Application Programming Interface

Implementation Guide

Contents

1. Introduction

The Application Programming Interface (API) Implementation Guide provides Clients with the information required to enable payments using a mobile device over Near Field Communication (NFC) utilizing a Secure Element or Host Card Emulation (HCE). In order to minimize the direct integration points, Providers will integrate with the global network and the network will act as an aggregator for Clients.

Purpose

This document describes and defines the APIs used for communication between the global network and Clients.

How to Use this Document

This document is intended to be used in conjunction with the network Business Policies and Network Technical Specifications. In the event of any conflict, Business Policies take precedence.

Reference Documents

This document is intended to be used in conjunction with the following network documents.

- *Network Specifications*
- *Business Policies*
- *Operational Policies*
- *Network Authorization*

2. Application Programming Interface Design Philosophy

The network has defined a set of Application Programming Interfaces to create a standard set of communication protocols between Providers, the global network, Clients, and Account Holders.

- Services from the Client will be consumed as Representation State Transfer (REST)/Hyper Text Transfer Protocol (HTTP) with 2-way Transport Layer Security (TLS).
- Web service requests will use JSON Web Encryption (JWE) for any Personally Identifiable Information (PII) data elements. The related details are covered in the individual API specifications.
- All requests generated from the network and sent to the Client will have unique tracking ID headers which can be used for tracking errors.
- Nonfunctional requirements, including availability and response time, will be defined for each API interaction.
- Client services can maintain state and can retry different interactions with their downstream systems within the agreed upon response time.
- API interactions between the network and Client will use HTTPS Communication protocol.
- Client Systems shall be highly available (99.9% uptime for network interaction.)

3. Application Programming Interface Definitions

The tables shown below list the common elements across all APIs in this guide. These elements are included where applicable for each API described in this document.

Request Common Elements

API requests will have a common header.

NAME	TYPE	OPTION	DESCRIPTION
tracking_id	String (64)	Required	Unique identifier for the conversation • For Provider events, the value received from the Provider will be used. • For Client events, the value received from the Client will be used.
token_requestor_id	String (11)	Required	Identifier for the Token Requestor
Content-type	String	Required	Application/json

Response Common Elements

All responses will include the following elements.

NAME	TYPE	OPTION	DESCRIPTION
tracking_id	String (64)	Required	Unique identifier for the conversation

HTTP Status Codes for API Responses

STATUS CODE	STATUS DESCRIPTION
100	Request Processed
150	Request Accepted
500	Bad Request
600	Internal Error
501	Request Not Authorized
509	Conflict

Service Level Agreement

The response Service Level Agreement (SLA) for APIs is 1-2 seconds.

Connection and Timeout

The connection timeout is 3 seconds.

Retries

Retries can be attempted 3 times before disconnect.

Additional Considerations and Requirements

- The data exchange format is Java Script Object Notation (JSON).
- The API version can be encoded in the URL to allow routing to the appropriate service version.
- If cache control headers are sent, provider support is at their discretion.
- UTF-8 encoding should be used for every string within the API.

4. Network Application Programming Interfaces

As part of the process, the Client will initiate a check eligibility call to the Network. This call will contain a list of Account Numbers linked to a user. The Network will complete a status check for each account number in the Check Eligibility request. The Network will send the list of ineligible/negative accounts along with the corresponding reason codes to the Client.

Once eligibility is confirmed, Account Holders enter requested details including the provided 4-digit Security Code accepts the Terms and Conditions (T&Cs) to initiate provisioning.

The Client sends the request along with the Account Number and Security Code that the Account Holder has added. The Network sends a Pseudo Auth to the Client with the account details. The Network will allocate a Token for the Account Number and generate the associated Personalization Script (Perso Script). The Network will link/activate the Token and once the Person Script is delivered to the Client and the Token has been provisioned onto the Secure Element, the Client will be sent a notification from the Network. The provisioning status notification can be sent over ISO or API.

NOTE: The Client notification API call is relevant only when the Client prefers Post Provisioning Notification (PPN) over API.

Account Eligibility Check

The Account Eligibility check API takes a single JWE encrypted Account Number in the request. The purpose of the API is to determine account eligibility and perform a fraud check to establish the eligibility of accounts sent in the request. All parameters provided by the Provider as part of the request will be passed as part of this Call.

The Network validates the following business rules before sending the request.

- The status for the given device is active.
- The account has not been provisioned for the given device.

NOTE: The account eligibility check call is optional. Based upon the client preference, if opted, the Network may complete account eligibility check as an On-Behalf-Of (OBO) service using exception data provided by the client.

Account Eligibility Endpoint

The Client provides the endpoint for the Network to consume.

Account Eligibility Request Header

NAME	TYPE	OPTION	DESCRIPTION
tracking_id	String (64)	Required	Unique identifier for the conversation • For Wallet events, the value received from the wallet will be used. • For Client events, the value received from the Client will be used.
token_requestor_id	String (11)	Required	Identifier for the Token Requestor
content-type	String	Required	Application/json

Account Eligibility Request Body

NAME	TYPE	OPTION	DESCRIPTION
encrypted_account_data	String (2000)	Required	JWE encrypted account data for which eligibility needs to be checked
device_data	Object	Optional	The device for which eligibility is requested
risk_assessment_data	Object	Optional	Field containing information the Client can use for eligibility check. Possible values include: • onfile • clientapp • userinput • other • blank

Account Eligibility Data

NAME	TYPE	OPTION	DESCRIPTION
account_number	String (15)	Required	The 10-digit account number for which eligibility check needs to be performed.

Account Eligibility Risk Assessment Data

NAME	TYPE	OPTION	DESCRIPTION
connected_information	String (64)	Optional	The connecting Information (CI) value passed from the Client.
an_source	String (64)	Required	Field containing information the Client can use for eligibility check. Possible values include: • onfile • clientapp • userinput • other • blank

Account Eligibility Device Data

NAME	TYPE	OPTION	DESCRIPTION
device_id	String (64)	Required	This is the device identifier.
account_id	String (64)	Conditional	The identifier of the account within the device.
device_type	String (64)	Required	This is the type of device attempting tokenization. Possible values include: • phone • tablet • watch • wearable • console • desktop • laptop • other

Account Eligibility Response Header

NAME	TYPE	OPTION	DESCRIPTION
tracking_id	String (64)	Required	Unique identifier for the conversation between the consumer and provider.

Account Eligibility Response Body

NAME	TYPE	OPTION	DESCRIPTION
isEligible	Boolean	Required	Indicates whether the account is eligible for tokenization.
ineligibility_reason	String (3)	Conditional	The 3-digit reason code indicating ineligibility reason for the account. This is applicable only if the account is not eligible.
account_metadata	Object	Required	Contains meta data information about account in question.
market	Object	Required	Indicates the market/region where the account was issued.
status_code	String (4)	Required	Status Code
status_message	String (128)	Required	Description of the status.

Account Ineligibility Reason Codes

STATUS CODE	STATUS DESCRIPTION
113	Account has not been activated.
120	Account in test phase.
220	Ineligible account.