API Basics

API Security

Client Authentication

Mastercard uses OAuth 1.0a for authenticating your application. You can manage your authentication keys from your Developer Dashboard after you create a project using the **Mastercard Send** API service.

> **TIP:** Do you want to learn more about the authentication scheme Mastercard uses? For that, read our Using OAuth 1.0a to Access Mastercard APIs guide.

Transport Encryption

The transport between client applications and Mastercard is secured using TLS/SSL , which means data are encrypted by default when transmitted across networks.

How to Consume the Funding APIs

There are multiple ways of integrating with the Funding service:

- Using a generated API client (recommended)
- Using a method of your choice

Generating Your Own API Client

Create customizable API clients from the Funding API specification and let Mastercard open-source client libraries handle the authentication for you. This approach offers more flexibility and is strongly recommended.

For this, please follow our Generating and Configuring a Mastercard API Client tutorial with the following API specification: funding-api-swagger.yaml (108KB)

Using a Method of Your Choice

The Funding service exposes REST APIs: you are free to use the REST/HTTP client of your choice and can still leverage the Mastercard open-source client libraries for signing your requests.

For the API specification, refer to API Reference.

Environments

The table below describes the three different environments that are available.

Environment	Description
Sandbox	Early-access environment containing limited-capacity mock APIs, enabling you to try the APIs quickly to assist with initial integration and solution development. The Sandbox returns mock responses for a defined request (see Sandbox Testing) and should not be used for full integration testing. Use your Sandbox keys to authenticate with this environment. The keys are set up when you create your project.
Mastercard Test Facility (MTF)	Pre-production test environment containing the latest pre-release version of the real APIs, intended for full integration testing prior to moving to production. Transactions in this environment are not executed against the networks. Use your Sandbox keys for authentication.
Production	Full production environment containing the latest production API release. Use your Production keys to authenticate with this environment. The keys are set up when you request Production access for your project (via your project page).

HTTP Headers

The API accepts requests in JSON or XML format. Use the Content-Type header to provide the data format in the request and use the Accept header to determine the response format:

- API requests with body content (e.g. POST requests): If the Accept header is not provided and Content-Type is provided, the response will be the same format as Content-Type.
- API requests with no body content (e.g. GET requests): If the Accept header is not provided, the response format defaults to XML.

Header	Description	Examples
Content-Type	The format of the body content being submitted: JSON or XML.	application/json application/xml
Content-Length	The length of the body content being submitted, in octets.	54138
Accept	The format you would like returned in the response: JSON or XML.	application/json application/xml

The response includes this header: