Режим SilentPay

- Передача параметров платежа
- Дополнительные параметры (для СПМ)
- 3D-Secure авторизация
  - 3D-Secure авторизация по протоколу версии 1
  - 3D-Secure авторизация по протоколу версии 2

Скрытый режим платежа, при котором все данные о заказе, о покупателе, о способе оплаты и платежном средстве передаются непосредственно предприятием, может быть выполнен с использованием карты или токена.

Передача параметров платежа

Для работы в данном режиме предусмотрен web-сервис *silentpay*.

URL запроса для скрытого режима оплаты:

https://<SERVER-NAME>/pay/silentpay.cfm

Параметры передаются методом POST в теле запроса в формате «ключ=значение», SOAP запросом, либо в формате JSON (swagger описание: https://docs.belassist.by/swagger/).

Список параметров, передаваемых в режиме silentpay:

Название	**Обязательное поле**	**Принимаемые значения**	**Значение по умолчанию**	**Описание**
Merchant_ID	Да	Число		Идентификатор предприятия в системе АПК Ассист
Login	Да	Строка		Ваш логин
Password	Да	Строка		Ваш пароль
OrderNumber	Да /Нет	128 символов		Номер заказа в системе расчетов предприятия.
OrderAmount	Да	Число, 15 цифр (разделители «.», «,»)		Сумма платежа в оригинальной валюте (например, 10.34)
OrderCurrency	Нет	3 символа	Валюта юр.лица или предприятия	Код валюты, в которой указана сумма платежа OrderAmount (RUB, USD, EUR)
OrderComment	Нет	4000 символов		Комментарий
Delay	Нет	0 – одностадийный механизм работы, 1- двустадийный механизм	0	Признак авторизации банковской карты при двустадийном механизме работы
Language	Нет	RU – русский EN - английский	Язык юр. лица или предприятия	Язык авторизационных страниц
ClientIP	Нет /Да			IP адрес покупателя. Параметр является обязательным для протокола 3-D Secure версии 2.

Cardtype	Нет	1 – VISA 2 - EC/MC 3 – DCL 4 – JCB 5- AMEX 6 - MIR		Идентификатор типа карты для оплаты.
Cardnumber	Да			Номер карты
Cardholder	Да	70 символов без цифр. Разделитель – пробел.		Держатель карты.
Expiremonth	Да	1-12		Месяц окончание действия карты
Expireyear	Да	Год в формате YYYY		Год окончания действия карты
Cvc2	Да			CVC2 код
Lastname	Да	70 символов без цифр		Фамилия покупателя
Firstname	Да	70 символов без цифр		Имя покупателя
Middlename	Нет	70 символов без цифр		Отчество покупателя
Email	Да	128 символов		E-mail покупателя
Address	Нет	256 символов		Адрес покупателя
HomePhone	Нет	64 символа		Домашний телефон покупателя
WorkPhone	Нет	20 символов		Рабочий телефон покупателя
MobilePhone	Нет	20 символа		Мобильный телефон покупателя
Fax	Нет	20 символа		Факс покупателя
Country	Нет	3 символа		Код страны покупателя
State	Нет	3 символа		Код региона покупателя
City	Нет	70 символа		Город покупателя
Zip	Нет	25 символа		Индекс предприятия связи покупателя
isConvert	Нет	0 - Не конвертировать в базовую валюту 1 - Не конвертировать при возможности 2 - Всегда конвертировать	1	Флаг конвертации валюты платежа в базовую валюту
Format	Нет	1 – CSV 3 – XML 4 – SOAP 5 - JSON	1	Формат выдачи результата. Если запрос передан в формате SOAP, то ответ также будет в SOAP, в остальных случаях в соответствии с переданным значением формата.

Signature	Нет	строка		Формируется строка по определенным правилам. На базе этой строки алгоритмом MD5 формируется дайджест. Дайджест подписывается закрытым RSA ключом мерчанта. Длина ключа - 1024. Полученная байтовая последовательность является подписью магазина. Подпись передается нам в виде дополнительного параметра, закодированного в виде строки BASE64. **Внимание!** Параметр необходим для того, чтобы обезопасить передаваемые данные от возможности их подмены злоумышленниками. Следует также включить настройку проверки кода или подписи в ЛК.
RecurringIndicator	Нет	1 – рекуррентный платеж 0 - обычный платеж	0	Признак рекуррентного платежа
RecurringMinAmount	Нет /Да	Число, 15 цифр (разделители «.», «,»)		Минимальная сумма рекуррентных платежей. Параметр обязателен при RecurringIndicator = 1
RecurringMaxAmount	Нет /Да	Число, 15 цифр (разделители «.», «,»)		Максимальная сумма рекуррентных платежей. Параметр обязателен при RecurringIndicator = 1
RecurringPeriod	Нет /Да	Число, 10 цифр		Периодичность рекуррентных платежей в днях. Параметр обязателен при RecurringIndicator = 1
RecurringMaxDate	Нет /Да	Строковое представление даты в формате DD.MM.YYYY		Дата окончания рекуррентных платежей. Параметр обязателен при RecurringIndicator = 1
CustomerNumber	Нет	32 символа		Внутренний номер клиента предприятия (мерчанта)
SaveCard	Нет	1 – карта привязывается к данному номеру клиента; 0 – карта не привязывается	0	В случае успешного платежа разрешает сохранять карту по данному номеру клиента для последующих платежей. Если карта для данного номера клиента уже была сохранена ранее, то параметр игнорируется.
Disable3DS	Нет	0 – проверять 3-D Secure согласно настройкам предприятия, 1 – проводить платеж без 3-D Secure.	0	Признак отключения 3-D Secure. Использование такого режима работы возможно по согласованию с Assist. Для настройки необходимо обратиться в службу технической поддержки support@belassist.by При использовании параметра его необходимо добавлять и в подпись заказа, которая формируется по определенным правилам.

Пример запроса HTTP POST проведения платежа в скрытом режиме silentpay:

```
<FORM ACTION="https://SERVER-NAME/pay/silentpay.cfm " method="POST">
<INPUT TYPE="hidden" NAME="Merchant_ID" VALUE=" Merchant_ID">
<INPUT TYPE="hidden" NAME="Login" VALUE=" ">
<INPUT TYPE="hidden" NAME="Password" VALUE=" ">
<INPUT TYPE="hidden" NAME="OrderNumber" VALUE="011001-10">
<INPUT TYPE="hidden" NAME="OrderAmount" VALUE="22">
<INPUT TYPE="hidden" NAME="OrderCurrency" VALUE="BYN">
<INPUT TYPE="hidden" NAME="OrderComment" VALUE="  011001-10">
<INPUT TYPE="hidden" NAME="Delay" VALUE="0">
<INPUT TYPE="hidden" NAME="isConvert" VALUE="1">
<INPUT TYPE="hidden" NAME="Language" VALUE="RU">
<INPUT TYPE="hidden" NAME="ClientIP" VALUE="IP  ">
<INPUT TYPE="hidden" NAME="Cardtype" VALUE=" ">
<INPUT TYPE="hidden" NAME="Cardnumber" VALUE=" ">
<INPUT TYPE="hidden" NAME="Cardholder" VALUE=" ">
<INPUT TYPE="hidden" NAME="Expiremonth" VALUE="   - ">
<INPUT TYPE="hidden" NAME="Expireyear" VALUE="    - ">
<INPUT TYPE="hidden" NAME="Cvc2" VALUE=" CVC2  CVV2">
<INPUT TYPE="hidden" NAME="Lastname" VALUE=" ">
<INPUT TYPE="hidden" NAME="Firstname" VALUE=" ">
<INPUT TYPE="hidden" NAME="Middlename" VALUE=" ">
<INPUT TYPE="hidden" NAME="Email" VALUE="Email ">
<INPUT TYPE="hidden" NAME="Address" VALUE="  ">
<INPUT TYPE="hidden" NAME="Homephone" VALUE="  ">
<INPUT TYPE="hidden" NAME="Workphone" VALUE="  ">
<INPUT TYPE="hidden" NAME="Mobilephone" VALUE="  ">
<INPUT TYPE="hidden" NAME="Fax" VALUE=" ">
<INPUT TYPE="hidden" NAME="Country" VALUE="">
<INPUT TYPE="hidden" NAME="State" VALUE="">
<INPUT TYPE="hidden" NAME="City" VALUE="">
<INPUT TYPE="hidden" NAME="Zip" VALUE="  ">
<INPUT TYPE="hidden" NAME="TestMode" VALUE=" ">
<INPUT TYPE="hidden" NAME="Format" VALUE="  ">
<INPUT TYPE="Submit"></FORM>
```

Описание веб-сервиса для формата SOAP:

https://<SERVER-NAME>/pay/silentpay.wsdl

Список возвращаемых параметров:

Название	**Значение**
ordernumber	Номер заказа
billnumber	Полный уникальный номер операции в системе
testmode	Тестовый режим
ordercomment	Комментарий
orderamount	Оригинальная сумма заказа
ordercurrency	Оригинальная валюта заказа
amount	Сумма операции
currency	Валюта операции

rate	Курс валюты
firstname	Имя плательщика
lastname	Фамилия плательщика
middlename	Отчество плательщика
email	Email плательщика
ipaddress	IP-адрес плательщика
meantypename	Тип платежного средства
meansubtype	Подтип платежного средства
meannumber	Номер платежного средства
cardholder	Держатель платежного средства
cardexpirationdate	Срок действия карты
issuebank	Название банка-эмитента
bankcountry	Страна банка-эмитента
orderdate	Дата заказа по Гринвичу (GMT)
orderstate	Статус заказа
responsecode	Код возврата
message	Сообщение
customermessage	Сообщение о результате для покупателя
recommendation	Рекомендации
approvalcode	Код авторизации
protocoltypename	Протокол
processingname	Процессинг
operationtype	Тип операции
packetdate	Дата формирования запроса по Гринвичу (GMT)

signature	Подпись. Создается по следующему алгоритму: 1. Формируется объединённая строка из параметров (в их строковом представлении, в формате как они переданы в ответе): *billnumber, ordernumber, responsecode, orderamount, ordercurrency, meannumber, approvalcode, orderstate, packetdate* (без разделителей) 2. Полученная строка подписывается закрытым ключом АПК Ассист. 3. Итоговая последовательность байт кодируется в BASE64.
pareq	Пакет запроса по 3D-Secure авторизации
ascurl	Адрес для переадресации плательщика для прохождения 3D-Secure авторизации

При использовании сервиса имеются ограничения по производительности.

Результат запроса в зависимости от выбранного формата получения будет выглядеть одним из следующих образов.

В формате CSV:

```
:   : .… :
```

В формате XML:

```
<?xml version='1.0' encoding='UTF-8' standalone='yes'?>
<!DOCTYPE result [
<result firstcode=' ' secondcode=' ' count='- '>
<orders><order>
<ordernumber> </ordernumber>
<responsecode> </responsecode>
<recommendation></recommendation>
<message></message>
<ordercomment></ordercomment>
<orderdate>   </orderdate>
<amount> </amount>
<currency> </currency>
<meantypename> </meantype>
<meannumber> </meannumber>
<lastname></lastname>
<firstname></firstname>
<middlename></middlename>
<issuebank> -</ issuebank >
<email>   </email>
<bankcountry>  -</bankcountry>
<rate> </rate>
<approvalcode> </approvalcode>
<meansubtype> </meansubtype>
<cardholder> </cardholder>
<cardexpirationdate>  </cardexpirationdate>
<ipaddress>IP- </ipaddress>
<protocoltypename> </protocoltypename>
<testmode>   </ testmode >
<customermassage>  </customermassage >
<orderstate></orderstate>
<processingname> </ processingname>
<operationtype> </operationtype>
<billnumber> </billnumber>
<orderamount>     </orderamount>
<ordercurrency>  </ordercurrency>
<paketdate>      </paketdate>
<signature> </signature>
<pareq> pareq </pareq>
<ascurl>URL - </ascurl>
</order></orders></result>
```

В формате SOAP:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ws="http://www.paysecure.ru/ws
/">
<soapenv:Header/>
<soapenv:Body>
<ws:SilentPayResponse>
<return>
<ordernumber xsi:type="xsd:string"> </ordernumber>
<responsecode xsi:type="xsd:string"> </responsecode>
<recommendation xsi:type="xsd:string"></recommendation>
<message xsi:type="xsd:string"></message>
<ordercomment xsi:type="xsd:string"></ordercomment>
<orderdate xsi:type="xsd:string">   </orderdate>
<amount xsi:type="xsd:string"> </amount>
<currency xsi:type="xsd:string"> </currency>
<meantypename xsi:type="xsd:string"> </meantype>
<meannumber xsi:type="xsd:string"> </meannumber>
<lastname xsi:type="xsd:string"></lastname>
<firstname xsi:type="xsd:string"></firstname>
<middlename xsi:type="xsd:string"></middlename>
<issuebank xsi:type="xsd:string"> -</ issuebank >
<email xsi:type="xsd:string">   </email>
<bankcountry xsi:type="xsd:string">  -</bankcountry>
<rate xsi:type="xsd:string"> </rate>
<approvalcode xsi:type="xsd:string"> </approvalcode>
<meansubtype xsi:type="xsd:string"> </meansubtype>
<cardholder xsi:type="xsd:string"> </cardholder>
<cardexpirationdate xsi:type='xsd:string'>  </cardexpirationdate>
<ipaddress xsi:type="xsd:string">IP- </ipaddress>
<protocoltypename xsi:type="xsd:string"> </protocoltypename>
<testmode xsi:type="xsd:string">   </ testmode >
<customermassage xsi:type="xsd:string"> </customermassage >
<orderstate xsi:type="xsd:string"></orderstate>
<processingname xsi:type="xsd:string"> </processingname>
<operationtype xsi:type="xsd:string"> </operationtype>
<billnumber xsi:type="xsd:string"> </billnumber>
<orderamount xsi:type="xsd:string">     </orderamount>
<ordercurrency xsi:type="xsd:string"> </ordercurrency>
<paketdate xsi:type="xsd:string">    </paketdate>
<signature xsi:type="xsd:string"> </signature>
<pareq xsi:type="xsd:string"> pareq </pareq>
<ascurl xsi:type="xsd:string">URL - </ascurl>
</return>
</ws:SilentPayResponse>
</soapenv:Body>
</soapenv:Envelope>
```

В случае успешной оплаты код возврата *responsecode* принимает значение AS000.

В случае неуспешной оплаты responsecode принимает значения AS100-AS998 (кроме специального кода AS110, если необходима авторизация по 3-D Secure, подробнее см. здесь).

Если запрос на оплату не может быть обработан, в результате вернутся ненулевые значения параметров firstcode, secondcode.

Если в ответе получен responsecode AS300, а статусы заказа (*orderstate*) и операции (*operationstate*) - *In Process* (В процессе), то актуальный статус оплаты можно получить позже через запрос к сервису получения результатов *orderresult*.

Если результат оплаты не получен (например, вследствие сетевых проблем), то его можно получить позже через запрос к сервису *orderresult*.

Пример результата запроса в формате XML, вернувшего ошибку (неправильный пароль):

```
<?xml version="1.0" encoding="utf-8" standalone="yes" ?>
  <!DOCTYPE result [...]>
  <result firstcode="7" secondcode="102" count="0"></result>
```

С описанием первого и второго кодов ошибок можно ознакомиться здесь.

Предприятие может также инициировать предоставление услуг по подписке для платежей, проводимых через процессинг UCS.

Дополнительные параметры (для СПМ)

Для магазинов, работающих по режиму *silentpay*, есть возможность передавать расширенные данные о клиенте для использования их системой противодействия мошенничеству.

Дополнительно к основному списку параметров, передаваемых в режиме *silentpay*, магазин может передать следующие необязательные параметры:

Название	**Принимаемые значения**	**Описание**
HEADER_HTTP_USER_AGENT	Строковый (255 байт)	Заголовок http запроса USER-AGENT
HEADER_HTTP_ACCEPT	Строковый (255 байт)	Заголовок http запроса ACCEPT
HEADER_HTTP_ACCEPT_LANGUAGE	Строковый (128 байт)	Заголовок http запроса ACCEPT-LANGUAGE
HEADER_HTTP_REFERER	Строковый (255 байт)	Заголовок http запроса REFERER
HEADER_REMOTE_HOST	Строковый (16 символов)	Переменная окружения REMOTE_ADDRESS.
HEADER_HTTP_FORWARDED	Строковый (16 байт)	Заголовок http запроса FORWARDED
HEADER_HTTP_X_FORWARDED_FOR	Строковый (16 байт)	Заголовок http запроса FORWARDED-FOR
HEADER_HTTP_VIA	Строковый (128 байт)	Заголовок http запроса VIA
CLIENT_JS_VER	Строковый (16 символов)	при помощи JS
CLIENT_LOCAL_TIME	Строковый (128 символов)	при помощи JS
CLIENT_SCREEN_RES	Строковый (16 символов)	Screen.width + 'x' + screen.height
CLIENT_SCREEN_COLORS	Числовой (15)	Screen.pixelDepth
CLIENT_JS_BROWSER_NAME	Строковый (255 символов)	navigator.appName
CLIENT_TIME_ZONE	Числовой (5)	Временная зона в часах. Формула перевода: (-GMT_H). Например, GMT +2 будет соответствовать значению -2.
CLIENT_COOKIES	Строковый (16 символов)	
CLIENT_JAVA	Логическое (true, false)	navigator.javaEnabled()
CLIENT_STYLESHEETS	Логическое (true, false)	Document.stylesheet.disabled
CLIENT_BROWSER_PLATFORM	Строковый (64 символа)	navigator.platform
CLIENT_SYSTEM_LANGUAGE	Строковый (5 байт)	navigator.systemLanguage
CLIENT_BROWSER_LANGUAGE	Строковый (5 байт)	navigator. language
CLIENT_USER_LANGUAGE	Строковый (5 байт)	navigator. userLanguage
CLIENT_PROCESSOR	Строковый (16 символов)	navigator.cpuClass

CLIENT_CONNECTION	Строковый (16 символов)	navigator.connectionType
CLIENT_HOSTADDRESS	Строковый (16 символов)	Вычисленный на базе HOST_ADDRESS и DNS lookup
CLIENT_HOSTNAME	Строковый (70 символов)	Переменная окружения HOST_ADDRESS

3D-Secure авторизация

Для магазинов, работающих по режиму silentpay, реализована возможность оплаты по картам, требующим 3D-Secure авторизации (в случае, если у магазина и процессинга выполнены соответствующие настройки).

При оплате картой, требующей авторизации по 3D-Secure, АПК Ассист возвращает код ответа (responsecode) AS110. В пакет ответа по режиму *silentpay* также добавляются дополнительные поля, позволяющие ТСП обеспечить дополнительную аутентификацию плательщика по технологиям 3-D Secure (карты VISA) и Mastercard SecureCode (карты Mastercard).

В настоящее время для дополнительной аутентификации плательщика большинство банков-эмитентов работает по версии 1 протокола 3-D Secure по всем типам карт.

Для более надежного процесса аутентификации банки-эмитенты и платежные системы переходят на новую версию 2 и выше протокола для всех типов карт (VISA, Mastercard). Для поддержки протокола нового поколения предприятию нужно внести изменения в процесс аутентификации плательщика.

Для начала оплаты заказа предприятие отправляет авторизационный запрос на сервер АПК Ассист. К обычным параметрам запроса необходимо добавить следующие данные об устройстве и браузере клиента, если это еще не было сделано ранее для работы с СПМ. В новом протоколе 3-D Secure версии 2 эти данные являются обязательными.

Название	**Принимаемые значения**	**Описание**
HEADER_HTTP_ACCEPT	Строка, 255 байт	Заголовок http запроса ACCEPT
HEADER_HTTP_USER_AGENT	Строка, 255 байт	Заголовок http запроса USER-AGENT
CLIENT_JAVA	Логическое (true, false)	navigator.javaEnabled()
CLIENT_BROWSER_LANGUAGE	Строковый (5 байт)	navigator. language
CLIENT_SCREEN_COLORS	Числовой (1, 4,8,15,16,24,32,48)	Screen.pixelDepth
CLIENT_SCREEN_RES	Строковый, 16 символов	Screen.width + 'x' + screen.height
ChallengeWindowSize	2 символа (01 – 250x400, 02 – 390x400, 03 – 500x600, 04 – 600x400, 05 – Full screen)	Размер iframe для прохождения проверки держателя карты
ClientIP	Максимум 15 цифр, 4 разделителя «.»	IP адрес покупателя

3D-Secure авторизация по протоколу версии 1

При оплате картой, требующей авторизации по протоколу версии 1, АПК Ассист возвращает код ответа (responsecode) AS110 и дополнительные поля pareq и acsurl в ответе на запрос авторизации.

Клиент должен быть перенаправлен на сайт банка-эмитента по адресу, указанному в параметре acsurl (acsurl - значение, полученное в пакете результата режима silentpay от АПК Ассист).

В форме должны содержаться следующие поля:

AcsUrl	Url банка-эмитента. Значение, полученное в пакете результата режима silentpay от АПК Ассист.

PaReq	Значение, полученное в пакете результата режима silentpay от АПК Ассист.
Term Url	Url магазина для получения результата от банка эмитента.
MD	Идентификатор, по которому в дальнейшем связывается результат, полученный от банка, и заказ. Данное поле возвращается от банка эмитента.

Пример запроса HTTP POST к банку-эмитенту:

```
<FORM ACTION="acsurl - ,        silentpay" method="POST">
<INPUT TYPE="hidden" NAME="PaReq" VALUE="pareq - ,        silentpay ">
<INPUT TYPE="hidden" NAME="TermUrl" VALUE="url      -">
<INPUT TYPE="hidden" NAME="MD" VALUE="  ">
<INPUT TYPE="submit" NAME="Submit_3DS" class="button" VALUE="">
</FORM>
```

Банк-эмитент возвращает следующие поля:

PaRes	Пакет результата
MD	Идентификатор, введенный ранее

Для продолжения процесса авторизации по 3D-Secure магазину необходимо передать в АПК Ассист пакет результата авторизации по 3D-Secure pares. Данная функциональность реализована в веб-сервисе get3DSec.

Get3DSec – веб-сервис передачи параметров авторизации карты по 3D-Secure

URL для передачи запроса:

https://<SERVER-NAME>/get3dsec/ws3dsec.cfm

Формат запроса и ответа SOAP**,** wsdl-описание сервиса доступно по URL:

https://<SERVER-NAME>/get3dsec/get3dsec.wsdl

Магазин должен отправить в АПК Ассист значение параметра pares, полученное в ответе от банка-эмитента. Для этого необходимо отправить запрос в формате SOAP.

Входные параметры:

Метод*: send3dsparams*

Параметр	**Обязательное поле**	**Описание**
merchant_id	Да	Идентификатор магазина в системе АПК Ассист
login	Да	Ваш логин
password	Да	Ваш пароль
ordernumber	Да	Номер заказа, для которого передаются параметры 3DS
pares	Да	Пакет результата по 3DS
language	Нет	Язык

Пример SOAP запроса:

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
<s:Body>
<send3dsparams xmlns="urn:assist-processor">
<merchant_id> </merchant_id>
<login> </login>
<password> </password>
<ordernumber> </ordernumber>
<language></language>
<pares>,      -</pares>
</send3dsparams>
<s:Body>
<s:Envelope>
```

Возвращаемая информация: пакет результата режима *silentpay.*

В случае возникновения ошибки:

```
<?xml version="1.0" encoding="windows-1251" standalone="no" ?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<SOAP-ENV:Body SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<SOAP-ENV:Fault>
<faultcode> </faultcode>
<faultstring> </faultstring>
<detail />
</SOAP-ENV:Fault>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

3D-Secure авторизация по протоколу версии 2

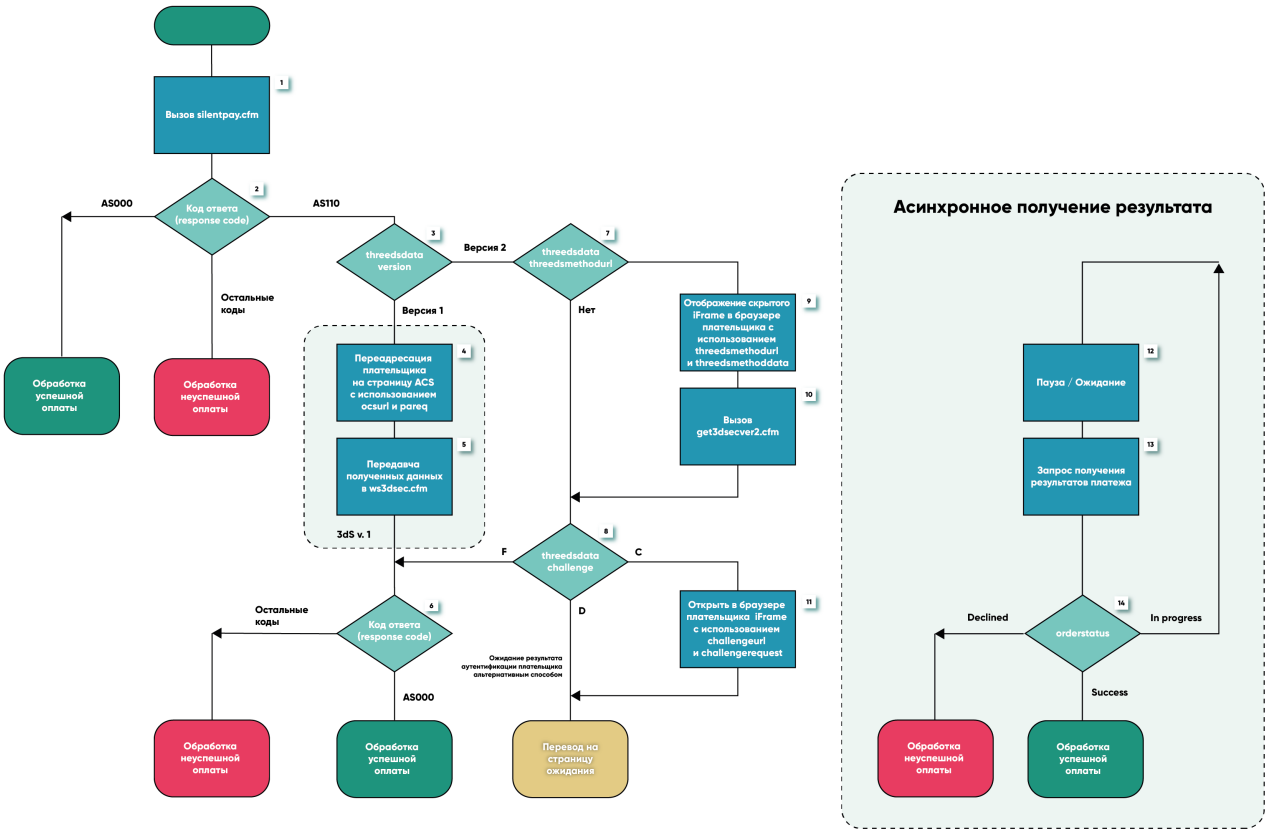
Важной особенностью новой версии протокола является тот факт, что плательщик может быть аутентифицирован без ввода дополнительного пароля (на основе дополнительных данных). Процесс аутентификации, при котором не происходит дополнительного взаимодействия с держателем карты, называется Frictionless Flow. Процесс аутентификации, при котором держателю карты требуется ввести дополнительный код подтверждения, называется процессом проверки (Challenge Flow).

Также перед аутентификацией по новому протоколу браузером клиента должен быть отправлен дополнительный запрос на ACS банка-эмитента (в дальнейшем мы будем называть его 3DSMethod).

Для работы с новым протоколом на стороне предприятию необходимо внести следующие изменения:

1. Проверять версию протокола 3D-Secure в ответе на авторизационный запрос к сервису Assist. Для протокола версии 1 поддерживать описанную выше схему работы.
2. Для протокола версии 2 сформировать скрытый iframe на платежной странице (детальное описание параметров см. ниже) и отправить на ACS банка-эмитента запрос 3DSMethod (при наличии).
3. Для продолжения аутентификации вызвать веб-сервис *ws3dsecver2* с дополнительными параметрами 3D-Secure. Если аутентификация произойдет без дополнительного взаимодействия с клиентом (Frictionless Flow), то АПК Ассист получит ее результат и отправит транзакцию авторизации в процессинг. В ответе предприятие получит полный результат оплаты, содержащий также и результат авторизации в процессинге. В случае необходимости дополнительной аутентификации клиента АПК Ассист вернет в ответе на запрос дополнительные поля для проведения проверки (Challenge Flow).
4. При наличии в ответе дополнительных полей, сообщающих о необходимости дополнительной проверки, предприятие на платежной странице формирует iFrame, в котором реализует отображение страницы ACS банка-эмитента для ввода одноразового пароля. Покупатель завершает аутентификацию.
5. Результат прохождения проверки АПК Ассист получит на сервер на своей стороне. В случае успешной проверки будет проведена транзакция оплаты в процессинге. В случае неуспешной проверки операция завершится с ошибкой.
6. Для того чтобы узнать окончательный результат оплаты заказа, предприятию необходимо использовать один из методов получения результата авторизации.

Логику работы нового протокола версии 2 отображает нижеследующая схема. Текстовое описание далее содержит ссылки на пронумерованные блоки схемы.



Для начала оплаты заказа предприятие отправляет авторизационный запрос на сервер АПК Ассист и необходимые дополнительные параметры (блок 1). Также могут использоваться необязательные дополнительные параметры.

При оплате картой, требующей авторизации по протоколу версии 2 АПК Ассист вернет в ответе код возврата AS110 (блок 2) и дополнительный блок параметров *threedsdata*. Полный список параметров, которые могут содержаться в блоке *threedsdata* предс тавлен в таблице ниже:

Название	**Принимаемые значения**	**Описание**	**В ответе сервиса**[1]
version	1[1] (1.0.0, 1.0.2) 2[1] (2.0, 2.1.0, 2.2.0)	Версия протокола 3-D Secure	1,2
threeDSServerTransID	Строка	ID транзакции в 3DS Server	1,2
threeDSMethodURL	Строка, до 256 символов	URL на стороне банка-эмитента или платежной системы	1
threeDSMethodData	Строка, до 256 символов	Закодированное в Base64 тело запроса	1
alphaauthresult	Y - успешно, N - неуспешно, A - Attempt, U – невозможно провести аутентификацию, R- отказ, E - ошибка, I - для информации	Результат аутентификации будет получен в ответе, если она произошла в одну стадию (Frictionless Flow)	1,2
challenge	F - Frictionless Flow C - Challenge Flow D - Decoupled Authentication	Взаимодействие с держателем карты (C – нужно, F – не нужно, D - отложенная аутентификация)	1,2
challengeurl[2]	Полное доменное имя (URL) https://acs.... Длина максимум 2048 символов	URL банка-эмитента или платежной системы для проверки плательщика	1,2
challengerequest[2]	Сообщение, закодированное методом Base64, длина переменная	Данные запроса, отправляемого на challengeurl	1,2

[1]Параметр может содержаться в ответе сервиса: 1- *silentpay*; 2 – *get3dsecver2*.

[2]В случае авторизации без дополнительной проверки (Frictionless Flow) и для отложенной аутентификации (Decoupled authentication) параметры *challengeurl* и *challengerequest* не будут возвращены.

В зависимости от содержания полученного блока *threedsdata* (блоки 3,7,8) аутентификация продолжается по-разному.

Основные сценарии работы для версии 2 определяются тем, требуется ли вызов *3DSMethod* (формирование скрытого iFrame в браузере клиента), а также требуется ли дополнительная аутентификация клиента и по какому сценарию она проходит:

- При наличии URL банка-эмитента *threeDSMethodURL* (блок 7) предприятие формирует скрытый HTML iFrame на платежной странице (блок 9), отправляет POST запрос с одним параметром *threeDSMethodData* на полученный адрес *threeDSMethodURL*, и далее вызывает сервис get3dsecver2 (блок 10).
- При наличии URL банка-эмитента *threeDSMethodURL* (блоки 7, 9, 10), но без необходимости дополнительного взаимодействия с держателем карты (блок 8) - *Frictionless Flow (F)*, АПК Ассист сразу проводит транзакцию в процессинге или завершает операцию с ошибкой. В ответе на вызов сервиса get3dsecver2 предприятие получит статус оплаты (блок 6).
- При наличии URL банка-эмитента *threeDSMethodURL* (блоки 7, 9, 10) и при необходимости дополнительного взаимодействия с держателем карты (блок 8) предприятие должно сформировать на платежной странице объект HTML iFrame и отправить методом HTTP POST запрос проверки держателя карты к указанному URL *challengeurl* (блок 11). В этом iFrame отображается страница ACS банка эмитента и плательщик вводит одноразовый пароль, полученный от банка. Это сценарий *Challenge Flow (C).*
- При наличии URL банка-эмитента *threeDSMethodURL* (блоки 7, 9, 10) при необходимости дополнительного взаимодействия с держателем карты (блок 8) и отложенной аутентификации предприятие должно оставить заказ в состоянии *В Процессе* и ожидать окончательного статуса оплаты (в рамках времени жизни заказа). Это сценарий *Decoupled Authentication (D)*.
- При отсутствии URL банка-эмитента *threeDSMethodURL* и когда дополнительное взаимодействие с держателем карты не требуется - *Frictionless Flow (F)*, сразу же будет проведена транзакция в процессинге, и процесс оплаты будет завершен (блок 6). Предприятие получит результат аутентификации и статус оплаты сразу в ответе на вызов сервиса *silentpay*.
- При отсутствии URL банка-эмитента *threeDSMethodURL* и при необходимости дополнительного взаимодействия с держателем карты (блок 8) для сценария *Challenge Flow (C)* предприятие должно сформировать на платежной странице объект HTML iFrame и отправить методом HTTP POST запрос проверки держателя карты к указанному URL *challengeurl* (блок 11). В этом iFrame отображается страница ACS банка эмитента и плательщик вводит одноразовый пароль, полученный от банка.
- При отсутствии URL банка-эмитента *threeDSMethodURL* и при необходимости дополнительного взаимодействия с держателем карты (блок 8) по сценарию отложенной аутентификации (D) предприятие должно оставить заказ в состоянии *В Процессе* и ожидать окончательного статуса оплаты (в рамках времени жизни заказа).

get3dsecver2 - веб-сервис продолжения аутентификации по 3D-Secure

URL для передачи запроса:

https://<SERVER-NAME>/get3dsec/get3dsecver2.cfm

Поддерживаемые форматы: SOAP, JSON.

Входные параметры:

Название	**Принимаемые значения**	**Описание**
Merchant_ID	Число	Идентификатор предприятия в системе АПК Ассист
Login	Строка	Ваш логин
Password	Строка	Ваш пароль
Billnumber	15 или 16 цифр или расширенный формат	Уникальный номер платежа в АПК Ассист
threeDSServerTransID	Строка	ID транзакции в 3DS Server

АПК Ассист продолжает процесс аутентификации плательщика в платежной системе и банке-эмитенте через 3DS Server.

Если дополнительная проверка покупателя не требуется (Frictionless Flow) (блок 8), АПК Ассист проводит транзакцию в процессинге или завершает операцию с ошибкой (в зависимости от настроек процессинга, предприятия и результата аутентификации) (блок 6).

Ответ на запрос в этом случае будет содержать один из конечных кодов возврата (AS000 – операция успешно завершена, AS100-AS109 – отказ в авторизации), все поля ответа, описанные выше, и дополнительный блок данных *threedsdata*, в котором параметр *challenge* равен F, а поле *alphaauthresult* содержит результат аутентификации *(Y, N, U, R, I*).

Получение кода возврата AS110 в ответе на вызов сервиса *get3dsecver2* означает, что нужна дополнительная проверка плательщика (Challenge Flow). Для сценария с дополнительной проверкой (*Challenge Flow*) в блоке данных *threedsdata* параметр *challenge* будет равен *C*, а параметры *challengeurl* и *challengerequest* будут заполнены (блок 8). Предприятие должно в этом случае сформировать на платежной странице объект HTML iFrame и отправить методом HTTP POST запрос проверки держателя карты к указанному URL (блок 11) с параметром *creq*, в котором передать полученное значение *challengerequest*. В этом iFrame отображается страница ACS банка-эмитента и плательщик вводит одноразовый пароль, полученный от банка.

В сценарии с отложенной аутентификацией в блоке данных *threedsdata* параметр *challenge* будет равен *D*, а параметры *challenge url* и *challengerequest* будут отсутствовать (блок 8). Предприятие должно в этом случае оставить заказ в состоянии *В Процессе* и ожидать окончательного статуса оплаты.

Результат этой проверки АПК Ассист получит на свой сервер в асинхронном режиме. В зависимости от результата аутентификации и настроек процессинга и предприятия, АПК Ассист проведет транзакцию оплаты в процессинге или закроет операцию с ошибкой.

Для того, чтобы после прохождения дополнительной проверки плательщик смог вернуться обратно на сайт предприятия, следует сообщить службе поддержки АПК Ассист URL для возврата покупателя и приема результата прохождения дополнительной проверки. Для предприятия получение этого запроса будет означать, что дополнительная проверка завершена, и оно может в этот момент перенаправить браузер плательщика на страницу результата на своей стороне и ожидать завершения платежной транзакции в процессинге.

Получение результата платежа после дополнительной проверки отражено на схеме блоками 12, 13, 14.

> Процесс получения результата дополнительной проверки на сервера АПК Ассист является асинхронным. Только после получения этого результата будет проведена (или не проведена) транзакция оплаты в процессинге, которая приведет к блокировке средств на карте клиента. Предприятию следует получить результат операции оплаты от АПК Ассист одним из стандартных способов. Предприятие может отправить запрос к сервису получения результата операции по номеру заказа, либо настроить на своей стороне получение результатов авторизации, отправляемых АПК Ассист на сервер предприятия.

Пример блока данных *threedsdata*, в котором дополнительной проверки держателя не требуется (при этом код возврата responsecode будет отличен от AS110):

```
<threedsdata>
<version>2.2</version>
<alphaauthresult>Y</alphaauthresult>
<challenge>F<challenge>
</threedsdata>
```

Пример блока данных threedsdata, в котором требуется дополнительная проверка держателя (код возврата responsecode равен AS110):

```
<threedsdata>
<version>2.2</version>
<challenge><challenge>
<challengeurl>https://acs.superbank.ru/version20/creq</challengeurl>
<challengerequest>eyJ0aHJlZURTU2VydmVyVHJhbnNJRCI6ImE3ZWJlMDU3LTg2ZjgtNGFmMS05MTJkHGNlYTc5Mzc0OWUxMiIsImFjc1RyYW
5zSUQiOiI5ODhmOWZmYS1kNzYyLTQ0YjktOWI0OS01ZDRkMjU5YmRkZWQiLCJkc1RyYW5zSUQiOiJkMGJmZGQzYy00YzdhLTVmNjktODAwMC0wMD
AwMDAwOGM3NjMiLCJtZXNzYWdlVHlwZSI6IkNSZXEiLCJtZXNzYWdlVmVyc2lvbiI6IjIuMS4wIiwiY2hhbGxlbmdlV2luZG93U2l6ZSI6IjA0In
0</challengerequest>
</threedsdata>
```

Чтобы получить ответ веб-сервиса в формате JSON, нужно передать в запросе content-type=application/json или format=5.

Описание параметров всех веб-сервисов АПК Ассист для формата JSON содержится в файле swagger по адресу:

https://docs.belassist.by/swagger/

Пример ответа в формате JSON для операции без дополнительной аутентификации:

```
{
   "threedsdata":    {
      "version": "2.2.0",
      "alphaauthresult": "Y",
      "challenge": "F"
   },
   "MakePaymentResponse":    {
      "customermessage": " ",
      "message": " ",
      "token": "",
      "testmode": "0",
      "operationtype": "100",
      "orderdate": "23.10.2019 10:45:47",
      "packetdate": "23.10.2019 10:49:48",
      "orderamount": "15.00",
      "ordercomment": "",
      "cardexpirationdate": "12/20",
      "ordercurrency": "BYN",
      "recommendation": "",
      "processingname": "Fake",
      "meannumber": "220000****0001",
      "orderstate": "Approved",
      "rate": "1",
      "amount": "15.00",
      "responsecode": "AS000",
      "meantypename": "VISA",
      "protocoltypename": "NET",
      "bankcountry": "UNKNOWN",
      "customer":       {
         "lastname": "Testov",
         "firstname": "",
         "middlename": "Testovich",
         "ipaddress": "10.10.10.10",
         "email": "null@assist.by"
      },
      "cardholder": "TEST",
      "approvalcode": "X38988",
      "billnumber": "5161957242913232.1",
      "issuebank": "UNKNOWN",
      "currency": "RUB",
      "ordernumber": "231020191345849_user2",
      "meansubtype": ""
   }
}
```


Пример ответа для операции с дополнительной аутентификацией:

```
{
    "threedsdata": {
        "version": "2.2.0",
        "challengerequest":
"eyJtZXNzYWdlVHlwZSI6IkNSZXEiLCJ0aHJlZURTU2VydmVyVHJhbnNJRCI6IjQxMWI2ODVjLWUzODAtNGZkYS05YmIzLWJiZjM2OTJiNGMyNiIsImFjc1RyYW5zSUQiOiJmY2FlMDMzNS0xODgwLTRlNjgtOWJjMy0wMDcyZDM4ZTkzODYiLCJjaGFsbGVuZ2VXaW5kb3dTaXplIjoiMDIiLCJtZXNzYWdlVmVyc2lvbiI6IjIuMS4wIn0",
        "challengeurl": "https://fake.3dss.t.paysecure.ru/acs/challenge",
        "challenge": "C"
    },
    "MakePaymentResponse": {
        "customermessage": "     3DSecure",
        "message": "     3DSecure",
        "testmode": 0,
        "operationtype": 100,
        "orderdate": "05.04.2022 11:19:32",
        "packetdate": "05.04.2022 11:19:34",
        "orderamount": 31.79,
        "ordercomment": "",
        "cardexpirationdate": "12/23",
        "ordercurrency": "BYN",
        "recommendation": "",
        "processingname": "Credx",
        "meannumber": "554373****6654",
        "orderstate": "In Process",
        "rate": 1,
        "amount": 31.79,
        "responsecode": "AS110",
        "meantypename": "MasterCard",
        "protocoltypename": "NET",
        "bankcountry": "",
        "customer": {
            "lastname": "Test",
            "firstname": "Auto",
            "middlename": "",
            "ipaddress": "127.0.0.1",
            "email": "null@assist.by"
        },
        "cardholder": "TEST",
        "approvalcode": "",
        "billnumber": "5817109255129273.1",
        "issuebank": "BANK",
        "currency": "BYN",
        "ordernumber": "6b510f3d-1327-4f3b-bc17-612daeed3aac",
        "meansubtype": "Platinum MasterCard Salary-Immediate Debit"
    }
}
```


Наверх