SAFETECH
SAFETY TECHNOLOGIES

PayControl

Программный комплекс
для подтверждения и проверки
подлинности электронных
документов

ООО «СэйфТек»

ОБЩИЕ СВЕДЕНИЯ

Термины и сокращения

АБС	Автоматизированная банковская система
АСУ ГД	Автоматизированная Система Гарантированной Доставки Уведомлений Банка
АРМ РКС	Автоматизированное рабочее место разбора конфликтных ситуаций и вывода детализированной информации
Компания	Общество с ограниченной ответственностью «СэйфТек»
СДБО	Система дистанционного банковского обслуживания
PayControl	Программный комплекс для подтверждения и проверки подлинности электронных документов PayControl, свидетельство о государственной регистрации программы для ЭВМ №2014611638 от «06» февраля 2014 г
ЭП	Электронная подпись

Сведения о Компании

Полное наименование	Общество с ограниченной ответственностью «СэйфТек»
Юридический адрес	143026, г. Москва, Территория инновационного центра «Сколково», Большой бульвар, дом 42, строение 1, часть помещения 334, этаж 1
Почтовый адрес	123308, г. Москва, 3-я Хорошёвская улица, дом 18, корпус 1, офис 104
ИНН/КПП	7719769327/773101001
Расчетный счет	40702810201500014776 в ТОЧКА ПАО БАНКА «ФК ОТКРЫТИЕ»
к/с	30101810845250000999
БИК	044525999
тел.	+7 (495) 120-99-09
E-mail	info@safe-tech.ru

ОПИСАНИЕ PAYCONTROL

PayControl – программный комплекс, предназначенный для подтверждения пользователем операций в системах дистанционного банковского обслуживания и/или электронного документооборота.

PayControl призван, в первую очередь, повысить уровень удобства подтверждения и информационной безопасности по сравнению с такими способами подтверждения как одноразовые пароли (One-Time Password), передаваемые через SMS и PUSH-каналы, скретч-карты, аппаратные и программные MAC-токены и пр.

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

Принцип работы

PayControl обеспечивает подтверждение операций (формирование и проверку электронной подписи) при помощи мобильного приложения (приложения Банка со встроенным PayControl SDK или отдельного приложения), установленного на смартфоне конечного пользователя.

При этом канал, в котором сформирован документ, может быть любым: интернет-банк, мобильный банк, АБС (автоматическое создание документов) и пр.

Подтверждение состоит из двух шагов:

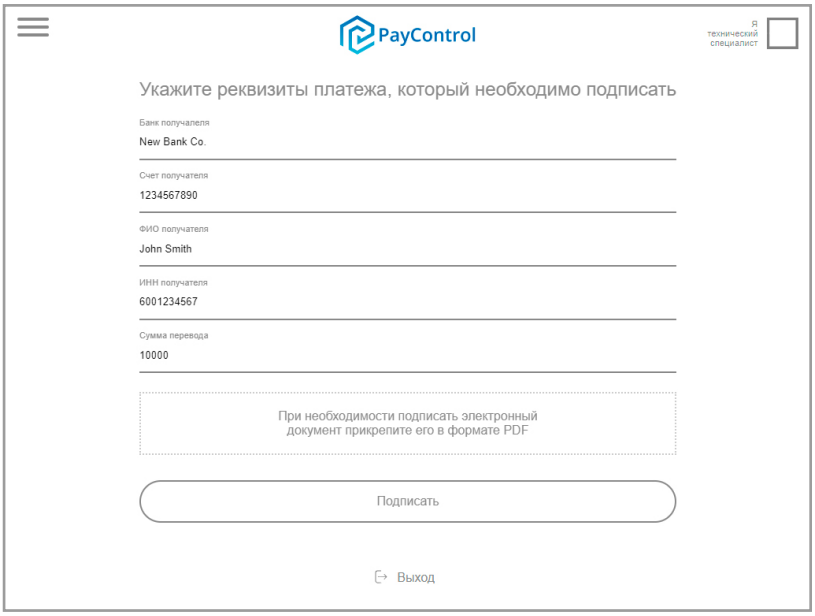
1. электронный документ передаётся на подписание в PayControl;
2. пользователь при помощи мобильного приложения формирует электронную подпись:
    a. если смартфон пользователя онлайн, то пользователь получает уведомление о новой операции, проверяет корректность содержания документа, подтверждает или отказывается от подписания;
    b. если смартфон офлайн, то пользователь сканирует QR-код с данными документа, проверяет корректность содержания, получает код подтверждения транзакции и вводит его в поле подтверждения.

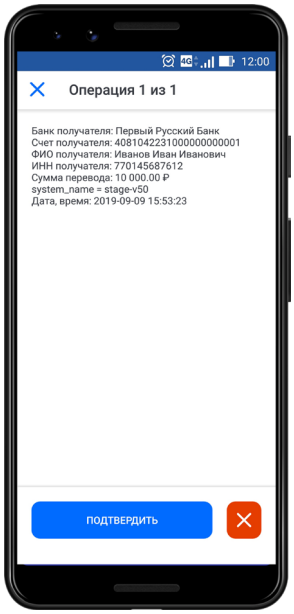
Выработка подписи (в любом режиме) защищена при помощи TouchID/FaceID, пароля с задаваемой политикой сложности или пин-кода.

В отличие от классических генераторов одноразовых паролей, принципы работы PayControl гарантируют защиту от фишинга, подмены документа, перехвата одноразовых паролей методом социальной инженерии и т.д., так как подпись вырабатывается мобильным приложением на основе 4-х составляющих:

- данные транзакции, включая идентификатор пользователя;
- время формирования кода подтверждения;
- ключевая информация пользователя;
- [опционально] отпечаток устройства.

Дополнительно, при работе в онлайн-режиме, который является базовым, пользователь не имеет возможности сообщить кому-либо значение подписи, что значительно повышает стойкость решения к методам социальной инженерии. В то же время, даже в офлайн-режиме пользователь имеет возможность контролировать, для подтверждения какой именно операции вырабатывается код подтверждения.





ОПИСАНИЕ PAYCONTROL

PayControl – программный комплекс, предназначенный для подтверждения пользователем операций в системах дистанционного банковского обслуживания и/или электронного документооборота.

PayControl призван, в первую очередь, повысить уровень удобства подтверждения и информационной безопасности по сравнению с такими способами подтверждения как одноразовые пароли (One-Time Password), передаваемые через SMS и PUSH-каналы, скретч-карты, аппаратные и программные MAC-токены и пр.

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

Состав

PayControl является платформой, имеющей модульную архитектуру, функциональность которой зависит от набора используемых модулей.

ЯДРО PAYCONTROL

Обеспечивает базовую функциональность PayControl, включая выполнение всех основных функций, таких как:

- взаимодействие с СДБО;
- управление пользователями и их ключами;
- персонализация мобильных приложений;
- взаимодействие с мобильными приложения для онлайн- и офлайн-подтверждений;
- проверка электронных подписей.

Базовой функциональности достаточно для замены таких способов подтверждения, как SMS, одноразовые пароли (One-Time Password), скретч-карты, MAC-токены и пр. Выработка и проверка подписи основана на симметричных криптографических алгоритмах, которые подразумевают использование одинакового набора ключей для выработки и проверки подписи.

МОДУЛЬ АСИММЕТРИЧНОЙ КРИПТОГРАФИИ

Данный модуль добавляет к базовой функциональности использование асимметричных криптографических алгоритмов для выработки и проверки подписи. Он расширяет два процесса PayControl:

1. процесс персонализации мобильного приложения пользователя:
   к основной процедуре добавляется выработка в смартфоне клиента уникальной ключевой пары: закрытого и открытого ключей. После выработки, открытый ключ безопасным способом регистрируется на сервере и в дальнейшем используется только для проверки подписей от имени пользователя; закрытый ключ, который используется для выработки подписи, никогда не покидает смартфон;
2. процесс проверки подписи:
   проверка подписи выполняется одновременно по симметричным и асимметричным криптографическим алгоритмам.

Модуль асимметричной криптографии позволяет обеспечить неотказуемость пользователя от факта подписания электронных документов, так как только он обладает закрытым ключом для выработки подписи.

Модуль сбора данных о клиентских устройствах

Модуль сбора данных позволяет собирать более 70-ти параметров о смартфоне, на котором формируется электронная подпись. Это позволяет, в первую очередь, выполнять более качественный анализ рисков операций в системах предотвращения мошенничества (антифрод-системах), а также использовать дополнительные данные для анализа аудитории.

В собираемую информацию входит:

- базовая информация об устройстве: производитель, модель, версия операционной системы, часовой пояс, выбранная локаль, сведения об аппаратных составляющих (марки процессора, дисплея и т. д.);
- сведения о наличии root/jailbreak и о потенциально опасных приложениях;
- состояние памяти устройства: объем карты памяти, объем встроенной памяти, объем оперативной памяти;
- информация о приложении банка;
- информация о Wi-Fi - подключении: название подключённой сети, IP- и MAC-адрес;
- информация о физических сенсорах устройства: акселерометр, датчик освещённости и т. д.;
- геопозиция;
- информации о телефоне и SIM-карте: оператор связи, количество SIM-карт, IMSI, IMEI.

МОДУЛЬ ИНТЕГРАЦИИ С СИСТЕМАМИ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Модуль позволяет использовать биометрию (распознавание лица) в качестве дополнительного фактора при подтверждении (выработке электронной подписи) высокорисковых операций, а также при выполнении потенциально опасных действий:

- при срабатывании антифрод-системы;
- подписании операции на сумму сверх лимитов;
- смена номера телефона;
- персонализация другого устройства;
- восстановление доступа;
- и пр.

Процесс биометрической идентификации встроен в механизмы подписания PayControl.

Для биометрической аутентификации используются технологии компаний-партнёров, которые приобретаются отдельно.Модуль интеграции с системами анализа рисков

Данный модуль обеспечивает интеграцию с системами анализа рисков, связанных с источником электронного документа и устройством выработки электронной подписи, на котором работает пользователь.

Такие системы выявляют вредоносные веб-инъекции, социальную инженерию, фишинг, бот-сети, захват учетной записи, сети нелегального обналичивания денег и другие виды банковского мошенничества. Если документ создан или подтверждается на устройстве, которое может быть скомпрометировано, документу присваивается повышенный уровень риска. Это позволяет более точно и адресно выявлять случаи мошенничества.

При использовании данного модуля оценка уровня риска будет передана СДБО вместе с значением подписи документа.

PayControl позволяет выполнять оценку средствами системы Group IB Secure-Bank .

МОДУЛЬ РАЗБОРА КОНФЛИКТНЫХ СИТУАЦИЙ И ВЫВОДА ДЕТАЛИЗОВАННОЙ ИНФОРМАЦИИ

Данный модуль содержит расширение функциональности PayControl, которое позволяет

— производить проверку значения электронной подписи ранее подписанного документа;
— выводить подробные сведения об учётной записи пользователя;
— выводить информацию по транзакциям пользователя и попыткам подтверждения;
— выводить информацию по событиям, связанным с учетной записью пользователя.

Для работы с выводимой информацией модуль включает АРМ РКС (автоматизированное рабочее место разбора конфликтных ситуаций и вывода детализированной информации), позволяющий выполнять все необходимые действия в веб-интерфейсе.

МОДУЛЬ ИНТЕГРАЦИИ С КРИПТОПРО DSS

Данный модуль позволяет использовать компонент PayControl, работающий на смартфоне пользователя (SDK в составе приложения Банка или самостоятельное приложение) в качестве аутентификатора для программно-аппаратного комплекса КриптоПро DSS, являющегося сертифицированным в соответствии с законодательством РФ средством электронной подписи .

Наличие аутентификатора в КриптоПро DSS обеспечивает функциональность выработки электронной подписи при помощи мобильного приложения.

РЕДАКЦИИ

PayControl поставляется в следующих редакциях

	LITE	Базовая	Расширенная	Максимальная
Ядро	√	√	√	√
Модуль асимметричной криптографии		√	√	√
Модуль сбора данных о клиенте			√	√
Модуль интеграции с системами анализа рисков			√	√
Модуль интеграции с системами биометрической аутентификации			√	√
Модуль разбора конфликтных ситуаций и вывода детализованной информации				√
Модуль интеграции с КриптоПро DSS				√