SUMMARY

HomeSend APIs for Third Party Providers

VERSION 01-01

Content

1. **Introduction** **3**
2. **Connectivity Requirements** **3**
3. **Balance Management** **3**
   3.1 API Overview 3
   3.2 How to use 4
4. **Payment Processing** **4**
   4.1 API Overview 4
   4.2 How to use 5

1. Introduction

On the basis of the second European Payment Services Directive (PSD2), Mastercard Transaction Services (Europe) SA, as a licensed Payment Institution and an Account Servicing Payment Service Provider, is required to provide for common and secure open standards of communication to Third Party Providers (TPPs), in the context ofaccount information services, payment initiation services and confirmation on the availability of funds provided by TPPs to the relevant customers of HomeSend.

The customer facing interfaces HomeSend offers to its Customers are API-based and consist of Balance Manager (BM) API (relevant for Account Information Service Providers (AISPs)) and a Payment Processing (HWS) API (relevant for Payment Initiation Service Providers (PISPs)), which are both free to use for all registered AISPs and PISPs.

This page provides additional information about how TPPs can interface with HomeSend APIs.

2. Connectivity Requirements

HomeSend will verify that the TPP presents the required eIDAS certificate and will require TPPs to be explicitly on-boarded by the HomeSend technical teams. This on-boarding process will be a manual process of identification and certificates exchange (mutual TLS authentication). The client certificate is then used to authenticate and identify the TPP when it performs API calls on behalf of a Customer.

In addition, and for PISPs only:

- The HWS API is secured by IP white listing, requiring PISPs to provide a list of source IP addressesto be authorized to connect to the API endpoint,
- HWS API client implementations are required to undergo a technical certification of their API implementation. This certification applies to all HWS API users and is not specific to PISPs. It needs to be completed only once, irrespective of the number of Customers the PISP will interface.
- If the PISP plans to initiate transactions involving card account numbers (send to card flows), thePISP is required to be PCI-DSS compliant and to provide the relevant evidence of this to HomeSend, upon on-boarding and on a regular basis, as per the PCI-DSS standard requirements.

3. Balance Management

3.1 API Overview

The BM API allows to get the current value, at request processing time, of any of the prefunded balancesthe Customer holds to support the processing of transactions by HomeSend, as well as the details of the additional prefunding added by the Customer daily to its prefunded balance as recorded by HomeSend.

The balance operations related to transactions cleared against the prefunded balance are not detailed inthe BM feature but taking into account to update the balance value. The balance value is updated in real time, possibly hundreds of times per second, as transactions are processed for the Customer, to track the remaining available prefunded amount so the Customer is able to manage its prefunding balance in real time.

The BM API is a REST-based API over HTTPS exclusively, consuming and producing JSON data.

The formal API specification, as a RAML 1.0 file, as well as the endpoint URLs are available upon request.

3.2 How to use

The BM API can be used by Customers directly, as well as by AISPs, provided they have been explicitly authorized by the Customer to access the balances via OpenID Connect (OAuth 2.0, Authentication code grant).

For an AISP meeting the API connectivity requirements, the workflow is the following:

- The AISP shall contact HomeSend for enrolling a new OAuth 2.0 client, providing valid redirect URIs, a QWAC eIDAS certificate, and a display name to be presented to the Customer when consenting the access to balancecs.
- The AISP shall follow the standard OAuth 2.0 Authentication code grant flow to obtain an access token via the Customer Strong Authentication through the HomeSend identity provider (id.homesend.com).
- Once the AISP has retrieved the access token, it shall use it to authorize subsequent calls the BM API on behalf of the Customer. Additional mTLS authentication using a valid QWAC eIDAScertificate is required when accessing the BM API.
- The access token is valid for 90 days. It might be revoked by the Customer at any time.

4. Payment Processing

4.1 API Overview

The HWS API is primarily used by HomeSend Customers. This is a server to process payment instructions initiated by the Customer's end-users.

Payment processing supports 2 flows:

- A two-step flow where a payment transaction starts with a quote, providing the amounts that will be charged, received, settled, prior to being confirmed (or cancelled or allowed to expire),
- A single-step flow, called "one shot payment", where no quote is provided and charged, received and settled amounts are returned once the payment has been successfully transmitted to the destination system, or completed.

In both cases:

- It is possible to provide the transaction amount as the amount to be received (i.e. the beneficiary amount is provided), the amount to be charged (the settled/charged amount is provided), or as the principal amount (the amount used to calculate related fees, apply FX conversions, etc).
- The actual payment instruction processing (upon one shot payment request or confirmation request after a quote) can provide the payment outcome either synchronously, or days or weekslater depending on the destination market capabilities. In such cases, a payment status responseis provided, and the client shall poll HomeSend with specific status requests to get the final transaction completion status. Webhooks events to be notified of such completions is also a technical option that can be offered in such cases.
- It is possible to request the cancellation of a pending transaction. Depending on its processing state, this request might or might not be honoured.

Depending on the destination market and channel, different transaction fields might be requested, usually related to the identity of the payer and the beneficiary, the purpose of the transaction, transaction type (P2P, B2B, ...), etc. These field requirements are communicated to the Customer whenit is on-boarded to reach new markets and channels, and PISPs intervening in this flow must be preparedto transparently forward these elements.

The HWS API is based on SOAP 1.1.

The formal API specification, as a WSDL file, as well as the endpoint URLs are available upon request.

4.2 How to use

The HWS API is used by Customers directly as this is the only transaction processing channel offered by HomeSend (exclusively server to server), and can be used by PISPs as well, provided they have been explicitly authorized by the Customer they process transactions for.

For a PISP, meeting the API connectivity requirements, the workflow is the following:

- The Customer informs HomeSend that a PISP shall be authorized to process transactions on its behalf. HomeSend configures its system accordingly with server-side authorization management, and generates a new set of credentials (login, password) communicated back to the Customer.
- The Customer communicates the credentials to the PISP
- The PISP performs HWS API calls using the provided credentials.