WAY4™ Authorisation Subsystem

Contents

This information is confidential and may be used exclusively to work with OpenWay software. It may not be duplicated, published or disclosed without written permission from OpenWay.

Introduction

This document gives an overview of the WAY4™ authorisation subsystem. It is intended for bank or processing centre employees responsible for online operation of the WAY4 system.

While working with this document, it is recommended to refer to the following reference material from OpenWay's documentation series:

- WAY4 NetServer documentation
- WAY4 Transaction Switch documentation
- Configuring WAY4™ for Magnetic Stripe Card Issuing

The following notation is used in this document:

- Field labels in screen forms are shown in *italics*.
- Button labels used in screen forms are shown in square brackets, such as [Approve].
- Menu selection sequences are shown using arrows, such as Configuration Setup → Contract Types.
- Warnings about potentially hazardous situations or actions are marked with the ⚠ sign.
- Messages marked with the ℹ sign contain information about important features, additional options, or the best use of certain system functions.

This information is confidential and may be used exclusively to work with OpenWay software. It may not be duplicated, published or disclosed without written permission from OpenWay.

Chapter 1. Authorisation Subsystem Overview

The authorisation subsystem is used to generate responses to authorisation requests received from NetServer interface channels or through Transaction Switch adapters (from payment systems, device networks, Web interfaces, etc.).

The following operations result in response generation:

- Authorisation request authentication either by the NetServer authorisation channel or Transaction Switch authorisation service using information received from the database. For example, during authentication, cryptographic values are validated using an encryption device.
- Checking of whether the operation is allowed by counterparty contract parameters; executed on the database server, this function includes checks of counterparty contract services and usage limiters.

This information is confidential and may be used exclusively to work with OpenWay software. It may not be duplicated, published or disclosed without written permission from OpenWay.

Chapter 2. Authorisation Subsystem Architecture

The WAY4 authorisation subsystem consists of the following components (see Fig. 1):

- NetServer authorisation channel or Transaction Switch adapter.
- NetServer encryption device channel or Transaction Switch encryption device adapter.
- Encryption device.
- Additional NetServer authorisation channel or Transaction Switch I-router.
- WAY4 database server. Provides responses to authorisation channel or authorisation service requests and executes necessary checks according to the authorisation request processing algorithm.
- Core Banking System (CBS) for which an online interface with WAY4 is provided.

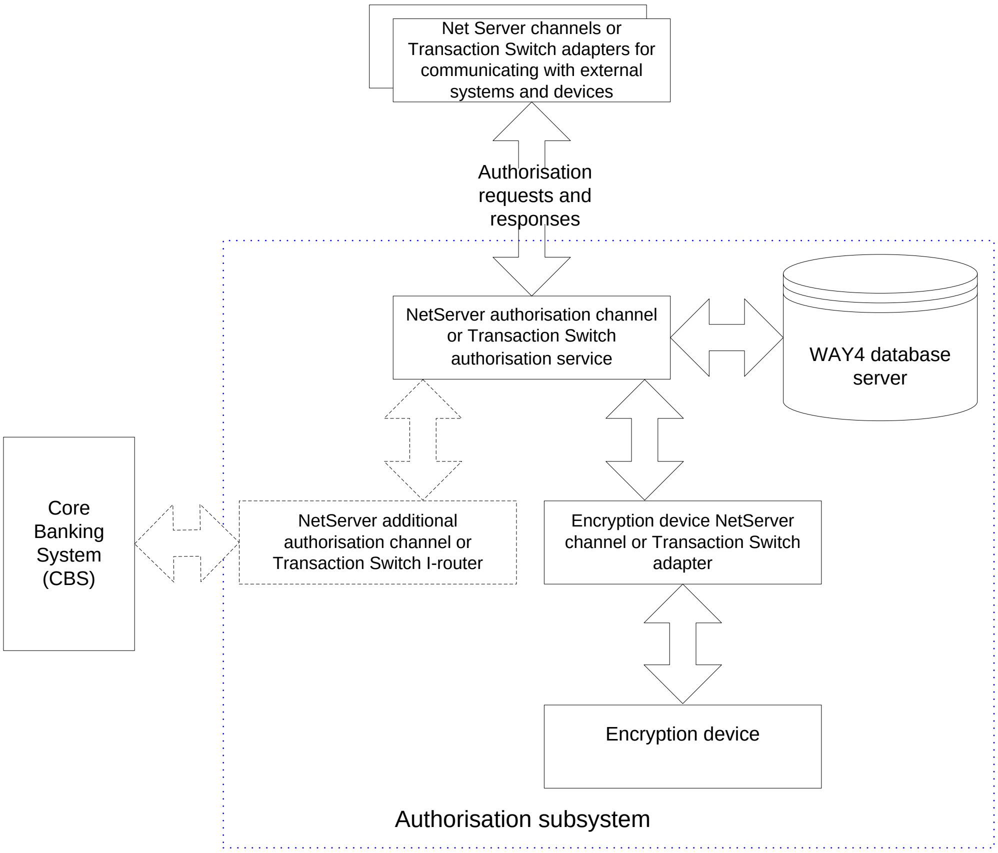

Net Server channels or Transaction Switch adapters for communicating with external systems and devices
Authorisation requests and responses
NetServer authorisation channel or Transaction Switch authorisation service
WAY4 database server
Core Banking System (CBS)
NetServer additional authorisation channel or Transaction Switch I-router
Encryption device NetServer channel or Transaction Switch adapter
Encryption device
Authorisation subsystem

Fig. 1 Authorisation subsystem architecture

Chapter 3. Operation of Authorisation Subsystem

Order of Authorisation Request Processing

Fig. 2 shows the order of request processing in the authorisation subsystem.

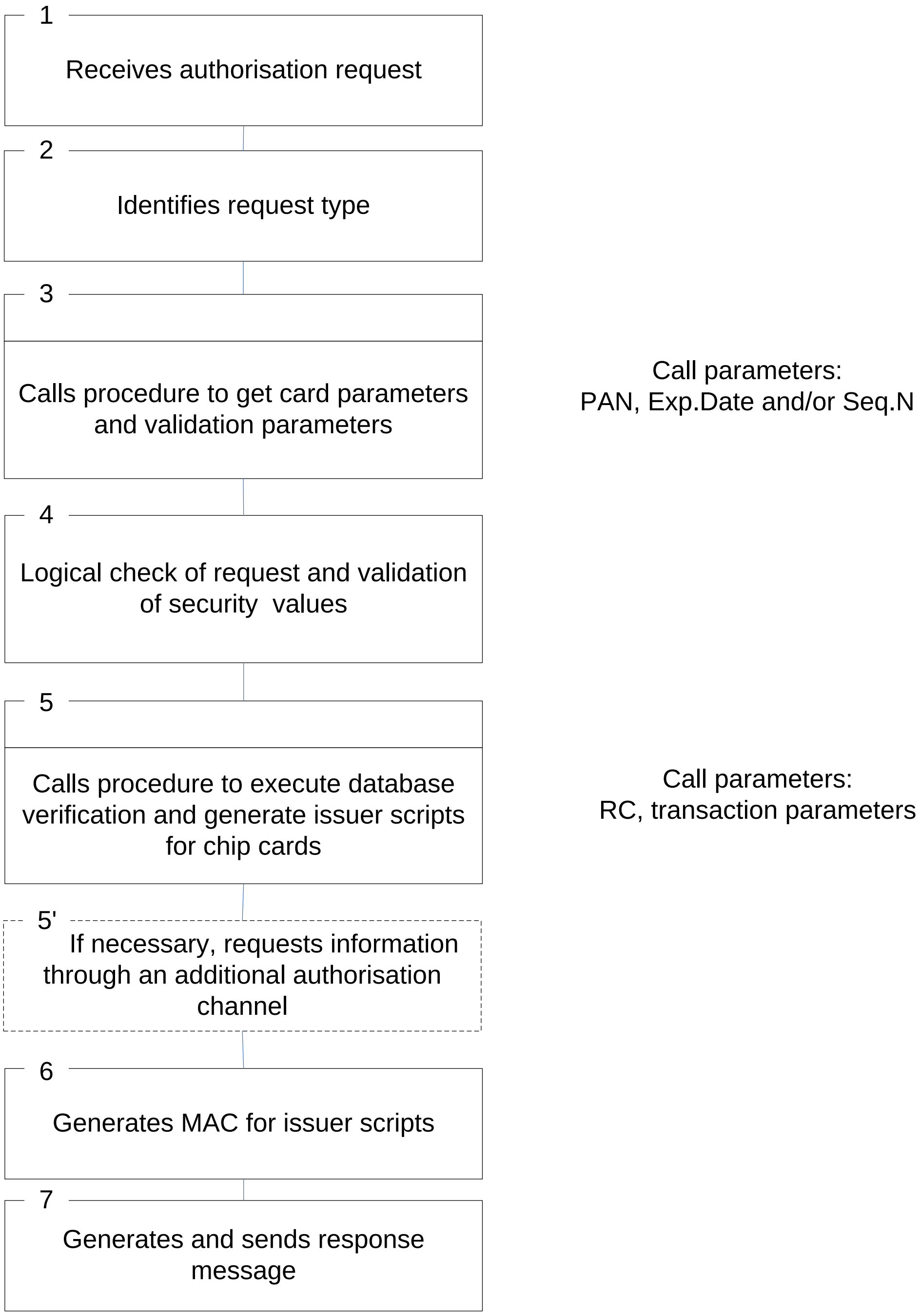

1
Receives authorisation request
2
Identifies request type
3
Calls procedure to get card parameters and validation parameters
Call parameters:
PAN, Exp.Date and/or Seq.N
4
Logical check of request and validation of security values
5
Calls procedure to execute database verification and generate issuer scripts for chip cards
Call parameters:
RC, transaction parameters
5'
If necessary, requests information through an additional authorisation channel
6
Generates MAC for issuer scripts
7
Generates and sends response message

Fig. 2 Order of authorisation request processing

The authorisation request processing algorithm consists of the following steps (numbered in Fig. 2).

This information is confidential and may be used exclusively to work with OpenWay software. It may not be duplicated, published or disclosed without written permission from OpenWay.

1. Receives an authorisation request from NetServer interface channels or through Transaction Switch adapters (from payment systems, device networks, Web interfaces, etc.).
2. Identifies the request type. If a request type is not identified, a negative response with response code 57 is generated, and request processing is terminated.
3. Sends a request to the database to get card parameters and parameters for validation of cryptographic values.
4. Performs a logical check of the request (checks whether contents of the request field correspond) and validates cryptographic values.
5. Addresses the database to check whether the operation is allowed and generate issuer scripts for chip card requests.

5'. If necessary, requests information, e.g. an amount available, through an additional authorisation channel or Transaction Switch I-router, to an external system (CBS). For more information see the functional specification " WAY4™ CB Gate".

6. Upon receiving a response from the database, generates MAC for issuer scripts if they have been generated in step 5.
7. Generates a response message and delivers it to the necessary NetServer interface channel or through Transaction Switch adapters.

Request Processing by Authorisation Channel or Authorisation Service

After an authorisation request type is identified and card parameters and parameters for validation of cryptographic values are received from the database (see steps 2 and 3 in Fig. 2 in the "Order of Authorisation Request Processing" section), the authorisation channel or authorisation service executes a logical check of the request and validates cryptographic values.

Note that the authorisation channel or authorisation service does not execute card parameter-related checks if the database response states that the card with the requested number does not exist.

The logical check of a request consists of the following operations:

- Check the Luhn digit of the request.
- Check whether the request contains a processing code.
- Check the integrity of track 1 and 2 of the magnetic stripe (executed using card parameters received from the database).
- Check whether the processing code corresponds to the merchant category code (MCC) and card type received from the database.
- Check whether the transaction condition corresponds to the merchant category code (e.g. an ATM transaction must be PIN-based).

- Check that the request contains a non-zero amount and transaction currency for the corresponding operation types.
- Check whether the request contains cryptographic values for the corresponding transaction conditions (CVV2/CVC2, magnetic stripe data for chip transactions, cryptograms and CVR for full grade chip transactions, CAVV/UCAF for 3-D Secure e-commerce operations with a certificate).
- Check whether the request contains cryptographic values (like PIN block or card expiration date) for the corresponding operation types (e.g. a balance inquiry must be PIN-based).

Validation of cryptographic values depends on the operation type and card parameters received by the authorisation channel from the WAY4 database. Therefore, this procedure has the following specifics:

- An authorisation request can contain an indicator of a precheck of certain cryptographic values by an external system (for example, by a payment system). The need to consider the results of this check is regulated by settings in WAY4, in particular, using the option "Trust to Prevalid. Rslt Sec.Val." (see the section "Validation Parameters" of the document "Configuring WAY4™ for Magnetic Stripe Card Issuing").
- When setting a new PIN, the need to check its length (relative to that defined in the corresponding card type's production parameters) is determined using the "PIN Length Check" option (possible values "Y"/"N"). The procedure to set options for card production parameters is described in the document "Configuring WAY4™ for Magnetic Stripe Card Issuing".

An encryption device (HSM) connected to NetServer or Transaction Switch is used to check cryptographic values.

In general, the authorisation channel (NetServer) or authorisation service (Transaction Switch):

- Checks a PIN code entered online (through the HSM) or offline (checks whether the card accepted the entered PIN).

  If a PVV is not stored in the database, the PVV value stored on the card's magnetic stripe (Track 2) is used.
- Checks the cryptogram contained in the request and generates a response cryptogram (through the HSM). A response cryptogram is generated if validation is successful and stored until a response after a database check is received.
- Performs an algorithmic check of CVR and TVR values. The check algorithm is specified in the database and passed to the authorisation channel in response to a card parameter request (see step 3 in Fig. 2 in section "Order of Authorisation Request Processing").
- Checks DAC/DN values through the HSM. The check can be switched off through authorisation channel configuration parameters.

  ⚠ This document does not describe configuration parameters. Specified parameters may only be changed by the system vendor.

- Checks CAVV/UCAF values through the HSM.
- Checks CVV/ICVV values through the HSM if the database supports this check.
- Checks CVV2/CVC2 values through the HSM.
- Checks special cryptographic values supported by the authorisation channel configuration of the bank or processing centre.
- Generates a request to the database irrespective of the result of the validation executed by the authorisation channel. If the validation is unsuccessful, a request to the database is generated, for example, to log authorisation results (that is, create an authorisation document). Verification executed in the database may change the response code for a more unfavourable one.

A request to the database (see step 5 in Fig. 2 in section "Order of Authorisation Request Processing") contains a preliminary response code and transaction parameters for further verification. For details on database verification, see "Request Processing on WAY4 Database".

The subsystem setup may assume that information can be requested through an additional authorisation channel, e.g. request of a contract's amount available in an external system.

Having received a response from the database and through an additional authorisation channel, the authorisation channel:

- Generates cryptographic values with the HSM:
  - Issuer script MAC for chip card requests
  - Response cryptogram for chip card requests if the response code is other than 00. If the response is positive, the response cryptogram generated before sending a request to the database is used.
- Generates and sends a response message.

Request Processing on WAY4 Database Server

Authorisation messages are processed in the WAY4 database according to authorisation channel requests in two steps.

Step 1: The first step ensures that the authorisation channel receives card parameters and parameters for validation of cryptographic values (see step 3 in Fig. 2 in the "Order of Authorisation Request Processing" section).

In the WAY4 DB, a search is made for an effective contract and current information about a plastic card according to the request's parameters.

If for a non-chip transaction there are several records for a plastic card that have the same effective period (for example, about a card that was blocked and unblocked due to reissue), information about the unblocked card is selected.

A response to an authorisation channel request may contain a negative response code for the following reasons:

- No contract is found for this card number.

- No plastic with the expiration date specified in the request is found for this card number.
- No set of cryptographic value validation parameters is found for this card number.

If verification is successful, the database returns data necessary for validation of cryptographic values. The corresponding data is contained in the table PM_PARMS (Full → Configuration Setup → Card Production Setup → Bank Production Parameters → [Validation]) for the card range to which the card number belongs and the PM Code value of the card stored in the CARD_INFO table (form "Plastics for…" opened from the card contract form by clicking the [Plastics] button).

Step 2: The second step of request processing (see step 5 in Fig. 2 in the "Order of Authorisation Request Processing" section) is the authorisation request verification itself.

At this step, the database:

- Identifies the transaction type taking into account MCC.
- Creates a document with the response code (RC) received from the authorisation channel.
- Logs the previous issuer script execution results and offline expenses data for chip cards. The system searches for the contract for which the card was issued and for which the issuer scripts were generated, while the authorisation request itself may be related to another contract.
- Searches for the original document for secondary documents (reversal, adjustment, advice).

  Fig. 3 shows processing of authorisation advice messages that may be received if the payment system is allowed to execute authorisations instead of the issuer.

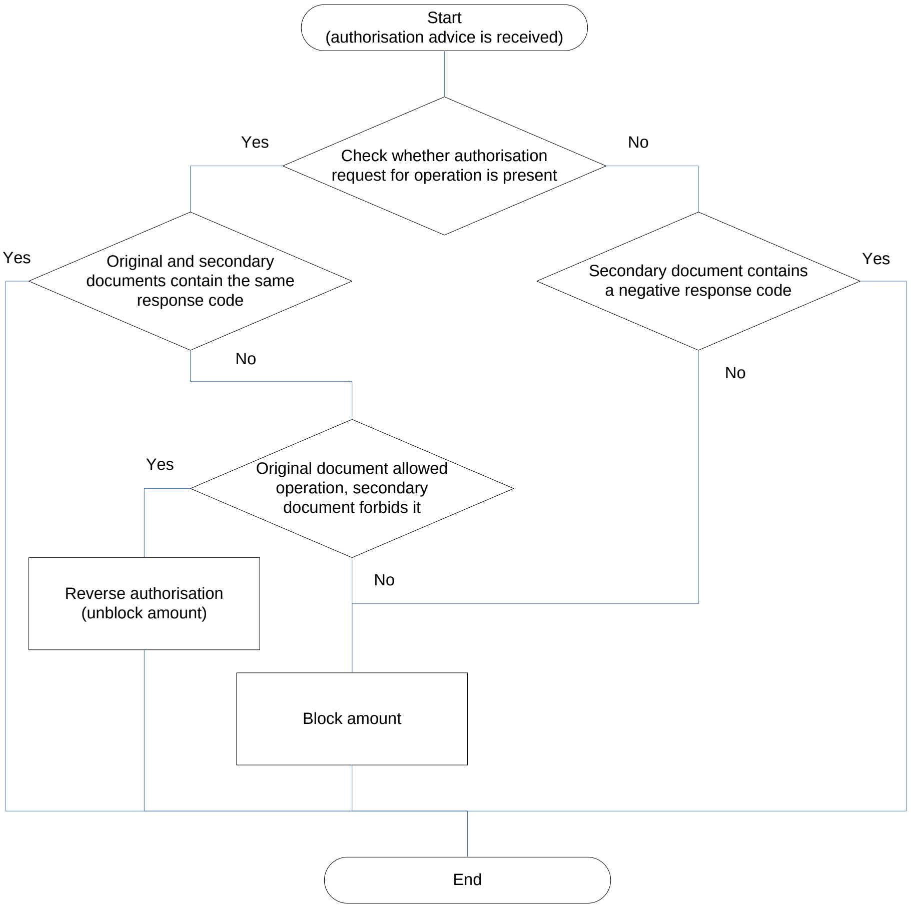

Start
(authorisation advice is received)
Check whether authorisation request for operation is present
Yes
No
Original and secondary documents contain the same response code
Yes
No
Secondary document contains a negative response code
Yes
No
Original document allowed operation, secondary document forbids it
Yes
No
Reverse authorisation (unblock amount)
Block amount
End

Fig. 3 Algorithm of authorisation advice processing

- Processes the PIN counter for PIN-based transactions. If the authorisation channel informs that the correct PIN has been entered and the counter value does not exceed the maximum allowed number, the counter is set to zero. If the PIN code is incorrect, the counter is increased by 1.
- Address verification, e.g. when processing a web transaction request.
- Checks the target contract, including the expiration date of its plastic, contract status and closing date.
- Checks the merchant stop list (Full → Stop List → Merchant Stop List), card stop list (Full → Stop List → Card Stop List) and client stop list (Full → Stop List → Client Stop List).
- Calculates fees according to the target contract Service for operations of this type.
- Converts the transaction amount and fee amount into the contract currency.
- Checks contract usage limiters.
- Blocks the amount on the contract or unblocks it if a secondary authorisation document is processed (see the section "Changing a Contract's Amount Available").
- Generates an authorisation code (a 6-digit number that does not start with 0).

- Generates a mini-statement (if required by the request) and determines the contract balances.
- Opens Events and generates messages, for example, cardholder notification of an executed authorisation.
- Generates issuer scripts and a cryptogram response code (ARPC RC) for chip operations.
- Saves the authorisation document with the data received during data processing (confirmed response code, card contract identifier, etc.)
- Changes an authorisation document response code after executing database verification.
- Sends a response to the authorisation channel to finish request processing (see "Request Processing by Authorisation Channel").

A response to the authorisation channel contains a response code (RC), a contract balance, a mini-statement (if required by the request), issuer scripts for chip cards, etc.

ⓘ Note that the database server sends a positive response code (RC=00) in response to authorisation requests like "Reversal", "Adjustment" or "Advice" irrespective of the code specified in the authorisation document generated after the verification.

Changing a Contract's Amount Available

When an authorisation message is processed, a record about the change in the contract's amount available is created (Credit_History table). The change in a contract's amount available depends on the type and status of the authorisation message.

Authorisation message types:

- "In Pending" – funds the contract possesses when the transaction is processed are blocked.
- "By Usage" – permit a transaction for which an "Overdraft" limiter is used in processing and/or the transaction is processed in "Stand-In Processing" ("STIP") mode. Part of the amount is blocked from available funds, and the remaining part from the limiter.
- "Credit Limit" – allocate/change a credit limit.
- "Additional Cr Limit" – allocate/change an additional credit limit.
- "Offline Used" – funds spent offline.
- "Offline Blocked" – funds blocked for making offline transactions.
- "Offline Presentment" – information about funds spent offline that was received after a financial document was posted.
- "Offline Increment" – change the volume of funds available for use offline for this card if an online transaction is being processed for a card.

This information is confidential and may be used exclusively to work with OpenWay software. It may not be duplicated, published or disclosed without written permission from OpenWay.

- "Offline Total Used" – technical record; used when processing transactions in the "WAY4™ Pre-Authorized Debit" solution.
- "Balance Inquiry" – contract balance inquiry.
- "Statement" – mini-statement request.
- "Additional Online Service" – additional online transaction.
- "Accounting" – accounting operations between accounts (contracts).
- "Ineffective" – service operations, for example, "Note Acceptance" – requests to accept cash from a bank cardholder. The only purpose of this request is to check whether the issuer allows this transactoin; the contract's amount available does not change.
- "Verification" – bankcard verification.
- "When Available" – a fee is charged when there is an amount available, including the credit limit.
- "When Credit" – a fee is charged when there is an amount available without consideration of the credit limit.

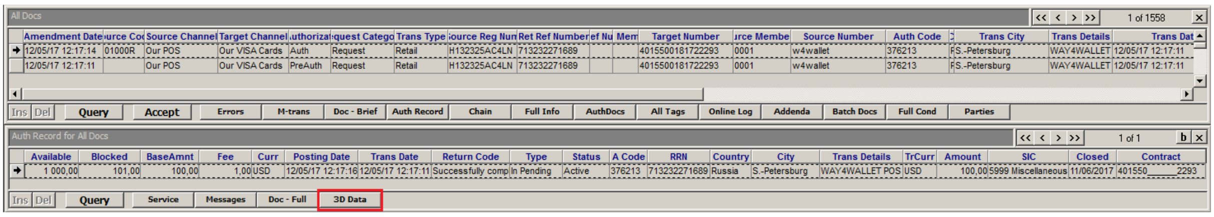
Authorisation message statuses:

- "Active" – there is no financial document for this transaction or it has not been posted, fund blocking is active.
- "Declined" – the transaction was declined.
- "Matched" – the transaction was confirmed after posting the financial document.
- "Reversed" – the transaction was reversed.
- "Closed" – blocking was closed manually or after a timeout.
- "Waiting" – status for a non-financial transaction waiting for posting.
- "Processed" – blocking funds for an offline transaction is active; an authorisation gets this status after the corresponding financial document has been posted.
- "Inactive" – blocking is not active; does not affect the contract's available funds.
- "History" – reserved value; not used in the current version.
- "Erased" – the value is used in test mode when forcing a balance change.

Viewing Authentication Conditions for 3-D Secure

For convenient processing of client requests, for example when processing dispute cases, e-commerce transaction authentication conditions can be viewed.

In the "All Docs" form, select a document generated as the result of an authorization request (see Fig. 4), menu item "Full → Documents Input & Update → Doc - General Form → All Docs → [Auth Record]".

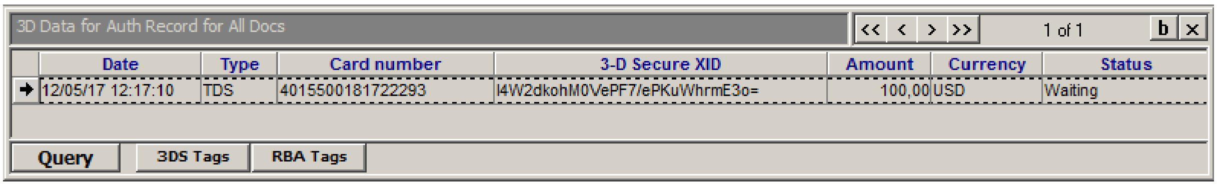


Amendment Date	urce Coc	Source Channel	Target Channel	uthorizat	quest Catego	Trans Type	ource Reg Num	Ret Ref Number	ef Nu	Mem	Target Number	urce Membe	Source Number	Auth Code	C	Trans City	Trans Details	Trans Dat
12/05/17 12:17:14	01000R	Our POS	Our VISA Cards	Auth	Request	Retail	H132325AC4LN	713232271689			4015500181722293	0001	w4wallet	376213	F	S.-Petersburg	WAY4WALLET	12/05/17 12:17:11
12/05/17 12:17:11		Our POS	Our VISA Cards	PreAuth	Request	Retail	H132325AC4LN	713232271689			4015500181722293	0001	w4wallet	376213	F	S.-Petersburg	WAY4WALLET	12/05/17 12:17:11

Available	Blocked	BaseAmnt	Fee	Curr	Posting Date	Trans Date	Return Code	Type	Status	A Code	RRN	Country	City	Trans Details	TrCurr	Amount	SIC	Closed	Contract
1 000,00	101,00	100,00	1,00	USD	12/05/17 12:17:16	12/05/17 12:17:11	Successfully comp	In Pending	Active	376213	713232271689	Russia	S.-Petersburg	WAY4WALLET POS	USD	100,00	5999 Miscellaneous	11/06/2017	401550______2293

Fig. 4. Authorization document

Click on the [3D Data] button to open the "3D Data for Auth Record" form (see Fig. 5).



Date	Type	Card number	3-D Secure XID	Amount	Currency	Status
12/05/17 12:17:10	TDS	4015500181722293	I4W2dkohM0VePF7/ePKuWhrmE3o=	100,00	USD	Waiting

Fig. 5. 3-D Secure authentication conditions

Field description:

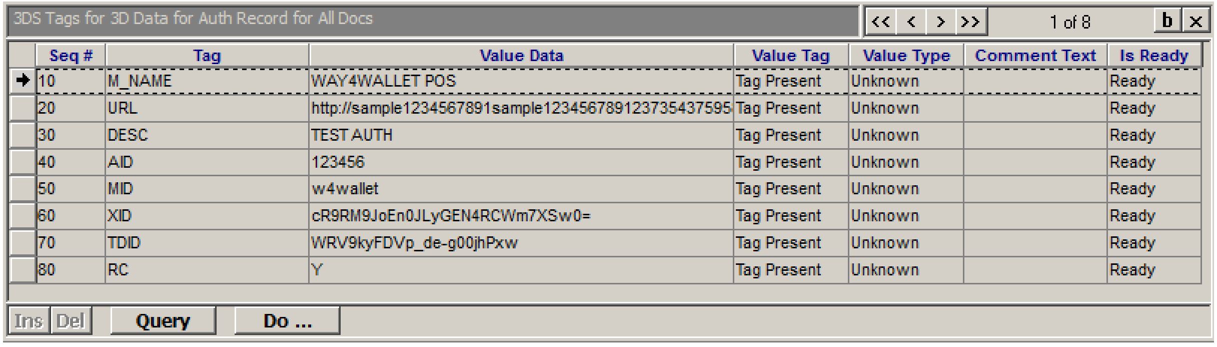
- *Date* – payer authentication request generation date and time.
- *Type* – authentication type; TDS – 3-D Secure.
- *Card number* – number of the card for the transaction.
- *3-D Secure XID* – data exchange ID allowing a payer authentication request (PAReq) to be linked to the response for this request (PARes). The identifier is generated by the merchant according to accepted encoding rules and is included in an authorization request (PAReq).

  PAReq (Payer Authentication Request) is a request to the issuer to make a purchase with this card.

  This request is generated by a merchant but comes into the ACS server from the cardholder's browser (as part of an HTTP-POST request), i.e. receipt of a PAReq indicates that a connection is established between the cardholder and ACS server.

  PARes (Payer Authentication Response) is the response to the payer authentication request. It is generated when authentication information is exchanged between the issuer and cardholder. By this message, the issuer confirms (or does not confirm) the purchase is permitted. The message is transmitted to the merchant through the cardholder's browser.
- *Amount* – transaction amount.
- *Currency* – transaction currency.
- *Status* – request status (see the section "Changing a Contract's Amount Available" for a description of authorization statuses).

Authentication conditions are tags in an authorization document's *Add Info* field. The list of tags and their values is available in the "3DS Tags for 3D Data for Auth Record" form opened by clicking on the [3DS Tags] button in the "3D Data for Auth Record" form (see Fig. 6).



	Seq #	Tag	Value Data	Value Tag	Value Type	Comment Text	Is Ready
➔	10	M_NAME	WAY4WALLET POS	Tag Present	Unknown		Ready
	20	URL	http://sample1234567891sample123456789123735437595	Tag Present	Unknown		Ready
	30	DESC	TEST AUTH	Tag Present	Unknown		Ready
	40	AID	123456	Tag Present	Unknown		Ready
	50	MID	w4wallet	Tag Present	Unknown		Ready
	60	XID	cR9RM9JoEn0JLyGEN4RCWm7XSw0=	Tag Present	Unknown		Ready
	70	TDID	WRV9kyFDVp_de-g00jhPxw	Tag Present	Unknown		Ready
	80	RC	Y	Tag Present	Unknown		Ready

Fig. 6. Authentication request tags

ⓘ This functionality is available only for authorisation on the Transaction Switch platform.