Operation Manual

Authorization System

03.52.30

04.07.2021

Contents

This document describes the operating principles of the Way4 authorization system.

The document is intended for bank and processing center employees who are responsible for Way4 operation online.

While working with this document, it is recommended that users refer to the following resources from the Way4 documentation series:

- NetServer System Administrator Manual
- Transaction Switch Platform Overview
- Configuring WAY4 for Smart Card Issuing.

The following notation is used in the document:

- Screen form field labels are shown in *italics*.
- Screen form button labels are shown in square brackets, such as [Approve].
- Sequences for selecting user menu items are shown using arrows as follows: "Issuing → Contracts Input & Update".
- Sequences for selecting system menu items are shown using arrows as follows: "Database => Change password".
- Key combinations in DB Manager are shown in angular brackets, for example <Ctrl>+<F3>.

⚠ Warnings about potentially hazardous situations or actions are marked with a special icon and highlighted.

ⓘ Information about important features, additional options, or the best use of certain system functions.

1 Purpose of the authorization system

The authorization system is used to generate responses to authorization requests coming in on NetServer interface channels or through Transaction Switch adapters (from payment systems, device networks, web interfaces, etc.).

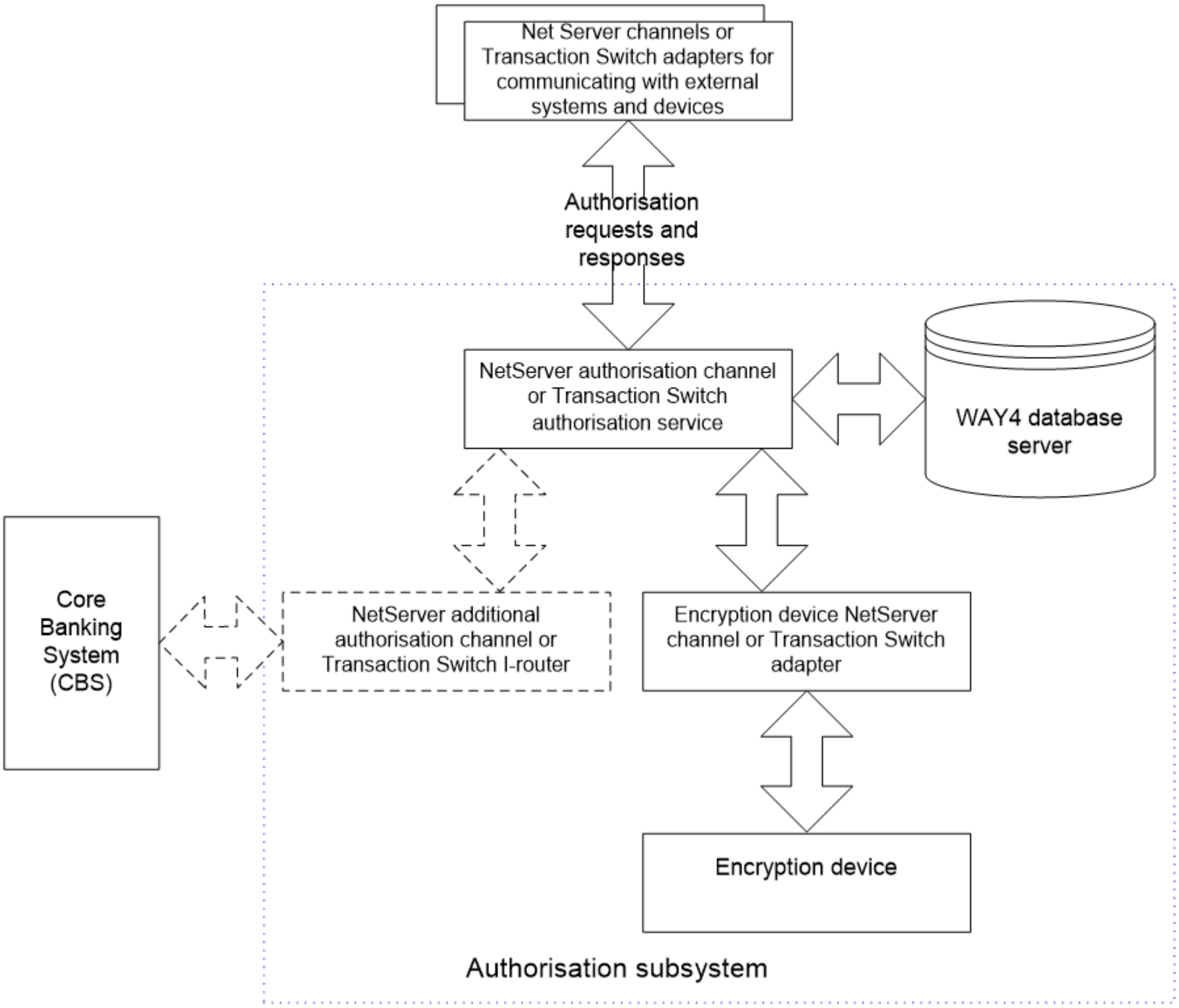
A response to an authorization request is generated based on the results of the following operations:

- Authorization request authentication performed by a NetServer authorization channel or by a Transaction Switch authorization service using information received from the database during authentication, in particular, cryptographic values are checked using cryptographic hardware.
- Check of whether the operation is allowed based on counterparty contract parameters. This check is made on the database server and includes a check of counterparty contract Services and usage limiters.

2 Authorization system structure and components

The Way4 authorization system includes the following components:

- NetServer authorization channel or Transaction Switch adapter.
- NetServer cryptographic device channel or Transaction Switch cryptographic device adapter
- Cryptographic device
- NetServer additional authorization channel or Transaction Switch IRouter.
- Way4 database server. Responsible for responses to authorization channel requests or authorization service requests and making checks according to the authorization request processing algorithm.
- Core Banking System (CBS) for which an online interface with Way4 is provided.

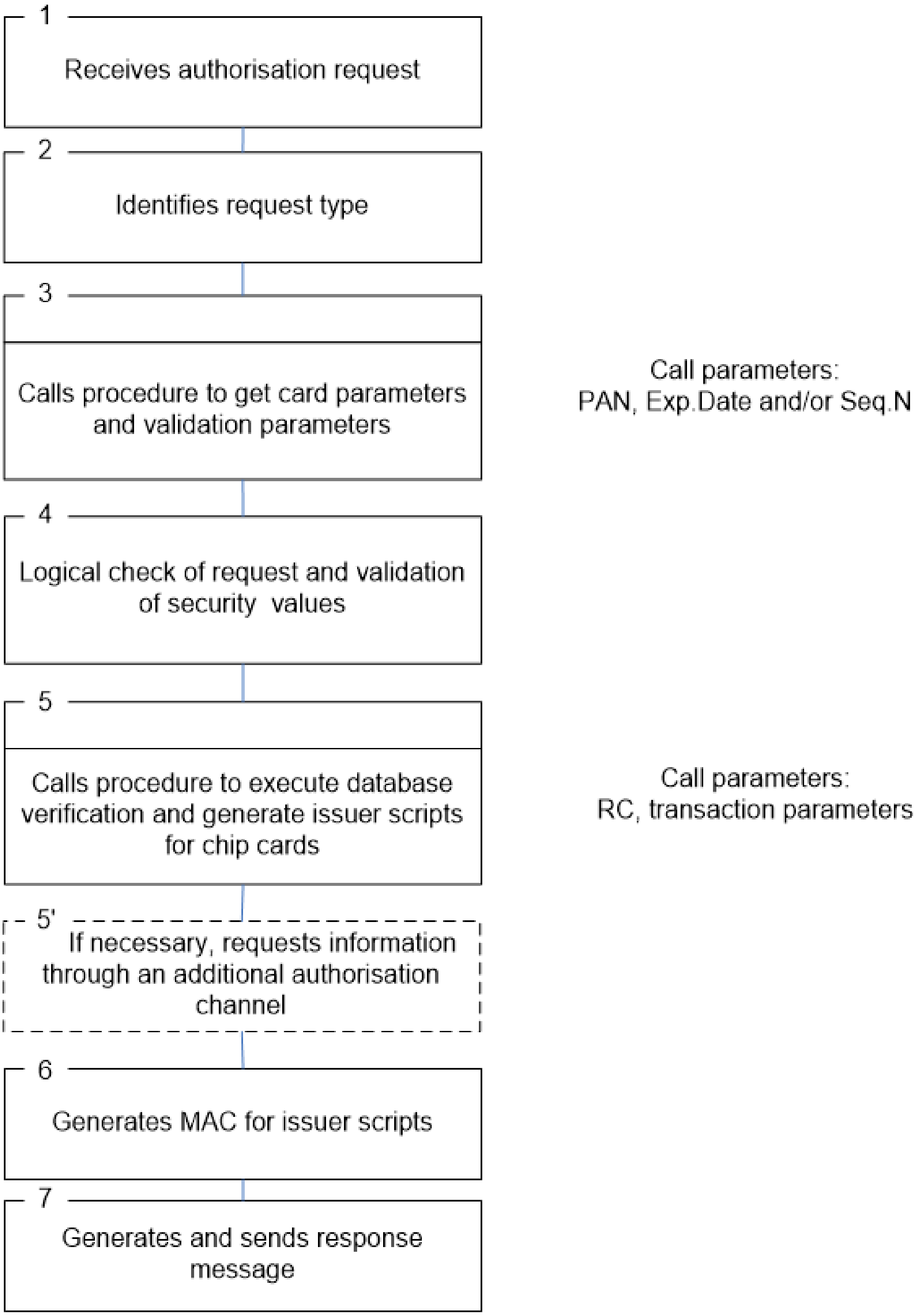

Net Server channels or Transaction Switch adapters for communicating with external systems and devices
Authorisation requests and responses
NetServer authorisation channel or Transaction Switch authorisation service
WAY4 database server
Core Banking System (CBS)
NetServer additional authorisation channel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

Authorization system structure

3 Operation of the authorization system

3.1 Authorization request processing workflow

The figure illustrates request processing workflow in the authorization system


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

Request processing workflow

The authorization request processing algorithm consists of the following steps, numbered in the figure.

1. An authorization request is received from NetServer interface channels or through Transaction Switch adapters (from payment systems, device networks, web interfaces, etc.).

2. Identification of the request type. If the request type was not identified, a negative response with the code RC=57 is generated and processing of the request is terminated.
3. A request is sent to the database to get card parameters and parameters for validation of cryptographic values.
4. A logical check of the request is made (of whether the content of the request's fields correspond to one another) and cryptographic values are validated.
5. The database is called to check whether the operation is allowed and to generate issuer scripts for chip card requests.
6. If necessary, information is requested, for example, about the amount available, through an additional authorization channel or Transaction Switch IRouter, in particular from an external system (CBS). For more information, see the functional specification "Way4 CB Gate Setup".
7. After a response is received from the database, an authentication code (MAC) is generated for issuer scripts if these scripts were generated in step 5.
8. A response message is generated and sent to the appropriate NetServer interface channel or through Transaction Switch adapters.

3.2 Request processing by an authorization channel or authorization service

After the authorization request type has been identified and card parameters and parameters for validating cryptographic values have been received from the database (see steps 2 – 3 in the figure in the section "Authorization request processing workflow"), the authorization channel or authorization service performs a logical check and validates cryptographic values.

> ⓘ Note that if the response from the database states that there is no card with this number, the authorization channel or authorization service does not perform checks that depend on card parameters.

A logical check of a request includes the following activities:

- 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 (this is done 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 transaction conditions correspond to the merchant category (for example, ATM transactions must be PIN-based).
- Check whether the request contains a non-zero amount and the transaction currency for the corresponding transaction 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 transactions with a certificate).

- Check whether the request contains cryptographic values (like PIN block or card expiration date) for the corresponding operation types (for example, a balance inquiry must be PIN-based). Validation of cryptographic values depends on the transaction type and card parameters received by the authorization channel from the Way4 database. Accordingly, the procedure has the following specifics:
- An authorization 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".

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

In general, the authorization channel (NetServer) or authorization service (Transaction Switch) does the following:

- 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 received 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 according to checks in the database is received.
- Performs algorithmic validation of CVR and TVR values. The validation algorithm is set in the database and is sent in the response to the authorization channel request for card parameters (see step 3 in the figure in the section "Authorization request processing workflow").
- Using the HSM, checks DAC/DN values. The check can be disabled by authorization channel configuration parameters.

> ⚠ This document does not describe configuration parameters. Only OpenWay representatives may change these parameters.

- Using the HSM, checks CAVV/UCAF values.
- Using the HSM, checks CVV/ICVV values, if this check is supported in the database.
- Using the HSM, checks CVV2/CVC2 values.
- Checks special cryptographic values supported by the configuration of the bank's or processing center's authorization channel.
- A request to the database is made regardless of whether validation by the authorization channel was successful. If validation was unsuccessful, a request to the database is made, in particular,

for logging authorization results (creation of an authorization document). Checks made in the database may change the response code to one that is less favorable.

A preliminary response code and transaction parameters are passed in a request (see step 5 in the figure in the section "Authorization request processing workflow") to the database for further validation. For information about checks in the database, see the section "Processing requests on the Way4 database server".

System setup may support requesting information through an additional authorization channel, for example, requesting a contract's amount available in an external system.

After getting a response from the database and through an additional authorization channel, the authorization channel does as follows:

- Using the HSM, generates cryptographic values:
- Issuer script authentication code for chip card requests.
- Response cryptogram for chip card requests if the response code is not "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.

3.3 Processing requests on the Way4 database server

Authorization messages are processed in two steps in the Way4 database, according to authorization channel requests.

Step 1. The first step ensures that the authorization channel gets card parameters and parameters for validation of cryptographic values (see step 3 in the figure in the section "Authorization request processing workflow").

In the Way4 database, a search is made for a valid contract and up-to-date information about a card, according to the request's parameters.

If for a non-chip transaction there are several records for a 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 authorization channel request may contain a negative response code for the following reasons:

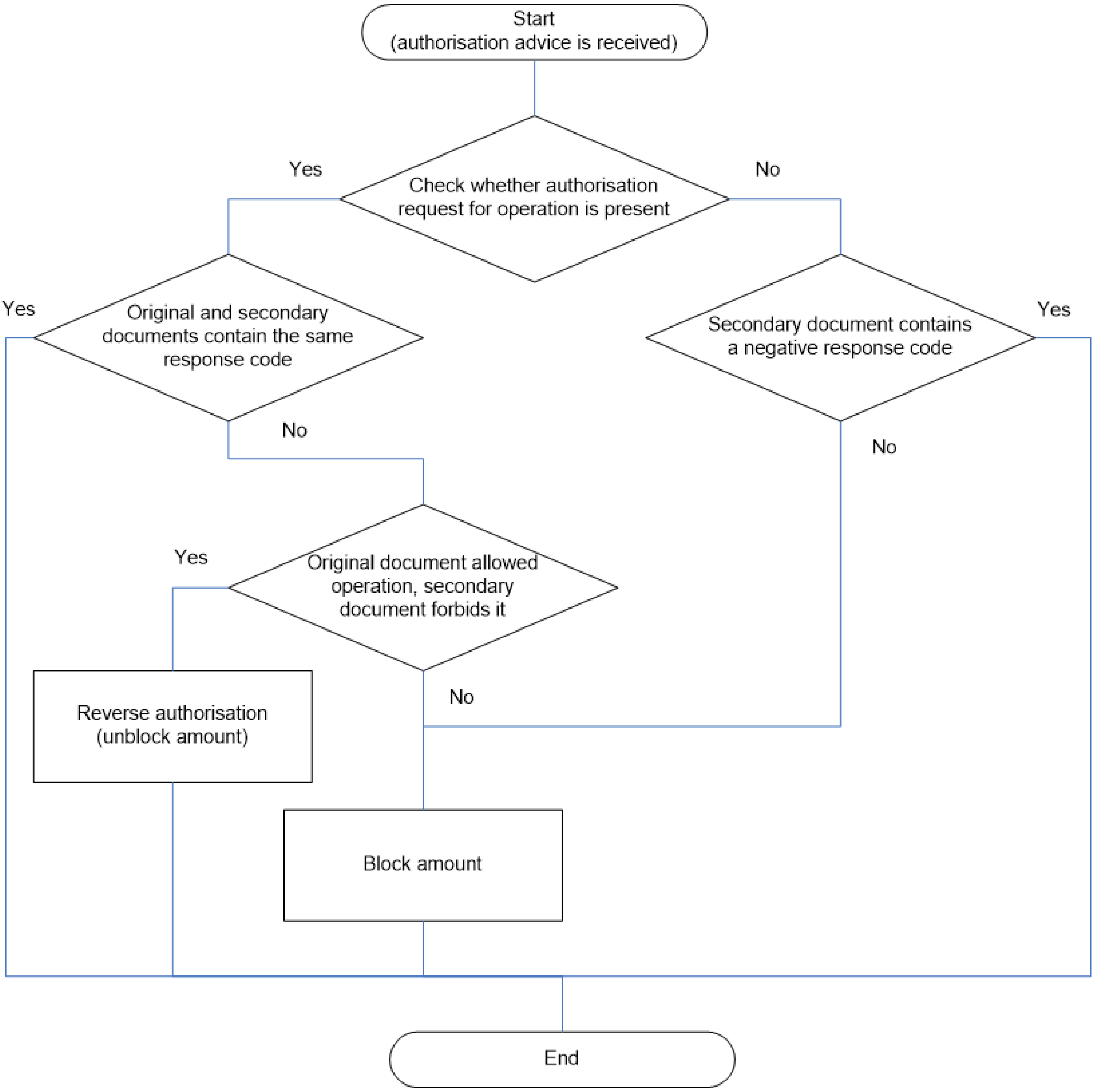
- No contract was found for this card number.
- No plastic card with the expiration date specified in the request was found for this card number.
- No set of cryptographic value validation parameters was found for this card number.

If these actions were successful, information required for validation of cryptographic values is returned. The corresponding data is contained in the PM_PARMS table (Full → Configuration Setup → Card Production Setup → Bank Production Parameters-> [Validation]) for the range of numbers that includes the card number, and the card's PM code value stored in the CARD_INFO table ("Plastics for..." form opened by clicking the [Plastics] button in the card contract form).

Step 2. The second step of processing a request (see step 5 in the figure in the section "Authorization request processing workflow") includes checks in the database that are made for the authorization request.

At this step, the following actions are performed in the database.

- The transaction type is identified, with consideration of MCC.
- A document is created with the response code (RC) from the authorization channel.
- Results of executing the previous issuer script and data about the amount of funds spent offline are logged for chip cards. A search is made for the contract for which the card was issued and for which issuer scripts were generated, while the authorization request itself may be related to another contract.
- A search is made for the original document for secondary documents (Reversal, Adjustment, Advice).
  Processing of Authorization Advice that may be received if the payment system is allowed to perform authorizations on behalf of the issuer is shown in the figure:


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

Algorithm for processing authorization advice

- The PIN counter for PIN-based transactions is processed. The counter is reset if the authorization channel informs that the correct PIN has been entered and the counter value does not exceed the maximum allowed number. If the PIN is incorrect, the counter increases by "1".
- The address sent in the request is verified, for example, when processing a request for an internet transaction.
- The target contract is checked, including a check of the card's expiration date, contract status and its closing date.
- 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) are checked.
- Fees are calculated according to the target contract Service for this transaction type.
- The transaction amount and fee amount are converted to the contract currency.

- Contract usage limiters are checked.
- Contract funds are blocked or are unblocked when processing a secondary authorization document (see the section "Changing a contract's amount available").
- An authorization code is generated (a 6-digit number that does not start with "0").
- A mini-statement is generated, if required by the request and contract balances are determined.
- Events are opened and messages are generated, for example, to notify the cardholder about authorization.
- Issuer scripts are generated and a cryptogram response code (ARPC RC) for chip transactions.
- The authorization document with information received during data processing (confirmed response code, card contract identifier, etc.) is saved.
- To complete request processing, a response is sent to the authorization channel (see "Request processing by an authorization channel").

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

> ⓘ Note that in response to authorization requests like "Reversal", "Adjustment", "Advice", the database server sends a positive response code (RC=00) regardless of the code that was specified in the authorization document generated after validation.

3.4 Changing a contract's amount available

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

Authorization 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 offline transactions.
- "Offline Presentment" – information about funds spent offline that was received after posting a financial document.
- "Offline Increment" – change the volume of funds available for use offline if an online transaciton is being processed for the card.
- "Offline Total Used" – technical record; used when processing transactions in the "Way 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 cardholder. The only purpose of this request is to check whether the issuer allows this transaction; the contract's amount available does not change.
- "Verification" – card 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 including the credit limit.

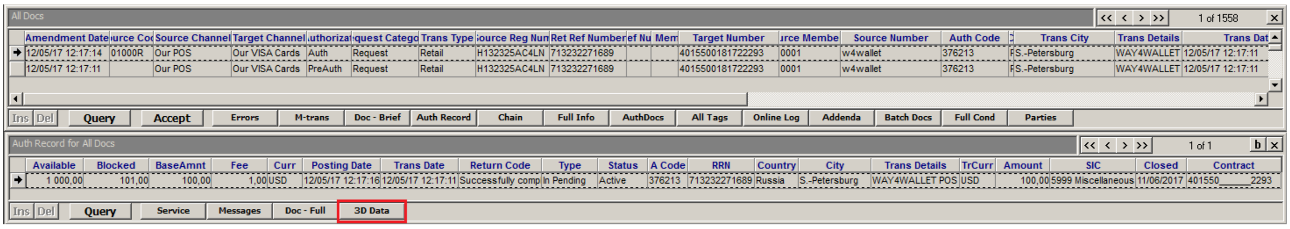
Authorization message statuses:

- "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 authorization 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.

3.5 Viewing 3-D secure authentication conditions

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, menu item "Full → Documents Input & Update → Doc – General Form → All Docs → [Auth Record]".

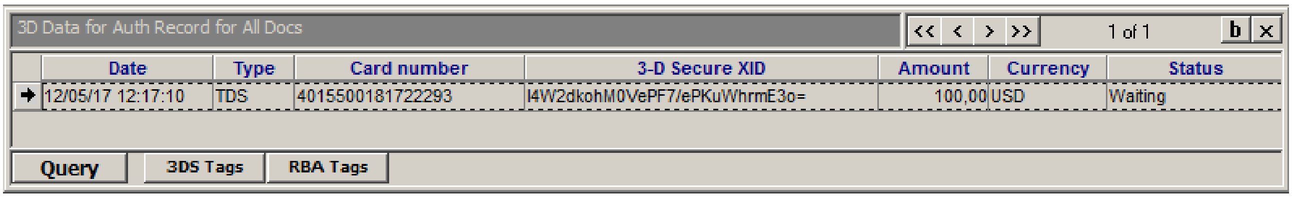


Amendment Date	urce Co	Source Channel	Target Channel	uthoriza	quest Catego	Trans Type	ource Reg Num	Ret Ref Number	ef Nu	Mem	Target Number	urce Membe	Source Number	Auth Code		Trans City	Trans Details	Trans Dat
12/05/17 12:17:14	01000R	Our POS	Our VISA Cards	Auth	Request	Retail	H132325AC4LN	713232271689			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

Authorization document

Click the [3D Data] button to open the "3D Data for Auth Record" form.



3D Data for Auth Record for All Docs

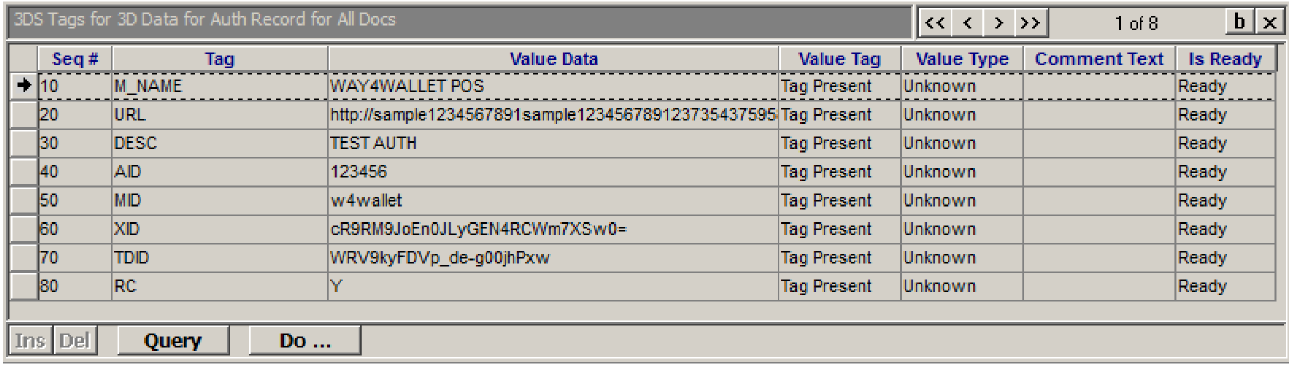
Date	Type	Card number	3-D Secure XID	Amount	Currency	Status
12/05/17 12:17:10	TDS	4015500181722293	I4W2dkohM0VePF7/ePKuWhrmE3o=	100,00	USD	Waiting

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 used for the transaction.
- *3-D Secure XID* – data exchange identifier allowing the payer authentication request (PAReq) to be linked with the response to this request (PARes). The identifier is generated by the merchant according to accepted encoding rules and is included in an authorisation 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 (authorization statuses are described in the section "Changing a contract's amount available").

Authentication conditions are specified in the authorization document’s *Add Info* field as tags. The "3DS Tags for 3D Data for Auth Record" form contains the list of tags and their values. To open the form, click the [3DS Tags] in the "3D Data for Auth Record" form.



3DS Tags for 3D Data for Auth Record for All Docs

Seq #	Tag	Value Data	Value Tag	Value Type	Comment Text	Is Ready
10	M_NAME	WAY4WALLET POS	Tag Present	Unknown		Ready
20	URL	http://sample1234567891sample12345678912373543759	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

Authentication request tags

ⓘ This functionality is only available for authorizations on the Way4 Transaction Switch platform.