TPP Solution Setup

Contents

Introduction

The Transport Payment Processing Solution is intended to overcome the main barriers to using bankcards to pay on public transportation:

- Slow transaction processing.
- Payments include a relatively high fee percentage.

The first barrier will be overcome through the ability to send a positive response to a turnstile before a response from the issuer is received (if the card is trusted on the basis of rules including form factor, card number ranges, the history of payments at this merchant, etc.).

The second barrier will be overcome through the ability to aggregate transactions for several trips, sending issuers authorizations for aggregated amounts according to a schedule that an be flexibly configured (if the card is trusted on the basis of rules like those mentioned above).

This document is intended for WAY4 TPPS administrators (acquirer or processing centre employees) responsible for the product's installation and setup.

When working with this document, it is recommended to use the following resources from the OpenWay documentation series:

- "Transport Payment Processing Solution", (Transport_Solution_Functional_Specification.pdf).
- "TPPS Operation", (TPPS_Operation.pdf).
- "DB Manager Manual".

The following notation is used in the document:

- Field labels in screen forms are shown in *italics.*
- Screen form button labels are encased in square brackets, such as [Approve].
- Sequences for selecting user menu items are shown with arrows, as in: "Issuing → Contracts Input & Update".
- Sequences for selecting system menu items are shown with arrows, like "Database => Change password".
- Key combinations used to work with DB Manager are shown in angular brackets, for example, <Ctrl>+<F3>.
- Variables such as directory and file names, file paths that differ for each local computer are shown in angular brackets, for example, <OWS_HOME>.
- Warnings about the danger of making errors are marked with the ⚠ sign.
- Messages marked with the ℹ sign contain information about important features, additional facilities or the optimal use of certain system functions.

Terminology

Transport Payment Processing Solution (TPPS) – transit solution with issuing of digital wallets based on reloadable Visa prepaid products.

Validator – POS terminal technically connected to a turnstile.

Service request – a cardholder's attempt to receive a transit service and pay at a validator.

Authorization – an attempt by the TPPS to get authorization from the card's issuer for the volume of services provided, including for services to be paid with On-Us cards.

Online authorization – authorization of a single service request performed at the same time the service is provided (if the issuer's response is negative, the validator will be sent a message that entry is not permitted).

Deferred authorization – authorization of a single service performed after the service has been provided (the validator is sent a message from the acquirer that entry is permitted, before a response to the authorization request is received from the issuer).

Aggregated authorization – a single authorization for several services provided, made for one card. This authorization's amount includes the amounts of several services that were provided. Aggregated authorization is performed after the services have been provided – the acquirer sends the validator a message that entry is permitted and authorization is performed when specific values are reached for the total amount, number and period of services provided.

Repeat rejected authorization – resending of a deferred authorization request or aggregated authorization that the issuer rejected earlier due to insufficient funds on the card or for another non-technical reason (see "Repeat authorization attempts").

Technical retry – resending of a deferred authorization request or aggregated authorization request that failed due to a timeout or issuer response related to a technical problem.

ℹ In general descriptions (not regarding form factor issues) the term "card" applies to all available form factors used for payment.

Chapter 1. Solution overview

System of card trust levels

A system of card trust levels is the basis for managing scenarios used to decide to admit a passenger into the transportation system and for selecting a mode to send an authorization request to the issuer (online, deferred authorization, aggregated mode).

A trust level is generated on the basis of two indicators:

1. Card status – long-term indicator of a card's trust level. A status can have one of the following values:
   - "deny" – service is denied. The TPPS sends the validator denial of entry without attempting to authorize. The "deny" value can be set in properties of the card itself in the TPPS card table (see "TPPS card table"), or by putting the record in a WAY4 global stop list or stop list for this merchant. If the card is put in a WAY4 global stop list or merchant stop list, it is possible that its status in the TPPS card table will not be "deny".
   - "gray" – online authorization only.
   - "green" – deferred authorization.
   - "white" – aggregated authorization.
2. Authorization history – short-term modifier changing card processing logic if the card's history includes:
   - Even one incomplete deferred authorization. In this case, the "yellow" modifier is applied when processing the card. The "yellow" modifier is only applicable for cards with the "green" status. In normal operation, this modifier is applied for up to 10 seconds – until a response from the issuer in deferred mode is received. The period for the modifier's use can be extended if there are technical problems on the channel for communication with the issuer. All authorization requests for a card with the "yellow" modifier are made online.
   - Even one unsuccessful deferred or aggregated authorization. In this case, the "black" modifier is used when processing the card. The "black" modifier is assigned to a card when a negative response not related to a technical problem is received from the issuer. This modifier, due to asynchronous provision of services and authorizations can be assigned to a card with any status, but is usually encountered for cards with the "green" or "deny" statuses. All authorizations for cards with the "black" modifier are made online.

Processing requests outside the trust level system

Before analysing the trust level, a decision about actions is made according to the following rules:

1. The validator will be given a message about denial without an attempt to authorize with the issuer, if the card is in one of the following stop lists:

- WAY4 global stop list.
- WAY4 global stop list of card number ranges.
- The merchant's stop list.
- The merchant's stop list of card number ranges.

The first time this card is presented, a record about it will not be created in the TPPS card table.

2. During the period set by the global parameter TPPS_CARD_NEAR_EXPIRE_DAYS, if the card is not present in stop lists, all authorizations are made online only, regardless of the card's status.

TPPS card table

Since the TPPS is a solution on the acquirer side, where there is no separate storage of information about "foreign" cards, a special WAY4 database table is used to store statuses and the history of authorizations, status modifiers. Information about all cards for which service requests were made is stored in this table. The table does not store information about cards for which authorization was rejected on the first attempt due to the card's presence in a stop list. Moreover, this table does not contain information about card contracts.

Chapter 2. TPPS setup and operation

TPPS setup procedure:

- Configure global parameters.
- Set up TPPS POS terminal types.
- Set up a device Service Package (see the section "Initial assignment of card status").
- In validator settings, disable processing partial authorizations, since processing of these operations is not supported.
- Specify transaction conditions.

Global parameters

Global parameters are configured using the DB Manager application (Full → Configuration Setup → Main Tables → Additional Global Parameters).

TPPS_CARD_NEAR_EXPIRE_DAYS

The TPPS_CARD_NEAR_EXPIRE_DAYS parameter specifies the number of days until the card expires during which all authorizations for this card will be made online only (if the card is not in a stop list) regardless of the card's status.

The default value is "5".

TPPS_WHITE_DECLINE_INTERVAL

The TPPS_WHITE_DECLINE_INTERVAL parameter specifies the number of months during which the card may not have a "black" modifier in order to get permission to change the card's status from "green" to "white".

The default value is "3".

ℹ The parameter is used together with the TPPS_WHITE_SUCCESS_INTERVAL parameter.

TPPS_WHITE_SUCCESS_INTERVAL

The TPPS_WHITE_SUCCESS_INTERVAL parameter specifies the number of months during which the card must have at least one successful authorization (any type) so its status can be changed from "green" to "white".

The default value is "1".

ℹ The parameter is used together with the TPPS_WHITE_DECLINE_INTERVAL parameter.

TPPS_RESP_CODE_FATAL

The TPPS_RESP_CODE_FATAL lists issuer response codes that are a reason for changing a card's status to "deny" – lost, stolen, etc. Values in the list are separated by commas.

The card's status in the TPPS card table does not change; this is to save history and for status to be restored more easily if the card was accidentally put in a stop list.

Example of the parameter's value – "4,5,7,14,41,43,54,62".

TPPS_GREEN_EXPIRE_DAYS

The TPPS_GREEN_EXPIRE_DAYS parameter specifies the number of days during which at least one successful online or deferred authorization must be made with a card in the "green" status. If no successful authorizations were made during the period set by this parameter, the next service request with a card in the "green" status will be processed online.

The default value is "14".

TPPS_EMERGENCY_MODE

The TPPS_EMERGENCY_MODE parameter sets the mode for TPPS operation in emergency (temporary) situations:

- "ONLINE" – all authorizations are made online (deferred and aggregated authorizations are not generated; deferred and aggregated authorizations accrued earlier are sent without changes in logic).
- "NONETTING" – aggregation is disabled, cards with the "white" status are processed like cards with the "green" status.
- "ODAONLY" – requests for all cards that don't support Offline Data Authentication (ODA) are denied (like for cards with the "deny" status) without attempting to authorize with the issuer.
- "DENYBLACK" – requests for all cards with the "black" modifier are denied (like for cards with the "deny" status) without attempting to authorize with the issuer (unlike in regular operation when online authorization is allowed for these cards).

Several values separated by commas can be simultaneously set for the parameter.

The default value is empty.

TPPS_NETTING_LIMIT_AMOUNT

The TPPS_NETTING_LIMIT_AMOUNT parameter specifies the amount (in the terminal currency) after which an aggregated authorization is put in the queue for sending to the issuer.

The default value is "40".

TPPS_NETTING_LIMIT_COUNT

The value of the TPPS_NETTING_LIMIT_COUNT parameter specifies the number of service requests after which an aggregated authorization is put in the queue for sending to the issuer.

The default value is"10".

TPPS_NETTING_SCHED

The TPPS_NETTING_SCHED parameter is used to set up the schedule for sending aggregated authorizations.

The parameter specifies the days of the week and the time for starting to send aggregated authorizations. Semicolons are used to separate days of the week and commas are used to separate times within one day.

For example : MON=11:00,19:00;TUE=19:00;WED=19:00;THU=19:00;FRI=18:00;SAT=13:00,16:30,20:00;SUN=13:00,16:30;.

By default, the parameter is not set – aggregated authorizations are not sent.

TPPS_NETTING_MAX_POSTPONE

The TPPS_NETTING_MAX_POSTPONE parameter specifies the maximum allowed interval (in hours) during which aggregation can be performed without sending an authorization request to the issuer.

The default value is "116".

ⓘ The parameter is only used if the TPPS_NETTING_SCHED parameter is set.

TPPS_RESP_CODE_TOUT

The TPPS_RESP_CODE_TOUT parameter specifies a list of codes (separated by commas) applied to a temporary technical error.

If this response code is received or if the request to the issuer times out, if the document being processed is a deferred or aggregated authorization, the authorization request is repeated in technical retry mode with the parameters ISSUER_TIMEOUT_RETRY_INTERVAL and ISSUER_TIMEOUT_RETRY_COUNT.

An example of the parameter's values is "82,91".

ISSUER_TIMEOUT_RETRY_INTERVAL

The ISSUER_TIMEOUT_RETRY_INTERVAL parameter specifies the interval (in minutes) with which an authorization request is repeated in technical retry mode.

The default value is "45".

ⓘ The parameter is used together with the ISSUER_TIMEOUT_RETRY_COUNT parameter.

ISSUER_TIMEOUT_RETRY_COUNT

The ISSUER_TIMEOUT_RETRY_COUNT parameter specifies the number of repeat authorization requests in technical retry mode that will be made with the interval specified as the ISSUER_TIMEOUT_RETRY_INTERVAL parameter value.

The default value is "1".

INSUFF_FUNDS_RETRY_INTERVAL

The INSUFF_FUNDS_RETRY_INTERVAL parameter specifies the interval (in a 24-hour period) with which an authorization request will be repeated in repeat rejected authorization mode.

The default value is "6".

ⓘ The parameter is used together with the INSUFF_FUNDS_RETRY_COUNT parameter.

INSUFF_FUNDS_RETRY_COUNT

The INSUFF_FUNDS_RETRY_COUNT parameter specifies the number of repeated authorization requests in repeat rejected authorization mode that will be made with the interval specified as the INSUFF_FUNDS_RETRY_INTERVAL parameter value.

The default value is "2".

TPPS_TRANS_ATTR

The TPPS_TRANS_ATTR parameter specifies transaction conditions.

Default values POS,KEY_ENTRY,NO_CARD,NO_CARDHOLDER.

Initial assignment of card status

A card status is initially assigned only for cards that successfully passed the stop list check when a service request was first made with a card not in the TPPS card table, for example, according to the following algorithm:

1. The PAN of an OnUs card is correct – the card is assigned the "gray" status.
2. If the previous item was not fulfilled and the service request was initiated using ODA, the card is assigned the "green" status (for information: at the end of the configured time interval, the card will get the "white" status).
3. If the previous item was not fulfilled and the card's form factor = card, the card is assigned the "green" status (for cards that don't support ODA the first authorization will be made online, according to the TPPS_GREEN_EXPIRE_DAYS parameter's logic).
4. If the previous item was not fulfilled, the card is assigned the "gray" status.

The first assignment is made through settings of the Service Package in the device:

- OnUs cards are checked according to the Service's *Target Type* field value.
- Support of ODA is checked by analyzing document tags (DOC_TAG=ODA in the Service's *Service Details* field).
- Form factor support can be checked (at the client's discretion) by analyzing document tags:
  - the TKN tag is assigned based on analysis of the BIN_TOKEN tag in the BIN table (DOC_TAG=TKN in the Service's *Service Details* field).
  - the FFIND=C tag is assigned based on analysis of the transaction message's field 55 (DOC_TAG=FFIND;DOC_TAG_VALUE=C in the Service's *Service Details* field).
- The result of card classification is determined on the basis of the selected Service's TPPS_TYPE tag (possible values are "GRAY", "GREEN", "WHITE", "DENY"; the "gray" status is assigned if the code is missing or incorrect).

When initial assignment logic changes, the statuses of card that have already been saved do not change.

Card status changes

Card statuses change while a cardholder gets a transportation provider's services in the following cases:

1. A card with the "green" status that supports ODA gets the "white" status when conditions set in the global parameters TPPS_WHITE_DECLINE_INTERVAL and TPPS_WHITE_SUCCESS_INTERVAL are met.
2. Cards with any status get the "deny" status when a response code specified with the global parameter TPPS_RESP_CODE_FATAL is received from the issuer.
2. For the TPPS_WHITE_DECLINE_INTERVAL parameter to work correctly, when a "black" modifier is received, the "white" status of a card always changes to "green".

Short-term change in card status

A short-term change in card status is made for cards with the "green" status that do not support ODA, if there were no successful online or deferred authorizations for the period specified as the value of the global parameter TPPS_GREEN_EXPIRE_DAYS. In this case, the first successful authorization must be made online. If it is successful, the card's "green" status is restored. If it is unsuccessful, the card automatically (since the aforementioned condition was not met) still requires online authorization until a successful response has been received from the issuer.

Emergency (temporary) modes of TPPS operation

The global parameter TPPS_EMERGENCY_MODE activates emergency (temporary) modes for TPPS operation.

Authorization transformation

Pursuant to PCI DSS, chip transaction data cannot be stored in the acquirer's database, only the first deferred authorization is made as a chip transaction (directly from Transaction Switch memory without writing information to the database). If this authorization is unsuccessful it is made like all aggregated authorizations as a Card-Not-Present authorization.

Sending aggregated authorizations

Aggregated authorizations are always sent to the issuer in deferred mode when any of three conditions is met:

- The amount of services provided for this card exceeded the value specified as the value of the global parameter TPPS_NETTING_LIMIT_AMOUNT. In this case, an aggregated authorization is sent to the queue for immediate sending, without limits on the time of day, since the cardholder is now travelling.

- The number of services provided for this card exceeded the value specified as the value of the global parameter TPPS_NETTING_LIMIT_COUNT. In this case, an aggregated authorization is sent to the queue for immediate sending, without limits on the time of day, since the cardholder is now travelling.
- The aggregation period length is approaching the value set by the TPPS_NETTING_MAX_POSTPONE parameter. An aggregated authorization is sent according to the schedule for sending aggregated authorizations set up using the global parameter TPPS_NETTING_SCHED. The maximum latest configured window will be selected for sending the aggregated authorization, not exceeding the number of hours set as the value of the global parameter TPPS_NETTING_MAX_POSTPONE.

  ℹ Note that this scenario will only be activated if TPPS_NETTING_MAX_POSTPONE and TPPS_NETTING_SCHED parameter values are set.

Repeat authorization attempts

In the event of a timeout or negative response to an online authorization, the validator is sent a rejection and the service is not provided. In the case of deferred or aggregated authorizations, additional attempts are made to repeat authorization, since the service has already been provided.

Scenario 1 – authorization rejected by the issuer

If a response code that is a value of the global parameter TPPS_RESP_CODE_FATAL is received from the issuer, the card is put in a merchant stop list. The document for which this response code was received gets the "Rejected" status and must be manually processed by the operator.

Scenario 2 – technical retry

If one of the response codes specified in the global parameter TPPS_RESP_CODE_TOUT was received from the issuer, and also if the request to the issuer timed out, TPPS goes into technical retry mode with the values set using the global parameters ISSUER_TIMEOUT_RETRY_INTERVAL and ISSUER_TIMEOUT_RETRY_COUNT. If all repeat attempts to authorize end with the same result (timeout or response code from the list of technical errors), processing continues according to the following scenario (see Scenario 3 – repeat rejected authorization). If a card has the "white" status, its status does not change to "green" (see the section "Card status changes").

Scenario 3 – repeat rejected authorization

If a response code that is not specified in the TPPS_RESP_CODE_FATAL and TPPS_RESP_CODE_TOUT parameters is received from the issuer when an authorization attempt is made (first or repeat after technical rejection), this usually means the cardholder's funds are insufficient and the TPPS goes into repeat rejected authorization mode. A rejected authorization attempt is repeated according to the values of the global parameters INSUFF_FUNDS_RETRY_INTERVAL and INSUFF_FUNDS_RETRY_COUNT. If all the attempts end with the same result after the time and/or number of attempts defined by these parameters, the document gets the "Rejected" status and must be processed manually by the operator. The card will keep the "black" modifier, and subsequent service requests will be permitted but processed online. If the number of attempts per scenario 2 being exhausted was not the reason for moving to scenario 3 and the card has the "white" status, its status is changed to "green" (see the section "Card status changes").

ⓘ The ISSUER_TIMEOUT_RETRY_COUNT and INSUFF_FUNDS_RETRY_COUNT parameters describe the number of additional repeated attempts and do not include the first main attempt. The maximum number of authorization attempts is equal to: (1 + ISSUER_TIMEOUT_RETRY_COUNT + INSUFF_FUNDS_RETRY_COUNT).

If authorization is successful (it can only be online authorization) for a card with a debt, an additional attempt to reauthorize for the debt is made. A repeat attempt is only made if:

- A document for this debt has not been transferred to the "Rejected" status.
- An interval exceeding the value set by the ISSUER_TIMEOUT_RETRY_INTERVAL remained before the next scheduled attempt.

Unscheduled repeat authorization attempts do not decrease the content of the counter whose value is compared with the value set by the INSUFF_FUNDS_RETRY_COUNT parameter but it updates the time of the last authorization attempt. As a result, the schedule at the time of unscheduled repeat authorization is recalculated (shifted ahead) according to this scenario's logic.

ⓘ Values of the TPPS_NETTING_SCHED parameter (schedule for sending aggregated authorizations) do not affect the time of sending repeat authorization requests.

Setting up a POS type for TPPS

If the "Device Configurator Item Type" form ("Full → Configuration Setup → Merchant Device Setup → Device Configurator Item Type") does not have a record with the DEV_TYPE_OVERRIDE code in the *Item type code* column, a new record must be created with the following values:

- *Item type code* – DEV_TYPE_OVERRIDE
- *Item type name* – Device tags override
- *Item type category* – Device Type Parameter.

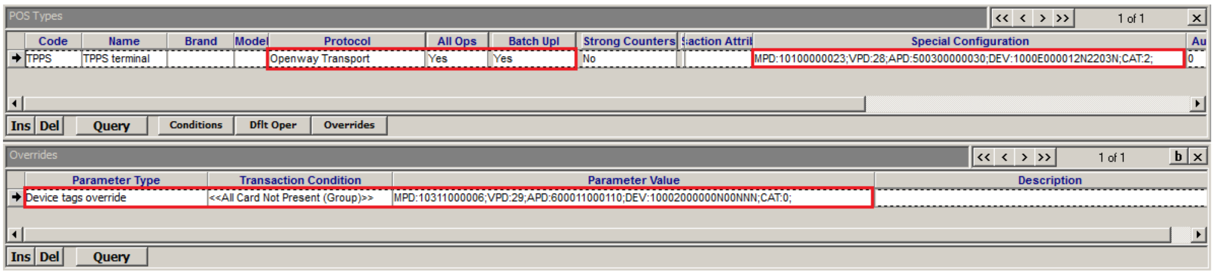
To support work with validators, set up a TPPS POS type in the "POS Types" ("Full → Configuration Setup → Merchant Device Setup → POS Types"):

- *Protocol* – Openway Transport
- *All Ops* – Yes
- *Batch Upload* – Yes

- *Special Configuration* – MPD:10100000023;VPD:28;APD:500300000030;DEV:1000E000012N2203N;CAT:2

Use the [Overrides] button to open the "Overrides" field and specify the following values (see Fig. 1):

- *Parameter type* – Device tags override
- *Transaction Condition* – <<All Card not present (Group)>>
- *Parameter Value* – MPD:10311000006;VPD:29;APD:600011000110;DEV:10002000000N00NNN;CAT:0;



Code	Name	Brand	Model	Protocol	All Ops	Batch Upl	Strong Counters	saction Attril	Special Configuration	Au
TPPS	TPPS terminal			Openway Transport	Yes	Yes	No		MPD:10100000023;VPD:28;APD:500300000030;DEV:1000E000012N2203N;CAT:2;	0

Parameter Type	Transaction Condition	Parameter Value	Description
Device tags override	<<All Card Not Present (Group)>>	MPD:10311000006;VPD:29;APD:600011000110;DEV:10002000000N00NNN;CAT:0;	

Fig. 1. Validator settings

Transaction conditions

Transaction attributes for aggregated authorizations and repeats of rejected authorizations are configured using the global parameter TPPS_TRANS_ATTR.