Tracker API 2.0

For SWIFT gpi

Specification

GetCorporatePaymentTransactions

This document provides the description of the APIs available on the gpi Tracker for g4C (gpi for Bank to Corporates)

27 July 2018
Table of Contents

Preface .................................................................................................................................................3

1 gpi API Overview ..........................................................................................................................4

2 gpi API ........................................................................................................................................6
   2.1 gpi API URL and RBAC Roles ..................................................................................................6
   2.2 gpi API supported ....................................................................................................................7
   2.3 gpi API description ..................................................................................................................7
   2.4 gpi API failure ..........................................................................................................................9
   2.5 gpi API detailed specifications ...............................................................................................9

Legal Notices ....................................................................................................................................10
Preface

About this document

These technical specifications provide information about how to use Web services to access Payment transaction information. The document describes the APIs in JSON format.

The purpose of this document is to provide the necessary information to assess the business use of the API by potential users of the API.

This document describes the API for corporates as part of version 2 of the gpi API.

Intended audience

This document is for the following audience:

- Business analysts to understand the functionality of the API
- Business architects to understand the functionality of the API and how to integrate the use of the API within their organisation
- Software developers of applications using the API to assess the complexity of the API

Related documentation

"Tracker API 2.0 for SWIFT gpi GetCorporatePaymentTransactions Detailed Specification" document provides details of the specific gpi for Bank to Corporates API, including the request and response body structures, the element types and the associated codelists and constraints.

"Tracker API 2.0 for SWIFT gpi Detailed Specifications" document provides details of the APIs, including the request and response body structures, the element types and the associated codelists and constraints.

"Tracker API 2.0 for SWIFT gpi Specification" document provides details of the transaction data which is used for the gpi API for Corporates.

"SWIFT gpi Customer Credit Transfer (gCCT) Rulebook" provides details of the business rules used for gpi in the payment, cover, and stop and recall flows.

Significant changes

This is the first edition of the the gpi for Bank to Corporates (g4C) API after the preliminary edition of 28 April 2018.

Changes are editorial only.
1 gpi API Overview

Overall context view of the API

Figure 1 shows the components that play a role when using the gpi APIs.

The components are the following:

- Institution's application(s) - this is the business application that requires an up-to-date information of a payment transaction involving gpi participants or that generate status confirmations.
- Corporate application or browser - in case the institution integrates the use of gpi APIs into its web applications offered to its corporate customers.
- The SWIFT provided gpi Connector runs at the institution and exposes the gpi APIs, which means this component act as a proxy that manages security aspects: The gpi Connector can run in two ways:
  - gpi Connector runs embedded in Alliance Access or Alliance Messaging Hub SAG/SNL + HSM
  - gpi Connector runs standalone using certificates on HSM SAG/SNL+HSM
- VPN box configured for SNL or the host running gpi Connector connecting the institution through the MV-SIPN.
- The components running in SWIFT's Operating Centre (OPC) providing the Tracker API.

Note  The information in this section is an introduction to configuration items or software deployments that are required to run the API. The information is provided to understand the overall picture of running the API, but is not needed to understand the purpose and use of the API itself.

API Specification in this document

The gpi API exposed to the institution's applications is the same API as used towards the API Gateway running at SWIFT.

The SWIFT provided API component (gpi Connector) running at the institution is managing the security aspects to properly authenticate the applications initiating the gpi API. This mandatory authentication is based on HMAC using a symmetric key. This authentication mechanism is not specific for the API specified in this document, but is a generic
requirement for all API services offered through SWIFT. Detailed information can be found in section Appendix A Local Authentication in the Tracker API 2.0 for SWIFT gpi Specification.

The API itself requires an API Key to identify the institution application that is using the API. The process to get the API Key is not further described in this document.

The API uses the SWIFTNet API framework that requires an authentication using the SWIFT Identity Services. The actual protocol of doing so is handled by the SWIFT provided API component and is not further described in this document.

REST design principles

The API follows REST design principles that provide simple and predictable URLs to access data.

API calls

HTTP requests use standard HTTP methods like GET, PUT, POST, and DELETE. The gpi APIs only use POST.

API responses

HTTP responses are UTF-8 encoded JSON objects.

gpi API live and pilot service

There is a live and a pilot API service. This is visible within the URLs to be used. For more information see gpi API URL and RBAC Roles on page 6 and gpi API supported on page 7.

Use of RBAC roles

The gpi API is only allowed when an appropriate RBAC (Role Based Access Control) role has been granted by the institution’s security officer(s) to the certificate that is used by the SWIFT provided API component to authenticate itself using the SWIFT Identity Services. These roles are different for updating or for retrieving information.

The roles are different for pilot and for live services.

The same certificate can be used for live or for pilot API services. This is under full control of the security officer(s).

See gpi API URL and RBAC Roles on page 6 for more information.

Multi-BIC support

The multi-BIC support is controlled through the appropriate RBAC role. This allows the same authenticated certificate to perform API calls for different BICs. See gpi API URL and RBAC Roles on page 6 for more information.

Type of information retrieved by the API

The gpi API is used to get information on a payment transaction. The concept of a payment transaction and the different participants is described in section Payment Transaction in the Tracker API 2.0 for SWIFT gpi Specification.

Type of information updated by the API

Updates are to provide status confirmation on the payment transaction or are related to the cancellation request and cancellation status updates.

gpi Payment Transaction Data

The payment transaction data is the appropriate subset of the payment message attributes and status confirmation attributes defined in the Tracker API 2.0 Specification for gCCT, gSRP, and gCOV.
2 gpi API

2.1 gpi API URL and RBAC Roles

How the URL identifies the live or test services

The URL used for each API consists of 2 items. One is the specific domain to be used in order to reach the SWIFT provided component within the financial institution and the remaining is the actual API call.

For live data, the URL looks like:
https://local-api-domain/swift-apitracker/v2/api-specific-part

For test data, the URL looks like:
https://local-api-domain/swift-apitracker-pilot/v2/api-specific-part

Note The exact name of the local-api-domain is not specified in this document. It will be described within the SWIFT provided component documentation. The SWIFT provided component maps the local-api-domain to the public domain apigtw.swiftnet.sipn.swift.com

The API-specific part

The API specific part consists of an indication of the resource it is managing and additional parameters. In section 2.3, the API-specific part of the URL is provided per API.

RBAC roles

SWIFT uses RBAC roles to control access to the payment transaction data. The main purpose is to identify what privileges are given by the security officer(s) of the institution to the certificate used to connect to SWIFT. This certificate is managed by the local SWIFT component but the roles are managed by the institution’s security officers.

There are currently 3 RBAC roles foreseen for live and 3 RBAC roles for test.

The roles are:

• Update - used to control who can perform a status update for a payment or request/respond a cancel payment message
• StandardViewer - used to control who can get the low sensitive information for a payment transaction
• FullViewer - used to control who can get all information for a payment

The scope of each of these roles is for a given 8-character BIC. This is indicated by qualifying the role name with the scope of a given BIC. Roles are therefore triples RoleName/Scope/BIC8

Examples are:
Update/Scope/bankbeb0
StandardViewer/Scope/zyacnl20
FullViewer/Scope/userus33

In these examples, the first two are for the test API service and the last for the live API service. This is because the two first have a Test&Training BIC and the last a live BIC.

It is possible to assign to the same certificate roles of a different 8-character BIC on condition that this has been provisioned by SWIFT. This provisioning is not described further in this document.

See gpi API description for more details on how to specify in the API what RBAC roles are applicable for a given API invocation.
Granting RBAC roles

This is done by the security officer(s) just like any other RBAC role. The result of the granting of the roles is that a given certificate used to establish a session with the API Gateway can issue API requests for other BICs.

Note: The service names are swift.apitracker for live and swift.apitracker!p for test. These service names are visible to the security officer(s) when assigning the RBAC roles. A simple convention is used to derive the URL used, namely replace the "." by a "-" and "!p" by "-pilot".

2.2 gpi API Supported

Current APIs

The APIs that are targeted for the second release are all related to payment transactions.

- POST .../v2/status_confirmations: Updating the status of a payment transaction
- POST .../v2/get_payment_transaction_details: Getting a payment transaction
- POST .../v2/get_payment_transactions: Searching for payment transactions
- POST .../v2/get_changed_payment_transactions: Getting the history of payment transactions
- POST .../v2/get_invalid_events: Getting invalid events
- POST .../v2/cancel_transaction: Requesting cancellation of a gCTT transaction
- POST .../v2/transaction_cancellation_status: Updating the status of a cancellation of a transaction
- POST .../v2/get_corporate_payment_transactions: Searching for corporate payment transactions

This document only addresses the last API. See gpi API description on page 7.

Future APIs

New APIs may be identified to cover the need of applications handling the current payment transaction data as described in section Payment Transaction in the Tracker API 2.0 for SWIFT gpi Specification.

New APIs are required in case the payment transaction data is extended to other type of data, for instance to supporting documentation of a payment transaction. Such APIs may be the appropriate way to handle such data flows.

2.3 gpi API Description

Specifying RBAC roles in the API

The designer of the application calling the gpi API can control the scope of a given API to be restricted to a given BIC or list of BICs.

The instruction is within a dedicated HTTP header. To ensure that the application exercises this control, this HTTP header is mandatory.

As an example, for the status update API the application calling the API needs to indicate for what BIC the update API is invoked. This is done through adding an RBACRole HTTP header as follows:

RBACRole: [Update/Scope/zyacgb20]

This example is for the test service since the BIC is a Test and Training BIC. It shows that the role is a triple separated by "/". The "[" and "]" brackets are mandatory.

In case more than one BIC is in scope, then those are enumerated as follows:

RBACRole: [Update/Scope/zyacgb20/zyacnl20]
This field is signed locally between the application generating the API and the gpi Connector. For more information, see Appendix A Local Authentication in the Tracker API 2.0 for SWIFT gpi Specification.

When both the role StandardViewer and FullViewer is granted to a given certificate, the tracker uses the FullViewer role.

Filtering attributes on responses

Besides the filtering of attributes based on the StandardViewer or FullViewer RBAC role, in some cases some payment events are not returned. This is according to the rules expressed into the gCCT rulebooks.

2.3.1 Payment Transactions: Searching for Corporate Payment Transactions

Purpose of the API

This API is a payment transaction search to get transaction-level information regarding all payments that match the search criteria. The result gives the information required for corporates. The API can also retrieve the information of one given payment transaction if the UETR is known. The information is only provided to the gpi instructing agent.

Examples of use cases are:

- UETR is known and corporate wants to check its payment
- Instructing agent wants to find all payment transactions that are to be reported as part of the gpi for Bank to Corporates service.

RBAC role required

The HTTP header requires a field specifying the RBAC role to be checked. There are 2 possible roles that can be used as shown in the table:

<table>
<thead>
<tr>
<th>RBACRole</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[StandardViewer/Scope/bankbeb0]</td>
<td>Low sensitive data is requested for a specific BIC to be checked to be in scope of the certificate</td>
</tr>
<tr>
<td>[FullViewer/Scope/bankbeb0]</td>
<td>Low and high sensitive data is requested for a specific BIC to be checked to be in scope of the certificate</td>
</tr>
</tbody>
</table>

Since the application is typically not aware about what roles are assigned to a given certificate, both roles should be put as follows:

RBACRole: [StandardViewer/Scope/bankbeb0] [FullViewer/Scope/bankbeb0]

In case multiple BIC are used these should be enumerated by adding additional BIC separated by a "/" as follows:

RBACRole: [StandardViewer/Scope/bankbeb0/usrvgb20] [FullViewer/Scope/bankbeb0/usrvgb20]

The 8-character BICs in the scope of the roles must be identical to those in MyInstitution in the request body.

The API succeeds when at least one of the roles is granted for all BICs enumerated to the certificate.

Constraints on arguments of the call

- MyInstitution must contain 8-character BICs.
- UETR and TimeWindow are mutually exclusive but one of them must be present.
- UETR and TransactionStatus are mutually exclusive.
- MaximumNumber must be between 1 and 100.
- TimeWindow cannot be more than 7 days in the past.
Request URI

POST …/get_corporate_payment_transactions

Request/Response body structure and attributes

Please refer to "GetCorporatePaymentTransactions" API in gpi Detailed API Specification.

2.4 gpi API Failure

For more information see Tracker API 2.0 Specification for gCCT, gSRP and gCOV.

The information relates to the structure of a status indicating a failure and how to retry mechanism to implement.

2.5 gpi API Detailed Specifications

For more information see Tracker API 2.0 Specification for gCCT, gSRP, and gCOV.

The information relates to

- additional restrictions on some data types specified in the detailed specifications,
- gpi specific code list
- Local Authentication
- Use of ApplAPIKey
Legal Notices

Copyright
SWIFT © 2018. All rights reserved.

Restricted Distribution
Do not distribute this publication outside your organisation unless your subscription or order expressly grants you that right, in which case ensure you comply with any other applicable conditions.

Disclaimer
SWIFT supplies this publication for information purposes only. The information in this publication may change from time to time. You must always refer to the latest available version.

Translations
The English version of SWIFT documentation is the only official and binding version.

Trademarks
SWIFT is the trade name of S.W.I.F.T. SCRL. The following are registered trademarks of SWIFT: the SWIFT logo, SWIFT, SWIFTNet, Sibos, 3SKey, Innotribe, the Standards Forum logo, MyStandards, and SWIFT Institute. Other product, service, or company names in this publication are trade names, trademarks, or registered trademarks of their respective owners.