



# PayControl

## Архитектура и принципы работы

---

### Оглавление

Назначение .....	2
Состав .....	2
Принципы работы PayControl.....	3
Процесс подтверждения транзакции .....	3
Электронная подпись в PayControl .....	5
Выработка кода подтверждения .....	6
Управление ключевой информацией пользователей .....	6
Состав ключевой информации .....	6
Распространение ключевой информации.....	6
Безопасность ключевой информации при хранении в мобильном устройстве .....	7
Использование ключевой информации для выработки кода подтверждения.....	7
Безопасность ключевой информации при хранении в базе данных сервера .....	8

## Назначение

PayControl – программный комплекс, предназначенный для подтверждения пользователем выполнения действий в системах дистанционного банковского обслуживания (ДБО) и/или электронного документооборота (ЭДО).

При помощи PayControl могут подтверждаться волеизъявления на совершение банковских транзакций, создание и исполнение документов, факты получения и/или ознакомления с определенной информацией.

## Состав

PayControl состоит из двух частей:

### 1. Серверная часть

Интегрируется с серверной частью прикладной системы (ДБО или ЭДО) и выполняет следующие функции:

- регистрация прикладных систем в PayControl;
- регистрация пользователей в PayControl;
- генерация и обновление ключевой информации пользователей PayControl;
- генерация QR-кодов с ключевой информацией и данными транзакций для подтверждения;
- проверка кодов подтверждения;
- формирование биллинговых и информационных отчетов.

Серверная часть представляет собой преднастроенный виртуальный или реальный сервер. Доступ к функциям PayControl со стороны прикладной системы осуществляется посредством вызовов веб-сервисов PayControl с использованием протокола Simple Object Access Protocol (SAOP), что позволяет выполнять интеграцию с любыми прикладными платформами.

Серверная часть должна быть установлена в пределах периметра безопасности прикладной системы.

### 2. Клиентская часть

Представляет собой приложение для мобильных платформ iOS (7.0 и выше) и Android (4.0 и выше), выполняющее следующие функции:

- сканирование QR-кодов с ключевой информацией и данными транзакций для подтверждения с использованием камеры мобильного телефона;
- отображение подтверждаемой информации на экране мобильного телефона;
- выработка кода подтверждения на основе данных транзакции, ключа пользователя, времени выработки и (опционально) отпечатка устройства;
- опциональное сохранение ключевой информации пользователя в зашифрованном виде в памяти мобильного телефона;
- управление различными наборами ключевой информации пользователя (сохранение, просмотр, удаление);

- формирование отпечатка устройства.

Клиентская часть представляется в виде встраиваемых библиотек для интеграции в собственное мобильное приложение или в виде самостоятельного приложения.

## Принципы работы PayControl

### Процесс подтверждения транзакции

Процесс взаимодействия серверной части PayControl, прикладной системы, клиентской части PayControl и пользователя приведен на рисунке 1.

Он состоит из нескольких основных шагов:

1. Пользователь создает документ и отправляет его на подтверждение в прикладную систему;
2. Прикладная система с использованием серверной части PayControl подписывает документ своей ЭП и генерирует QR-код с основными полями транзакции, которая требует подтверждения. Поля и информация, на основе которой будет выработан код подтверждения, определяются прикладной системой;
3. Прикладная система отображает в пользовательском интерфейсе QR-код, предоставленный серверной частью PayControl;
4. Пользователь с использованием клиентской части (мобильного приложения PayControl или собственного приложения с интегрированным SDK для мобильных платформ) считывает данные транзакции из пользовательского интерфейса прикладной системы через QR-код;
5. Клиентская часть генерирует код подтверждения;
6. Пользователь вводит код подтверждения в пользовательском интерфейсе прикладной системы;
7. Прикладная система с использованием серверной части PayControl проверяет валидность кода подтверждения, предоставленного пользователем.

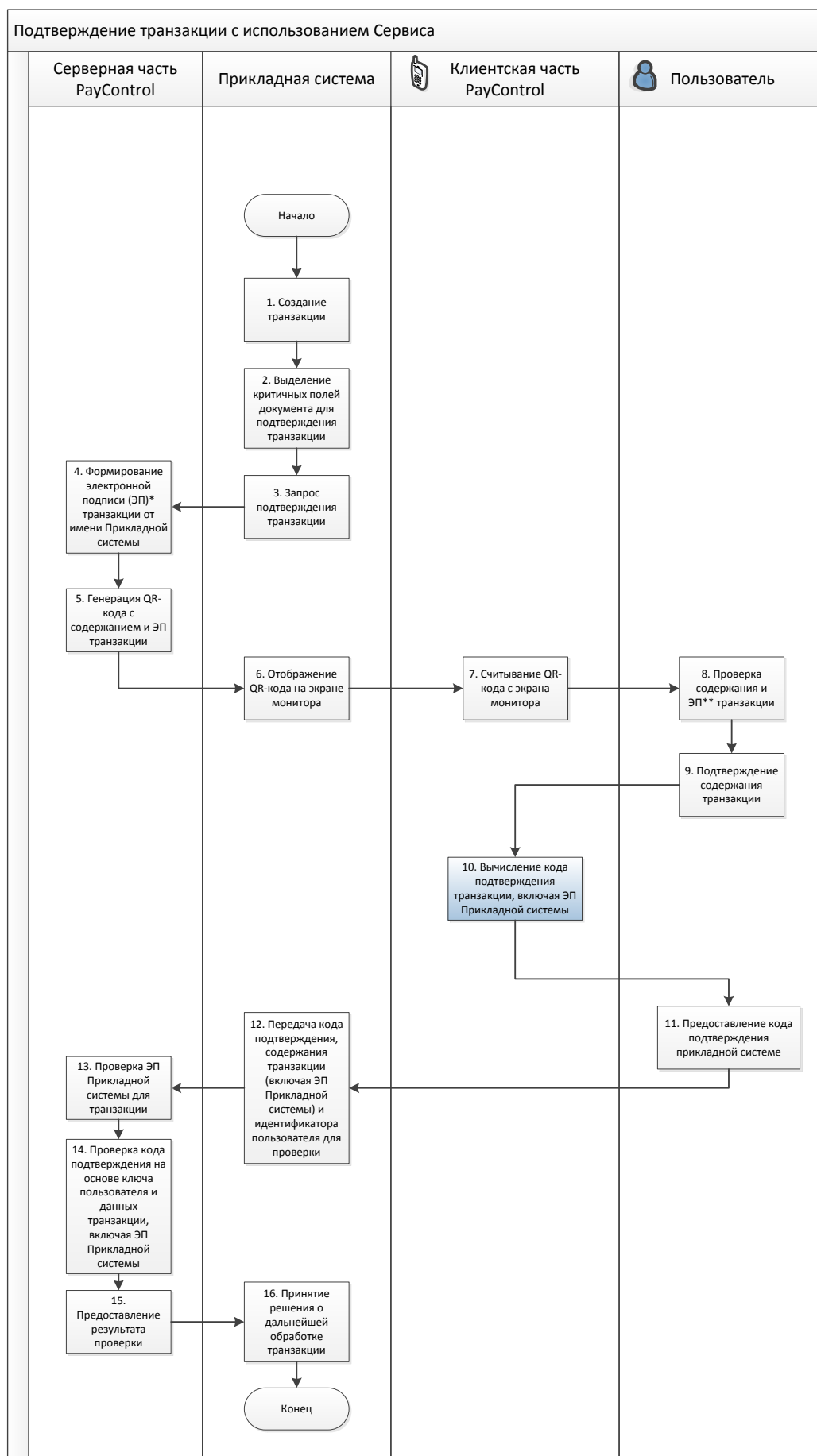


Рисунок 1 – процесс подтверждения транзакции с использованием PayControl

## Электронная подпись в PayControl

В терминологии Федерального Закона №63-ФЗ «Об электронной подписи» в PayControl используется два вида электронной подписи (ЭП): усиленная<sup>1</sup> и простая.

В процессе формирования QR-кода с данными транзакции для подтверждения серверная часть выполняет формирование ЭП для данных транзакции. После формирования ЭП серверной части (то есть владельца прикладной системы – Банка или оператора ЭДО) присоединяется к данным транзакции.

Прикладная система получает QR-код, в котором содержатся данные транзакции вместе с ЭП владельца прикладной системы. Таким образом, после считывания QR-кода, пользователь видит на своем мобильном телефоне данные транзакции, подписанные электронной подписью владельца прикладной системы.



Платеж в банк «Первый русский»  
Перевод на счет № 40810123000000000000  
Получатель: Иванов Иван Иванович  
ИНН: 707001001001  
Сумма: 10 000 рублей  
Идентификатор платежа (ЭП):  
010203040506070809101112131415161718  
192021222342526272829300102030405060  
708091011121314151617181920212223425  
262728293001020304

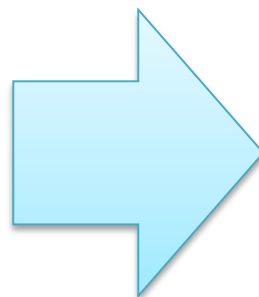
Рисунок 2 – содержание данных для подтверждения пользователем

После проверки корректности данных транзакции пользователь с использованием мобильного приложения PayControl формирует простую ЭП. Простая ЭП пользователя подтверждает корректность данных транзакции, а также корректность и принятие электронной подписи владельца системы.

Платеж в банк «Первый русский»  
Перевод на счет № 40810123000000000000  
Получатель: Иванов Иван Иванович  
ИНН: 707001001001  
Сумма: 10 000 рублей  
Идентификатор платежа (ЭП):  
0102030405060708091011121314151617181920  
2122234252627282930010203040506070809101  
1121314151617181920212223425262728293001  
020304

Ключ пользователя + отпечаток устройства  
(опционально)  
01020304050607080910

Время выработки  
01.01.2015 12:00



Код подтверждения

**123456**

<sup>1</sup> Может использоваться как усиленная квалифицированная, так и усиленная подпись

Рисунок 3 – выработка простой электронной подписи на стороне пользователя

## Выработка кода подтверждения

Код подтверждения данных транзакции вырабатывается на основе стандартизованных алгоритмов и представляет собой Time-Based One-Time Password.

Код подтверждения представляет собой функцию

$$\text{OTP} = \text{TOTP} (\text{K}_{\text{OTP}}, \text{SHA-1}(\text{HMAC}_{\text{message}} + \text{T} + \text{Fingerprint}), \text{D}), \text{ где}$$

TOTP – функция выработки одноразового пароля в соответствии с RFC6238;

SHA-1 – функция хеширования SHA-1;

$\text{K}_{\text{OTP}}$  – ключ пользователя для генерации OTP;

$\text{HMAC}_{\text{message}}$  – результат вычисления HMAC от данных транзакции, включая электронную подпись;

T – дискретное значение времени, интервал дискретизации – 180 секунд;

Fingerprint – отпечаток устройства клиентской части (опционально);

D – количество символов в результирующем OTP;

Операция «+» означает конкатенацию значений байтов.

$\text{HMAC}_{\text{message}}$  вычисляется следующим образом:

$$\text{HMAC}_{\text{message}} = \text{HMAC} (\text{K}_{\text{HMAC}}, \text{Data} + \text{UserID}), \text{ где}$$

HMAC – функция выработки кода аутентификации сообщения в соответствии с RFC2104, основанная на хеш-функции SHA-1;

$\text{K}_{\text{HMAC}}$  – ключ для генерации HMAC сообщения;

Data – данные транзакции;

UserID – идентификатор пользователя в Сервисе.

Операция «+» означает конкатенацию значений байтов.

## Управление ключевой информацией пользователей

### Состав ключевой информации

Ключевая информация пользователя в PayControl состоит из следующих данных:

1. Идентификатор пользователя в системе PayControl;
2. Ключ пользователя для генерации OTP –  $\text{K}_{\text{OTP}}$ ;
3. Ключ пользователя для генерации HMAC –  $\text{K}_{\text{HMAC}}$ ;
4. Срок действия ключевой информации.

Ключи  $\text{K}_{\text{OTP}}$  и  $\text{K}_{\text{HMAC}}$  представляют собой случайные наборы по 20 байт (160 бит) каждый.

Ключи пользователей генерируются серверной частью системы и возвращаются прикладной системе для дальнейшей их передачи пользователю посредством пользовательского интерфейса.

### Распространение ключевой информации

PayControl предполагает распространение ключевой информации среди пользователей двумя способами:

1. Путем передачи пользователю карточки с отпечатанным QR-кодом, который содержит набор ключевой информации.

Данный способ подразумевает, что пользователь должен посетить офис обслуживания клиентов и лично получить карточку с ключевой информацией.

Клиенту предоставляется на выбор возможность либо сохранить ключ в памяти телефона, либо сканировать его каждый раз при подтверждении транзакций.

2. Удаленная передача ключевой информации.

В данном случае PayControl разделяет ключевую информацию на две части. Первая часть содержит половину ключа  $K_{OTP}$  и половину  $K_{HMAC}$ , вторая – вторые половины ключей, идентификатор пользователя и срок действия ключевой информации.

Первая часть должна быть отправлена пользователю прикладной системой по SMS-каналу. Вторая – отображена в пользовательском интерфейсе прикладной системы в виде QR-кода.

Пользователь, получив SMS с первой частью ключа и отсканировав QR-код со второй частью ключа имеет возможность сохранить полный набор ключевой информации в приложении PayControl для мобильного телефона.

### **Безопасность ключевой информации при хранении в мобильном устройстве**

Ключевая информация может быть сохранена в мобильном телефоне пользователя или может каждый раз считываться из QR-кода, напечатанного на карточке с ключами.

При хранении ключевой информации в мобильном телефоне, доступ к ней может быть получен только после ввода пароля. Длина пароля ограничивается минимальной длиной в 4 символа.

При этом ни сам пароль, ни его производные (например, значение хеш-функции от пароля) не сохраняются в памяти мобильного телефона ни в каком виде.

При сохранении ключевой информации выполняется ее шифрование. В качестве ключа шифрования используется значение хеш-функции SHA-256 от пароля. Зашифрованная ключевая информация сохраняется в памяти мобильного телефона.

Для получения доступа к ключевой информации при выработке кода подтверждения, приложение для мобильного телефона запрашивает пароль, вычисляет значение хеш-функции и расшифровывает с использованием полученного значения ключевую информацию.

Таким образом, кража ключей пользователя или данных приложения для мобильного телефона, а также возможная модификация кода мобильного приложения не даст результата без знания пароля для доступа к ключевой информации.

### **Использование ключевой информации для выработки кода подтверждения**

При выработке кода подтверждения используется ключевая информация пользователя, которая может быть получена мобильным приложением из двух источников:

1. При сканировании QR-кода с карточки с ключевой информацией

При использовании данного источника ключевой информации в мобильном телефоне не сохраняется никакой информации, которая может быть использована в дальнейшем.

При этом средство вычисления кода подтверждения (мобильный телефон) и ключевая информация физически разделены по месту хранения. Карточка с ключевой информацией может храниться в бумажнике или другом доступном только для владельца месте.

2. Из сохраненного в мобильном телефоне набора ключевой информации, защищенного паролем пользователя

В данном случае ключевая информация извлекается из памяти мобильного телефона (см. *Безопасность ключевой информации при хранении в мобильном устройстве*) с использованием пароля пользователя.

Так как ключевая информация хранится в приложении для мобильного телефона, данный способ предоставляет бОльший уровень удобства для пользователя, в том числе позволяет использовать схему удаленной передачи ключей без необходимости посещения пользователем офиса обслуживания банка.

### **Безопасность ключевой информации при хранении в базе данных сервера**

Серверная часть PayControl в стандартной конфигурации включает в себя прикладное программное обеспечение и сервер баз данных, которые функционируют на одной физической или виртуальной машине. Эта машина должна располагаться внутри периметра безопасности серверной части прикладной системы. Другими словами, обеспечение противодействия угрозам несанкционированного доступа к серверной части PayControl со стороны внешних нарушителей должно решаться средствами построения периметра безопасности.

Для противодействия внутреннему нарушителю ключевая информация пользователей, хранящаяся в базе данных PayControl, может быть зашифрована ключом серверной части PayControl. В этом случае сервер баз данных и сервер приложений PayControl должны быть разделены и находиться в зонах ответственности разных администраторов.

То есть администратор, имеющий доступ к приложению PayControl, который потенциально может скомпрометировать ключи серверной части, не должен иметь доступа к базе данных PayControl, где хранятся ключи пользователей. Администратор, имеющий доступ к базе данных PayControl, не должен иметь доступ к приложению PayControl, где хранится ключевая информация серверной части.

В этом случае безопасность ключевой информации пользователей, хранящейся в базе данных PayControl, обеспечивается разделением зон ответственности и может быть нарушена только при сговоре двух администраторов.