.
   b. 6 to 30 characters in length.
   c. A-Z, a-z, _, @, and - can be used.
   d. No spaces or commas can be used.
2. Create and verify a password.

   Your password must meet these requirements:

   a. Minimum of one alphabetic character.
   b. Minimum of one nonalphabetic character such as 0-9,!,@,$...
   c. Maximum of two repeated characters.
   d. Minimum length of eight characters.
   e. Password cannot match the user ID.
3. Select two security questions and answers.
4. Click **Next**.

Step 2: Sign Up - About you

Figure 26: About you section



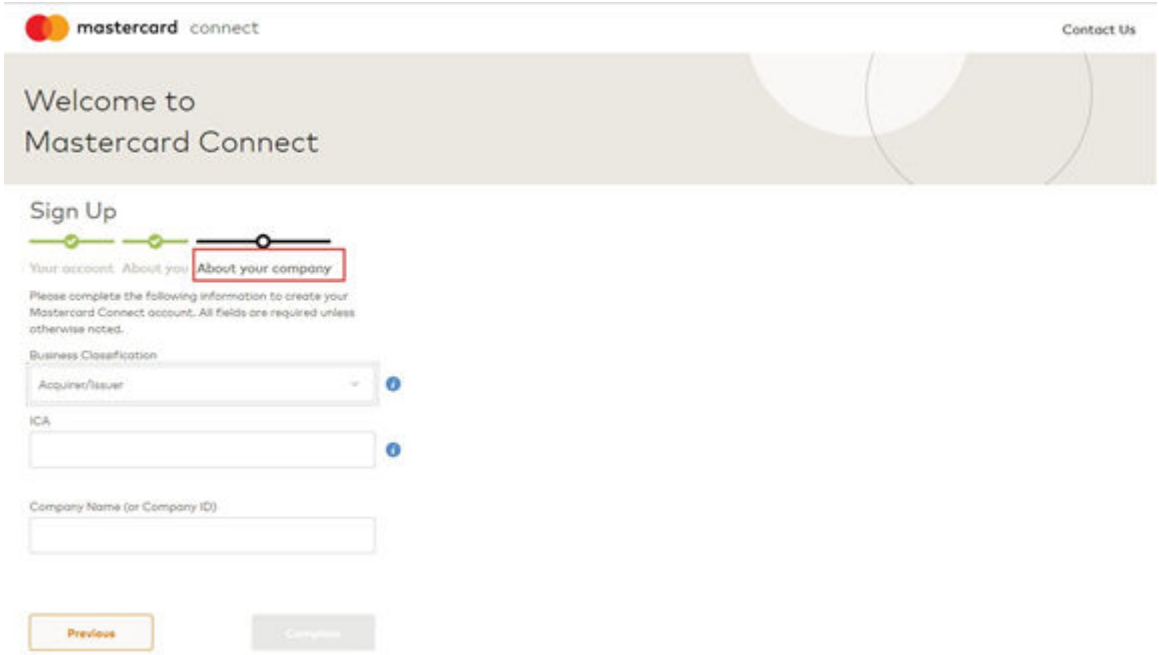
1. Enter your first and last name.
2. Enter your business email.

   This email will be used to send notifications to you.
3. Enter your business phone number.
4. Optionally, enter text in the **Comments** section, for example, you can send a message to your security administrator.
5. Agree to the terms of use and the global privacy policy.

   If you do not agree, you cannot create a Mastercard Connect™ account.
6. Click **Next**.

Step 3: Sign Up - About your company

Figure 27: About your company section



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.

   The ICA number is a 3- to 8-digit identifier.
3. Enter your company name or the 6-digit company ID (CID) assigned to you by Mastercard.
4. Click **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. 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.

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 Technical Resource Center (TRC). Go to the Rules collection of the References section for centralized information.