

# Подсистема авторизации WAY4™

# Содержание

ВВЕДЕНИЕ	2
ГЛАВА 1. НАЗНАЧЕНИЕ ПОДСИСТЕМЫ АВТОРИЗАЦИИ	3
ГЛАВА 2. СТРУКТУРА И КОМПОНЕНТЫ ПОДСИСТЕМЫ АВТОРИЗАЦИИ	4
ГЛАВА 3. РАБОТА ПОДСИСТЕМЫ АВТОРИЗАЦИИ	5
Последовательность обработки авторизационного запроса	5
Обработка запроса каналом авторизации или сервисом авторизации	6
Обработка запроса на сервере базы данных WAY4	9
Изменение доступных средств контракта	11
Просмотр условий аутентификации по протоколу 3-D Secure	13

## Введение



Данный документ описывает принципы работы подсистемы авторизации WAY4™.

Документ предназначен для сотрудников банков и процессинговых центров, обеспечивающих работу системы WAY4 в режиме онлайн.

При работе с данным документом рекомендуется пользоваться следующими источниками из комплекта документации WAY4:

- документы по NetServer системы WAY4;
- документы по Transaction Switch системы WAY4;
- "Настройка параметров системы WAY4™ для выпуска карт с магнитной полосой".

В документе используются следующие обозначения:

- названия полей экранных форм выделяются *курсивом*;
- названия кнопок экранных форм приводятся в квадратных скобках, например [Approve];
- последовательность выбора пункта в меню пользователя отображается с помощью стрелок следующим образом: "Configuration Setup → Contract Types";
- предостережения в связи с возможностью совершения неправильных действий отмечены знаком ;
- сообщения, помеченные знаком , содержат информацию о важных особенностях, дополнительных возможностях или оптимальном использовании некоторых функций системы.

## Глава 1. Назначение подсистемы авторизации

Подсистема авторизации предназначена для формирования ответа на авторизационный запрос, поступающий из интерфейсных каналов NetServer, либо через адаптеры Transaction Switch (от платежных систем, сетей устройств, WEB-интерфейсов и т. д.).

Ответ на авторизационный запрос формируется по результатам выполнения следующих операций:

- аутентификации авторизационного запроса, выполняемой либо каналом авторизации NetServer, либо сервисом авторизации Transaction Switch с помощью информации, полученной из базы данных (БД); в процессе аутентификации, в частности, проверяются с помощью криптографического оборудования криптографические величины;
- проверки допустимости выполнения операции по параметрам контрактов-контрагентов, выполняемой на сервере БД и включающей в себя проверку Сервисов и ограничителей активности контрактов-контрагентов.

## Глава 2. Структура и компоненты подсистемы авторизации

Подсистема авторизации WAY4 включает в себя следующие компоненты (см. Рис. 1):

- Канал авторизации NetServer или адаптер Transaction Switch;
- Канал криптографического устройства NetServer или адаптер криптографического устройства Transaction Switch;
- Криптографическое устройство;
- Дополнительный канал авторизации NetServer или I-router Transaction Switch;
- Сервер БД системы WAY4, обеспечивающая ответы на запросы канала авторизации, либо сервиса авторизации и выполнение проверок в соответствии с алгоритмом обработки авторизационного запроса;
- Core Banking System (CBS), для которой обеспечивается онлайн-интерфейс с системой WAY4.

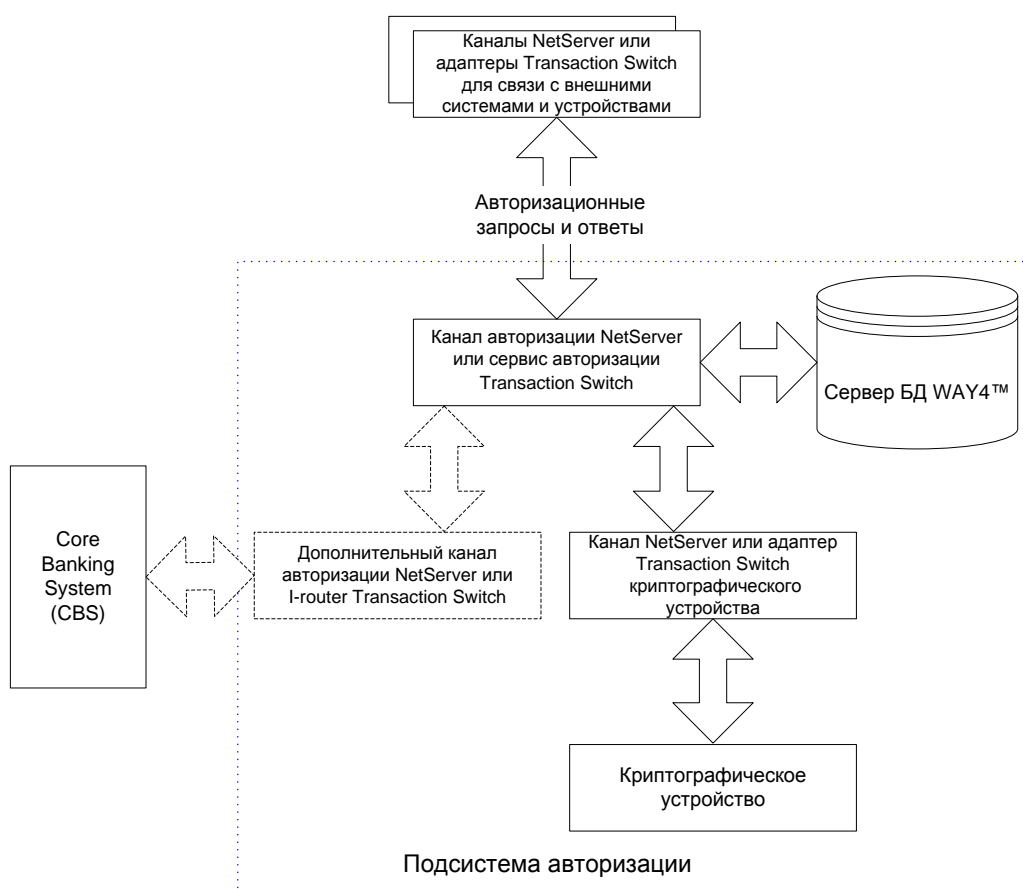


Рис. 1. Структура подсистемы авторизации

## Глава 3. Работа подсистемы авторизации

### Последовательность обработки авторизационного запроса

Последовательность обработки запроса подсистемой авторизации иллюстрируется на Рис. 2.

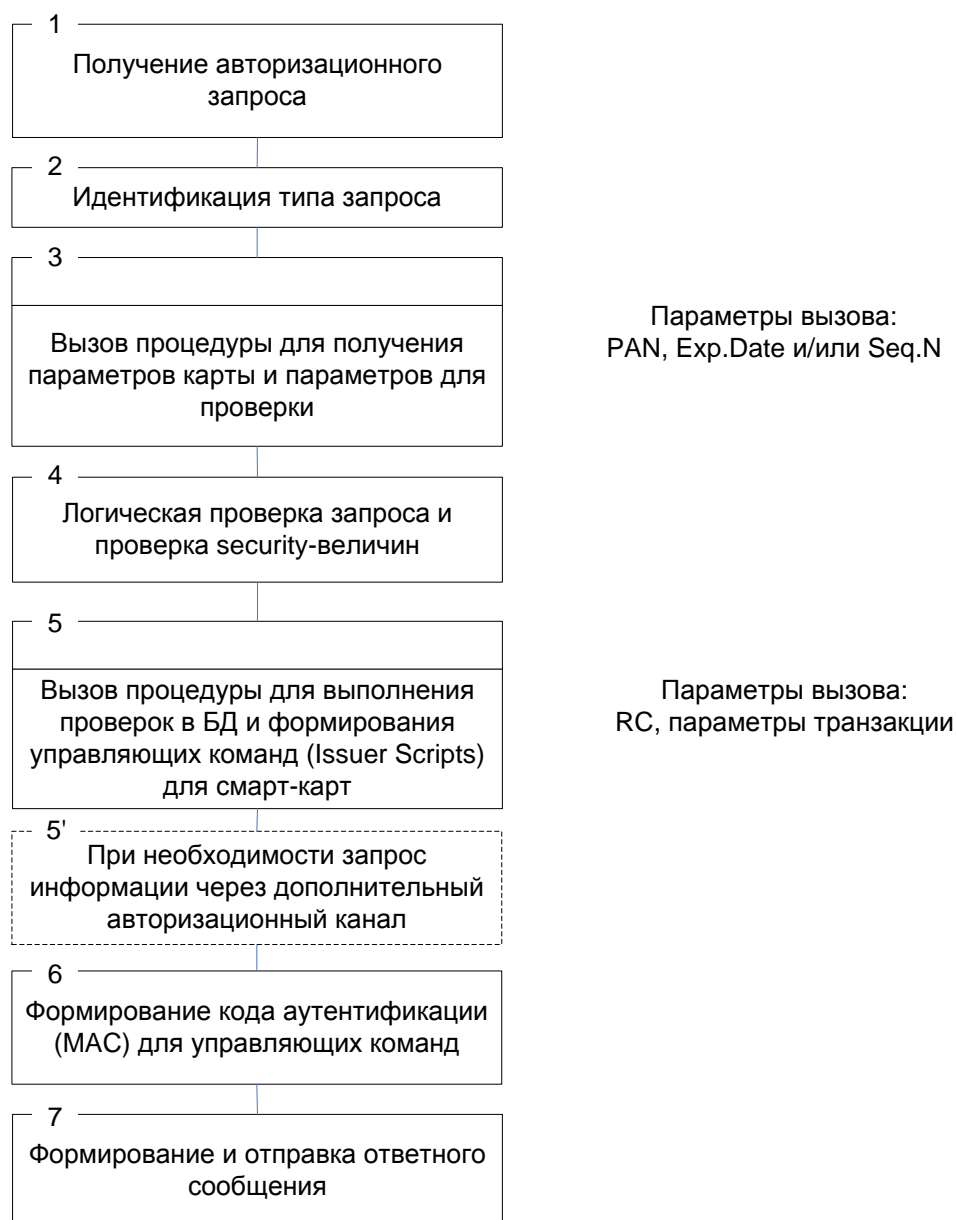


Рис. 2. Последовательность обработки авторизационного запроса

Алгоритм обработки авторизационного запроса состоит из следующих этапов, отмеченных номерами на Рис. 2.

1. Получение авторизационного запроса из интерфейсных каналов NetServer или через адаптеры Transaction Switch (от платежных систем, сетей устройств, WEB-интерфейсов и т. д.).
2. Идентификация типа запроса. Если запрос не был идентифицирован, формируется отрицательный ответ с кодом RC=57, и обработка запроса завершается.
3. Запрос к БД для получения параметров карты и параметров для проверки (validation) криптографических величин.
4. Логическая проверка запроса (проверка соответствия содержимого полей запроса друг другу) и проверка криптографических величин.
5. Обращение к БД для выполнения проверок допустимости выполнения операции и формирования управляющих команд (Issuer Scripts) для запросов по смарт-картам.
- 5'. При необходимости запрос информации, например, о сумме доступных средств, через дополнительный авторизационный канал или I-router Transaction Switch, в частности, к внешней системе (CBS). Подробнее см. функциональную спецификацию "WAY4™ CB Gate".
6. После получения ответа от БД формируется код аутентификации (MAC) управляющих команд, если они сформированы в п. 5.
7. Формируется ответное сообщение, которое передается в соответствующий интерфейсный канал NetServer или через адаптеры Transaction Switch.

## Обработка запроса каналом авторизации или сервисом авторизации

После идентификации типа авторизационного запроса и получения от БД параметров карты и параметров для проверки криптографических величин (см. п.п. 2 – 3 на Рис. 2 в разделе "Последовательность обработки авторизационного запроса") канал авторизации или сервис авторизации выполняет логическую проверку запроса и проверку криптографических величин.



Следует иметь в виду, что в случае если в ответе БД сообщается об отсутствии карты с запрошенным номером, канал авторизации или сервис авторизации не выполняет проверок, зависящих от параметров карты.

Логическая проверка запроса включает в себя следующие операции.

- Проверка числа Луна (Luhn digit) для запроса.
- Проверка наличия в запросе Processing Code.
- Проверка целостности данных 1-ой и 2-ой дорожки магнитной полосы (данная проверка выполняется с использованием параметров карты, содержащихся в ответе БД).
- Проверка соответствия Processing Code категории торговой точки (MCC) и типу карты, который сообщен базой данных.

- Проверка соответствия условий выполнения транзакции (Transaction Condition) категории торговой точки (например, транзакции на банкомате должны сопровождаться вводом PIN-кода).
- Проверка, что в запросе содержится ненулевая сумма и валюта транзакции для соответствующих типов операций.
- Проверка наличия в запросе определенных криптографических величин для соответствующих условий выполнения транзакции (CVV2/CVC2, данные магнитной полосы для чиповых транзакций, криптограммы и CVR для чиповых транзакций Full Grade, CAVV/UCAF для операций электронной коммерции 3-D Secure с сертификатом).
- Проверка наличия в запросе определенных криптографических величин (таких как PIN-блок, дата окончания срока действия карты) для соответствующих типов операций, например, запрос баланса должен сопровождаться вводом PIN-кода.

Проверки криптографических величин зависят от типа операции и параметров карты, полученных каналом авторизации из базы данных WAY4. С этим связаны следующие особенности их выполнения:

- авторизационный запрос может содержать признак предварительной проверки определенных криптографических величин сторонней (например, платежной) системой. Необходимость учитывать результаты данной проверки регулируется настройками системы WAY4, в частности с помощью опции "Trust to Prevalid. Rslt Sec.Val." (см. разделе "Параметры контроля подлинности" документа "Настройка параметров системы WAY4™ для выпуска карт с магнитной полосой").
- при выполнении операции установки нового PIN необходимость проверки его длины (относительно заданной в параметрах производства карт соответствующего типа) определяется с помощью опции "PIN Length Check" (возможные значения: "Y"/"N"). Порядок установки опций для параметров производства карт описан в документе "Настройка параметров системы WAY4™ для выпуска карт с магнитной полосой".

Проверки криптографических величин выполняются с использованием подключенного к NetServer или Transaction Switch криптографического оборудования (HSM).

В общем случае канал авторизации (NetServer) или сервис авторизации (Transaction Switch) выполняет следующие действия.

- Проверяет PIN-код, введенный в режиме онлайн, (с помощью HSM) или PIN-код, введенный в режиме офлайн (проверяется, признала ли карта указанный PIN-код).

Если значение PVV не хранится в БД, используется значение PVV, хранящееся на магнитной полосе карты (Track 2).

- Проверка криптограммы, полученной в запросе, и формирование ответной криптограммы (с помощью HSM). Ответная криптограмма



формируется, если все проверки были выполнены успешно, и сохраняется до получения ответа по результатам проверок в БД.

- Алгоритмическая проверка величин CVR, TVR. Алгоритм проверки задается в БД и передается в ответе на запрос канала авторизации о параметрах карты (см. п.3 на Рис. 2 в разделе "Последовательность обработки авторизационного запроса").
- Проверка с использованием HSM величин DAC/DN. Данные проверки могут быть отключены параметрами конфигурации авторизационного канала.



Параметры конфигурации в данном документе не описываются. Изменение указанных параметров может выполняться только представителями поставщика системы.

- Проверка с использованием HSM величин CAVV/UCAF.
- Проверка с использованием HSM величин CVV/ICVV, если данная проверка предусмотрена в БД.
- Проверка величин CVV2/CVC2 с помощью HSM.
- Проверки специальных криптографических величин, предусмотренные конфигурацией канала авторизации конкретного банка или процессингового центра.
- Запрос к БД, выполняемый как при положительном, так и при отрицательном результате проверок запроса, выполненных каналом авторизации. При отрицательном результате проверки запрос к БД выполняется, в частности, для протоколирования результатов авторизации (создания авторизационного документа). Проверки, выполненные на БД, могут изменить в худшую сторону код ответа.

В запросе (см. п. 5 на Рис. 2 в разделе "Последовательность обработки авторизационного запроса") к базе данных для дальнейшей проверки передается предварительный код ответа и параметры транзакции. О проверке в БД см. раздел "Обработка запроса на сервере базы данных WAY4".

Настройкой подсистемы может быть предусмотрен запрос информации через дополнительный канал авторизации, например, запрос суммы доступных средств контракта в сторонней системе.

После получения ответа из БД и по дополнительному каналу авторизации канал авторизации выполняет следующие действия.

- Формирует криптографические величины с помощью HSM:
  - Код аутентификации (MAC) управляющих команд (Issuer Scripts) для запросов по смарт-картам.
  - Ответную криптограмму для запросов по смарт-картам, если код ответа не равен "00". Если ответ положительный, используется ответная криптограмма, сформированная ранее, до запроса БД.
- Формирует и отправляет ответное сообщение.

## Обработка запроса на сервере базы данных WAY4

Обработка авторизационного сообщения в БД системы WAY4 выполняется в соответствии с запросами канала авторизации в два этапа.

I. Первый этап обеспечивает получение каналом авторизации параметров карты и параметров для проверки (validation) криптографических величин (см. п.3 на Рис. 2 в разделе "Последовательность обработки авторизационного запроса").

В БД WAY4 осуществляется поиск действующего контракта и актуальных сведений о пластиковой карте в соответствии с параметрами запроса.

Если для нечиповой транзакции имеется несколько записей о пластиковой карте с одинаковым сроком действия (например, о заблокированной и разблокированной картах вследствие перевыпуска), выбираются сведения о разблокированном пластике.

В ответе на запрос канала авторизации может возвращаться отрицательный код ответа по следующим причинам:

- не обнаружен контракт для данного номера карты;
- для данного номера карты нет пластика с указанным в запросе сроком действия;
- для данного номера карты не обнаружен набор параметров контроля криптографических величин.

Если указанные проверки выполнены успешно, возвращается информация для контроля криптографических величин. Соответствующие данные содержатся в таблице PM\_PARMS (Full → Configuration Setup → Card Production Setup → Bank Production Parameters-> [Validation]) для диапазона номеров, в который попадает номер карты, и значения PM Code, хранящегося для карты в таблице CARD\_INFO (форма "Plastics for...", вызываемая из формы карточного контракта нажатием на кнопку [Plastics]).

II. Второй этап обработки запроса (см. п. 5 на Рис. 2 в разделе "Последовательность обработки авторизационного запроса") включает в себя собственно проверки, выполняемые для авторизационного запроса в БД.

На этом этапе в БД выполняются следующие действия.

- Идентификация типа транзакции, в том числе с учетом кода MCC.
- Создание документа с кодом ответа (RC), присланным каналом авторизации.
- Регистрация результатов выполнения предыдущей управляющей команды (Issuer Script) и данных о тратах в режиме офлайн для смарт-карт. Выполняется поиск карточного контракта, по которому была выпущена карта, и для которого были сформированы управляющие команды, в то время как сам авторизационный запрос может относиться к другому контракту (related).

- Поиск оригинального документа для вторичных документов (Reversal, Adjustment, Advice).

Обработка авторизационных уведомлений (Authorisation Advice), получение которых возможно при делегировании платежной системе права выполнять авторизацию за эмитента, представлена на Рис. 3.

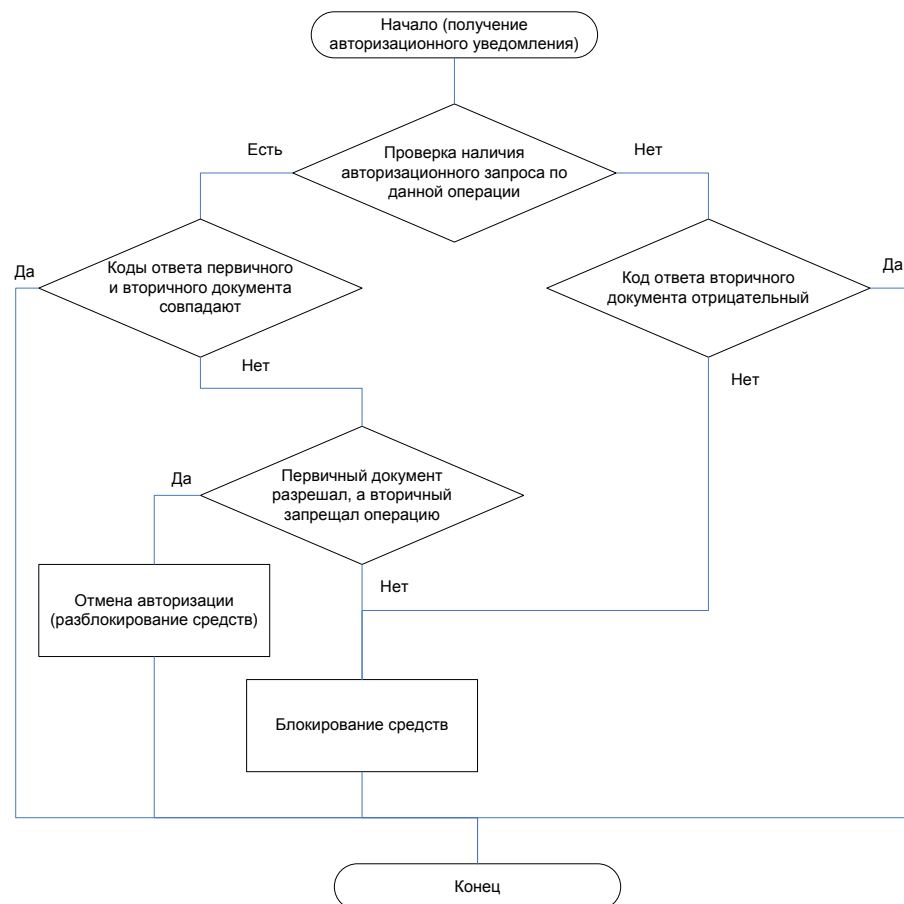


Рис. 3. Алгоритм обработки авторизационных уведомлений

- Обработка счетчика попыток ввода неправильного PIN-кода для транзакций, выполняемых с вводом PIN-кода (PBT). При этом выполняется обнуление счетчика, если канал авторизации сообщил о том, что введенный PIN-код правильный и содержимое счетчика не превышает максимально допустимого значения. Если PIN-код неправильный, содержимое указанного счетчика увеличивается на "1".
- Проверка присланного в запросе адреса (Address verification), например, при обработке запроса по Internet-транзакции.
- Проверка контракта-получателя, включающая проверку срока действия пластика, статуса контракта и его даты закрытия.
- Проверка стоп-листа торговцев (Full → Stop List → Merchant Stop List), стоп-листа карт (Full → Stop List → Card Stop List) и стоп-листа клиентов (Full → Stop List → Client Stop List).
- Расчет комиссий в соответствии с параметрами найденного для контракта-получателя Сервиса по операции данного типа.

- Конвертация суммы транзакции и суммы комиссии в валюту контракта.
- Проверки ограничителей активности контракта (Usage Limiters).
- Блокирование средств контракта или их разблокирование при обработке вторичного авторизационного документа (см. раздел "Изменение доступных средств контракта").
- Формирование кода авторизации (6-разрядное число, не начинающееся с "0").
- Формирование мини-выписки, если это предусмотрено запросом, и определение балансов контракта.
- Открытие Событий и формирование сообщений, например, для оповещения держателя карты о выполнении авторизации.
- Формирование управляющих команд эмитента (Issuer Scripts) и кода ответа криптограммы (ARPC RC) для операций по смарт-картам с использованием чипа.
- Сохранение авторизационного документа, дополненного полученными в процессе обработки данными (уточненный код ответа, идентификатор карточного контракта и т. д.).
- Передача ответа каналу авторизации для завершения обработки запроса (см. "Обработка запроса каналом авторизации").

В ответе каналу авторизации передается код ответа (RC), баланс контракта, мини-выписка (если это предусмотрено запросом), управляющие команды для смарт-карты и др.



Следует иметь в виду, что в ответ на авторизационные запросы с такими значениями категории запроса/уведомления, как "Reversal", "Adjustment", "Advice" сервер БД передает код положительного ответа (RC=00) независимо от того, какой код ответа указан в сформированном авторизационном документе по результатам проверки.

## Изменение доступных средств контракта

В результате обработки авторизационного сообщения формируются записи по изменению доступных средств контакта (таблица Credit\_History). Изменение суммы доступных средств контракта зависит от типа и статуса авторизационного сообщения.

Типы авторизационных сообщений:

- "In Pending" – блокирование средств контракта, имеющихся на момент обработки операции.
- "By Usage" – разрешение операции, при обработке которой используется ограничитель с типом "Overdraft" и/или обработка операции в режиме "Stand-In Processing" ("STIP"). Часть суммы блокируется за счет имеющихся доступных средств, оставшаяся часть – за счет ограничителя.

- "Credit Limit" – назначение/изменение кредитного лимита.
- "Additional Cr Limit" – назначение/изменение дополнительного кредитного лимита.
- "Offline Used" – средства, потраченные в режиме офлайн.
- "Offline Blocked" – средства, заблокированные для проведения операций в режиме офлайн.
- "Offline Presentment" – информация о средствах, потраченных в режиме офлайн, получена после обработки подтверждающего финансового документа.
- "Offline Increment" – изменение объема средств, доступных для использования в режиме офлайн по данной карте, если по карте обрабатывается онлайн-операция.
- "Offline Total Used" – техническая запись; используется при обработке операций в решении "WAY4™ Pre-Authorized Debit".
- "Balance Inquiry" – запрос баланса контракта.
- "Statement" – запрос мини-выписки.
- "Additional Online Service" – дополнительная онлайн-операция.
- "Accounting" – бухгалтерские операции между счетами (контрактами).
- "Ineffective" – служебные операции, например, операции типа "Note Acceptance" – запросы на выполнение операции приема наличных от держателя банковской карты. Назначение такого запроса состоит только в том, чтобы проверить разрешена ли данная операция эмитентом; доступные средства контракта при этом не изменяются.
- "Verification" – верификация банковской карты.
- "When Available" – комиссия взимается при наличии доступных средств с учетом кредитного лимита
- "When Credit" – комиссия взимается при наличии доступных средств без учета кредитного лимита.

Статусы авторизационных сообщений:

- "Active" – финансовый документ по данной операции отсутствует или не обработан, блокировка средств активна.
- "Declined" – операция отклонена.
- "Matched" – операция подтверждена после обработки финансового документа.
- "Reversed" – операция отменена.
- "Closed" – блокировка закрыта вручную или по истечении времени.
- "Waiting" – статус для нефинансовой операции, ожидающей обработки.

- "Processed" – блокировка средств по офлайн-операции активна; данный статус авторизация получает после обработки соответствующего финансового документа.
- "Inactive" – блокировка не активна; не влияет на доступные средства контракта.
- "History" – значение зарезервировано, в текущей версии не используется.
- "Erased" – значение используется в тестовом режиме при принудительном изменении баланса.

## Просмотр условий аутентификации по протоколу 3-D Secure

Для удобства обработки обращений клиентов, например при обработке претензионных дел, предоставляется возможность просмотра условий аутентификации для операций электронной коммерции.

В форме "All Docs" следует выбрать документ, сформированный в результате авторизационного запроса (см. Рис. 4.), пункт меню "Full → Documents Input & Update → Doc - General Form → All Docs → [Auth Record]".

The screenshot shows the 'All Docs' window with a table of documents. The 'Auth Record' tab is active. In the bottom navigation bar, the '3D Data' button is highlighted with a red box.

Рис. 4. Авторизационный документ

С помощью кнопки [3D Data] открыть форму "3D Data for Auth Record" (см. Рис. 5).

The screenshot shows the '3D Data for Auth Record for All Docs' form. It contains a table with the following data:

Date	Type	Card number	3-D Secure XID	Amount	Currency	Status
12/05/17 12:17:10	TDS	4015500181722293	I4W2dkohM0VePF7/ePKuWWhrmE3o=	100,00	USD	Waiting

Below the table, there are buttons for 'Query', '3DS Tags', and 'RBA Tags'.

Рис. 5. Условия аутентификации по протоколу 3-D Secure

Описание полей:

- *Date* – дата и время формирования запроса на аутентификацию плательщика.
- *Type* – тип аутентификации; TDS – 3-D Secure.
- *Card number* – номер карты, с помощью которой осуществляется операция.

- *3-D Secure XID* – идентификатор обмена данными, позволяющий связать запрос на аутентификацию плательщика (PAREq) с ответом на данный запрос (PAREs). Идентификатор формируется торговцем в соответствии с принятыми правилами кодировки и включается в авторизационный запрос (PAREq).

PAREq – запрос аутентификации плательщика (Payer Authentication Request) представляет собой запрос эмитенту о возможности проведения покупки по данной карте.

Данный запрос генерируется торговой точкой, но поступает на ACS-сервер непосредственно через браузер держателя карты (в составе HTTP-POST запроса), т.е. получение PAREq свидетельствует о том, что соединение между держателем карты и ACS-сервером установлено.


PAREs – ответ на запрос аутентификации плательщика (Payer Authentication Response). Формируется, как результат обмена аутентификационной информацией между эмитентом и держателем карты. Данным сообщением эмитент подтверждает (или не подтверждает) свое разрешение на проведение покупки. Сообщение транслируется торговой точке через браузер держателя карты.

- *Amount* – сумма операции.
- *Currency* – валюта операции.
- *Status* – статус запроса (описание статусов авторизаций см. в разделе Изменение доступных средств контракта).

Условия аутентификации помещается в поле *Add Info* авторизационного документа в виде тегов. Перечень тегов и их значений доступен в форме "3DS Tags for 3D Data for Auth Record". Форма открывается с помощью кнопки [3DS Tags] в форме "3D Data for Auth Record" (см. Рис. 6).

3DS Tags for 3D Data for Auth Record for All Docs							<< < > >>		1 of 8	b	x
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-g00jhPcw	Tag Present	Unknown		Ready					
80	RC	Y	Tag Present	Unknown		Ready					

Рис. 6. Теги запроса аутентификации

 Данная функциональность доступна только для авторизации на платформе WAY4 Transaction Switch.