# Платформа для мобильных платежей и сервисов «Digital Services Platform»: Система DSP FastTack

# Описание межсистемных сообщений V 1.3.17

# Лист изменений

| Версия документа | Дата изменений | Краткое описание | Автор |
|---|---|---|---|
| 1.0 | 10.03.2018 | Разработка документа | В. Гузов |
| 1.2.6 | 02.09.2019 | Добавлено опциональное поле walletId в запрос confirmProvisioning | В. Гузов |
| 1.3.0 | 12.11.2019 | Реструктуризация документа;<br>Исправлено описание к полю correlationId;<br>Добавлены новые коды в запросе tokenStatusUpdated;<br>Добавлены новые поля в ответе Get Card Info Short;<br>Обновлена макс. длина поля clientWalletAccountId и описание поля clientWalletAccountID в методах Create Opaque Payment Card и Get Token by Wallet Id;<br>Добавлены примеры для запроса Card Status Verification | В. Гузов |
| 1.3.1 | 12.23.2019 | Исправлено описание к полю productConfigID в методах getCardInfoShort и confirmProvisioning<br>Добавлен комментарий к полю clientWalletAccountID в методах Get Token by Wallet Id;<br>Добавлено поле tokenType в confirmProvisioning | В. Гузов |
| 1.3.2 | 01.31.2020 | Добавлен новый код ответа в confirmProvisioning | В. Гузов |
| 1.3.3 | 03.03.2020 | Обновлено описание поля tokenizationPath в confirmProvisioning | В. Гузов |
| 1.3.4 | 09.04.2020 | Добавлено новое поле otpReason в sendOTP<br>Добавлен новый код ответа в confirmProvisioning<br>Обновлено описание к методу createOpaquePaymentCard | В. Гузов |
| 1.3.5 | 28.04.2020 | Обновлено описание к методу tokenStatusUpdated | В. Гузов |
| 1.3.6 | 09.07.2020 | Обновлено описание к методу getTokenByWalletId | В. Гузов |
| 1.3.7 | 03.08.2020 | Обновлено описание к методу tokenStatusUpdated | В. Гузов |
| 1.3.8 | 17.09.2020 | Обновлено описание к методу confirmProvisioning | В. Гузов |
| 1.3.9 | 28.09.2020 | Новый метод deviceBinding | В. Гузов |
| 1.3.10 | 10.11.2020 | Обновлено описание к методам confirmProvisioning и cardTokenized | В. Гузов |
| 1.3.11 | 14.01.2021 | Коррекции терминологии | А. Капий |
| 1.3.12 | 19.03.2021 | Обновлены методы deviceBinding и sendNotificationToCustomer | В. Гузов |
| 1.3.14 | 9.06.2021 | Добавлены разъяснения по методам | А. Аушев |
| 1.3.14 | 24.06.2021 | Сценарии токенизации карт VISA и Mastercard | А. Аушев |
| 1.3.15 | 14.07.2021 | Уточнение описания полей для Push-provisioning метод createOpaquePaymentCard | А. Аушев |
| 1.3.15 | 18.08.2021 | В методе Token Update поле newAccountPan является обязательным | И. Старовит |
| 1.3.15 | 26.08.2021 | В методе Confirm Provisioning в поле Decision обновлено описание | А. Аушев |
| 1.3.15 | 30.08.2021 | В методе Token Update поле oldAccountPan является условным | И. Старовит |
| 1.3.15 | 08.09.2021 | В список возможных значений параметра messageReasonCode запроса Token Status Updated добавлено новое значение LUK_REPLENISHMENT | Д. Ищенко |

| | | | |
|---|---|---|---|
| 1.3.15 | 14.10.2021 | Дополнение к описанию использования метода Get Customer Identifier | А.Аушев |
| 1.3.15 | 26.10.2021 | Метод Get Card Info Shot - OK Success карта найдена ( активная , неактивна , закончен срок ) | А.Аушев |
| 1.3.16 | 2.11.2021 | Добавлены диаграммы для схем PushProvisioning , InAppProvisioning | А.Аушев |
| 1.3.16 | 10.11.2021 | Добавлено разъяснение по формату сообщений SOAP/XML (раздел JSON/XML processing) | Д. Ищенко |
| 1.3.16 | 19.11.2021 | Изменено описание полей expiryMonth и expiryYear в запросе Confirm Provisioning. Значения в этих полях являются опциональными | |
| 1.3.17 | 06.12.2021 | Добавлен раздел «Рекомендуемый порядок обработки запроса confirmProvisioning для карт Mastercard» | Д. Ищенко |
| 1.3.17 | 06.12.2021 | Добавлен раздел “Рекомендуемый порядок обработки запроса confirmProvisioning для карт VISA” | Д. Ищенко |

# Содержание

## Термины и сокращения

| Термин/сокращение | Определение |
|---|---|
| DSP, Платформа | Платформа для мобильных платежей и сервисов «Digital Services Platform» |
| Система, DSP FastTack | Система DSP FastTack – одна из систем платформы для мобильных платежей и сервисов «Digital Ser Platform » |
| Токен | Token – уникальный набор символов, который присваивается банковской карте в процессе оцифро (токенизации) и позволяет обезопасить электронные платежи за счет устранения реальных карточн данных из каналов, оборудования и систем, обслуживающих процесс приема карт к оплате |
| MDES | MasterCard Digital Enablement Service– облачный сервис токенизации платежной системы Mastercar (ресурсы для эмитента, позволяющие взаимодействовать с платежной системой по вопросам, связанным с оцифрованными картами: токенизация карты, процессирование транзакций по токену обработка событий, связанных с жизненным циклом токена) |
| VTS | Visa Token Service – облачный сервис токенизации платежной системы VISA (ресурсы для эмитента, позволяющие взаимодействовать с платежной системой по вопросам, связанным с оцифрованным картами: токенизация карты, процессирование транзакций по токену, обработка событий, связанны жизненным циклом токена) |
| Токенизация | Оцифровка банковской карты – комплекс технических решений, основанный на технологиях MDES/ позволяющий создать уникальный токен банковской платежной карты и осуществлять в дальнейше платежи (в том числе в POS-терминале без физического присутствия карты) |
| МПС | Международные платежные системы |
| Эмитент (банк-эмитент) | Банк, выпускающий в обращение (эмитирующий) денежные знаки или ценные бумаги и платёжно-расчётные инструменты (банковские карты, чековые книжки) |
| Цифровой кошелек | Мобильный кошелек – мобильное приложение, система мобильных (электронных) платежей с мобильных устройств под управлением Android и IOS |
| API | Программный интерфейс приложения |
| DWP | Digital Wallet Provider – провайдер цифрового кошелька |

## Цель документа

Документ представляет собой описание межсистемных сообщений DSP FastTack (далее – Система) – модуля платформы для мобильных платежей и сервисов:

# Задействованные системы

## Tokenization services

Сервисы токенизации карт. Выполняет токенизацию карты клиента, выпуск и поддержку токена - оцифрованной карты с другим номером. Выполняют reDSPping pan-token/token-pan во время обработки авторизационных запросов и формировании клиринговых файлов. Токенизационные сервисы у платёжных систем (МПС) называются:

- Visa Token Service, VTS;
- Mastercard Digitalization Enablement Service - MDES.

## FASTTACK

Система обеспечивающая взаимодействие между системами банка и платформами токенизации VTS (VISA) и MDES (Mastercard) в схеме, когда карты банка оцифровываются через стороннего провайдера мобильного кошелька (например Google Pay).

## BANK- Система Банка

Система Банка. Обслуживает все запросы, связанные с получением данных и выполнением операций в системах банка и процессинга.

## Google Pay – Digital Walllet Platform

Разработанная компанией Google система электронных платежей с мобильных устройств (смартфонов, планшетов и умных часов), работающих под операционной системой Android.

# Universal Issuer API

Взаимодействие FT с банковскими сервисами основывается на REST-сервисах (входящие/исходящие JSON сообщения) либо с использованием протокола SOAP/XML (только исходящие сообщения).

## Защита соединения

Для защиты данных используется TLS

## URL Scheme

Используются Rest-сервисы с отдельным Endpoint-URL для каждого сервиса.
HTTP-Method POST.
Обязательно использование HTTP-заголовков, запрещающих кеширование ответов на сетевом оборудовании и в app-серверах.

## JSON/XML processing

Для возможности расширения API системы Банка и FASTTACK должны быть готовы принимать “незнакомые” параметры.

Правила обработки JSON:

- FAIL_ON_UNKNOWN_PROPERTIES = false;
- FAIL_ON_EMPTY_BEANS = false;

Запросы и ответы SOAP/XML передаются в SOAP-"конвертах" следующего вида:

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
 <SOAP-ENV:Header/>
 <SOAP-ENV:Body>

   здесь находится собственно запрос или ответ

 </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Примеры запросов и ответов в документе приведены без таких “конвертов” для облегчения их чтения. Кроме того, в примерах присутствует служебная строка

```
<?xml version="1.0" encoding="UTF-8"?>
```

Она должна находиться перед SOAP-“конвертом”.

Запросы и ответы REST/XML передаются без SOAP-”конвертов”.

# Токенизация

## Confirm Provisioning

### Outbound:

Запрос Confirm Provisioning отправляется в банковскую систему с целью получения окончательного подтверждения со стороны банка, позволено ли данной карте быть токенизированной или нет.
Ответ : внутренний номер карты , продукт , номер телефона

Интерфейс веб-службы: CardToken
Метод: confirmProvisioning
SOAP Endpoint: http(s)://{domain}:{port}/{context}/CardToken
REST Endpoint: http(s)://{domain}:{port}/{context}/confirmProvisioning
Ожидаемое время отклика: <=500 ms.

Пример:
https://fasttack.test.platform.****bank.ua:8553/ft/uaservices/confirmProvisioning

***Запрос***

| Поле | Тип параметра | Описание | Присутствие в сообщении |
|---|---|---|---|
| requestId | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | M |
| conversationId | *Строка, 14-36 симв.* | Сквозной идентификатор серии запросов выполняющихся при токенизации карты. Аналог CorrelationId (MDES) | M |
| pan | *Строка, 13..19 цифр* | Номер карты для оцифровки | M |
| expiryMonth | *Строка, 2 цифры* | Месяц окончания срока действия карты | O |
| expiryYear | *Строка, 2 цифры* | Год окончания срока (последние две цифры) действия карты | O |
| lang | *Строка, 2 симв.* | Язык интерфейса приложения на момент ввода данных карты. Значение может использоваться, например, для отправки OTP кода с сопроводительным текстом на указанном языке. Допустимые значения - из ISO 639-1:<br>uk - Украинский<br>ru - Русский<br>en – Английский | O |
| panSource | *Строка, 1 символ* | Источник номера карты. Допустимые значения:<br>K-KEY_ENTERED (MDES:ACCOUNT_ADDED_MANUALLY) | M |

| | | | |
|---|---|---|---|
| | | M-MOBILE_BANKING_APP (MDES:ACCOUNT_ADDED_VIA_APPLICATION)<br>O – On file (MDES: ACCOUNT_ON_FILE)<br>T – TOKEN (VISA только)<br>C – CHIP_DIP (VISA только)<br>L – CONTACTLESS_DIP (VISA только) | |
| ips | *Строка, 1 символ* | МПС: возможные значения<br>M - Mastercard<br>V - Visa | M |
| paymentAppInstId | *Строка, 1..48 символов* | Идентификатор экземпляра приложения (кошелька), в котором создается токен | O |
| tokenRequestorId | *Строка, 11 символов* | Идентификатор провайдера цифровых кошельков | O |
| tokenRefId | *Строка, 24..64 симв.,* | Unique ID for the token associated with the PAN. This ID can be used in lieu of the token for subsequent calls, such as life cycle events | O |
| tokenizationPath | *Строка, 11 символов* | Путь токенизации соответствующий определенному уровню риска. Значение определяется провайдером цифрового кошелька. Возможные значения: GREEN/YELLOW/ORANGE/RED | O |
| deviceName | Строка, 1..128 символов | The name that the Cardholder has associated to the device with the Payment App Provide | O |
| walletId | Строка, 3 символа | Идентификатор провайдера кошелька (только MDES).<br>Список известных значений:<br>• 101 (PPOL Remote) This value is present if the wallet data was created manually by the cardholder by entering the data at a consumer-controlled device;<br>• 102 (PPOL Remote NFC Payment) This value is present if the wallet data was initially created by the cardholder by tapping their PayPass card or device at a contactless card reader. (For example, a PayPass card reader or an ultrabook enabled to read PayPass cards.)<br>• 103 Apple Pay;<br>• 216 Android Pay;<br>• 217 Samsung Pay;<br>• 327 MC MDES for Merchants. | O |
| tokenType | Строка | Идентификатор типа кошелька (только VTS)<br>• SECURE_ELEMENT<br>• HCE (Android)<br>• CARD_ON_FILE<br>• ECOMMERCE<br>• QRC<br>По требованиям VISA, токенизация должна осуществляться по зеленому пути (Gree Path) при получении значений CARD_ON_FILE и ECOMMERCE, т.е. банк не должен возвращать «REQUIRE_ADDITIONAL_AUTHENTICATION» в ответе на confirmProvisioning, а только «APPROVED» или «DECLINED». | O |
| otpReason | *Строка 1..64 симв* | Для VISA только<br>Причина получения запроса на OTP код. Если поле отсутствует, то по умолчанию принимается как “PROVISIONING”. Возможные значения: | O |

| | | | |
|---|---|---|---|
| | | PROVISIONING, PAYMENT, TOKEN_DEVICE_BINDING, CARDHOLDER_STEPUP, TRUSTED_LISTING_ENROLLMENT.<br>Если будет значение TOKEN_DEVICE_BINDING в ответе ожидается REQUIRE_ADDITIONAL_AUTHENTICATION и тогда отправляется ОТП | |

***Ответ***

Ответ содержит решение банка об активации сервиса оцифровки для данной карты. В случае если токенизация разрешена, в ответе обычно возвращается номер телефона для отправки клиенту OTP кода.

Операцию считаем успешной, если поле code== 0;

| Поле | Тип параметра | Описание | Присутствие в сообщении |
|---|---|---|---|
| decision | *Строка, 1..33 симв.* | Может иметь одно из следующих значений<br>APPROVED – оцифровка разрешена; - *рекомендация VISA, если значение panSource = «T», «M» и возвращать Code =0*<br>*Если значение 'O' банк должен перепроверить, что Token RequestorID - не "кошелек", и только тогда отвечать APPROVED.*<br>DECLINED - оцифровка отклонена;<br>REQUIRE_ADDITIONAL_AUTHENTICATION – оцифровка разрешена, но требуется дополнительная проверка клиента<br>Применяется если в запросе в поле otpReason будет значение TOKEN_DEVICE_BINDING | M |
| panInternalId | *Строка, 1..30 симв.* | Уникальный идентификатор карты в банковской системе.<br>Обязательным является один из двух параметров: panInternalId / panInternalGUID | C |
| panInternalGUID | *Строка, 1..32 симв.* | Уникальный идентификатор карты в банковской системе.<br>Обязательным является один из двух параметров: panInternalGUID / panInternalId | C |
| code | *Строка, 1..3 симв.* | Код завершения операции.<br>Возможные варианты значений:<br>“0” - OK Success<br>“1” – parseException (невалидная информация),<br>“2” - nothingFoundException (по пришедшей информации ничего не найдено)<br>“3” - exception (что-то пошло не так).<br>“4” – Invalid Exp. Date (PAN корректный)<br>“5” – Suspicious activity | M |
| errorMessage | *Строка, 1..2000 симв.* | Журналируем как доп. информацию. Может быть заполнено для отказов.<br>Заполняется для ошибок (code != 0). | C |
| customerPhone | *Строка,* 12..13 симв. . | Номер телефона пользователя (“380505554433”,”+380505554433”)<br>Обязательно заполняется в случае panSource = «K» | C |
| productConfigID | *Строка, 1-32 символ* | Уникальный идентификатор соответствующий конфигурации продукта. | O |
| *cardIssueDate* | *Строка,* | Дата выпуска карты в формате DDMMYYYY | O |

| | | | |
|---|---|---|---|
| | *8 символов* | | |

### Пример 1. SOAP/XML

Запрос

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:confirmProvisioning xmlns:ns2="http://sab/"
xmlns:ns4="http://ws.wso2.org/dataservice">
    <ns2:requestId>53b7cc3f-d3c2-4fb0-ad6e-9d85702c00fd</ns2:requestId>
    <ns2:conversationId>4f7d4164-24c9-4c54-bebf-97534bd338f6</ns2:conversationId>
    <ns2:pan>4102321250000006</ns2:pan>
    <ns2:lang>en</ns2:lang>
    <ns2:panSource>K</ns2:panSource>
    <ns2:ips>V</ns2:ips>
    <ns2:paymentAppInstId>6Gt02SAokOGBxPoKPuP6yVpV</ns2:paymentAppInstId>
    <ns2:tokenRefId>DNITHE301736046984008735</ns2:tokenRefId>
    <ns2:tokenRequestorId>40010030273</ns2:tokenRequestorId>
    <ns2:deviceName>MyPhone</ns2:deviceName>
</ns2:confirmProvisioning>
```

Ответ

```
<?xml version="1.0" encoding="UTF-8"?>
<sab:confirmProvisioningResponse xmlns:sab="http://sab/">
    <sab:decision>REQUIRE_ADDITIONAL_AUTHENTICATION</sab:decision>
    <sab:panInternalId>AXvqBAifyEHk</sab:panInternalId>
    <sab:panInternalGUID>YuKDIUgnPrgB</sab:panInternalGUID>
    <sab:code>0</sab:code>
    <sab:customerPhone>380503123456</sab:customerPhone>
</sab:confirmProvisioningResponse>
```

### Пример 2. REST/JSON

Запрос

```
{
    "requestId": "53b7cc3f-d3c2-4fb0-ad6e-9d85702c00fd",
    "conversationId": "4f7d4164-24c9-4c54-bebf-97534bd338f6",
    "pan": "4444441250000006",
    "lang": "en",
    "panSource": "K",
    "ips": "V",
    "paymentAppInstId": "6Gt02SAokOGBxPoKPuP6yVpV",
    "tokenRefId": "DNITHE301736046984008735",
    "tokenRequestorId": "40010030273",
    "deviceName": "MyPhone"
}
```

Ответ

```
{
    "decision": "REQUIRE_ADDITIONAL_AUTHENTICATION",
    "panInternalId": "AXvqBAifyEHk",
    "panInternalGUID": "YuKDIUgnPrgB",
    "code": "0",
    "customerPhone": "380503123456"
}
```

# Send OTP

## Outbound

Обычно данный запрос выполняется в случае, когда клиент выбрал дополнительный метод верификации путем проверки OTP кода. Начиная с 2020 года VISA начала использовать данный тип запроса для верификации клиентов в иных сценариях. Например, запрос sendOTP может прийти с целью добавления устройства в список доверенных устройств, с которых позднее клиент собирается выполнять покупки.

Данный запрос передается во внутреннюю систему банка для отправки значения OTP в теле SMS.

Интерфейс веб-службы: CardToken
Метод: sendOTP
SOAP Endpoint: http(s)://{domain}:{port}/{context}/CardToken
REST Endpoint: http(s)://{domain}:{port}/{context}/sendOTP

***Запрос***

| Поле | Тип параметра | Описание | Присутствие в сообщении |
|---|---|---|---|
| requestId | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | M |
| conversationId | *Строка, 14-36 симв.* | Сквозной идентификатор серии запросов, выполняющихся при токенизации карты. Аналог CorrelationId (MDES) | M |
| tokenRefId | *Строка, 24..64 симв.,* | Unique ID for the token associated with the PAN. This ID can be used in lieu of the token for subsequent calls, such as life cycle events | O |
| tokenRequestorId | *Строка, 11 симв.* | Unique ID assigned to the initiator of the token request | O |
| tokenRequestorName | *Строка, 1..64 симв.* | Название в виде текста (“GOOGLE_PAY”, “VISA_CHECKOUT”, “NETFLIX”) ассоциированное с tokenRequestorId. Заполняется в случае наличия соотв. записи в таблице TOKEN_REQUESTOR | O |
| lastFourOfPAN | *Строка, 4 симв.* | Последние четыре цифры номера карты | M |
| panInternalId | *Строка, 1..30 симв.* | Уникальный идентификатор карты в банковской системе. Обязательным является один из двух параметров: panInternalId / panInternalGUID | C |
| panInternalGUID | *Строка, 1..32 симв.* | Уникальный идентификатор карты в банковской системе. Обязательным является один из двух параметров: panInternalGUID / panInternalId | C |
| otp | *Строка, 1-32 симв.* | Код проверки | M |
| customerPhone | *Строка, 12..13 симв.* | Номер телефона пользователя (“380505554433”,”+380505554433”) | M |
| deviceType | *Строка 1..64 симв* | Форм фактор устройства, на котором выполняется токенизация. Новые значения могут быть добавлены в любой момент и должны приниматься без ошибок. Возможные значения: PHONE, TABLET, TABLET_OR_EREADER, WATCH, WATCH_OR_WRISTBAND,CARD,STICKER, PC, DEVICE_PERIPHERAL, TAG, JEWELRY ,FASHION_ACCESSORY, | O |

| | | | |
|---|---|---|---|
| | | GARMENT, DOMESTIC_APPLIANCE,VEHICLE,<br>MEDIA_OR_GAMING_DEVICE, UNDEFINED | |
| otpReason | *Строка*<br>*1..64 симв* | Для VISA только<br>Код причины для отправки OTP кода. Если поле в запросе отсутствует, то по умолчанию принимается как “PROVISIONING”.<br>Возможные значения: PROVISIONING, PAYMENT, TOKEN_DEVICE_BINDING, CARDHOLDER_STEPUP, TRUSTED_LISTING_ENROLLMENT | C |

***Ответ***

| Поле | Тип параметра | Описание | Присутствие в сообщении |
|---|---|---|---|
| requestId | *Строка,*<br>*36 симв.,*<br>*GUID* | Уникальный идентификатор запроса. | O |
| code | *Строка,*<br>*1..3 симв.* | Код завершения операции.<br>Возможные варианты значений:<br>“0” - OK Success<br>От “1” и больше – ошибка<br>1 (parseException- невалидная информация),<br>2 (nothingFoundException - по пришедшей информации ничего не найдено)<br>3 (exception - что-то пошло не так). | M |
| errorMessage | *Строка,*<br>*1..2000 симв* | Дополнительная информация.<br>Заполняется для отказов или ошибок (code != 0). | C |

Пример 1. SOAP/XML

Запрос

```
<ns2:sendOTP xmlns:ns2="http://sab/" xmlns:ns4="http://ws.wso2.org/dataservice">
         <ns2:requestId>bffcdbf8-4391-4372-af78-12dac96eedfe</ns2:requestId>
         <ns2:tokenRefId>DNITHE000302000200028965</ns2:tokenRefId>
         <ns2:conversationId>cd0bcacf-d4bc-4b75-b1e0-256ab743650c</ns2:conversa-
tionId>
         <ns2:panInternalId>dN7Pix7WzQh8</ns2:panInternalId>
         <ns2:panInternalGUID>2540ed95-1f20-440e-809a-cfa92da4c6ce</ns2:panIn-
ternalGUID>
         <ns2:otp>363538</ns2:otp>
         <ns2:customerPhone>380503124439</ns2:customerPhone>
         <ns2:deviceType>MOBILE_PHONE</ns2:deviceType>
         <ns2:tokenRequestorId>40010030273</ns2:tokenRequestorId>
         <ns2:lastFourOfPAN>0006</ns2:lastFourOfPAN>
</ns2:sendOTP>
```

Ответ

```
<sab:sendOTPResponse>
 <sab:requestId>bffcdbf8-4391-4372-af78-12dac96eedfe</sab:requestId>
 <sab:code>0</sab:code>
 <sab:errorMessage />
</sab:sendOTPResponse>
```

Пример 2. REST/JSON

Запрос


```
{
   "requestId": "29b44eb3-25dc-4042-b035-c31c4803b47a",
   "tokenRefId": "DNITHE000302000200028965",
   "conversationId": "cd0bcacf-d4bc-4b75-b1e0-256ab743650c",
   "panInternalId": "dN7Pix7WzQh8",
   "panInternalGUID": "2540ed95-1f20-440e-809a-cfa92da4c6ce",
   "otp": "363538",
   "customerPhone": "380503123456",
   "deviceType": "MOBILE_PHONE",
   "tokenRequestorId": "40010030273",
   "lastFourOfPAN": "0006"
}
```


Ответ


```
{
      "requestId": "29b44eb3-25dc-4042-b035-c31c4803b47a",
      "code": "0"
}
```


## Card Tokenized

### Outbound

Запрос выполняется при создании токена на стороне VTS/MDES.
Используется для извещения о создании токена в банковскую систему. Возвращается уникальный номер карты и телефон

Интерфейс веб-службы: CardToken
Метод: cardTokenized
SOAP Endpoint: http(s)://{domain}:{port}/{context}/CardToken
REST Endpoint: http(s)://{domain}:{port}/{context}/cardTokenized

***Запрос***

| Поле | Тип параметра | Описание | Присутствие в сообщении |
|---|---|---|---|
| requestId | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | M |
| conversationId | *Строка, 14-36 симв.* | Сквозной идентификатор серии запросов, выполняющихся при токенизации карты. Аналог CorrelationId (MDES) | M |
| tokenRefId | *Строка, 24..64 симв.,* | Unique ID for the token associated with the PAN. This ID can be used in lieu of the token for subsequent calls, such as life cycle events | M |
| tokenRequestorId | *Строка, 11 симв.* | Unique ID assigned to the initiator of the token request | M |
| status | *Строка, 1 симв.,* | I-In progress (Token has not yet been activated)<br>A-Active (Token is active and ready to transact)<br>S-Suspended (Token is suspended and unable to transact) | M |

| | | | |
|---|---|---|---|
| | | D-Deleted (Token has been permanently deactivated) | |
| panInternalId | *Строка, 1..30 симв.* | Уникальный идентификатор карты в банковской системе. Заполняется если присутствует в БД на момент формирования запроса. | O |
| panInternalGUID | *Строка, 1..32 симв.* | Уникальный идентификатор карты в банковской системе. Заполняется если присутствует в БД на момент формирования запроса. | O |
| pan | *Строка, 13..19 цифр* | Номер карты для оцифровки. | M |
| expiryMonth | *Строка, 2 цифры* | Месяц окончания срока действия карты. | O |
| expiryYear | *Строка, 2 цифры* | Год окончания срока (последние две цифры) действия карты. | O |
| token | *Строка, 12..19 цифр* | Номер токена | M |
| tokenExpiryMonth | *Строка, 2 цифры* | Месяц окончания срока действия токена | M |
| tokenExpiryYear | *Строка, 2 цифры* | Год окончания срока (последние две цифры) действия токена. | M |
| tokenActivationDate | *Строка, 29 цифры* | Expressed in ISO 8601 extended format as one of the following - YYYY-MM-DDThh:mm:ss[ .sss ]Z, YYYY-MM-DDThh:mm:ss[ .sss ]±hh:mm, Where [ .sss ] is optional and can be 1 to 3 digits. | M |
| ips | *Строка, 1 символ* | МПС: возможные значения<br>M – Mastercard;<br>V – Visa; | M |
| panSource | *Строка, 1 символ* | Источник номера карты. Допустимые значения:<br>K-KEY_ENTERED (MDES:ACCOUNT_ADDED_MANUALLY)<br>M-MOBILE_BANKING_APP (MDES:ACCOUNT_ADDED_VIA_APPLICATION)<br>O – On file (MDES: CARD_ON_FILE)<br>T – TOKEN (VISA только)<br>C – CHIP_DIP (VISA только)<br>L – CONTACTLESS_DIP (VISA только) | O |
| paymentAppInstId | *Строка, 1..48 символов* | Идентификатор экземпляра приложения (кошелька), в котором создается токен | O |
| deviceType | *Строка 1..64 симв.* | Форм фактор устройства на котором происходит оцифровка карты. Новые значения могут добавляться МПС без предварительного уведомления. На данный момент поддерживаются следующие значения: PHONE, TABLET, TABLET_OR_EREADER, WATCH, WATCH_OR_WRISTBAND,CARD, STICKER, PC, DEVICE_PERIPHERAL, TAG, JEWELRY ,FASHION_ACCESSORY, GARMENT, DOMESTIC_APPLIANCE,VEHICLE, MEDIA_OR_GAMING_DEVICE, UNDEFINED | O |
| storageTechnology | *Строка 1..64 симв.* | Технология, используемая для хранения токена в устройстве. MDES: DEVICE_MEMORY, DEVICE_MEMORY_PROTECTED_TPM, TEE , SE ,SERVER , VEE | O |

| | | | |
|---|---|---|---|
| | | VTS: SOFTWARE, TRUSTED_EXECUTION_ENVIRONMENT, SECURE_ELEMENT, CLOUD | |
| deviceName | *Строка, 1..128 символов* | The name that the Cardholder has associated to the device with the Payment App Provider | O |

***Ответ***

| **Поле** | **Тип параметра** | **Описание** | **Присутствие в сообщении** |
|---|---|---|---|
| requestId | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | O |
| conversationId | *Строка, 14-36 симв.* | Сквозной идентификатор серии запросов, выполняющихся при токенизации карты. Аналог CorrelationId (MDES) | O |
| panInternalId | *Строка, 1..30 симв.* | Уникальный идентификатор карты в банковской системе. Обязательным является один из двух параметров: panInternalId / panInternalGUID | C |
| panInternalGUID | *Строка, 1..32 симв.* | Уникальный идентификатор карты в банковской системе. Обязательным является один из двух параметров: panInternalGUID / panInternalId | C |
| customerPhone | *Строка, 12..13 симв.* | Номер телефона пользователя (“380505554433”,”+380505554433”) | O |
| customerId | *Строка, 64 симв.* | Внутренний идентификатор контрагента | O |
| code | *Строка, 1..3 симв.* | Код завершения операции.<br>Возможные варианты значений:<br>“0” - OK Success<br>“1” - parseException (невалидный запрос)<br>“2” - nothingFoundException (по пришедшей информации ничего не найдено)<br>“3” exception (что-то пошло не так) | M |
| errorMessage | *Строка, 1..2000 симв* | Журналируем как доп. информацию. Может быть заполнено для отказов.<br>Заполняется для ошибок (code != 0). | C |

Пример 1. SOAP/XML

Запрос

```
<ns2:cardTokenized xmlns:ns2="http://sab/" xmlns:ns4="http://ws.wso2.org/da-
taservice">
         <ns2:requestId>f42ecc499121c49ea9f316a7a2288201</ns2:requestId>
         <ns2:conversationId>3fcbec5f-b1b5-4190-8334-5f5f38395352</ns2:conversa-
tionId>
         <ns2:tokenRequestorId>40010030273</ns2:tokenRequestorId>
         <ns2:tokenRefId>DNITHE40736046984008738</ns2:tokenRefId>
         <ns2:status>A</ns2:status>
         <ns2:pan>4102321250000006</ns2:pan>
         <ns2:expiryMonth>12</ns2:expiryMonth>
         <ns2:expiryYear>20</ns2:expiryYear>
         <ns2:token>4551360150000027</ns2:token>
         <ns2:tokenExpiryMonth>12</ns2:tokenExpiryMonth>
         <ns2:tokenExpiryYear>23</ns2:tokenExpiryYear>
         <ns2:tokenActivationDate>2019-01-24T12:44:47+02:00</ns2:tokenActiva-
tionDate>
         <ns2:ips>V</ns2:ips>
         <ns2:panSource>K</ns2:panSource>
         <ns2:paymentAppInstId>uGrOxzwW2ghVx1nuoC2Fnwko</ns2:paymentAppInstId>
         <ns2:deviceType>MOBILE_PHONE</ns2:deviceType>
         <ns2:storageTechnology>SOFTWARE</ns2:storageTechnology>
      </ns2:cardTokenized>
```

Ответ

```
<sab:cardTokenizedResponse>
         <sab:requestId>f42ecc499121c49ea9f316a7a2288201</sab:requestId>
         <sab:conversationId>3fcbec5f-b1b5-4190-8334-5f5f38395352</sab:conversa-
tionId>
         <sab:customerId>C0000001</sab:customerId>
         <sab:customerPhone>3801234567</sab:customerPhone>
         <sab:panInternalGUID>CardID4</sab:panInternalGUID>
         <sab:panInternalId>CardID00000000000004</sab:panInternalId>
         <sab:code>0</sab:code>
</sab:cardTokenizedResponse>
```

Пример 2. REST/JSON

Запрос

```
{
   "requestId": "f42ecc499121c49ea9f316a7a2288201",
   "conversationId": "3fcbec5f-b1b5-4190-8334-5f5f38395352",
   "tokenRequestorId": "40010030273",
   "tokenRefId": "DNITHE40736046984008738",
   "status": "A",
   "pan": "4102321250000006",
   "expiryMonth": "12",
   "expiryYear": "20",
   "token": "4551360150000027",
   "tokenExpiryMonth": "12",
   "tokenExpiryYear": "23",
   "tokenActivationDate": "2019-01-24T12:44:47+02:00",
   "ips": "V",
   "panSource": "K",
   "paymentAppInstId": "uGrOxzwW2ghVx1nuoC2Fnwko",
   "deviceType": "MOBILE_PHONE",
   "storageTechnology": "SOFTWARE"
}
```

Ответ


```
{
    "requestId": "f42ecc499121c49ea9f316a7a2288201",
    "conversationId": "3fcbec5f-b1b5-4190-8334-5f5f38395352",
    "customerPhone": "3801234567",
    "code": "0"
}
```


## Card Status Verification (Account Verification)

### Outbound

Account Status Inquiry Service – инструмент разработанный платежными системами для получения статуса счета и проверку CVV2, если он присутствовал в запросе.

Формат запроса может отличаться, в зависимости от процессинговой системы используемой в Банке.

Интерфейс веб-службы: CardSV
Метод: avs1
SOAP Endpoint: http(s)://{domain}:{port}/{context}/CardSV
REST Endpoint: http(s)://{domain}:{port}/{context}/avs1
Ожидаемое время отклика: <=500 ms.

***Запрос***

| **Поле** | **Тип/ длина параметра:** | **Описание параметра:** | |
|---|---|---|---|
| requestId | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | M |
| merchantID | *Строка, 1..64 симв.,* | Идентификатор торговца | O |
| terminalID | *Строка, 1..64 симв.,* | Идентификатор | O |
| cardInfo | | Структура может присутствовать при отключенном шифровании | C |
| encryptionKeyIndex | *Строка, 8 цифр* | Поле присутствует при включенном шифровании.<br><br>Индекс симметричного DES ключа (двойной длины) для шифрования данных | C |
| encryptedData | *Строка, 1-512  симв.* | Поле присутствует при включенном шифровании.<br><br>Возможные символы 0..9 и A..F в верхнем регистре (к примеру, 1 байт представлен в виде 2х символов, где каждый 4х битовый ниббл (полубайт) это один символ). | C |

| | | | |
|---|---|---|---|
| | | Для шифрования блока данных применяется 3DES CBC алгоритм с PKCS#5 паддингом. Вектор инициализации определяется на момент конфигурации. | |

| **encryptedDataa** | | | |
|---|---|---|---|
| cardInfo | | | |

| **cardInfo** | | | |
|---|---|---|---|
| pan | *Строка, 13..19 цифр* | Номер карты для оцифровки | M |
| expiryMonth | *Строка, 2 цифры* | Месяц окончания срока действия карты | M |
| expiryYear | *Строка, 2 цифры* | Год окончания срока (последние две цифры) действия карты | M |
| cvNum | *Строка, 3 цифры* | CVV2/CVC код | O |

Пример SOAP запроса с отключенным шифрованием,

```
<?xml version="1.0" encoding="UTF-8"?> <soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:sab="http://sab/">
<soapenv:Header />

<soapenv:Body>

<sab:AVS1Request>

<sab:requestId>53b7cc3f-d3c2-4fb0-ad6e-9d85702c00fd</sab:requestId>
<sab:merchantID>E2387468</sab:merchantID>

<sab:terminalID>100001</sab:terminalID>

<sab:cardInfo>

<sab:pan>5555551234567890</sab:pan>

<sab:expiryMonth>12</sab:expiryMonth>

<sab:expiryYear>21</sab:expiryYear>

<sab:cvNum>135</sab:cvNum>

</sab:cardInfo> </sab:AVS1Request>

</soapenv:Body>

</soapenv:Envelope>
```

Пример SOAP запроса с шифрованием,

```
<?xml version="1.0" encoding="UTF-8"?> <soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:sab="http://sab/">
<soapenv:Header />

<soapenv:Body>

<avs1:AVS1Request>

<avs1:requestId>53b7cc3f-d3c2-4fb0-ad6e-9d85702c00fd</sab:requestId>

<avs1:merchantID>E2387468</sab:merchantID>

<avs1:terminalID>100001</sab:terminalID>

<avs1:encryptedData>943FEBD0F52E3BC1D167DC6F3C76A29A31971EB6F0AAE7DDC969D5618DCE2D305E6BB
75F1C061A0F2088854944F4031F747C37BB4F85D0668D78B9735EAF6E1363BF8C78F9C3454A2C1BA3EE868938
FA01A28FFB2C5C095681C51424FCEB0D40E401896E1D9BAFF299D619B6A794B36431FF2DCD52F0096F17577C6
921C22FED757203DDD1997A43CED6F87F101FD6154C3BCF171D0DF49CBCECCD5AB52627D0E4D46E407C80B0B0
17B89D5DBE358298D1D64C3DB8C6954D77EC7CF75FA97CC7273D40C0EFD1B1CD4192C8A62C5DDA7ACCE86D2EB
DCAC8B0ECA1234BA9CC94030AF88180F6896B5E96F18CB90A2DB5A6F76DCFE3B3549D627468E83DFEC08320C5
72E196450CBD6CFD757B50286D4CC15A05918998152DE9EC16CAFC3CF8E78F</avs1:encryptedData>

</avs1:AVS1Request>

</soapenv:Body>

</soapenv:Envelope>
```

Содержимое encryptedData после расшифровки (3DES,CBC, DES ключ = 10101010101010101010101010101010, iv=0001020304050607)

```
<?xml version="1.0" encoding="UTF-8"?>

<avs1:cardInfo xmlns:avs1="http://www.bpc.ru/apigate/command/avs1/">
<avs1:pan>5120700080016065</avs1:pan>

<avs1:expiryMonth>11</avs1:expiryMonth>

<avs1:expiryYear>23</avs1:expiryYear>

<avs1:cvNum>123</avs1:cvNum>

</avs1:cardInfo>
```

Пример JSON запроса с шифрованием,

{"requestId":"5eb44af7-14ce-4818-aa9f-5eb0464d0534","encryptionKeyIndex":"1","encryptedData":"5F258F693EA67AA3B265C160AA214BD8052ADB6C9AB9900DCBA9E1C419A0E80EEE7692476F9B12DCE9F419C8272F77CA101AC4B031BDE78CF4C95E6BD93C7FF75F94C678FE8087D7FD7D3E3D0767D17407E8B3C2647693618332E7A6C41CA6EC"}

Содержимое encryptedData после расшифровки (3DES,CBC, DES ключ = 10101010101010101010101010101010, iv=0001020304050607)

{"cardInfo":{"pan":"5120700080016065","expiryMonth":"11","expiryYear":"23","cvNum":"123"}}

Пример JSON запроса без шифрования

{"requestId":"9ec6b859-a9ad-49cc-b08f-ad576df3e659","cardInfo":{"pan":"5120700080016065","expiryMonth":"11","expiryYear":"23","cvNum":"123"}}

***Ответ***

| **Поле** | **Тип/ длина параметра:** | **Описание параметра:** | |
|---|---|---|---|
| requestId | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | M |
| code | *Строка 1..3 симв.* | Код завершения операции.<br>000 – успешно, CVV2 matched (MDES - “MATCH”)<br>Пояснение: Проверка полученного набора значений pan + expiryMonth + expiryYear + CVV2 выполнена успешно. Карта активна.<br>CVV2 может отсутствовать, тогда проверяется pan + expiryMonth + expiryYear<br>001 – отказ, CVV2 not mached<br>Пояснение: Проверка pan + проверка expiryMonth + expiryYear выполнена успешно, а проверка CVV2 неуспешно (т.е. значение CVV2 было передано и проверено неуспешно)<br>003 - отказ (other reasons)<br>Пояснение: любые другие причины, не предусмотренные данным документом<br>005 - отказ (incorrect expiration date)<br>Пояснение: Проверка pan – успешно, а expiryMonth + expiryYear = неуспешно (т.е. значение CVV2 было передано и проверено неуспешно) | M |

Пример SOAP ответа

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:sab="http://sab/">

<soapenv:Header />

<soapenv:Body>

<sab:AVS1Response>

<sab:requestId>53b7cc3f-d3c2-4fb0-ad6e-9d85702c00fd</sab:requestId>
<sab:code>000</sab:code>

</sab:AVS1Response>

</soapenv:Body>

</soapenv:Envelope>
```

Пример JSON ответа

{

“requestId” :” 53b7cc3f-d3c2-4fb0-ad6e-9d85702c00fd</sab:requestId”,

“code”:”000”

}

# Жизненный цикл токена (Token Lifecycle)

## Outbound:

### Token Status Updated

Запрос выполняется при изменении статуса токена на стороне VTS/MDES
Информирование системы банка об изменении статуса токена на ресурсах VTS/MDES .
Интерфейс веб-службы: CardToken
Метод: tokenStatusUpdated
SOAP Endpoint: http(s)://{domain}:{port}/{context}/CardToken
REST Endpoint: http(s)://{domain}:{port}/{context}/tokenStatusUpdated

***Запрос***

| Поле | Тип параметра | Описание | Присутствие в сообщении |
|---|---|---|---|
| requestId | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | M |
| tokenRefId | *Строка, 32..64 симв.,* | Unique ID for the token associated with the PAN. This ID can be used in lieu of the token for subsequent calls, such as life cycle events | M |
| tokenRequestorId | *Строка, 11 симв.* | Unique ID assigned to the initiator of the token request | M |
| panInternalId | *Строка 1..30 симв.* | Уникальный идентификатор карты в банковской системе. Обязательным является один из двух параметров: panInternalId / panInternalGUID | C |
| panInternalGUID | *Строка, 1..32 симв.* | Уникальный идентификатор карты в банковской системе. Обязательным является один из двух параметров: panInternalGUID / panInternalId | C |
| messageReasonCode | *Строка, 1..64 симв.* | Возможные значения (ips = V, VTS Issuer API v2):<br>3701 – Token Deactivate<br>3702 – Token Suspend<br>3703 – Token Resume<br>3713 – Call Center Activation<br>3714 – Mobile Banking App Activation<br><br>Возможные значения (ips = V, VTS Issuer API v3):<br>• TOKEN_DEACTIVATED<br>• TOKEN_SUSPEND<br>• TOKEN_RESUME<br>• CALL_CENTER_ACTIVATION<br>• OTP_VERIFICATION_RESULT<br>• MOBILE_BANK_APP_ACTIVATION<br>• TOKEN_EXPIRY_DATE_UPDATED<br>• TOKEN_DEVICE_BINDING_RESULT | M |

| | | | |
|---|---|---|---|
| | | • TOKEN_DEVICE_BINDING_REMOVED<br>• LUK_REPLENISHMENT<br><br>Возможные значения (ips = M):<br><br>STATUS_UPDATE<br>REDIGITIZATION_COMPLETE<br>DELETED_FROM_CONSUMER_APP | |
| messageEventResult | *Строка, 1..64 симв* | Значения для messageReasonCode="TOKEN_DEVICE_BINDING_RESULT":<br>• DEVICE_BINDING_APPROVED<br>• DEVICE_BINDING_OTP<br>• DEVICE_BINDING_CALL_CENTER<br>• DEVICE_BINDING_ISSUER_APP<br><br>Значения для messageReasonCode="TOKEN_DEVICE_BINDING_REMOVED":<br><br>• DEVICE_BINDING_REMOVED | C |
| status | *Строка, 1 симв.* | A - Active (Token is active and ready to transact)<br>S - Suspended (Token is suspended and unable to transact)<br>D - Deactivated (Token has been permanently deactivated)<br>I - Inactive (Token has not yet been activated) | M |
| tokenExpiryMonth | *Строка, 2 симв.* | Месяц окончания срока действия токена | M |
| tokenExpiryYear | *Строка, 2 симв.* | Год окончания срока действия токена (2 последние цифры) | M |
| ips | *Строка, 1 симв.* | МПС. Возможные значения:<br>M - Mastercard<br>V - VISA | M |
| device | | | C |

| **device** | | | |
|---|---|---|---|
| deviceIndex | | *Обязательно передается для*<br>• TOKEN_DEVICE_BINDING_RESULT<br>• TOKEN_DEVICE_BINDING_REMOVED | C |

***Ответ***

| **Поле** | **Тип параметра** | **Описание** | **Присутствие в сообщении** |
|---|---|---|---|
| requestId | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | O |

| | | | |
|---|---|---|---|
| code | *Строка, 1..3 симв.* | Код завершения операции.<br>Возможные варианты значений:<br>“0” - OK Success<br>От “1” и больше – ошибка<br>1 (parseException- невалидная информация),<br>2 (nothingFoundException - по пришедшей информации ничего не найдено)<br>3 (exception - что-то пошло не так). | M |
| errorMessage | *Строка, 1..2000 симв* | Дополнительная информация.<br>Заполняется для отказов или ошибок (code != 0). | C |

Пример 1. SOAP/XML

Запрос

```
<ns2:tokenStatusUpdated xmlns:ns2="http://sab/"
xmlns:ns4="http://ws.wso2.org/dataservice">
   <ns2:requestId>23551060-5040-40ff-9743-3960c52ba2c0</ns2:requestId>

<ns2:tokenRefId>DTC1MC0000171740bf9605c539fe4c418341000005397714</ns2:tokenRefId
>
   <ns2:tokenRequestorId>51111130273</ns2:tokenRequestorId>
   <ns2:messageReasonCode>STATUS_UPDATE</ns2:messageReasonCode>
   <ns2:status>I</ns2:status>
   <ns2:tokenExpiryMonth>02</ns2:tokenExpiryMonth>
   <ns2:tokenExpiryYear>21</ns2:tokenExpiryYear>
   <ns2:ips>M</ns2:ips>
   <ns2:panInternalId>c6JceXtO3vGg</ns2:panInternalId>
   <ns2:panInternalGUID>CpxJEBHzzMpm</ns2:panInternalGUID>
</ns2:tokenStatusUpdated>
```

Ответ

```
      <sab:tokenStatusUpdatedResponse>
      <sab:requestId>23551060-5040-40ff-9743-3960c52ba2c0</sab:requestId>
     <sab:code>0</sab:code>
     </sab:tokenStatusUpdatedResponse>
```

Пример 2. REST/JSON

Запрос

```
{
   "requestId": "23551060-5040-40ff-9743-3960c52ba2c0",
   "tokenRefId": "DTC1MC0000171740bf9605c539fe4c418341000005397714",
   "tokenRequestorId": "51111130273",
   "messageReasonCode": "STATUS_UPDATE",
   "status": "I",
   "tokenExpiryMonth": "02",
   "tokenExpiryYear": "21",
   "ips": "M",
   "panInternalId": "c6JceXtO3vGg",
   "panInternalGUID": "CpxJEBHzzMpm"
}
```

Ответ


```
{
 "requestId": "23551060-5040-40ff-9743-3960c52ba2c0",
 "code": "0"
}
```


# Device Binding

## Outbound

Запрос Device Binding отправляется в банковскую систему с целью получения подтверждения со стороны банка на привязку устройства к токену.

Интерфейс веб-службы: cardToken
Метод: deviceBinding
SOAP Endpoint: http(s)://{domain}:{port}/{context}/cardToken
REST Endpoint: http(s)://{domain}:{port}/{context}/deviceBinding
Ожидаемое время отклика: <=500 ms.

***Запрос***

| Поле | Тип параметра | Описание | Присутствие в сообщении |
|---|---|---|---|
| requestId | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | M |
| tokenRequestorId | *Строка, 11 символов* | Идентификатор провайдера цифровых кошельков | M |
| tokenRefId | *Строка, 24..64 симв.,* | Unique ID for the token associated with the PAN. This ID can be used in lieu of the token for subsequent calls, such as life cycle events | M |
| panInternalId | *Строка, 1..30 симв.* | Уникальный идентификатор карты в банковской системе. Обязательным является один из двух параметров: panInternalId / panInternalGUID | C |
| panInternalGUID | *Строка, 1..32 симв.* | Уникальный идентификатор карты в банковской системе. Обязательным является один из двух параметров: panInternalGUID / panInternalId | C |
| lang | *Строка, 2 симв.* | Язык интерфейса приложения на момент ввода данных карты. Значение может использоваться, например, для отправки OTP кода с сопроводительным текстом на указанном языке. Допустимые значения - из ISO 639-1:<br>uk - Украинский<br>ru - Русский<br>en – Английский | O |
| paymentAppInstId | *Строка, 1..48 символов* | Идентификатор экземпляра приложения (кошелька), в котором создается токен | O |

| | | | |
|---|---|---|---|
| device | | | M |

| **device** | | | |
|---|---|---|---|
| deviceIndex | *Строка 1..2 симв* | Индекс устройства (например “42”) | M |
| deviceID | *Строка 1..48 симв* | Значение определяется DWP. Может включать в себя символы алфавита и специальные символы. | O |

***Ответ***

Ответ содержит решение банка для привязки устройства к токену. В случае если токенизация разрешена, в ответе возвращается номер телефона для отправки клиенту OTP кода.
Операцию считаем успешной (включая отказ), если поле code== 0;

| **Поле** | **Тип параметра** | **Описание** | **Присутствие в сообщении** |
|---|---|---|---|
| decision | *Строка, 1..33 симв.* | Может иметь одно из следующих значений<br>APPROVED – привязка устройства к токену разрешена;<br>DECLINED - привязка устройства к токену отклонена;<br>STEPUP – привязка устройства к токену, но требуется дополнительная проверка клиента | M |
| code | *Строка, 1..3 симв.* | Код завершения операции.<br>Возможные варианты значений:<br>“0” - OK Success<br>“1” – parseException (невалидная информация),<br>“2” - nothingFoundException (по пришедшей информации ничего не найдено)<br>“3” - exception (что-то пошло не так).<br>“4” – Invalid Exp. Date ~~(PAN корректный)~~<br>~~“5” – Suspicious activity~~ | M |
| customerPhone | *Строка, 12..13 симв.* | Номер телефона пользователя (“380505554433”,”+380505554433”) | C |
| errorMessage | *Строка, 1..2000 симв.* | Журналируем как доп. информацию. Может быть заполнено для отказов.<br>Заполняется для ошибок (code != 0). | C |

Пример 1. SOAP/XML

Запрос

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:deviceBinding xmlns:ns2="http://sab/" xmlns:ns4="http://ws.wso2.org/da-
taservice">
   <ns2:requestId>53b7cc3f-d3c2-4fb0-ad6e-9d85702c00fd</ns2:requestId>
   <ns2:tokenRefId>DNITHE301736046984008735</ns2:tokenRefId>
   <ns2:tokenRequestorId>50010030001</ns2:tokenRequestorId>
   <ns2:panInternalId>1203</ns2:panInternalId >
   <ns2:lang>en</ns2:lang>
   <ns2:paymentAppInstId>6Gt02SAokOGBxPoKPuP6yVpV</ns2:paymentAppInstId>
   <ns2:device>
        <ns2:deviceIndex>2</ns3:deviceIndex>
        <ns2:deviceId>zmi...zA</ns3:deviceId>
   </ns2:device>
</ns2:deviceBinding>
```

Ответ

```
<?xml version="1.0" encoding="UTF-8"?>
<sab:deviceBindingResponse xmlns:sab="http://sab/">
   <sab:decision>STEPUP</sab:decision>
   <sab:customerPhone>+380501234567</sab:customerPhone>
   <sab:code>0</sab:code>
</sab:deviceBindingResponse>
```

## Пример 2. REST/JSON

Запрос

```
{
   "requestId": "53b7cc3f-d3c2-4fb0-ad6e-9d85702c00fd",
   "tokenRefId": "DNITHE301736046984008735",
   "tokenRequestorId": "50010030001",
   "panInternalId": "1203",
   "lang": "en",
   "paymentAppInstId": "6Gt02SAokOGBxPoKPuP6yVpV",
   "device":
   {
      "deviceIndex":"2",
      "deviceId":"zmi...zA"
   }
}
```

Ответ

```
{
   "decision": "STEPUP",
   "customerPhone": "+380501234567",
   "code": "0"
}
```

# Inbound:

## Token Update

Изменение PAN and/or ExpDate (PAN) по Токену. Используется при перевыпуске токенизированной карты

Запрос выполняется из банковской системы для перепривязки новой карты к токену, когда старая карта закончилась. Новая карта должна быть из того же продукта , активной и не разу не было попыток токенизации.

По данному методу МПС нотификацию не присылают .

Метод: tokenUpdate

REST Endpoint: http(s)://{domain}:{port}/{context}/tokenUpdate

***Запрос***

| Поле | Тип параметра | Описание | Присутствие в сообщении |
|---|---|---|---|
| requestId | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | M |
| tokenRefId | *Строка, 24..64 симв.,* | Unique ID for the token associated with the PAN. This ID can be used in lieu of the token for subsequent calls, such as life cycle events<br><br>Если поле tokenRefId присутствует, то поля panInternalId (или panInternalGUID) передавать необязательно.<br>! Для карт VISA значение tokenRefId не используется. | C |
| tokenRequestorId | *Строка, 11 симв.* | Unique ID assigned to the initiator of the token request<br><br>Присутствует обязательно, если передается поле tokenRefId<br>! Для карт VISA значение tokenRequestorId не используется. | C |
| panInternalId | *Строка, 1..30 симв.* | Уникальный идентификатор карты в банковской системе.<br><br>Обязательным является один из двух параметров: panInternalId / panInternalGUID<br><br>Если поле panInternalId присутствует, то поля tokenRefId итokenRequestorId передавать необязательно.<br><br>Требуется обязательно для карт VISA<br>(FT использует данный идентификатор для поиска всех токенов в БД привязанных к данной карте и отправке запросов на перепривязку токена к новой карте либо же обновлении срока действия | C |
| panInternalGUID | *Строка, 1..32 симв.* | Уникальный идентификатор карты в банковской системе.<br>Обязательным является один из двух параметров: panInternalGUID / panInternalId<br><br>Если поле panInternalGUID присутствует, то поля tokenRefId и tokenRequestorId передавать необязательно.<br><br>Требуется обязательно для карт VISA<br>(FT использует данный идентификатор для поиска всех токенов в БД привязанных к данной карте и отправке запросов на | C |

| | | | |
|---|---|---|---|
| | | перепривязку токена к новой карте либо же обновлении срока действия) | |
| oldAccountPan | *Строка, 13..19 цифр* | Номер карты которую необходимо обновить .<br>Должен присутствовать для карт (токенов) Visa | C |
| oldExpiryMonth | *Строка, 2 цифры* | Месяц окончания срока действия старой карты.<br><br>Поддерживается только для карты VISA | C |
| oldExpiryYear | *Строка, 2 цифры* | Год окончания срока (последние две цифры) действия старой карты.<br><br>Обязательно передается для карты VISA | C |
| newAccountPan | *Строка, 13..19 цифр* | Номер новой карты для привязки к токену. | M |
| newPanInternalId | *Строка, 1..30 симв.* | Уникальный идентификатор карты в банковской системе.<br><br>Обязательным является хотя бы один из двух параметров: newPanInternalId / newPanInternalGUID | C |
| newPanInternalGUID | *Строка, 1..32 симв.* | Уникальный идентификатор карты в банковской системе.<br>Обязательным является хотя бы один из двух параметров: newPanInternalGUID / newPanInternalId | C |
| newExpiryMonth | *Строка, 2 цифры* | Месяц окончания срока действия новой карты. | C |
| newExpiryYear | *Строка, 2 цифры* | Год окончания срока (последние две цифры) действия новой карты. | C |
| ips | *Строка, 1 символ* | МПС: возможные значения<br>M - Mastercard<br>V - Visa | M |
| updateWalletProviderIndicator | *Строка, 1 символ* | For IPS = M only<br><br>Indicates whether the updated token information should be provided to the Wallet Provider. Valid values:<br>"0" - Pass the updated information to the Wallet Provider<br>"1" - Do not pass the updated information to the Wallet Provider. | O |
| commentText | *Строка 1..500 симв* | Mastercard only<br><br>Comment related to the action.<br><br>Example: Activated after confirming cardholder identity | O |
| reasonCode | | Reason for the Update token action.<br><br>Free form. | M |
| auditInfo | | | M |

| auditInfo | | | |
|---|---|---|---|
| userId | *Строка, 1..50 симв* | User ID (as assigned by the Issuer/Processor) of the Customer Service Representative who triggered the API request. String of up to 50 characters. | M |
| userName | *Строка, 1..200 симв* | User Name of the Customer Service Representative who triggered the API request. String of up to 200 characters. | M |

**! VTS MDES не присылает нотификацию по запросу Token Update**
**! Старая и новая карта должны быть в одно реньже**
**! Новая карта должна быть не оцифрованной ранее**
**! Новая карта должна быть активной**
**! Если выполняется перепривязка из веб интерфейса , выполняется проверка карты принадлежат одному клиенту**

***Ответ***

| Поле | Тип параметра | Описание | Присутствие в сообщении |
|---|---|---|---|
| requestId | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | M |
| code | *Строка 1..3 симв.* | Код завершения операции.<br>Возможные варианты значений:<br>“0” - OK Success<br>“1” - INVALID FIELD LENGTH, MISSING FIELD, INCOMPATIBLE_FIELDS, etc (неправильные входные данные)<br>“2” - NO DATA FOUND (не найден токен в БД)<br>“3” - INTERNAL ERROR | M |
| errorMessage | *Строка 1..2000 симв* | Журналируем как доп. информацию. Может быть заполнено для отказов.<br>Заполняется для ошибок (code != 0). | C |

Пример 1. REST/XML

Запрос

```
<TokenUpdateRequest>
        <requestId>c9a2d77b-be99-4e86-87c0-b332dab8aae0</requestId>
        <tokenRefId>DNITHE301736046984008715</tokenRefId>
        <tokenRequestorId>40010075001</tokenRequestorId>
        <newAccountPan>4244447899991111</newAccountPan>
        <newExpiryMonth>12</newExpiryMonth>
        <newExpiryYear>22</newExpiryYear>
        <newPanInternalId>12345</newPanInternalId>
        <newPanInternalGUID>card000000012345</newPanInternalGUID>
        <ips>V</ips>
        <reasonCode>Just update old PAN</reasonCode>
        <commentText>bla bla bla</commentText>
        <auditInfo>
                <userId>operator</userId>
                <userName>Testovenko</userName>
        </auditInfo>
</TokenUpdateRequest>
```

Ответ

```
<TokenUpdateResponse>
        <requestId>c9a2d77b-be99-4e86-87c0-b332dab8aae0</requestId>
        <code>0</code>
</TokenUpdateResponse>
```

Пример 2. REST/JSON

### Запрос


```
{
   "requestId": "4934b6ca-2ea9-47ee-a6e2-d90533012753",
   "tokenRefId": "DNITHE301805438659196336",
   "tokenRequestorId": "40010075001",
   "newAccountPan": "4234567899991111",
   "newExpiryMonth": "12",
   "newExpiryYear": "22",
   "newPanInternalId": "12345",
   "newPanInternalGUID": "card000000012345",
   "ips": "V",
   "reasonCode": "Just update old PAN",
   "commentText": "bla bla bla",
   "auditInfo": {
      "userId": "operator",
      "userName": "Testovenko"
   }
}
```


Ответ


```
{
    "requestId": "4934b6ca-2ea9-47ee-a6e2-d90533012753",
    "code": "0",
    "errorMessage": null
}
```


## Activate/Delete/Suspend/Resume Token

Запрос формируется из банковской системы и позволяет выполнить в MDES/VTS одно из действий (активацию, удаление, приостановку или возобновление) над токеном (или токенами) в привязке к карте).

Метод: tokenLifecycle
REST Endpoint: http(s)://{domain}:{port}/{context}/tokenLifecycle

***Запрос***

| Поле | Тип параметра | Описание | Присутствие в сообщении |
|---|---|---|---|
| requestId | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | M |
| tokenRefId | *Строка, 24..64 симв.,* | Unique ID for the token associated with the PAN. This ID can be used in lieu of the token for subsequent calls, such as life cycle events<br><br>Если поле tokenRefId присутствует, то поля panInternalId (или panInternalGUID) не передаются. | C |
| tokenRequestorId | *Строка, 11 симв.* | Unique ID assigned to the initiator of the token request<br><br>Присутствует обязательно, если передается поле tokenRefI | C |

| | | | |
|---|---|---|---|
| panInternalId | *Строка, 1..30 симв.* | Уникальный идентификатор карты в банковской системе.<br><br>Если поля tokenRefId и tokenRequestorId отсутствуют, то хотя бы один из параметров panInternalGUID или panInternalId должен присутсвовать. | C |
| panInternalGUID | *Строка, 1..32 симв.* | Уникальный идентификатор карты в банковской системе.<br><br>Если поля tokenRefId и tokenRequestorId отсутствуют, то хотя бы один из параметров panInternalGUID или panInternalId должен присутсвовать. | C |
| pan | *Строка, 13..19 цифр* | Номер карты. Используется только для Активации токена только для ips=M.<br><br>Если поле PAN присутствует, то поля panInternalId (или panInternalGUID), а так же tokenRefId и tokenRequestorId не передаются. | C |
| ips | *Строка, 1 символ* | МПС: возможные значения<br>M - Mastercard<br>V - Visa | M |
| paymentAppInstanceId | *Строка, [0-9,A-Z,a-z,-,_] , 1-48симв.* | Клиентский идентификатор владельца кошелька. Должен совпадать со значением, которое присылает TWP в запросе provisioning.<br>Используется только при активации токена.<br>Обязательно присутствует, при наличии поля pan | C |
| action | *Строка, 1..30 симв* | • Activate<br>• Deactivate<br>• Suspend<br>• Resume | M |
| reasonCode | *Строка, 1..254 симв* | Mastecard<br><br>Reason for the Activate action.<br><br>Valid values:<br>"A" = Cardholder successfully authenticated prior to activation.<br>"C" = Cardholder successfully authenticated with a customer service agent prior to activation.<br><br>The reason for the token Suspend action.<br>Valid values:<br>"L" - Cardholder reported token device lost.<br>"S" - Cardholder reported token device stolen.<br>"T" - Issue or cardholder reported fraudulent token transactions.<br>"Z" - Other.<br><br>The reason for the token Resume action.<br>Valid values:<br>"F" - Cardholder reported token device found or not stolen<br>"T" - Issuer or cardholder confirmed no fraudulent token transactions<br>"Z" - Other.<br><br>The reason for the token Delete action.<br>Valid values: | M |

| | | | |
|---|---|---|---|
| | | "L" - Cardholder confirmed token device lost<br>"S" - Cardholder confirmed token device stolen<br>"F" - Issuer or cardholder confirmed fraudulent token transactions (Deprecated)<br>"T" - Issuer or cardholder confirmed fraudulent token transactions<br>"C" - Account closed<br>"Z" - Other<br><br>VISA<br><br>Free form, should be descriptive enough so that if the issuer performs action, but then the consumer calls DWP Customer Support, DPW Customer Support needs to be able to read the reason and act accordingly, such as, advice the consumer.<br>For example, if the token is suspended, Request Reason may say “Suspended due to lost device”. | |
| commentText | *Строка, 1..500 симв* | Mastercard only<br><br>Comment related to the action.<br><br>Example: Activated after confirming cardholder identity | O |
| auditInfo | | | M |

| **auditInfo** | | | |
|---|---|---|---|
| userId | *Строка, 1..50 симв* | User ID (as assigned by the Issuer/Processor) of the Customer Service Representative who triggered the API request. String of up to 50 characters. | M |
| userName | *Строка, 1..200 симв* | User Name of the Customer Service Representative who triggered the API request. String of up to 200 characters. | M |

***Ответ***

| **Поле** | **Тип параметра** | **Описание** | **Присутствие в сообщении** |
|---|---|---|---|
| requestId | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | M |
| code | *Строка, 1..3 симв.* | Код завершения операции.<br>Возможные варианты значений:<br>“0” - OK Success<br>От “1” и больше – ошибка, список ошибок:1 - неправильные входные данные (INVALID FIELD LENGTH, MISSING FIELD, etc)<br>2 - NO DATA FOUND (например когда не найден токен в БД)<br>3 - INTERNAL ERROR | M |
| errorMessage | *Строка, 1..2000 симв* | Журналируем как доп. информацию. Может быть заполнено для отказов. | C |

| | | | |
|---|---|---|---|
| | | Заполняется для ошибок (code != 0). | |

Пример 1. REST/XML

Запрос

```
<?xml version="1.0" encoding="UTF-8"?>
<TokenLifecycleRequest>
<requestId>98400b0c-50c3-427f-9384-62512a54aaff</requestId>
<panInternalId>CardID141</panInternalId>
<panInternalGUID>CardID111111111113</panInternalGUID>
<ips>M</ips>
<action>Activate</action>
<reasonCode>C</reasonCode>
<commentText>bla bla bla</commentText>
<auditInfo>
        <userId>operator</userId>
        <userName>Testovenko</userName>
</auditInfo>
</TokenLifecycleRequest>
```

Ответ

```
<TokenLifecycleResponse>
    <requestId>98400b0c-50c3-427f-9384-62512a54aaff</requestId>
    <code>0</code>
    <errorMessage/>
</TokenLifecycleResponse>
```

Пример 2. REST/JSON

Запрос

```
{
   "requestId": "98400b0c-50c3-427f-9384-62512a54aaff",
   "panInternalId": "CardID141",
   "panInternalGUID": "CardID111111111113",
   "ips": "M",
   "action": "Activate",
   "reasonCode": "C",
   "commentText": "bla bla bla",
   "auditInfo": {
      "userId": "operator",
      "userName": "Testovenko"
   }
}
```

Ответ

```
{
    "requestId": "98400b0c-50c3-427f-9384-62512a54aaff",
    "code": "0",
    "errorMessage": null
}
```

## Get Token Info

### Inbound

Запрос позволяет запросить в MDES/VTS полную актуальную информацию о токене или токенах привязанных к карте

Метод: tokenInfo
REST Endpoint: http(s)://{domain}:{port}/{context}/tokenInfo

***Запрос***

| Поле | Тип параметра | Описание | Присутствие в сообщении |
|---|---|---|---|
| requestId | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | M |
| tokenRefId | *Строка, 1..64 симв.,* | Unique ID for the token associated with the PAN. This ID can be used in lieu of the token for subsequent calls, such as life cycle events<br><br>Если поле tokenRefId присутствует, то поля panInternalId (или panInternalGUID), а также pan и paymentAppInstanceId не передаются. | C |
| tokenRequestorId | *Строка, 11 симв.* | Unique ID assigned to the initiator of the token request<br><br>Присутствует обязательно, если передается поле tokenRefId | C |
| panInternalId | *Строка 1..30 симв* | Уникальный идентификатор карты в банковской системе.<br><br>Обязательным является один из двух параметров: panInternalId / panInternalGUID<br><br>Если поле panInternalId присутствует, то поля tokenRefId и tokenRequestorI, а также pan и paymentAppInstanceId не передаются. | C |
| panInternalGUID | *Строка, 1..32 симв.* | Уникальный идентификатор карты в банковской системе. Обязательным является один из двух параметров: panInternalGUID / panInternalId<br><br>Если поле panInternalGUID присутствует, то поля tokenRefId и tokenRequestorId, а также pan и paymentAppInstanceId не передаются. | C |
| pan | *Строка, 13..19 цифр* | Номер карты<br><br>Если поле PAN присутствует, то поля panInternalId (или panInternalGUID), а так же tokenRefId и tokenRequestorId не передаются. | C |
| ips | *Строка,* | МПС: возможные значения | M |

| | | | |
|---|---|---|---|
| | *1 символ* | M - Mastercard<br>V - Visa | |
| paymentAppInstanceId | *Строка, [0-9,A-Z,a-z,-,_] , 1-48 симв.* | Клиентский идентификатор владельца кошелька. Должен совпадать со значением, которое присылает TWP в запросе provisioning.<br>Обязательно присутствует, при наличии поля pan | C |
| auditinfo | | | M |

| **auditInfo** | | | |
|---|---|---|---|
| userId | *Строка, 1..50 симв* | User ID (as assigned by the Issuer/Processor) of the Customer Service Representative who triggered the API request. String of up to 50 characters. | M |
| userName | *Строка, 1..200 симв* | User Name of the Customer Service Representative who triggered the API request. String of up to 200 characters. | M |

***Ответ***

| **Поле** | **Тип параметра** | **Описание** | **Присутствие в сообщении** |
|---|---|---|---|
| requestId | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | M |
| code | *Строка, 1..3 симв.* | Код завершения операции.<br>Возможные варианты значений:<br>“0” - OK Success<br>От “1” и больше – ошибка, список ошибок согласовать | M |
| errorMessage | *Строка, 1..2000 симв* | Журналируем как доп. информацию. Может быть заполнено для отказов.<br>Заполняется для ошибок (code != 0). | C |
| tokens | | Array | C |

| **tokens Array** | | | |
|---|---|---|---|
| token | | | M |

| **token** | | | |
|---|---|---|---|
| accountPanSuffix | *Строка, 4 цифры* | | Последние 4ре цифры PAN |
| panExpirationDate | *MMyy* | только MDES | |
| tokenRefId | *Строка, до 64 симв.* | | |
| tokenSuffix | *Строка, 4 цифры* | | Последние 4ре цифры токена |
| tokenExpiryMonth | *MM* | | |
| tokenExpiryYear | *yy* | | |
| correlationId | *Строка, 14 симв.* | Сквозной идентификатор серии запросов, выполняющихся при токенизации карты. Аналог CorrelationId (MDES) | |
| currentStatusCode | *Строка, 1 символ* | набор значений, как в VTS | |
| currentStatusDescription | | | |
| currentStatusDateTime | *ISO 8601 DateTime* | | |
| digitizationRequestDateTime | *ISO 8601 DateTime* | только MDES | |
| lastCommentId | | только MDES | |
| paymentAppInstanceId | *Строка, до 48 симв.* | | |
| provisioningStatusCode | *Строка, 1 символ* | только MDES | |
| storageTechnology | *Строка, до 64 симв.* | набор “длинных” значений Storage Technology MDES<br>для VTS - производная от tokenType, из набора Token Protection Method только SECURE_ELEMENT и CLOUD | |
| tokenActivatedDateTime | *ISO 8601 DateTime* | | |
| tokenRequestorId | *Строка, до 11 симв.* | | |
| tokenRequestorName | *Строка, до 128 симв* | | |

| | | | |
|---|---|---|---|
| tokenType | *Строка, 1 символ* | набор значений, как в VTS | |
| panInternalId | *Строка, до 30 симв.* | | |
| panInternalGUID | *Строка, до 32 симв.* | | |
| ips | *Строка, 1 символ* | M, V | |
| device | | | |

| **device** | | | |
|---|---|---|---|
| deviceId | | | |
| deviceName | | | |
| deviceType | *Строка, до 64 симв.* | набор “длинных” значений Form Factor MDES | |
| secureElementId | | | |

Пример 1. REST/XML

Запрос

```
<?xml version="1.0" encoding="UTF-8" ?>
<TokenInfoRequest>
    <requestId>98400b0c-50c3-427f-9384-62512a54aaff</requestId>
    <panInternalId>CardID141</panInternalId>
    <panInternalGUID>CardID111111111113</panInternalGUID>
    <ips>M</ips>
    <auditInfo>
        <userId>operator</userId>
        <userName>Testovenko</userName>
    </auditInfo>
</TokenInfoRequest>
```

Ответ

```
<TokenInfoResponse>
    <requestId>98400b0c-50c3-427f-9384-62512a54aaff</requestId>
    <code>0</code>
    <errorMessage/>
    <tokens>
        <token>
            <accountPanSuffix>1234</accountPanSuffix>
            <panExpirationDate>1215</panExpirationDate>
            <tokenRefId>DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45</token-
RefId>
            <tokenSuffix>7890</tokenSuffix>
            <tokenExpiryMonth>10</tokenExpiryMonth>
            <tokenExpiryYear>16</tokenExpiryYear>
            <correlationId>98765432101234</correlationId>
            <currentStatusCode>A</currentStatusCode>
            <currentStatusDescription>Active</currentStatusDescription>
            <currentStatusDateTime>2015-01-21T00:04:35.000Z</currentSta-
tusDateTime>
            <digitizationRequestDateTime>2015-01-21T00:04:35.000Z</digitization-
RequestDateTime>
            <lastCommentId>ABC123456</lastCommentId>
            <paymentAppIn-
stanceId>645b532a245e4723d7a9c4f62b24f24a24ba98e27d43e34e</paymentAppInstanceId>
            <provisioningStatusCode>S</provisioningStatusCode>
            <storageTechnology>DEVICE_MEMORY</storageTechnology>
            <tokenActivatedDateTime>2015-01-21T00:04:35.000Z</tokenActivat-
edDateTime>
            <tokenRequestorId>50000000001</tokenRequestorId>
            <tokenRequestorName>Wallet Provider 103</tokenRequestorName>
            <tokenType>S</tokenType>
            <panInternalId>CardID141</panInternalId>
            <panInternalGUID>CardID111111111113</panInternalGUID>
            <ips>M</ips>
            <device>
                <de-
viceId>6b24f24a24ba98e27d43e345b532a245e4723d7a9c4f624e93452c92de9357a5</de-
viceId>
                <deviceName>John's Phone</deviceName>
                <deviceType>PHONE</deviceType>
                <secureElementId>92de9357a535b2c21a3566e446f43c532a46b54c46</se-
cureElementId>
            </device>
        </token>
        <token>
            <accountPanSuffix>1234</accountPanSuffix>
            <panExpirationDate>1215</panExpirationDate>
            <tokenRefId>DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a46</token-
RefId>
            <tokenSuffix>7891</tokenSuffix>
            <tokenExpiryMonth>10</tokenExpiryMonth>
            <tokenExpiryYear>16</tokenExpiryYear>
            <correlationId>98765432101234</correlationId>
            <currentStatusCode>A</currentStatusCode>
            <currentStatusDescription>Active</currentStatusDescription>
            <currentStatusDateTime>2015-01-21T00:04:35.000Z</currentSta-
tusDateTime>



}
```

Пример 1. REST/JSON

Запрос


```
{
   "requestId": "98400b0c-50c3-427f-9384-62512a54aaff",
   "panInternalId": "CardID141",
   "panInternalGUID": "CardID111111111113",
   "ips": "M",
   "auditInfo": {
      "userId": "operator",
      "userName": "Testovenko"
   }
}
```

## Ответ


```
{
    "requestId": "98400b0c-50c3-427f-9384-62512a54aaff",
    "code": "0",
    "errorMessage": null,
    "tokens": [
        {
            "accountPanSuffix": "1234",
            "panExpirationDate": "1215",
            "tokenRefId": "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a45",
            "tokenSuffix": "7890",
            "tokenExpiryMonth": "10",
            "tokenExpiryYear": "16",
            "correlationId": "98765432101234",
            "currentStatusCode": "A",
            "currentStatusDescription": "Active",
            "currentStatusDateTime": "2015-01-21T00:04:35.000Z",
            "digitizationRequestDateTime": "2015-01-21T00:04:35.000Z",
            "lastCommentId": "ABC123456",
            "paymentAppInstanceId":
"645b532a245e4723d7a9c4f62b24f24a24ba98e27d43e34e",
            "provisioningStatusCode": "S",
            "storageTechnology": "DEVICE_MEMORY",
            "tokenActivatedDateTime": "2015-01-21T00:04:35.000Z",
            "tokenRequestorId": "50000000001",
            "tokenRequestorName": "Wallet Provider 103",
            "tokenType": "S",
            "panInternalId": "CardID141",
            "panInternalGUID": "CardID111111111113",
            "ips": "M",
            "device": {
                "deviceId":
"6b24f24a24ba98e27d43e345b532a245e4723d7a9c4f624e93452c92de9357a5",
                "deviceName": "John's Phone",
                "deviceType": "PHONE",
                "secureElementId": "92de9357a535b2c21a3566e446f43c532a46b54c46"
            }
        },
        {
            "accountPanSuffix": "1234",
            "panExpirationDate": "1215",
            "tokenRefId": "DWSPMC000000000132d72d4fcb2f4136a0532d3093ff1a46",
            "tokenSuffix": "7891",
            "tokenExpiryMonth": "10",
            "tokenExpiryYear": "16",
            "correlationId": "98765432101234",
            "currentStatusCode": "A",
            "currentStatusDescription": "Active",
            "currentStatusDateTime": "2015-01-21T00:04:35.000Z",
            "digitizationRequestDateTime": "2015-01-21T00:04:35.000Z",
            "lastCommentId": "ABC123456",
            "paymentAppInstanceId":
"645b532a245e4723d7a9c4f62b24f24a24ba98e27d43e34e",
            "provisioningStatusCode": "S",
            "storageTechnology": "DEVICE_MEMORY",
            "tokenActivatedDateTime": "2015-01-21T00:04:35.000Z",
            "tokenRequestorId": "50000000001",
            "tokenRequestorName": "Wallet Provider 103",
```

## Card Data Update

Запрос позволяет обновить данные карты локально (в БД FastTack). Запрос cardDataUpdate используется банком в случае необходимости обновить в БД FT информацию о привязке новой карты к токену. Такая необходимость, к примеру, может возникнуть в случае, когда МПС не прислал tokenUpdate о перепривязке токенов к новой карте.

Этот метод позволяет установить правильные значения новой карты newPanInternalId, newPanInternalGUID.

Метод: /cardDataUpdate
REST Endpoint: http(s)://{domain}:{port}/{context}/cardDataUpdate

***Запрос***

| Поле | Тип параметра | Описание | Присутствие в сообщении |
|---|---|---|---|
| requestId | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | M |
| tokenRefId | *Строка, 1..64 симв.,* | Unique ID for the token associated with the PAN. This ID can be used in lieu of the token for subsequent calls, such as life cycle events | M |
| tokenRequestorId | *Строка, 11 симв.* | Unique ID assigned to the initiator of the token request | M |
| newAccountPan | *Строка, 13..19 цифр* | Номер новой карты для привязки к токену. | O |
| newPanInternalId | *Строка 1..30 симв.* | Новый уникальный идентификатор карты в банковской системе.<br><br>Обязательным является хотя бы один из двух параметров: newPanInternalId / newPanInternalGUID | M O |
| newPanInternalGUID | *Строка 1..32 симв.* | Новый уникальный идентификатор карты в банковской системе. Обязательным является хотя бы один из двух параметров: newPanInternalGUID / newPanInternalId | O M |

***Ответ***

| Поле | Тип параметра | Описание | Присутствие в сообщении |
|---|---|---|---|
| requestId | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | M |
| code | *Строка 1..3 симв* | Код завершения операции.<br>Возможные варианты значений:<br>“0” - OK Success<br>От “1” и больше – ошибка, список ошибок согласовать | M |
| errorMessage | *Строка 1..2000 симв.* | Журналируем как доп. информацию. Может быть заполнено для отказов.<br>Заполняется для ошибок (code != 0). | C |

Пример 1. REST/XML

Запрос

```
<CardDataUpdateRequest>
   <requestId>a41b63d2-abaa-43ec-9750-1a997d13d9ea</requestId>
   <tokenRefId>DTC1MC0000171740bf9605c539fe4c418341000005400816</tokenRefId>
      <newPanInternalId>CardID00000000000003</newPanInternalId>
   <tokenRequestorId>50100000001</tokenRequestorId>
</CardDataUpdateRequest>
```

Ответ

```
<CardDataUpdateResponse>
   <requestId>a41b63d2-abaa-43ec-9750-1a997d13d9ea</requestId>
   <code>0</code>
   <errorMessage />
</CardDataUpdateResponse>
```

Пример 2. REST/JSON

Запрос

```
{
    "requestId":"f455a4a1wf3ffw4fc3w9e04wa1bec901d27b",
    "tokenRefId":"DTC1MC0000171740bf9605c539fe4c41834520eeb0719138",
    "tokenRequestorId":"50100000001",
    "newPanInternalId":"CardID00000000000003"
}
```

Ответ

```
{
    "requestId": "f455a4a1wf3ffw4fc3w9e04wa1bec901d27b",
    "code": "0",
    "errorMessage": null
}
```

# Push-Provisioning, In-App Provisioning

## Create Opaque Payment Card (Push-Provisioning)

## (Google pay, Samsung Pay, Xiaomi Pay)

### Inbound

API который позволяет зашифровать данные публичным ключом МПС. Запрос выполняется для шифрования sensitive data карты и сопутствующих данных публичным ключом соответствующей МПС для последующей передачи данных в мобильное приложение. Шифрование выполняется на стороне FT

Метод: createOpaquePaymentCard
REST Endpoint: http(s)://{domain}:{port}/{context}/createOpaquePaymentCard

***Запрос***

| Поле | Тип параметра | Описание | Присутствие в сообщении |
|---|---|---|---|
| requestId | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | M |
| pan | *Строка, 13..19 цифр* | Номер карты | M |
| expiryMonth | *Строка, 2 цифры* | Месяц окончания срока действия карты | M |
| expiryYear | *Строка, 2 цифры* | Год окончания срока (последние две цифры) действия карты | M |
| country | *Строка, 2 симв.* | Код страны согласно ISO 3166-1, например, "UA" | M |
| intent | *ENUM* | Используется одно из следующих значений:<br>PUSH_PROV_MOBILE<br>PUSH_PROV_ONFILE<br>Значение PUSH_PROV_MOBILE означает, что банк эмитент передает PAN карты для получения и сохранения токена на мобильное устройство клиента.<br>Значение PUSH_PROV_ONFILE означает, что банк эмитент передает PAN карты для получения и сохранения токена в облаке, для последующего использования в е-коммерции. | M |
| clientWalletProvider | *Строка, [0-9,A-Z,a-z,-,_],*<br>*50 симв.* | Клиентский идентификатор провайдера цифрового кошелька представляет собой ID инициатора запроса на токен (TRID), который выдается провайдеру кошелька в рамках onboarding процесса.<br>Пример значения: "40000000047"<br>Для Google Pay в Mastercard – 50120834693<br>Для Google Pay в VISA – 40010075001 | M |
| clientWalletAccountID | *Строка,* | Клиентский идентификатор (экземпляра) кошелька, в котором создается токен. Для VISA совпадает со значением в поле | M |

| | | | |
|---|---|---|---|
| | *[0-9,A-Z,a-z,-,_] , 24 симв.* | paymentAppInstId, которое присылает TWP в запросе provisioning. Для MC совпадает только с первыми 24мя символами значения из paymentAppInstId. Этот идентификатор экземпляра кошелька (Payment Application Instance ID в терминологии Mastercard), который нужно запросить в мобильном приложении банка непосредственно у кошелька Google Pay . | |
| clientDeviceID | *Строка, [0-9,A-Z,a-z,-,_] , 24 симв* | Неизменяемый набор данных, определяемых провайдером кошелька, однозначно идентифицирующий мобильное устройство. Может быть вычислен, или ID, привязанный к оборудованию, например, такой как TEE_ID или SE_ID.<br>Поле должно совпадать со значением, которое присылает TWP в запросе provisioning.<br>Обязательно к заполнению, если значение параметра intent равно “PUSH_PROV_MOBILE”.<br>Пример: "ed6abb56323ba656521ac476" | C |
| clientAppID | *Строка, [A-Z][a-z][0-9,-] , 36 симв* | Уникальный идентификатор клиентского приложения, которое используется для шифрования данных карты. Эмитент должен определить значение clientAppID в процессе onboarding.<br>Обязательно к заполнению, если значение параметра intent равно “PUSH_PROV_MOBILE”.<br>Пример: "MyBank Mobile App" -название банковского приложения<br>Visa- обязательное значение<br>MC- любое не пустое значение | C |
| isIDnV | *Строка* | Строковое поле указывает, желает ли эмитент выполнить ID&V по данной карте. Если значение равно «false» или отсутствует, тогда эмитент не получит на хост сообщения 0100 TAR или 0100 AV, и соответственно step-up не будет инициирован в процессе provisioning.<br>Может принимать два значения “true” или “false”. | M |
| cardholderName | *Строка, 27 символов* | Имя держателя карты в формате<br><br>LASTNAME/FIRSTNAME<br>или<br>FIRSTNAME LASTNAME | M |
| ips | *Строка, 1 символ* | МПС: возможные значения<br>M - Mastercard<br>V – Visa | M |

***Ответ***

| Поле | Тип параметра | Описание | Присутствие в сообщении |
|---|---|---|---|
| opaqueBody | *Строка, 1..4000 симв.* | Зашифрованный блок данных для передачи в VISA/MDES через TWP. Используется кодировка в формате Base64 | M |
| code | *Строка 1..3 симв.* | Код завершения операции.<br>Возможные варианты значений:<br>“0” - OK Success<br>“1” - Cryptography error | M |

| | | | |
|---|---|---|---|
| errorMessage | *Строка 1..2000 симв* | Журналируем как доп. информацию. Может быть заполнено для отказов.<br>Заполняется для ошибок (code != 0). | C |

Пример 1. REST/XML

Запрос

```
<CreateOpaquePaymentCardRequest>
    <requestId>db79581f-90c4-44e6-96cb-a0d366d1a6fe</requestId>
    <pan>444444*****5035</pan>
    <expiryMonth>12</expiryMonth>
    <expiryYear>20</expiryYear>
    <country>UA</country>
    <intent>PUSH_PROV_MOBILE</intent>
<clientWalletProvider>0010075001</clientWalletProvider>
<clientWalletAccountID>uljnYNEQh9Xr9DWN5G7jMCNj</clientWalletAccountID>
    <isIDnV>false</isIDnV>
    <cardholderName>ELENA PREKRASNAYA</cardholderName>
    <ips>V</ips>
<clientDeviceID>EbHhO8o5y5NP8V1IbUug15Cr</clientDeviceID>
    <clientAppID>MOBILE</clientAppID>
</CreateOpaquePaymentCardRequest>
```

Ответ

```
<CreateOpaquePaymentCardResponse>

<opaqueBody>eyJhbGciOiJBMjU2R0NNS1ciLCJpdiI6IlplQnRHOEtXaVhEYnZadXIiLCJ0YWciOiJ1
elQ5NFNxYm9xMUtoTUdac1JuU3NnIiwiZW5jIjoiQTI1NkdDTSIsInR5cCI6IkpPU0UiLCJraWQiOi-
JOQzlIVk5BS1FTOUZSMFFVMDY4TzIxTm-
lEV1pxUV9yQzFLVVg4bTd2ZlpQa0RFVng0IiwiY2hhbm5lbFNlY3VyaXR5Q29udGV4dCI6IlNIQVJFRF
9TRUNSRVQiLCJpYXQiOiIxNTQ5Mjg4NDY4In0.GBHZ9l7PTc0u2PwBGz7VdwW7kz0ZbEVBVzj-
I_mwTtA.0mZ4tDat9NTTxS-X.M97oaht7E4OgfsIDjW2vSLcr4ALyfMROZqVVY7EqUFyavuZE-
gFAjHLdceIY1mYYF19FtZ0oePte23Rss8SN9ZmlPgExLAEoErVwUKVDLfn71FVaUJ-ysrE-
ZUmcCpOdOw4H0DmkqIfEvWoaOE-U9yjUErHDNk_2hEQTFnavfr_f1vWwcF9T_6ZDkeWVsM8U-
7aWR6BuEUxaDynwEIp2TPWeHabv_YWJjmRIgdXBpJhnWTpHMM_nbOU0mVxBsv4SwO3yKsMhCz4GsAgPN
9zoabdIQqDmrumaKC14f8kfBpWyhApyCu9yPZ6Ooxi1O-TGZ-
t3N0mL3gtpNCy5soBNksUSGCUpeTHcPCgNinDzkY8N5gjO9_uwi99qpDmGomXikcQv3tUtectTyAa-
KoPGpLYOJRgUeu7A5mEBA6euGBlKIgHJWpnNSa-A7BuAAtO8N3cdnEKuCBprPUBL-
WnfvMwGYpHk7rZ.-xbDmIXKE8X7WHN09sjq-Q</opaqueBody>
    <code>0</code>
</CreateOpaquePaymentCardResponse>
```

Пример 2. REST/JSON

Запрос


```
{
  "requestId": " db79581f-90c4-44e6-96cb-a0d366d1a6fe",
  "pan": "444444*****15035",
  "expiryMonth": "12",
  "expiryYear": "20",
  "country": "UA",
  "intent": "PUSH_PROV_MOBILE",
  "clientWalletProvider": "0010075001",
  "clientWalletAccountID": "uljnYNEQh9Xr9DWN5G7jMCNj",
  "isIDnV": "false",
  "cardholderName": "ELENA PREKRASNAYA",
  "ips": "V",
  "clientDeviceID": "EbHhO8o5y5NP8V1IbUug15Cr",
  "clientAppID": "MOBILE"
}
```

Ответ

{
"opaqueBody":
"eyJhbGciOiJBMjU2R0NNS1ciLCJpdiI6IjQ1TTB4SjV4X0h2ekRadDUiLCJ0YWciOiJpWWZZakF1d0wtYUtSdmprek5WZUtRIiwiZW5jIjoiQTI1NkdDTSIsInR5cCI6IkpPU0UiLCJraWQiOiJOQzlIVk5BS1FTOUZSMFFVMDY4TzIxTmlEV1pxUV9yQzFLVVg4bTd2ZlpQa0RFVng0IiwiY2hhbm5lbFNlY3VyaXR5Q29udGV4dCI6IlNIQVJFRF9TRUNSRVQiLCJpYXQiOiIxNTQ5Mjg5OTU4In0.wIhVba2wqQ2xjHLBdEJaaSHGrVTl6ChbhrrWjeZtMXE.tRcEAYEPz7imn0L7.LOmtxkxdMtFIHKeTV4tA1tg4e8OW4K96-BJwfJAB-ETxHFD8jKVKwefA2LdWJ2tZGfn6mtMmWRy7Ta-Q7six6UrURydurNrBnWtjXGnfdM2DOCL9VPOYFFfQxV7WrOUA6bujYDYrxqV3T32VjOsFxnsnW3Xr2RFbzjOF6S8tf8BYB4KNywxYfY27xql0BbJf1h4OlZJdl7zVfvAhz0JEuzOYAReLFloElunJ-qfPGTsa9R0zO6CTwBa-F6eNLO9UJ4wFKzOf0vWXW6LBd5lVaSNh8IR3aR4uOJlY66evmdekDmIK-TNUcJT0gs9xENTgeZZqaNzl5RXphIjnBLz9tUemYxERWXiBGD0yIB-KDwfyWUrnoSJrPIi3YXd-t6qUIAo1SUykgHVVp4nkB26govG1D9Ca3wreBc0X64F1F5IVD6Lyy9xXkBTk5lFYux0SCXinroX_EZm5hshKg_-gWJXy8SLS.IeaBdpujOCNfS6U6bbcE_g",
"code": "0"
}

## Create InApp Provisioning Data

API который позволяет сформировать данные для способа передачи данных карты In-App Provisioning в Apple Pay. Запрос выполняется для шифрования sensitive data карты и сопутствующих данных ключами Apple и, опционально, ключами соответствующей МПС для последующей передачи данных в мобильное приложение. Шифрование выполняется на стороне FT.

Метод: createInAppProvisioningData
REST Endpoint: http(s)://{domain}:{port}/{context}/createInAppProvisioningData

***Запрос***

| Поле | Тип параметра | Описание | Присутствие в сообщении |
|---|---|---|---|
| requestId | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | M |
| pan | *Строка, 13..19 цифр* | Номер карты | M |
| expiryMonth | *Строка, 2 цифры* | Месяц окончания срока действия карты | M |

| | | | |
|---|---|---|---|
| expiryYear | *Строка, 2 цифры* | Год окончания срока (последние две цифры) действия карты | M |
| cardholderName | *Строка, 27 символов* | Имя держателя карты в формате<br><br>FIRSTNAME LASTNAME | M |
| ips | *Строка, 1 символ* | МПС: возможные значения<br>M - Mastercard<br>V – Visa | M |
| nonce | *Строка, HEX-ASCII* | Случайное значение, полученное мобильным приложением от Apple Wallet. Представлено в виде набора шестнадцатеричных цифр в кодировке ASCII. Количество цифр - четное | M |
| nonceSignature | *Строка, HEX-ASCII* | Подпись случайного значения nonce, полученная мобильным приложением от Apple Wallet. Представлена в виде набора шестнадцатеричных цифр в кодировке ASCII. Количество цифр - четное | M |
| certificates | *Массив элементов certificate* | Массив элементов certificate с данными о сертификатах Apple, полученных мобильным приложением от Apple Wallet. Описание элементов см. в следующей строке | M |
| certificate | *Строка* | Сертификат Apple, DER-кодированное значение. Представлено в кодировке Base64 | M |

***Ответ***

| **Поле** | **Тип параметра** | **Описание** | **Присутствие в сообщении** |
|---|---|---|---|
| encryptedPassData | *Строка* | Зашифрованный блок данных о карте для передачи через мобильное приложение в Apple Wallet. Представлено в кодировке Base64 | M |
| activationData | *Строка* | Зашифрованный блок данных, подтверждающих активацию токена, для передачи через мобильное приложение в Apple Wallet. Представлено в кодировке Base64 | M |
| ephemeralPublicKey | *Строка* | Разовый публичный ключ, использующийся в шифровании ECC. Значение представлено в кодировке Base64 | M |
| authcode | *Строка, 6 символов* | “Код авторизации”. Этот код передается в составе шифрованных данных activationData в VTS. В дальнейшем он служит для идентификации кодов активации при возникновении вопросов по процессу In-App Provisioning. Присутствует только в случае ips = ‘V’ в запросе. | C |
| code | *Строка 1..3 симв.* | Код завершения операции.<br>Возможные варианты значений:<br>“0” - OK Success | M |

| | | | |
|---|---|---|---|
| | | От “1” и больше – ошибка, список ошибок согласовать | |
| errorMessage | *Строка 1..2000 симв* | Журналируем как доп. информацию. Может быть заполнено для отказов.<br>Заполняется для ошибок (code != 0). | C |

Пример 1. REST/XML

Запрос

```
<CreateInAppProvisioningDataRequest>
<requestId>1da5f3f8-2378-40da-9c26-2d59ab6f1db8</requestId>
<pan>444444*****56789</pan>
<expiryMonth>12</expiryMonth>
<expiryYear>20</expiryYear>
<cardholderName>FIRSTNAME LASTNAME</cardholderName>
<ips>V</ips>
<nonce>9c023092</nonce>
<nonceSigna-
ture>4082f883ae62d0700c283e225ee9d286713ef74456ba1f07376cf17d71bf0be013f926d4866
19394060ced56030f41f84df916eaab5504e456a8530dc9c821f6ed3e3af62b5d8f3e4a22ca20186
70fee4e</nonceSignature>
<certificates>
<certificate>
MIIEEzCCA7igAwIBAgIIEvD9KtxTuV0wCgYIKoZIzj0EAwIwgYExOzA5BgNVBAMMMlRlc3QgQXBw
bGUgV29ybGR3aWRlIERldmVsb3BlcnMgUmVsYXRpb25zIENBIC0gRUNDMSAwHgYDVQQLDBdDZXJ0
aWZpY2F0aW9uIEF1dGhvcml0eTETMBEGA1UECgwKQXBwbGUgSW5jLjELMAkGA1UEBhMCVVMwHhcN
MTcwNTIwMDQxNTU3WhcNMTkwNjE5MDQxNTU3WjBtMTYwNAYDVQQDDC1lY2MtY3J5cHRvLXNlcnZp
Y2VzLWVuY2lwaGVybWVudF9VQzYtSW5NZW1vcnkxETAPBgNVBAsMCEFwcGxlUGF5MRMwEQYDVQQK
DApBcHBsZSBJbmMuMQswCQYDVQQGEwJVUzBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABC4+XM9r
mrBL56IvP6zP3nPIfocVU5SjSBVAiolsoYo3TaxmmvO/YiD8hjdn9K9HUHxbwiH8ShmHTa85tAdO
PrijggIrMIICJzBPBggrBgEFBQcBAQRDMEEwPwYIKwYBBQUHMAGGM2h0dHA6Ly9vY3NwLXVhdC5j
b3JwLmFwcGxlLmNvbS9vY3NwMDQtdGVzdHd3ZHJjYWVjYzAdBgNVHQ4EFgQUrS6jy340wu3uQ2hO
JxEfzEkzOdAwDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAWgBTW1tVa5f/9wnw0w0PevWh2XDapvjCC
AR0GA1UdIASCARQwggEQMIIBDAYJKoZIhvdjZAUBMIH+MIHDBggrBgEFBQcCAjCBtgyBs1JlbGlh
bmNlIG9uIHRoaXMgY2VydGlmaWNhdGUgYnkgYW55IHBhcnR5IGFzc3VtZXMgYWNjZXB0YW5jZSBv
ZiB0aGUgdGhlbiBhcHBsaWNhYmxlIHN0YW5kYXJkIHRlcm1zIGFuZCBjb25kaXRpb25zIG9mIHVz
ZSwgY2VydGlmaWNhdGUgcG9saWN5IGFuZCBjZXJ0aWZpY2F0aW9uIHByYWN0aWNlIHN0YXRlbWVu
dHMuMDYGCCsGAQUFBwIBFipodHRwOi8vd3d3LmFwcGxlLmNvbS9jZXJ0aWZpY2F0ZWF1dGhvcml0
eS8wQQYDVR0fBDowODA2oDSgMoYwaHR0cDovL2NybC11YXQuY29ycC5hcHBsZS5jb20vYXBwbGV3
d2RyY2FlY2MuY3JsMA4GA1UdDwEB/wQEAwIDKDASBgkqhkiG92NkBicBAf8EAgUAMAoGCCqGSM49
BAMCA0kAMEYCIQCMvUq2YUxY/RqTWE4FqsPTr9zGyilCunIU3FSobtep7gIhAN7Vdx3B0p7DTCqX
Hd05IPsZGLdIDG1NTxOk2Oj/N7GG
</certificate>
<certificate>
MIIC5zCCAoygAwIBAgIIR1pCSszYnvcwCgYIKoZIzj0EAwIwZzEhMB8GA1UEAwwYVGVzdCBBcHBs
ZSBSb290IENBIC0gRUNDMSAwHgYDVQQLDBdDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTETMBEGA1UE
CgwKQXBwbGUgSW5jLjELMAkGA1UEBhMCVVMwHhcNMTQwMjA2MTYxODI5WhcNMjQwMjA0MTYxODI5
WjCBgTE7MDkGA1UEAwwyVGVzdCBBcHBsZSBXb3JsZHdpZGUgRGV2ZWxvcGVycyBSZWxhdGlvbnMg
Q0EgLSBFQ0MxIDAeBgNVBAsMF0NlcnRpZmljYXRpb24gQXV0aG9yaXR5MRMwEQYDVQQKDApBcHBs
ZSBJbmMuMQswCQYDVQQGEwJVUzBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABDzb9Lsna4XrUdRw
Ijl36m9hTGhxQrW5Ls3wYr07kaZ/5tMOEG5jOBeHtI+x8YHmkgp0Ry43nmZTik3vosay+6ajggEF
MIIBATBUBggrBgEFBQcBAQRIMEYwRAYIKwYBBQUHMAGGOGh0dHA6Ly9vY3NwLXVhdC5jb3JwLmFw
cGxlLmNvbS9vY3NwMDQtdGVzdGFwcGxlcm9vdGNhZWNjMB0GA1UdDgQWBBTW1tVa5f/9wnw0w0Pe
vWh2XDapvjASBgNVHRMBAf8ECDAGAQH/AgEAMB8GA1UdIwQYMBaAFNJH4sU0ccYQjZPuBEMf4RsP
4c0RMEUGA1UdHwQ+MDwwOqA4oDaGNGh0dHA6Ly9jcmwtdWF0LmNvcnAuYXBwbGUuY29tL3Rlc3Rh
cHBsZXJvb3RjYWVjYy5jcmwwDgYDVR0PAQH/BAQDAgEGMAoGCCqGSM49BAMCA0kAMEYCIQCd4eDj
SiTu55mDKWCaD7Tqe4hp86pJ1Fsw7SlPKmH+bQIhAJ5coaJ3uarz81Im19NGcrU45h1A8hNDTz55
QPEHujS5
</certificate>
</certificates>
</CreateInAppProvisioningDataRequest>
```

Ответ

```
<CreateInAppProvisioningDataResponse>
    <encryptedPassData>irehODkajUJHywDcqDdNBltgNmlEVWVjaCxh-
dooCBzmzuF72gU8NxloadbNqFBchfs4x2RB5/Sg/DN7dgG-
pzk8N/Kyr3RQ7qHCQ3wrNvLd5MUeYrBiCtJp2kN4d84N4QRwz5pvs+kSjU7gvA/RnyE46+AvQR2ucjtV
uKwrLl2iI7e+g5bm35Ks08U+rs5chzbC64jo/lb0ROuSOcGVQGErHa8R5JgY3jss9htEkdVLd8ViS-
Jmuem6wWjcGbMfIhUfle1RdpWjBIzV7mbLnUlgh509EnIdM1YBqMbSsWzVWlhUzthQrOi-
SoDQx614a7t76qGkLGXAVSqkNgMcwmXYOYbV95F162Y2HjmtpAH-
qUUoG+GFtoqI/29ZnUKm1ERG4NvLjRkL1NCNbLPA2VarzMo9EhH3p4P16i9d8MlMjiW4DtmfS91rz7H3
9NyT+rDq7L59MG9ArZeQnySDzrXR59GLNGnjHRyZuVfRKvo7MrO/MeDaxnxPyD-
AaCVR6cZXTLtjN3tq56smc26h/ObdmNMaRlJVO++K3UfVHYTU7lBI-
wEiMP391SH+ri3synUDrnlAQpwEXNLq9Sq0TZwRfFBFahb5/rZjgKs7cbIuLgIvvP7jFQqSMKg4PvZis
ezDqEbynux3xAR4zHtI6wJO1Bfg7lfaj4/bslHalRO2Lcq/BfFymkoA5aU-
bRe4lQ2c6jZ7KBp0N8R/IsJ56Hi7FM+VpdbRqa9fxieGOtwlaEvAaBcv5bG5adkfkQ==</encrypt-
edPassData>
    <activationData>TUJQQUMtMS1GSy00NzYxMjYuMS0tVERFQS1EMU-
JBREUyMEZFMkE3QjM2NjI2NDQ5N0E5NzcxQTQ4MEI0OUFFNUQ3NEI3RTEzQzA5MjFFNzVGQzI0MzNBQj
hGQThCQzc1NTIwREJFNDBCRQ==</activationData>
    <ephemeralPublicKey>BBD/v2BfOQNI/OT-
mggcr/t9556jYs1J9X2qIPENydRZ3oWF5ojAOy/n2ZzOhXVUL9u/cwUwszYQcNgjvyxydLb0=</ephem
eralPublicKey>
    <authcode>1MCCHD</authcode>
    <code>0</code>
</CreateInAppProvisioningDataResponse>
```

Пример 2. REST/JSON

### Запрос


```
{
   "requestId": "1da5f3f8-2378-40da-9c26-2d59ab6f1db8",
   "pan": "444444*****56789",
   "expiryMonth": "12",
   "expiryYear": "20",
   "cardholderName": "FIRSTNAME LASTNAME",
   "ips": "V",
   "nonce": "9c023092",
   "nonceSignature":
"4082f883ae62d0700c283e225ee9d286713ef74456ba1f07376cf17d71bf0be013f926d48661939
4060ced56030f41f84df916eaab5504e456a8530dc9c821f6ed3e3af62b5d8f3e4a22ca2018670fe
e4e",
   "certificates": [
      "MIIEEzCCA7igAwIBAgIIEvD9KtxTuV0wCgYIKoZIzj0EA-
wIwgYExOzA5BgNVBAMMMlRlc3QgQXBw\nbGUgV29ybGR3aWRlIERldmVsb3BlcnM-
gUmVsYXRpb25zIENBIC0gRUNDMSAwHgYDVQQLDBdDZXJ0\na-
WZpY2F0aW9uIEF1dGhvcml0eTETMBEGA1UECgwKQXBwbGUgSW5jLjELMAkGA1UEBhMCVVMwHhcN\nMTc
wNTI-
wMDQxNTU3WhcNMTkwNjE5MDQxNTU3WjBtMTYwNAYDVQQDDC1lY2MtY3J5cHRvLXNlcnZp\nY2VzLWVuY
2lwaGVybWVudF9VQzYtSW5NZW1vcnkxETAPBgNVBAsMCEFwcGxlUGF5MRMwEQYDVQQK\nDApBcHBsZS-
BJbm-
MuMQswCQYDVQQGEwJVUzBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABC4+XM9r\nmrBL56IvP6zP3nPI
focVU5SjSBVAiolsoYo3TaxmmvO/YiD8hjdn9K9HUHxbwiH8ShmHTa85tAdO\nPrijg-
gIrMIICJzBPBggrBgEFBQcBAQRDMEEwPwYIKwYBBQUHM-
AGGM2h0dHA6Ly9vY3NwLXVhdC5j\nb3JwLmFwcGxlLmNvbS9vY3NwMDQtdGVzdHd3ZHJjYWVjYzAdBgN
VHQ4EFgQUrS6jy340wu3uQ2hO\nJxEfzEkzOdAwDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAW-
gBTW1tVa5f/9wnw0w0PevWh2XDapvjCC\nAR0GA1UdIASCARQwggEQMIIBDAYJKoZIhvdjZAUB-
MIH+MIHDBggrBgEFBQcCAjCBtgyBs1JlbGlh\nbmNlIG9uIHRoaXMgY2VydGlmaWNhdGUgYn-
kgYW55IHBhcnR5IGFzc3VtZXMgYWNjZXB0YW5jZSBv\nZiB0aGUgdGhlbiBhcHBsaWN-
hYmxlIHN0YW5kYXJkIHRlcm1zIGFuZCBjb25kaXRpb25zIG9mIHVz\nZSwgY2VydGlmaWN-
hdGUgcG9saWN5IGFuZCBjZXJ0aWZpY2F0aW9uIHByYWN0aWNlIHN0YXRlbWVu\ndHMuMDY-
GCCsGAQUFBwIBFipodH-
RwOi8vd3d3LmFwcGxlLmNvbS9jZXJ0aWZpY2F0ZWF1dGhvcml0\neS8wQQYDVR0fBDowODA2oDSgMoY-
waHR0cDovL2NybC11YXQuY29ycC5hcHBsZS5jb20vYXBwbGV3\nd2RyY2FlY2MuY3JsMA4GA1UdDwEB/
wQEAwIDKDASBgkqhkiG92NkBicBAf8EA-
gUAMAoGCCqGSM49\nBAMCA0kAMEYCIQCMvUq2YUxY/RqTWE4FqsPTr9zGyilCunIU3FSobtep7gI-
hAN7Vdx3B0p7DTCqX\nHd05IPsZGLdIDG1NTxOk2Oj/N7GG",      "MIIC5zCCAoygAwI-
BAgIIR1pCSszYnvcwCgYIKoZIzj0EAwIwZzEhMB8GA1UEAwwYVGVzdCBB-
cHBs\nZSBSb290IENBIC0gRUNDMSAwHgYDVQQLDBdDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTETMBEGA1
UE\nCgwKQXBwbGUgSW5jLjELMAkGA1UEBhMCVVMwHhcNMTQwMjA2MTYxODI5WhcNMjQwMjA0MTYx-
ODI5\nWjCBgTE7MDkGA1UEAwwyVGVzdCBBcHBsZSBXb3JsZHdpZGUg-
RGV2ZWxvcGVycyBSZWxhdGlvbnMg\nQ0EgLSBFQ0MxI-
DAeBgNVBAsMF0NlcnRpZmljYXRpb24gQXV0aG9yaXR5MRMwEQYDVQQKDApBcHBs\nZSBJbm-
MuMQswCQYDVQQGEwJVUzBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABDzb9Lsna4XrUdRw\nIjl36m9h
TGhxQrW5Ls3wYr07kaZ/5tMOEG5jOBeHtI+x8YHmkgp0Ry43nmZTik3vosay+6ajggEF\nMIIBATBUB-
ggrBgEFBQcBAQRIMEYwRAYIKwYBBQUHMAG-
GOGh0dHA6Ly9vY3NwLXVhdC5jb3JwLmFw\ncGxlLmNvbS9vY3NwMDQtdGVzdGFwcGxlcm9vdGNhZWNjM
B0GA1UdDgQWBBTW1tVa5f/9wnw0w0Pe\nvWh2XDapvjASBgNVHRMBAf8ECDAGAQH/AgEAMB8GA1UdI-
wQYMBaAFNJH4sU0ccYQjZPuBEMf4RsP\n4c0RMEUGA1UdHwQ+MDw-
wOqA4oDaGNGh0dHA6Ly9jcmwtdWF0LmNvcnAuYXBwbGUuY29tL3Rlc3Rh\ncH-
BsZXJvb3RjYWVjYy5jcmwwDgYDVR0PAQH/BAQDAgEG-
MAoGCCqGSM49BAMCA0kAMEYCIQCd4eDj\nSiTu55mDKW-
CaD7Tqe4hp86pJ1Fsw7SlPKmH+bQIhAJ5coaJ3uarz81Im19NGcrU45h1A8hNDTz55\nQPEHujS5"
      ]
}
```

### Ответ


```
{
    "encryptedPassData":
"oyEdHtXV2JGZcge4UmcZLd7wyWEaViosDGMeTzhgVXQsJlm1ZVZQS9DLVtck5tdmU8mdLZesiKLeK4b
6W1P+77QYl5eZi606eKSMe5/KFuAFgBxVry8mBQWuKfaJ6j2Qyn0xDjgKtPtukWhzn5VnTR6MKHnAfVR
ycWW132Fv8ad9i2W9nGHvLHQ5NHXxE-
qdPryFD/lj1p9t9o+Cz6TKhp+vtVWUM6/0k0vOpFMOzoNePJM5SyjtC5kv7MJ2acA8rvzAF2dgsNe/iO
22t79nMLIboA5muPu0QIMlo38nmLqReCMuWeitYGjJTNXLXYZdCj/CYEeb36cvbqN3RaOBsSWkkyW6PV
0q5W820jdgQOISHTGZgH7gnEPmlBq/IgBY9Iy18HvkVSYQrLIMvowQE7O284nfcA+4E1rgAA3AB6vr7Y
fMeKh9VKrVfOsw/J9Baw4+VeXyczRxYQZOUtDL/VpPMkslXQ5HaHwMJnVHXy/voRef-
cRU15F/lZMX+ELS6NiFzQ0cn8zSNPmooUO/cPtOtYi44fkXtwOqBTzXngQu7LVuxo-
aYQaDQXE3SoQOrK0EhVcDZ0SngrWOqLHUE5eBka2rJIoto5R9DfQDqgl+mhYvKqitcjydSHXDDH3LsIk
rqFoENphGPOTp91BOFPjOa/5o+CH1G4U0QBNaYi62mfE0XcXUY-
oKSQn/nVdG8QQBK7O+oY+Oy17O6R0vp6rmCzZHK7UA2GuHwktH2zHa0tpF2LagvUIE/g==",
    "activationData":
"TUJQQUMtMS1GSy00NzYxMjYuMS0tVERFQS1FMzlBREUyRjU4QTQwNTZCM0JCREM1MEY2QTY2RUE0ODl
GM0VDODE3OUNDQTkxMUQ5MDBFMDc1MTE4NTJDNjQwMzRCNUE5MEVBNzc4NDVGRg==",
    "ephemeralPublicKey":
"BAO1+QEPTPYqk2ZnPsoFgzZW7kdKFthgGV1X3bJVzmsq8zGejBa0hm54zNKqhCpWqUI679NBfWFIhZm
wBm7DIcg=",
    "authcode": "1NET91",
    "code": "0"
}
```


## Get Token by Wallet ID

### Inbound

Запрос, который по clientWalletAccountId и clientWalletProvider вернет список CardId, у которых есть токен в данном кошельке (в любом из статусов, отличных от “удален” или “деактивирован”). Метод применяется при реализации схемы PushProvisioning с кошельком Google Pay, когда в банковском мобильном приложении необходимо реализовать функционал добавления еще не токенизированной карты в кошелек Google Pay.

Для Mastercard при передаче запроса GetTokenByWalletId в параметре clientWalletAccountId присылайте значение, полученное конкатенацией clientDeviceId и clientWalletAccountId.

Внимание! Данный метод не используется при работе с Apple Pay API. Компания Apple для данной цели предлагает другую реалиазацию, описание которой вы можете найти в документации Apple («Add to Apple Wallet»).

Метод: getTokenByWalletId

REST Endpoint: http(s)://{domain}:{port}/{context}/getTokenByWalletId

***Запрос***

| Поле | Тип параметра | Описание | Присутствие в сообщении |
|---|---|---|---|
| requestID | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | O |
| clientWalletAccountId | *Строка, 24-48 симв.* | Клиентский идентификатор (экземпляра) кошелька, в котором создается токен. Должен совпадать со значением (см. поле paymentAppInstId), которое присылает TWP в запросе provisioning. | M |

| | | | |
|---|---|---|---|
| | | Для Mastercard только! В поле clientWalletAccountId следует присылать значение, полученное конкатенацией clientDeviceId и clientWalletAccountId (информация актуальна на 2020 год). Значение для clientDeviceId получается с помощью вызова метода getStableHardwareId (24 символа). | |
| clientWalletProvider | *Строка, [0-9,A-Z,a-z,-,_], 50 симв.* | Клиентский идентификатор провайдера цифрового кошелька представляет собой ID инициатора запроса на токен (TRID), который выдается провайдеру кошелька в рамках onboarding процесса. Пример значения: "40000000047" | M |

***Ответ***

| **Поле** | **Тип параметра** | **Описание** | **Присутствие в сообщении** |
|---|---|---|---|
| **cardAndToken** | | Массив данных, по каждой карте:<br>Включает в себя только “живые” токены, т.е. токены, у которых статус не равен DELETED/DEACTIVATED. При этом токен включается в ответ, только если у него определены cardID или cardGUID | C |

| **cardAndToken Array** | | | |
|---|---|---|---|
| cardId | *Строка, 1..30 симв.* | Внутренний идентификатор (старый формат) карты. Должен присутствовать как минимум один из двух параметров cardId/ cardGUID | C |
| cardGUID | *Строка, 1..30 симв.* | Внутренний идентификатор (новый формат) карты. Должен присутствовать как минимум один из двух параметров cardId/ cardGUID | C |
| tokenReferenceId | *Строка, 1..64 симв.* | Уникальный идентификатор ссылающийся на оригинальный токен | M |
| panRefId | *Строка, 24..64 симв.* | Уникальный присваеваемый VISA/MC ассоцированный с PAN идентификатор (поле при необходимости может быть использовано при реализации inApp Provisioning схемы. Передается при условии активации в соотв. конф. файле. ) | C |

В случае, если в запросе отсутствуют обязательные поля, возвращаем HTTP ошибку 400.

Пример 1. REST/XML

Запрос

```
<GetTokenByWalletIdRequest>
  <requestId>4f19e2e6-6fd6-422f-adb9-943a9314d9ee</requestId>
  <clientWalletAccountId>uGrOxzwW2ghVx1nuoC2Fnwko</clientWalletAccountId>
  <clientWalletProvider>40010030273</clientWalletProvider>
</GetTokenByWalletIdRequest>
```

Ответ

```
<GetTokenByWalletIdResponse>
    <cardAndToken>
        <cardId>TcyC8pQM8Zyx</cardId>
        <cardGUID>RQPcVLrNfY1U</cardGUID>
        <tokenReferenceId>DNITHE000302000200024700</tokenReferenceId>
        <panRefId>V-3017192484534844832252</panRefId>
    </cardAndToken>
    <cardAndToken>
        <cardId>3uJX0SMND66j</cardId>
        <cardGUID>uEgw4TKqtDSf</cardGUID>
        <tokenReferenceId>DNITHE000302000200026417</tokenReferenceId>
        <panRefId>V-3017192484534844832001</panRefId>
    </cardAndToken>
    <cardAndToken>
        <cardId>HBdnhMTV409m</cardId>
        <cardGUID>bixa5ZNj69yC</cardGUID>
        <tokenReferenceId>DNITHE000302000200024701</tokenReferenceId>
        <panRefId>V-3017192484534844832009</panRefId>
    </cardAndToken>
 </GetTokenByWalletIdResponse>
```

Пример 2. REST/JSON

Запрос

```
{
        "requestId": "dc5b81c3-91f0-4928-aec9-7af1b20ced8f",
   "clientWalletAccountId": "uGrOxzwW2ghVx1nuoC2Fnwko",
   "clientWalletProvider": "40010030273"
 }
```

### Ответ


```
{
    "cardAndToken": [
        {
            "cardId": "TcyC8pQM8Zyx",
            "cardGUID": "RQPcVLrNfY1U",
            "tokenReferenceId": "DNITHE000302000200024700",
            "panRefId": "V-3017192484534844832252"
},
        {
            "cardId": "3uJX0SMND66j",
            "cardGUID": "uEgw4TKqtDSf",
            "tokenReferenceId": "DNITHE000302000200026417",
            "panRefId": "V-3017192484534844475356"

        },
        {
            "cardId": "HBdnhMTV409m",
            "cardGUID": "bixa5ZNj69yC",
            "tokenReferenceId": "DNITHE000302000200024701",
            "panRefId": "V-3017192484534844832253"
        }

    ]
}
```

# Дополнительные запросы

## 1. Get Card Info Short

### Outbound

Запрос в банковскую систему, выполняется для получения внутренних идентификаторов карты cardId/cardGUID и номера мобильного телефона держателя карты *customerPhone* по номеру карты (PAN) и ее сроку действия. Запрос используется в поисковой форме административной панели , если вводится номер карточки (карточка может быть активной и не активной)

Только для VTS Issuer API v.3:

Метод getCardInfoShort так же вызывается, когда FastTack получает из VTS запрос checkEligibility. В этом случае поле productConfigID (когда присутствует в ответе от банка) будет передано в ответе checkEligibility в поле profileID.

Интерфейс веб-службы: CardPT
Метод: getCardInfoShort
SOAP Endpoint: http(s)://{domain}:{port}/{context}/CardPT
REST Endpoint: http(s)://{domain}:{port}/{context}/getCardInfoShort

***Запрос***

| Поле | Тип параметра | Описание | Присутствие в сообщении |
|---|---|---|---|
| requestId | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | O |
| pan | *Строка, 13..19 цифр* | Номер карты для оцифровки | M |

***Ответ***

| Поле | Тип параметра | Описание | Присутствие в сообщении |
|---|---|---|---|
| requestId | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | O |
| cardID | *Строка, 1..30 симв.* | Уникальный идентификатор карты в банковской системе. Обязательным является один из двух параметров: panInternalId / panInternalGUID | C |
| cardGUID | *Строка, 1..32 симв.* | Уникальный идентификатор карты в банковской системе. Обязательным является один из двух параметров: panInternalGUID / panInternalId | C |
| phoneNumber | *Строка, 12..13 симв.* | Номер телефона пользователя (“380505554433”,”+380505554433”) | C |
| productConfigID | *Строка, 1-32 символ* | Уникальный идентификатор соответствующий конфигурации продукта. | C |

| | | | |
|---|---|---|---|
| cardIssueDate | *Строка, 8 символов* | Дата выпуска карты в формате DDMMYYYY | O |
| customerID | *Строка, 64 симв.* | Внутренний идентификатор контрагента | O |
| code | *Строка, 1..3 симв.* | Код завершения операции.<br>Возможные варианты значений:<br>“0” - OK Success карта найдена ( активная , неактивна , закончен срок )<br>От “1” и больше – ошибка<br>1 (parseException- невалидная информация),<br>2 (nothingFoundException - по пришедшей информации ничего не найдено)<br>3 (exception - что-то пошло не так). | M (O-Alfa) |
| errorMessage | *Строка, 1..2000 симв* | Дополнительная информация.<br>Заполняется для отказов или ошибок (code != 0). | O |

Пример 1. SOAP/XML

Запрос

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:getCardInfoShort xmlns:ns2="http://sab/" xmlns:ns4="http://ws.wso2.org/da-
taservice">
   <ns2:requestId>23551060-5040-40ff-9743-3960c52ba2c0</ns2:requestId>
   <ns2:pan>444444*****1111</ns2:pan>
</ns2:getCardInfoShort>
```

Ответ

```
<?xml version="1.0" encoding="UTF-8"?>
<sab:getCardInfoShortResponse xmlns:sab="http://sab/">
   <sab:getCardInfoShortItem>
      <sab:requestId>23551060-5040-40ff-9743-3960c52ba2c0</sab:requestId>
      <sab:cardID>CardID3</sab:cardID>
      <sab:cardGUID>CardID3111111111</sab:cardGUID>
      <sab:phoneNumber>380503124439</sab:phoneNumber>
      <sab:productConfigID>12321321</sab:productConfigID>
   </sab:getCardInfoShortItem>
</sab:getCardInfoShortResponse>
```

Пример 2. REST/JSON

Запрос

```
{
   "requestId": "23551060-5040-40ff-9743-3960c52ba2c0",
   "pan": "444444*****1111"
}
```

Ответ

```
{
 "requestId": "53e7eddd-b713-465d-b9b6-45255777214e",
 "cardID": "527651",
  "phoneNumber": "380505895603",
 "productConfigID": "DCGREEN",
 "cardIssueDate": "19052021",
 "customerID": "363826",
  "code": "0"
}
```

# 2. Get Customer Identifier

## Outbound

Запрос выполняется для получения внутреннего идентификатора клиента (контрагента) по cardID, cardGUID или cardNum. Данный запрос используется в поисковых формах Fasttack.

Метод используется при поиске токенов в форме "Показать все токены". Форма позволяет искать все токены по всем картам клиента. Метод Get Customer Identifier возвращает идентификатор пользователя, а затем осуществляется поиск всех токенов для этого пользователя. Он может вызываться и в процессе обработки других запросов, полученных FastTack от VTS

Интерфейс веб-службы: CardPT
Метод: getCustomerID
SOAP Endpoint: http(s)://{domain}:{port}/{context}/CardPT
REST Endpoint: http(s)://{domain}:{port}/{context}/getCustomerID

***Запрос***

| Поле | Тип параметра | Описание | Присутствие в сообщении |
|---|---|---|---|
| cardNum | *Строка, 1..30 симв.* | Pan карты.<br>Если cardNum присутствует, то поля *cardGUID / cardId / hashNum не передаются.* | C |
| cardID | *Строка, 1..30 симв.* | Уникальный идентификатор карты в банковской системе.<br><br>Если cardID присутствует, то поля cardNum */ hashNum не передаются.*<br>*В зависимости от схемы работы, может передаваться вместе с полем* cardGUID | C |
| cardGUID | *Строка, 1..32 симв.* | Уникальный идентификатор карты в банковской системе.<br>Если cardGUID присутствует, то поля cardNum */ hashNum не передаются.*<br>*В зависимости от схемы работы, может передаваться вместе с полем* cardID | C |
| hashNum | *Строка, 1..30 симв.* | Hash карты.<br>Если hashNum присутствует, то поля *cardGUID / cardId /* cardNum *не передаются.* | C |

***Ответ***

| Поле | Тип параметра | Описание | Присутствие в сообщении |
|---|---|---|---|
| customerID | *Строка, 1..64 симв.* | Внутренний идентификатор контрагента | M |
| code | *Строка 1..3 симв.* | Код завершения операции.<br>Возможные варианты значений:<br>“0” - OK Success | M |

| | | | |
|---|---|---|---|
| | | От “1” и больше – ошибка | |
| errorMessage | *Строка 1..2000 симв.* | Дополнительная информация.<br>Заполняется для ошибок или отказов (code != 0). | C |

Пример 1. SOAP/XML

Запрос

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:getCustomerID xmlns:ns2="http://sab/" xmlns:ns4="http://ws.wso2.org/da-
taservice">
<ns2:requestId>666f373f-e0ae-485d-9e06-ec3a2b079ba0</ns2:requestId>
<ns2:cardNum>555555******5554</ns2:cardNum>
</ns2:getCustomerID>
```

Ответ

```
<?xml version="1.0" encoding="UTF-8"?>
<sab:getCustomerIDResponse xmlns:sab="http://sab/">
<sab::requestId>666f373f-e0ae-485d-9e06-ec3a2b079ba0</sab:requestId>
<sab:getCustomerIDItem>
      <sab:customerID>1000001</sab:customerID>
      <sab:code>0</sab:code>
</sab:getCustomerIDItem>
</sab:getCustomerIDResponse>
```

Пример 2. REST/JSON

Запрос

```
{
   "requestId": "23551060-5040-40ff-9743-3960c52ba2c0",
   "cardNum": "444444*****1111"
}
```

Ответ

```
{
   "requestId": "23551060-5040-40ff-9743-3960c52ba2c0",
   "customerID": "12345678",
   "code": "0"
}
```

# 3. Send Notification to Customer

## Outbound

Запрос выполняется в систему отправки смс сообщений при необходимости отправить нотификацию клиенту банка. Типы нотификаций, которые в настоящий момент поддерживаются:

TOKEN_ACTIVATION_REMINDER - нотификация отправляется клиенту в качестве напоминания о необходимости завершить процесс токенизации с помощью одного из поддерживаемых банком методов верификации;
TOKEN_ACTIVATED - нотификация отправляется клиенту в качестве поздравления с успешной активацией токена;

Интерфейс веб-службы: CardToken
Метод: sendNotificationToCustomer
SOAP Endpoint: http(s)://{domain}:{port}/{context}/CardToken
REST Endpoint: http(s)://{domain}:{port}/{context}/sendNotificationToCustomer

***Запрос***

| Поле | Тип параметра | Описание | Присутствие в сообщении |
|---|---|---|---|
| requestId | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | M |
| tokenRefId | *Строка, 32..64 симв.,* | Unique ID for the token associated with the PAN. This ID can be used in lieu of the token for subsequent calls, such as life cycle events | M |
| tokenRequestorId | *Строка, 11 симв.* | Unique ID assigned to the initiator of the token request | M |
| conversationId | *Строка, 14-36 симв.* | Сквозной идентификатор серии запросов выполняющихся при токенизации карты. Аналог CorrelationId (MDES) | O |
| tokenRequestorName | *Строка, 1..64 симв.* | Название в виде текста (“GOOGLE_PAY”, “VISA_CHECKOUT”, “NETFLIX”) ассоциированное с tokenRequestorId. Заполняется в случае наличия соотв. записи в таблице TOKEN_REQUESTOR | O |
| panInternalId | *Строка, 1..30 симв.* | Уникальный идентификатор карты в банковской системе. Обязательным является один из двух параметров: panInternalId / panInternalGUID | C |
| panInternalGUID | *Строка, 1..32 симв.* | Уникальный идентификатор карты в банковской системе. Обязательным является один из двух параметров: panInternalGUID / panInternalId | C |
| notificationType | *Строка, 1..64 симв* | Поддерживаемые типы нотификаций:<br>• TOKEN_ACTIVATION_REMINDER<br>• TOKEN_ACTIVATED | M |
| lastFourOfPAN | *Строка, 4 симв* | Последние четыре цифры номера карты | M |

| | | | |
|---|---|---|---|
| reminderPeriod | *Строка, 1-4 симв* | Прошедшее время (в часах) с момента создания токена, по истечении которого было отправлено данное сообщение “Send Notification to Customer” | C |
| customerPhone | *Строка, 12..13 симв.* | Номер телефона пользователя (“380505554433”,”+380505554433”) | O |
| deviceType | *Строка 1..64 симв* | Форм фактор устройства, на котором выполняется токенизация. Новые значения могут быть добавлены в любой момент и должны приниматься без ошибок. Возможные значения: PHONE, TABLET, TABLET_OR_EREADER, WATCH, WATCH_OR_WRISTBAND,CARD,STICKER, PC, DEVICE_PERIPHERAL, TAG, JEWELRY ,FASHION_ACCESSORY, GARMENT, DOMESTIC_APPLIANCE,VEHICLE, MEDIA_OR_GAMING_DEVICE, UNDEFINED | O |

***Ответ***

| **Поле** | **Тип параметра** | **Описание** | **Присутствие в сообщении** |
|---|---|---|---|
| requestId | *Строка, 36 симв., GUID* | Уникальный идентификатор запроса. | O |
| code | *Строка, 1..3 симв.* | Код завершения операции.<br>Возможные варианты значений:<br>“0” - OK Success<br>“1” – parseException (невалидный запрос)<br>“2” - nothingFoundException (по пришедшей информации ничего не найдено)<br>“3” - exception (что-то пошло не так). | M |
| errorMessage | *Строка, 1..2000 симв* | Дополнительная информация.<br>Заполняется для отказов или ошибок (code != 0). | C |

Если тело ответа отсутствует, необходимо вернуть код HTTP статуса из таблицы ниже:

| HTTP Status | |
|---|---|
| 200 | NORMAL RESPONSE |
| 400 | BAD REQUEST |
| 400 | REQUIRED DATA MISSING |
| 400 | INVALID DATA |
| 500 | INTERNAL SYSTEM ERROR |
| 401 | UNAUTHORIZED |
| 404 | NOT FOUND |

Пример 1. SOAP/XML

Запрос

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:sendNotificationToCustomer xmlns:ns2="http://sab/"
xmlns:ns4="http://ws.wso2.org/dataservice">
   <ns2:requestId>09fab8ff-77c5-49f9-a39f-91bb8913643b</ns2:requestId>
   <ns2:tokenRefId>DNITHE40736046984008737</ns2:tokenRefId>
   <ns2:tokenRequestorId>40010030273</ns2:tokenRequestorId>
   <ns2:notificationType>TOKEN_ACTIVATED</ns2:notificationType>
   <ns2:lastFourOfPAN>0006</ns2:lastFourOfPAN>
   <ns2:customerPhone>3801234567</ns2:customerPhone>
</ns2:sendNotificationToCustomer>
```

Ответ

```
<sab:sendNotificationToCustomerResponse xmlns:sab="http://sab/">
         <sab:requestId>09fab8ff-77c5-49f9-a39f-91bb8913643b </sab:requestId>
         <sab:code>0</sab:code>
</sab:sendNotificationToCustomerResponse>
```

Пример 2. REST/JSON

Запрос

```
{
   "requestId": "09fab8ff-77c5-49f9-a39f-91bb8913643b",
   "tokenRefId": "DNITHE40736046984008737",
   "tokenRequestorId": "40010030273",
   "notificationType": "TOKEN_ACTIVATED",
   "lastFourOfPAN": "0006",
   "customerPhone": "3801234567"
}
```

Ответ

```
{
   "requestId": "09fab8ff-77c5-49f9-a39f-91bb8913643b",
   "code": "0"
}
```

# Сценарии токенизации карт VISA и детали используемых API

## Регистрация карты VISA (верификация пользователя с помощью OTP-пароля)

На диаграмме отображен стандартный сценарий оцифровки карт в стороннем цифровом кошельке (например, Apple Pay) при взаимодействии следующих участников (**Ошибка! Источник ссылки не найден.**):

- мобильное приложение цифрового кошелька – AP wallet,
- провайдер цифрового кошелька – DWP;
- VTS;
- Система – DSP FastTack;
- авторизационная система банка - ISS Host (UPC).

Описание сценария:

1. Клиент регистрирует в мобильном кошельке (к примеру Google Wallet) карту для токенизации. DWP транслирует запрос Card Enrolment с карточными данными далее в VTS.
2. VTS, получив от DWP номер карты клиента, отправляет на DSP FastTack (ISS VTS API) запрос «Check Eligibility».
3. DSP FastTack транслирует полученный запрос на шину банка в виде getCardInfoShort. В ответ, на данный запрос банк может вернуть ИД профиля карты.
4. Клиент подтверждает «Terms&Conditions», после чего приложение отправляет запрос «Provision Req». DWP, получив данные карты от клиента (PAN, срок действия, CVV2), инициирует запрос.
5. VTS, получив от DWP данные по карте клиента для оцифровывания в запросе «Provision Req», в свою очередь, отправляет в DSP FastTack запрос Approve Provisioning.
6. VTS инициирует два параллельных запроса на шину банка – Confirm Provisioning и Card Status Verification.
    1. Card Status Verification вызывается на стороне Issuer Host для проверки данных карты (PAN,EXP.Date,CVV2);
    2. Confirm Provisioning выполняется на стороне Bank Backend. В ответе на запрос необходимо вернуть решение по токенизации карты в поле decision– “DECLINED” либо «REQUIRED_ADDITIONAL_AUTHENTICATION». В последнем случае ответ сопровождается номером телефона клиента.
7. VTS запрашивает список методов верификации клиента с помощью запроса «Get CVM» (Card Verification Methods). DSP FastTack дополняет, формирует и отправляет в VTS ответ с полным перечнем методов проверки клиента.
8. Клиент выбирает опцию проверки с помощью ввода ОТП кода.
9. DWP передает далее в VTS способ проверки карты с помощью ввода ОТП кода.
10. VTS генерирует ОТП код и отправляет его в DSP FastTack в виде запроса Send OTP.
11. DSP FastTack транслирует запрос Send OTP на шину банка, где далее ОТП отправляется на телефон клиента.
12. Клиент, получив OTP код, вводит его в интерфейсе мобильного кошелька, после чего, DWP отправляет его на проверку в VTS.
13. VTS выполняет проверку OTP кода и, в случае успеха, переводит токен в состояние «Active». VTS инициирует этап «Replenishment», в котором DSP FastTack не принимает участие.
14. Мобильное приложение сообщает DWP об успешном завершении токенизации с помощью “Provisioning Confirmation”, где DWP транслирует его в VTS.
15. Получив “Provisioning Confirmation”, VTS отправляет на DSP FastTack нотификацию в виде «Token Create Notification».
16. DSP FastTack перенаправляет в банк полученную нотификацию в виде запроса Card Tokenized.

17. Параллельно VTS присылает нотификацию «Token Notification Update» с кодом MessageReasonCode=«Device Provisioning Result Notification» и «OTP_Verifcation_Result».
18. DSP FastTack перенаправляет в банк полученную нотификацию в виде Token Status Update.

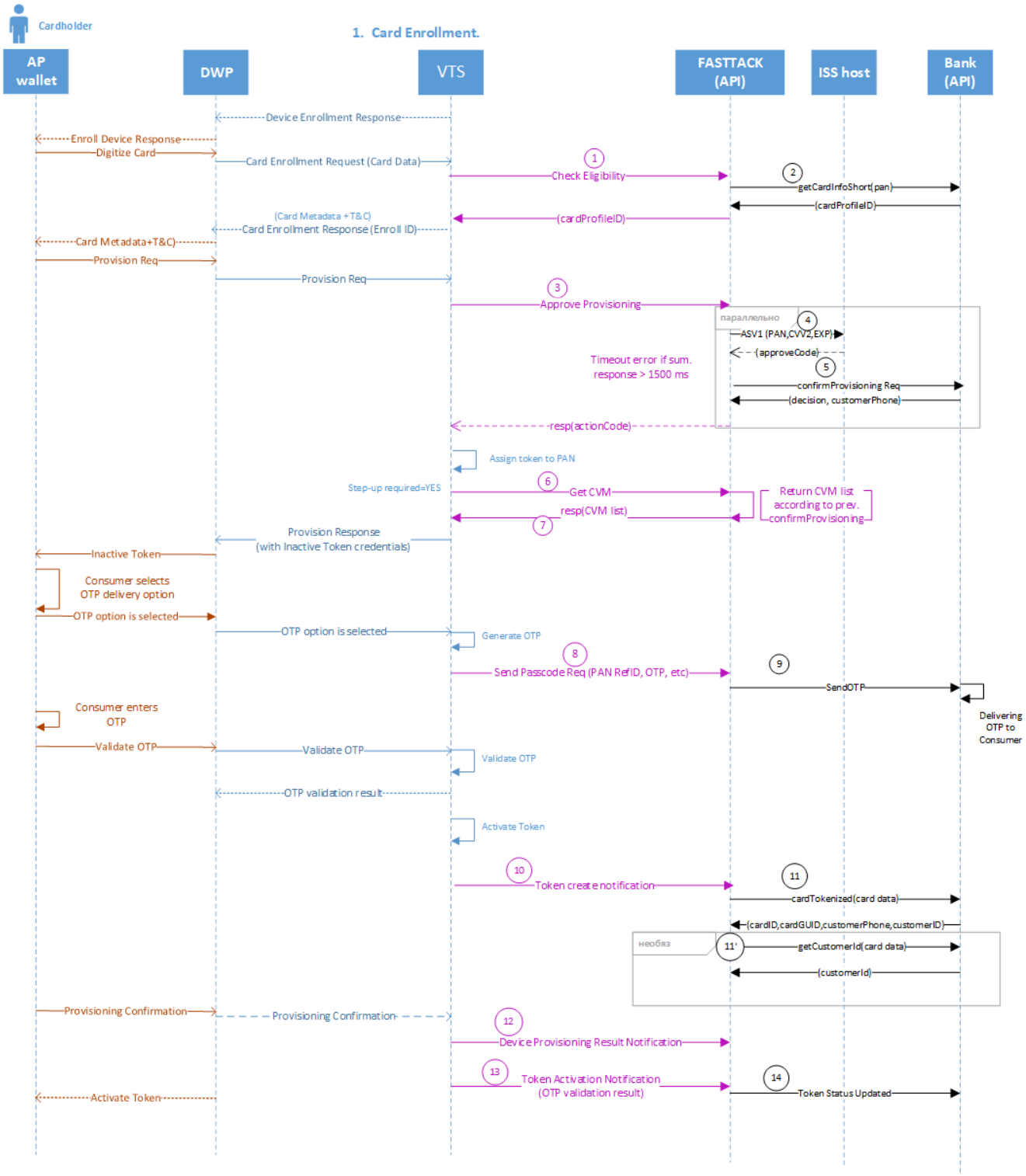
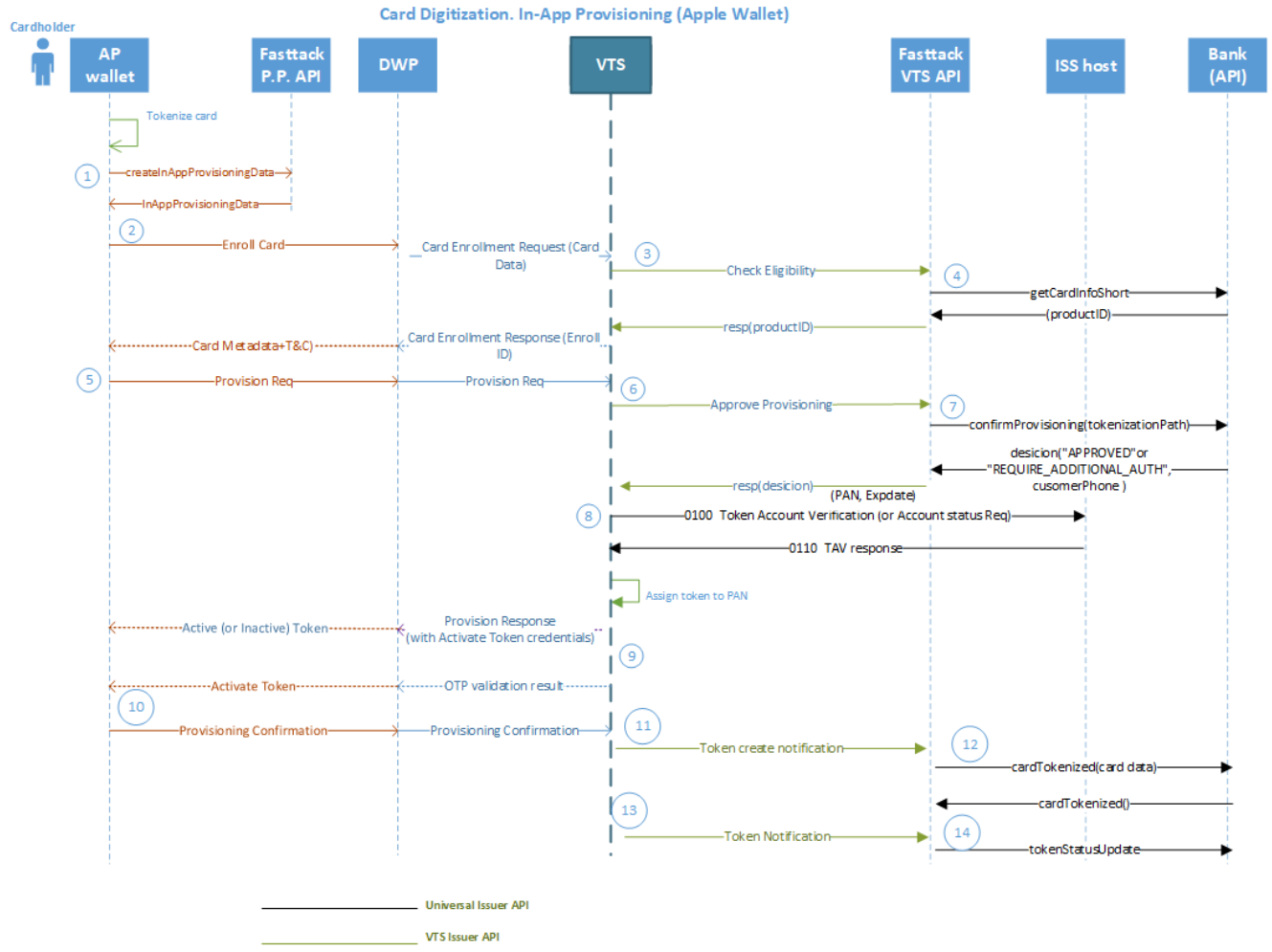
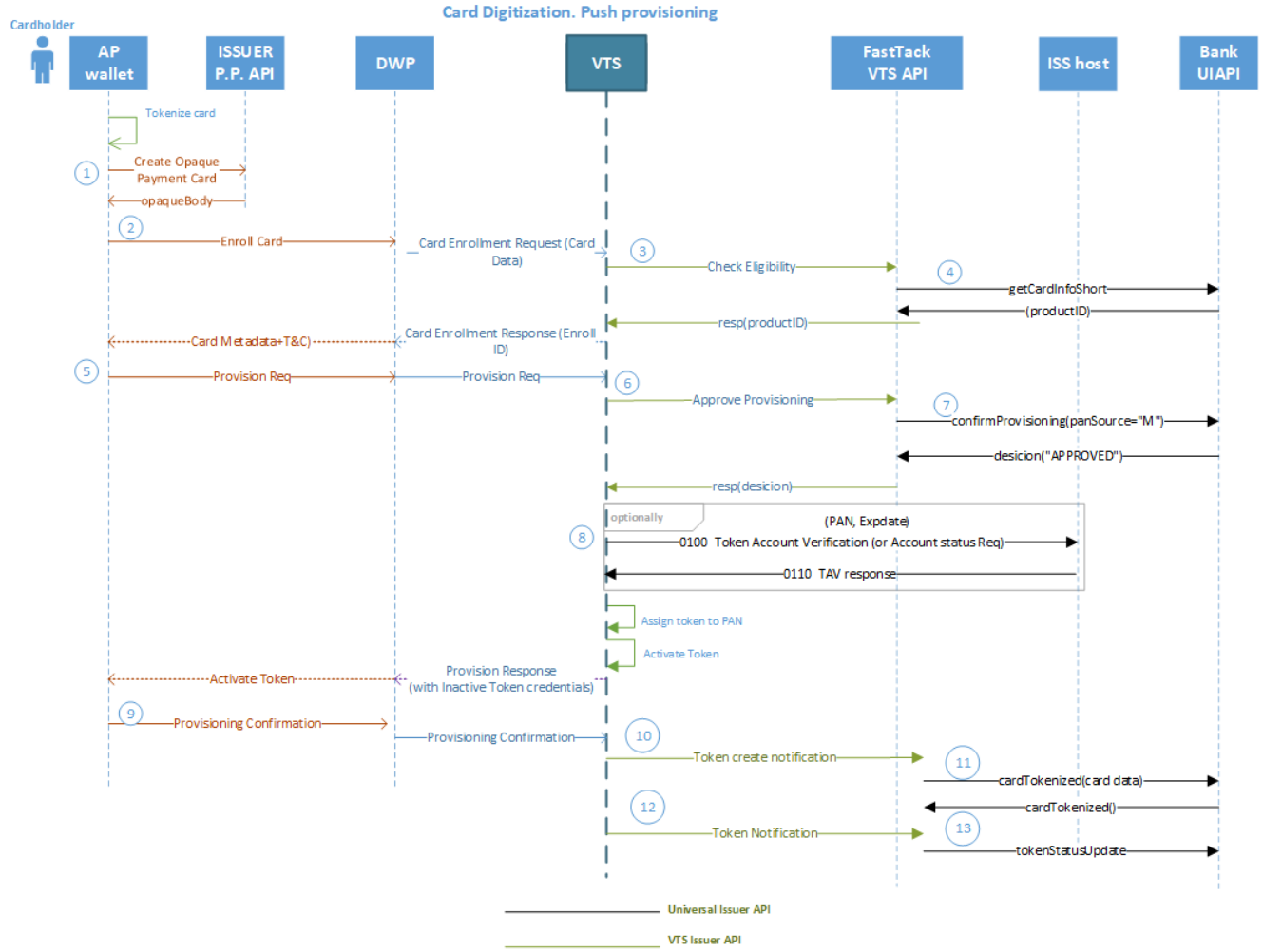



Диаграмма последовательности «Оцифровывание карты VISA (верификация пользователя с помощью OTP-пароля)»




Токенизация карточки с использованием мобильного приложения банка и метода InAppProvisioningData (InApp Provisioning) для ApplePay




Токенизация карточки с использованием мобильного приложения банка и метода Create Opaque PaymentCard (Push Provisioning) для GooglePay

Важно !!!

Шаг 3-8 могут отсутствовать для VTS если в Visa Risk Management настроено правило для зеленого пути по согласованию с банком . В этом случае ответ на запрос Card Tokenized (10) является важным для формирования записи токена и ссылки на карточку.

# Сценарий токенизации карты Mastercard

## Токенизация карты Mastercard (аутентификация с помощью OTP-пароля)

На диаграмме отображен стандартный сценарий оцифровки карт в цифровом кошельке при взаимодействии следующих участников (**Ошибка! Источник ссылки не найден.**):

- мобильное приложение цифрового кошелька – AP wallet
- провайдер цифрового кошелька – DWP,
- MDES,
- Системы банка, включая DSP FastTack– Issuer (API),
- авторизационная система банка - ISS Host (UPC).

Описание сценария:

1. DWP, получив данные карты от клиента (PAN, срок действия, CVV2), инициирует запрос «Check Eligibility» в систему MDES. Если для бина карты разрешена токенизация, MDES возвращает в ответ текст «Terms&Conditions», ознакомление и согласие, с которым позволят клиенту продолжить процесс токенизации карты.
2. MDES, получив от DWP данные по карте клиента для оцифровывания, передает их в Систему в запросе «Authorize Service».
3. Система, на основании сообщения «Authorize Service» (и в соответствии с конфигурацией в таблице бинов) отправляет в ISS Host (UPC) запрос «ASV» («Account Status Verification», шаг 3) с целью проверки CVV2 кода.
4. На основании полученных ответов Система формирует и отправляет ответ для DWP. DWP, получив разрешение на оцифровку карты, передает в AP wallet список методов проверки.
5. Клиент выбирает в качестве метода верификации получение OTP кода, о чем DWP извещает MDES.
6. MDES генерирует OTP код и отправляет его в Систему в сообщении «Deliver Activation Code». Система, на основании полученного в «Deliver Activation Code» токена, находит номер телефона клиента и отправляет OTP код вместе с номером в сообщении «Send OTP» через Bank API.
7. Клиент, получив OTP код, вводит его в интерфейсе AP wallet, после чего, DWP отправляет его на проверку в MDES.
8. MDES выполняет проверку OTP кода и, в случае успеха, переводит токен в состояние «Active».
9. Система, на основании полученного сообщения «Notify Service Activated», формирует и отправляет в MDES ответ, обновляет локально статус токена.
10. MDES инициирует этапы «Provision» (и «Replenishment»), в которых Система не принимает участие.

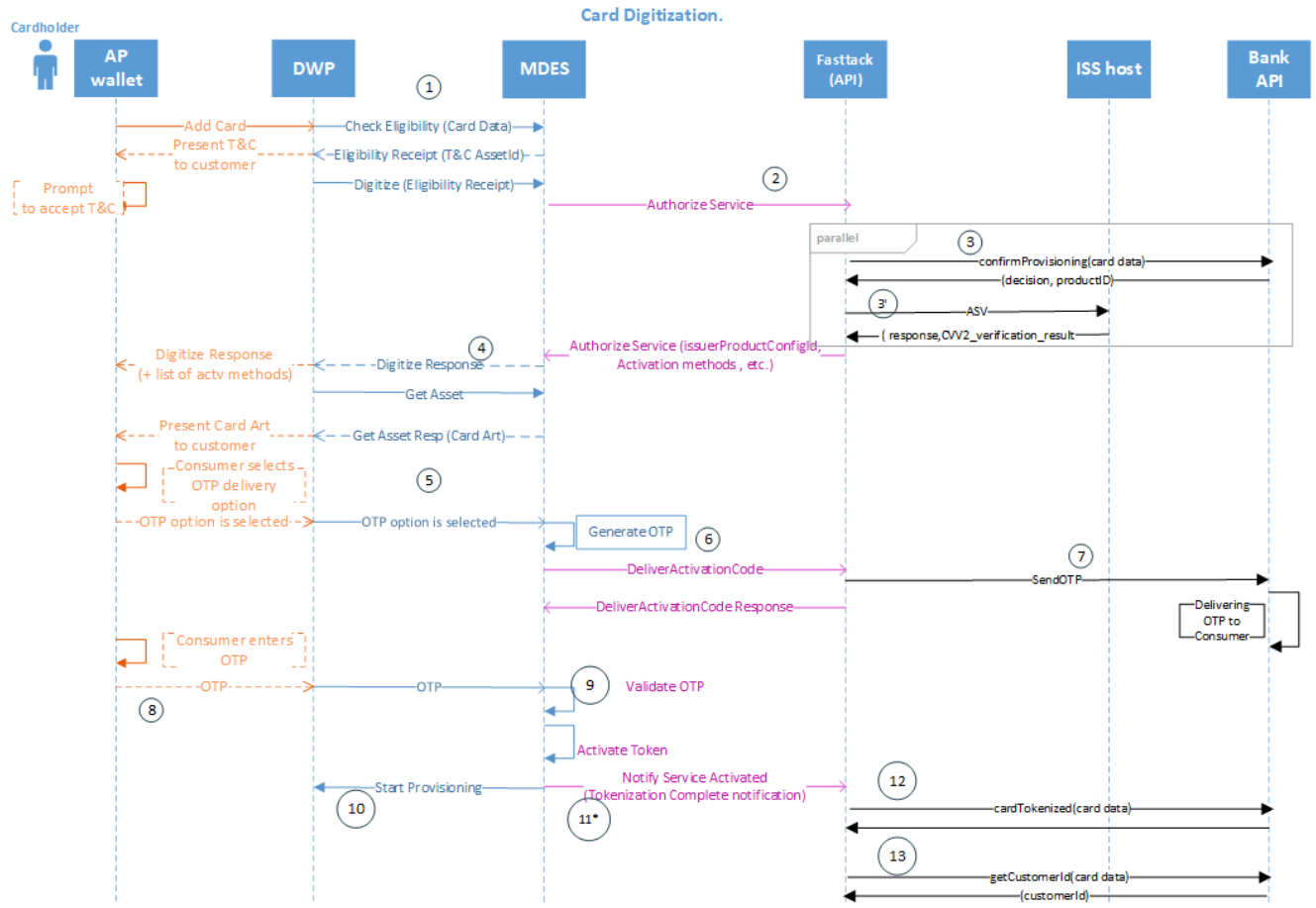



Диаграмма последовательности «Оцифровывание карты Mastercard (верификация пользователя с помощью OTP-пароля)»

## Рекомендуемый порядок обработки запроса confirmProvisioning для карт Mastercard.

1. Выполнить общие проверки по карте:

- если есть запрет на токенизацию карты в виде обслуживания - вернуть DECLINED
- если tokenizationPath == 'RED' - вернуть DECLINED
- если карта имеет статус, отличный от нормального (в стоп-списке и т.д.) - вернуть DECLINED
- если в запросе присутствует срок действия карты, и он не совпадает со сроком действия карты в БД - вернуть DECLINED

2. В случае walletId == 327 (это программа MDES 4 Merchants):

  - если panSource != 'M' - вернуть APPROVED
  - иначе вернуть DECLINED

3. В случае других значений walletId:

- если tokenRequestorId НЕ входит в список провайдеров "больших" кошельков (Google Pay, Apple Pay и т.д.):
  - если panSource != 'M' - вернуть REQUIRE_ADDITIONAL_AUTHENTICATION и номер телефона
  - иначе вернуть DECLINED
- если tokenRequestorId входит в список провайдеров "больших" кошельков (Google Pay, Apple Pay и т.д.):
  - если panSource == 'M' - вернуть APPROVED
  - иначе вернуть REQUIRE_ADDITIONAL_AUTHENTICATION и номер телефона

## Рекомендуемый порядок обработки запроса confirmProvisioning для карт VISA.

**1. Выполнить общие проверки по карте:**

1.1. если есть запрет на токенизацию карты в настройках ее обслуживания - вернуть DECLINED

1.2. если tokenizationPath == 'RED' - вернуть DECLINED

1.3. если карта имеет статус, отличный от нормального (в стоп-списке и т.д.) - вернуть DECLINED

1.4. если в запросе присутствует срок действия карты, и он не совпадает со сроком действия карты в БД - вернуть DECLINED

| Условие | Ответ |
|---|---|
| если есть запрет на токенизацию карты в настройках ее обслуживания | DECLINED |
| если tokenizationPath == 'RED' | DECLINED |
| если карта имеет статус, отличный от нормального (в стоп-списке и т.д.) | DECLINED |
| если в запросе присутствует срок действия карты, и он не совпадает со сроком действия карты в БД | DECLINED |

**2. В случае otpReason == TOKEN_DEVICE_BINDING:**

2.1. если для держателя карты зарегистрирован номер мобильного телефона - вернуть REQUIRE_ADDITIONAL_AUTHENTICATION и номер телефона

2.2. иначе вернуть DECLINED

| Условие | Ответ |
|---|---|
| если для держателя карты зарегистрирован номер мобильного телефона | REQUIRE_ADDITIONAL_AUTHENTICATION и номер телефона |
| если для держателя карты **НЕ** зарегистрирован номер мобильного телефона | DECLINED |

**3. В случае otpReason == PROVISIONING или отсутствия otpReason вообще:**

3.1. если panSource == 'T'

3.1.1. если состояние карты нррмальное - вернуть APPROVED

3.1.2. иначе вернуть DECLINED

| Условие | Ответ |
|---|---|
| если состояние карты нормальное | APPROVED |
| иначе | DECLINED |

3.2. если tokenRequestorId **НЕ входит** в список провайдеров "больших" кошельков (Google Pay, Apple Pay, Garmin Pay и т.д.):

3.2.1. если panSource != 'M' - вернуть APPROVED

3.2.2. иначе вернуть DECLINED

| Условие | Ответ |
|---|---|
| если panSource != 'M' | APPROVED |
| иначе | DECLINED |

3.3. если tokenRequestorId **входит** в список провайдеров "больших" кошельков (Google Pay, Apple Pay и т.д.):
3.3.1. если panSource == 'M' - вернуть APPROVED
3.3.2. иначе вернуть REQUIRE_ADDITIONAL_AUTHENTICATION (безусловно) и номер телефона (при условии наличия такового)

| Условие | Ответ |
|---|---|
| если panSource == 'M' | APPROVED |
| иначе | REQUIRE_ADDITIONAL_AUTHENTICATION (безусловно) и номер телефона (при условии наличия такового) |

**4. В случае других значений otpReason:**
4.1. если panSource != 'M' и банк поддерживает участие в программе для otpReason == PAYMENT или otpReason == CARDHOLDER_STEPUP:
4.1.1. если для держателя карты зарегистрирован номер мобильного телефона - вернуть REQUIRE_ADDITIONAL_AUTHENTICATION и номер телефона
4.1.2. иначе вернуть DECLINED
4.2. если panSource != 'M' и банк поддерживает участие в программе для otpReason == TRUSTED_LISTING_ENROLLMENT - вернуть APPROVED
4.3. иначе вернуть DECLINED

## Список документации.

1.FASTTACK Database Structure
2.FASTTACK Функциональное описание модуля
3.MDES Pre-Digitization API,  Version 1.7
4.MDES Customer Service API,  Version 2
5.VTS Issuer Web Service Interface Development Guide,  Release 1.25.
6.VTS Issuer API Specifications, Version 2.2
7.VTS Push Provisioning , Encrypted Payment Instrument, Version 1.11
8.Visa Digital Solutions API Reference Guide , January 17, 201
9.UPC, Account Verification, Версия 1.0