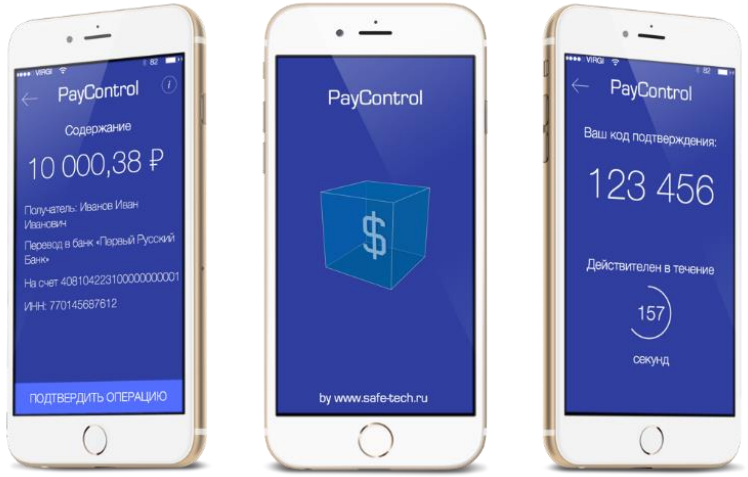
SafeTech
SAFETY TECHNOLOGIES



Подтверждение транзакций и подпись документов на мобильном устройстве

Простота и безопасность для пользователей, надежность и снижение расходов для Банков

Sk Сколково

О КОМПАНИИ SAFETECH (СЭЙФТЕК)

SafeTech
SAFETY TECHNOLOGIES

АК БАРС БАНК

МОСКОВСКИЙ ИНДУСТРИАЛЬНЫЙ БАНК

РоссельхозБанк

МТС Банк

Запсибкомбанк

ВОЗРОЖДЕНИЕ БАНК

БАНК ЦЕНТР-ИНВЕСТ

Sk Skolkovo

Sk IT

Резидент Инновационного Центра «СКОЛКОВО»

- Основана в 2010 году, как разработчик средств безопасности для систем дистанционного банкинга;
- Лицензиат ФСТЭК на разработку и производство средств защиты конфиденциальной информации;
- На сегодняшний день клиентами компании являются более 60-ти российских банков, в том числе, входящих в список ТОП-10;
- В продуктовую линейку компании входят решения как для юридических, так и для физических лиц

БИЗНЕС + БЕЗОПАСНОСТЬ = ☺

Чего хочет бизнес	Чем можем помочь
Высокий процентный доход (ниже риски, выше лимиты)	Защита от всех современных угроз
Больше транзакций	Работа с любого устройства Удобное подтверждение операций
Общение с клиентом только на приятные темы	Никаких установок СКЗИ, CSP, JCP, PKIClient и т.д. и т.п.
Сохранность денег Банка	Соответствие требованиям законодательства
Дополнительный непроцентный доход	Безопасность тоже можно продать

КЛАССИКИ и СОВРЕМЕННИКИ

Классик работает
за компьютером/ноутбуком
в Интернет-банке или Клиент-банке
с токеном, криптопровадером

Современник работает
со смартфоном/планшетом
в Интернет-банке или Моб. клиенте
с SMS-ками/OTP

Удаленное управление
Подмена реквизитов платежа

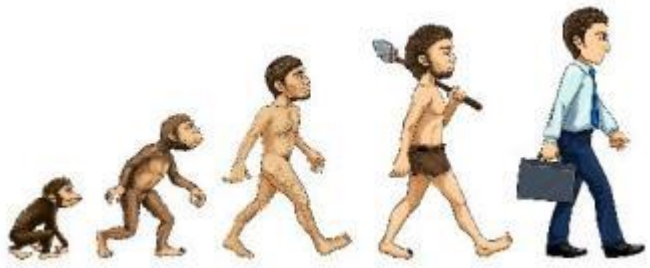
Фишинг
Перехват SMS
Подмена SIM-карт
Социальная инженерия

ДЛЯ КЛАССИКОВ – SAFETOUCH

- Защита от всех известных на сегодняшний день удаленных атак
  - Визуальный контроль данных, передаваемых в смарт-карту
  - Блокирование операции подписи до момента нажатия кнопки подтверждения
- Соответствие новой редакции Положения ЦБ «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств…» №382-П
  - «…оператор по переводу денежных средств обеспечивает реализацию технологических мер по разделению контуров подготовки и подтверждения клиентом электронных сообщений…»
- Отлично продается в составе пакета «Безопасность класса премиум» и приносит банкам доход от 1000 до 2500 руб. на одно рабочее место системы Интернет-банкинга

ДЛЯ СОВРЕМЕННИКОВ – В БЕЗОПАСНОСТИ ЗАСТОЙ?

ДБО	JAVA/ ActiveX	Web	Mobile	Messengers
Платежи/ переводы	По реквизитам счета	P2P	+ фото карты	По номеру моб.



ЭП	USB-токен	USB-токен	USB-токен	USB-токен
Подтверждение	SMS	SMS	SMS	SMS/Push

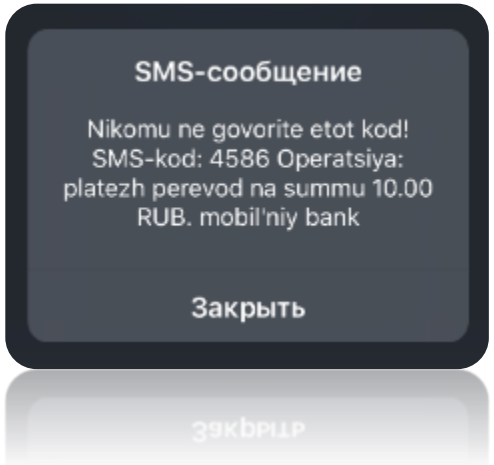
БЕЗОПАСНОСТЬ

Одноразовые пароли через SMS

- задержки в доставке
- возможность перехвата на уровне канала связи или ввода в систему
- возможность перехвата на уровне оператора мобильной связи
- возможность переоформления сим-карты клиента на мошенника по поддельной доверенности (и перехвата SMS)
- возможность направления клиенту SMS-сообщений с подменного номера
- рост операционных затрат пропорционально клиентской базе

Одноразовые пароли через PUSH

- негарантированная доставка
- прямой запрет Apple/Google/Microsoft на использование для передачи конфиденциальной информации
- предназначение – только информирование



НЕБЕЗОПАСНО

LIFESTYLE - В КАРМАНЕ ТОЛЬКО ТЕЛЕФОН

Общение
Здоровье
Билеты
Банковские карты
и еще много всего
и ... подпись

PayControl

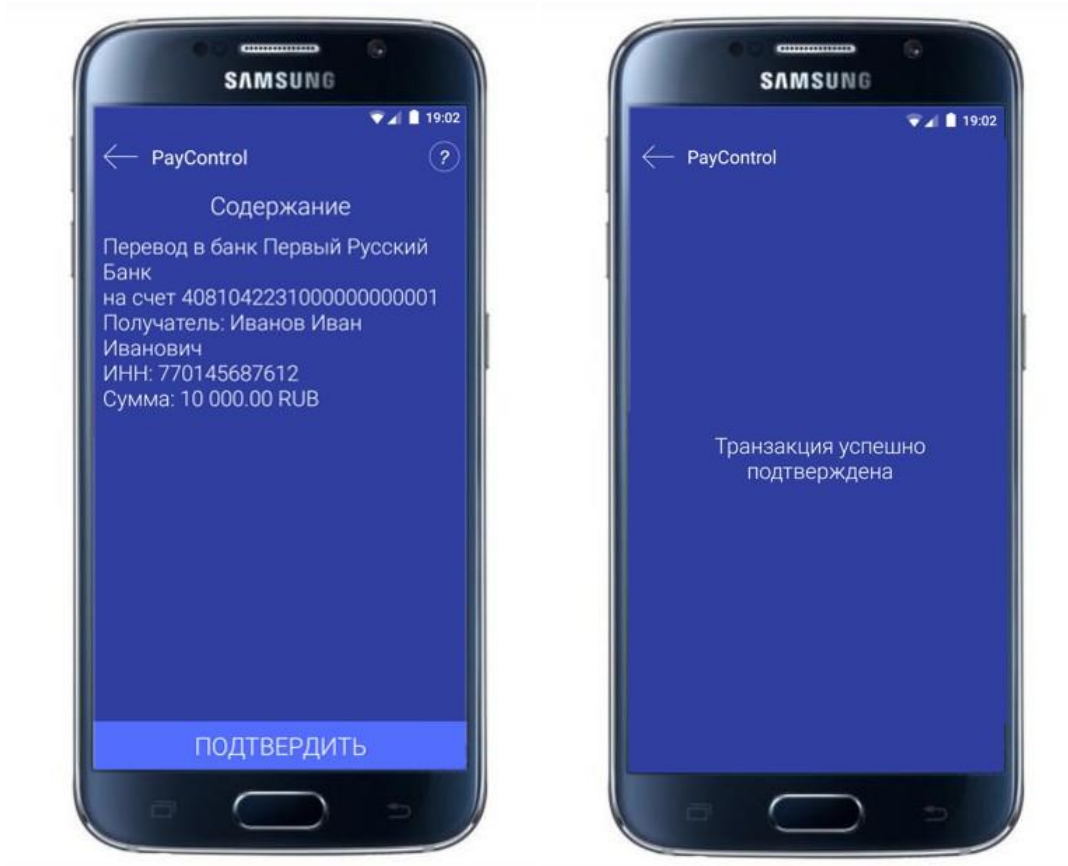
технология подтверждения и электронной подписи документов «в смартфоне»

- позволяет избавиться от ~~дорогих~~, ~~небезопасных~~ и ~~устаревших~~ кодов подтверждения по ~~SMS~~ и ~~PUSH~~
- перейти на усиленную неквалифицированную подпись вместо простой подписи (по 63-ФЗ)
- безопасно подтверждать любые электронные документы и операции прямо в Мобильном Банке без ручных операций, одним нажатием
- подтверждать документы даже при отсутствии Интернет-соединения и сотовой связи на мобильном телефоне

КАК ЭТО ВЫГЛЯДИТ

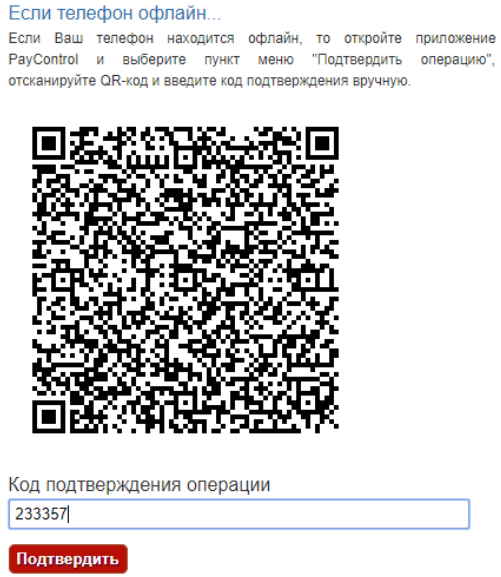
0. Клиент/оператор создает операцию в Интернет- или Мобильном Банке
1. Информация об операции приходит в Мобильное приложение Банка
2. Клиент нажимает «Подтвердить»

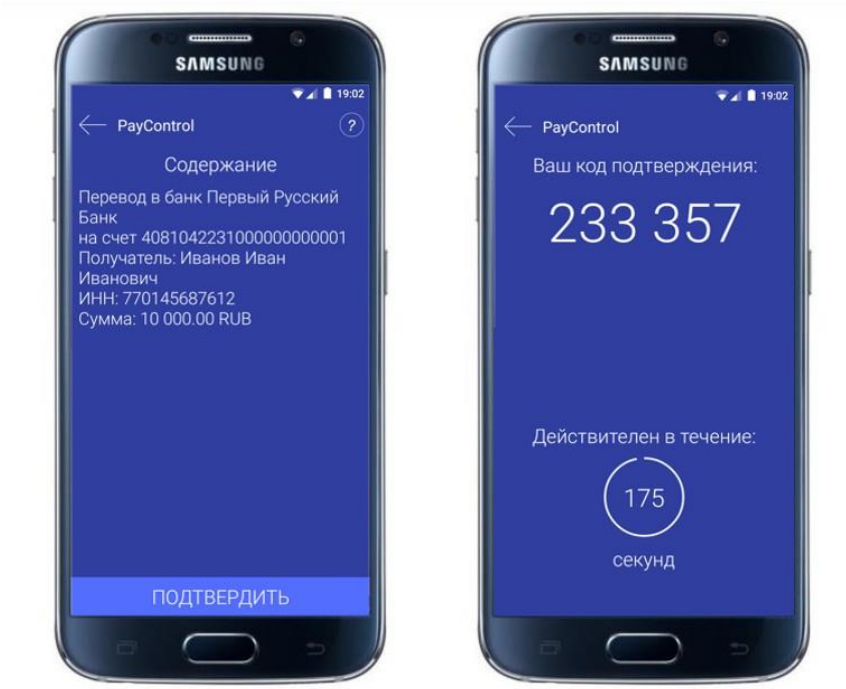
Документ подтверждён



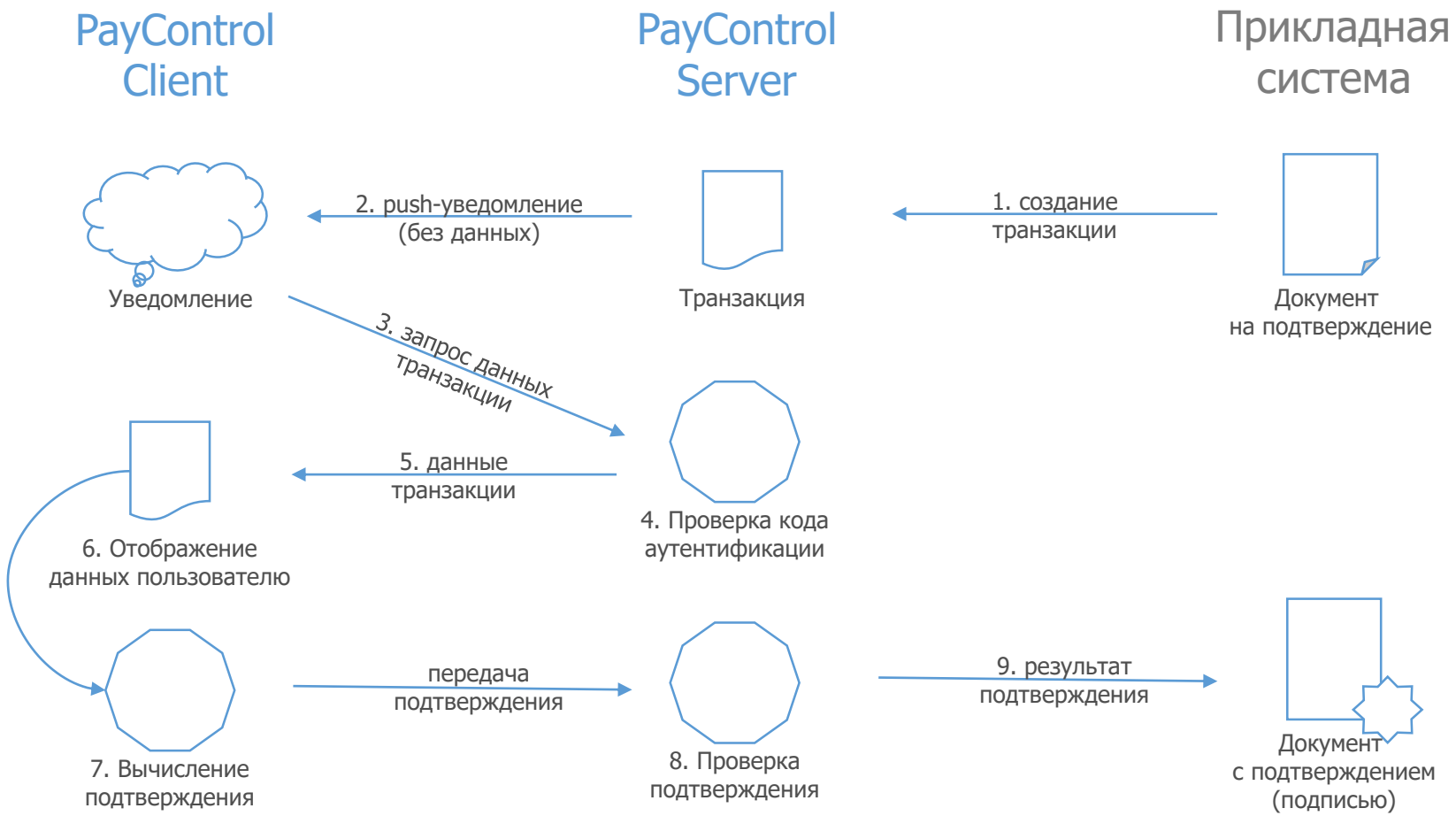
КАК ЭТО ВЫГЛЯДИТ

0. Клиент создает операцию в Интернет-Банке
1. На странице Интернет-Банка появляется QR-код
2. Клиент заходит в Мобильное приложение Банка, сканирует QR код, появляются детали операции
3. Клиент нажимает «Подтвердить», генерируется код подтверждения
4. Клиент вводит код подтверждения

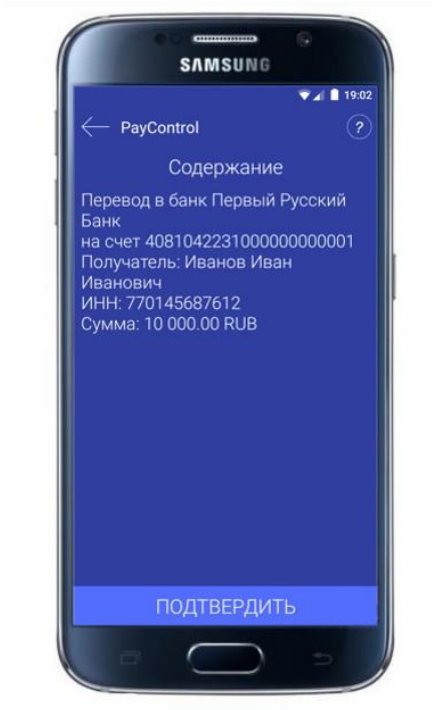




КАК ЭТО РАБОТАЕТ



КАК ЭТО РАБОТАЕТ



$HMAC_{MESSAGE}$ = Truncate (HMAC (K_{HMAC}, Data+UserID+Отпечаток+T), D), где

- HMAC – функция выработки кода аутентификации сообщения в соответствии с RFC2104, основанная на хеш-функции в зависимости от типа используемой прикладной системы
- K_{HMAC} – ключ для генерации HMAC сообщения
- Data – данные транзакции в формате TLV
- UserID – идентификатор пользователя в PayControl в формате TLV
- Отпечаток – отпечаток устройства в формате TLV
- T – дискретное значение времени, интервал дискретизации – 180 секунд в формате TLV
- Truncate – функция обрезания значения HMAC до D десятичных знаков; допустимые значения D – от 6 до 10; при D = 0 используется полное значение HMAC
- Операция «+» означает конкатенацию значений байтов

$SIGNATURE_{MESSAGE}$ = SIGN ($K_{PRIVATE}$, Data+UserID+Отпечаток+T), где

- SIGN – функция выработки электронной подписи
- $K_{PRIVATE}$ – закрытый ключ из ключевой пары пользователя
- Data – данные транзакции в формате TLV
- UserID – идентификатор пользователя в PayControl в формате TLV
- Отпечаток – отпечаток устройства в формате TLV
- T – дискретное значение времени, интервал дискретизации – 180 секунд в формате TLV
- Операция «+» означает конкатенацию значений байтов

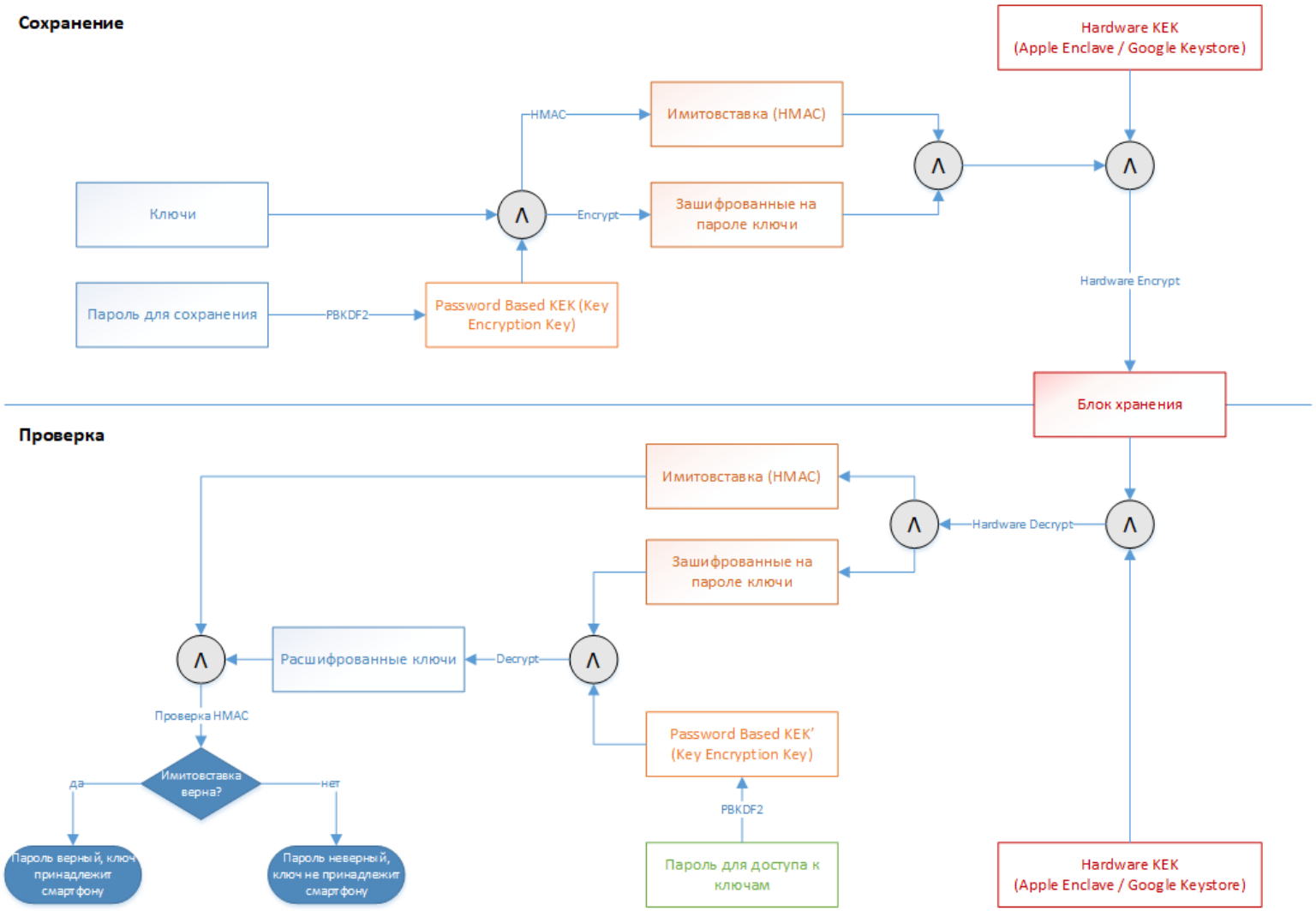
Используемые алгоритмы:

ECDSA, SHA-256, AES-256

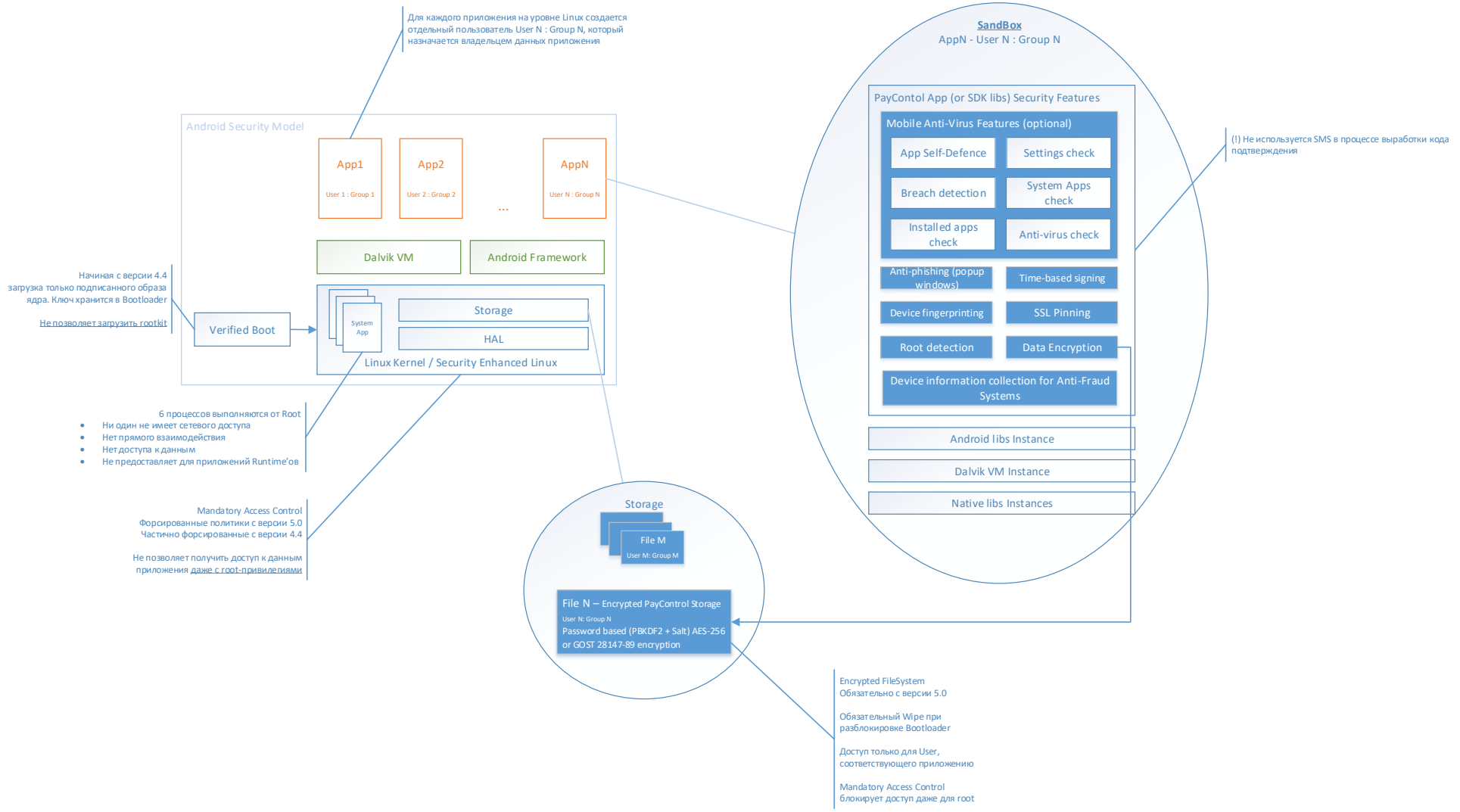
ГОСТ Р 34.11-2012, ГОСТ 28147-89

И САМОЕ ИНТЕРЕСНОЕ

- Ключи хранятся в библиотеках SDK в зашифрованном виде
- Ключей шифрования ключей – два: производная от пароля и аппаратный ключ смартфона
- Пароль не хранится на устройстве ни в каком виде
- Вместо (или вместе) с паролем может использоваться Apple TouchID / Apple FaceID / Google Imprint



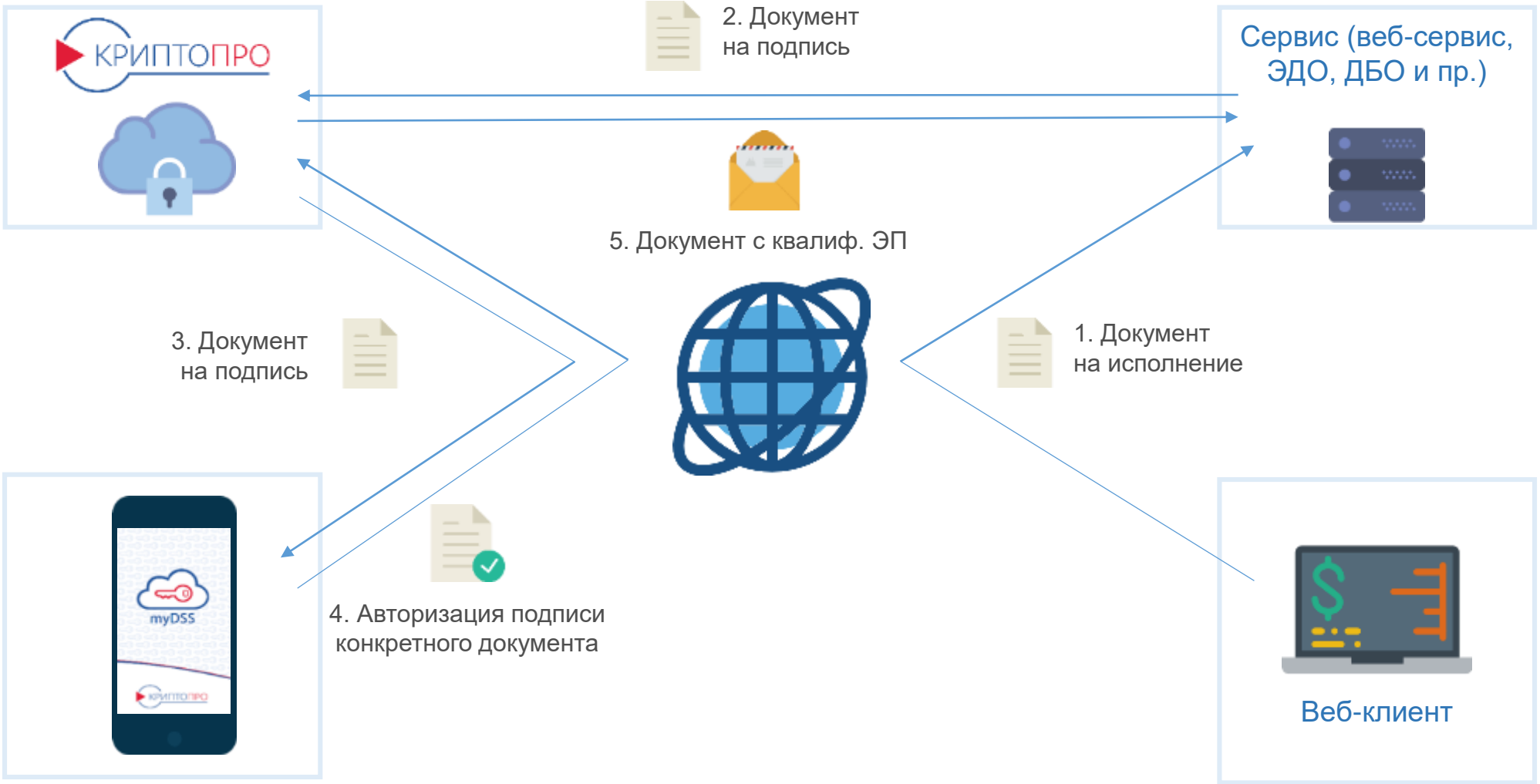
И КРОМЕ ЭТОГО



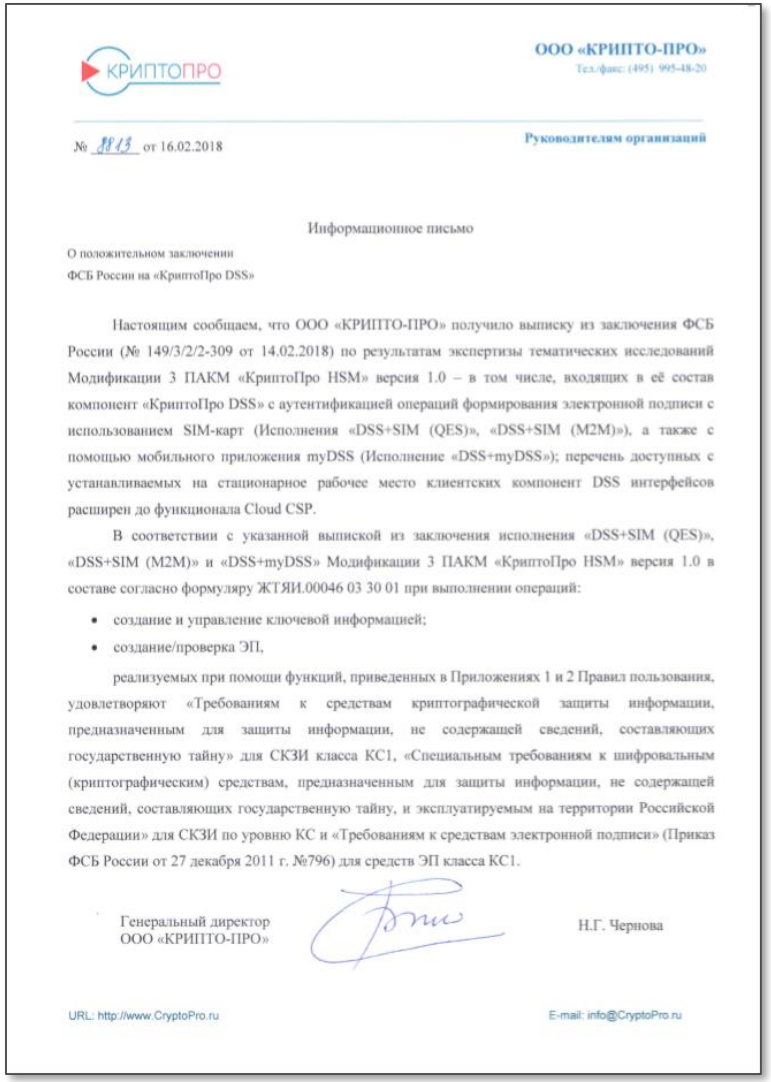
А ТЕПЕРЬ ЕЩЕ ИНТЕРЕСНЕЕ

Гибридная технология облачной подписи КриптоПро DSS и подтверждения операций PayControl

КАК ЭТО РАБОТАЕТ



DSS + myDSS – положительное заключение ФСБ



КРИПТОПРО

ООО «КРИПТО-ПРО»
Тел./факс: (495) 995-48-20

№ 8813 от 16.02.2018

Руководителям организаций

Информационное письмо

О положительном заключении
ФСБ России на «КриптоПро DSS»

Настоящим сообщаем, что ООО «КРИПТО-ПРО» получило выписку из заключения ФСБ России (№ 149/3/2/2-309 от 14.02.2018) по результатам экспертизы тематических исследований Модификации 3 ПАКМ «КриптоПро HSM» версия 1.0 – в том числе, входящих в её состав компонент «КриптоПро DSS» с аутентификацией операций формирования электронной подписи с использованием SIM-карт (Исполнения «DSS+SIM (QES)», «DSS+SIM (M2M)»), а также с помощью мобильного приложения myDSS (Исполнение «DSS+myDSS»); перечень доступных с устанавливаемых на стационарное рабочее место клиентских компонент DSS интерфейсов расширен до функционала Cloud CSP.

В соответствии с указанной выпиской из заключения исполнения «DSS+SIM (QES)», «DSS+SIM (M2M)» и «DSS+myDSS» Модификации 3 ПАКМ «КриптоПро HSM» версия 1.0 в составе согласно формуляру ЖТЯИ.00046 03 30 01 при выполнении операций:

- создание и управление ключевой информацией;
- создание/проверка ЭП,

реализуемых при помощи функций, приведенных в Приложениях 1 и 2 Правил пользования, удовлетворяют «Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» для СКЗИ класса КС1, «Специальным требованиям к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, и эксплуатируемым на территории Российской Федерации» для СКЗИ по уровню КС и «Требованиям к средствам электронной подписи» (Приказ ФСБ России от 27 декабря 2011 г. №796) для средств ЭП класса КС1.

Генеральный директор
ООО «КРИПТО-ПРО» Н.Г. Чернова

URL: http://www.CryptoPro.ru E-mail: info@CryptoPro.ru

ЧТО ЭТО ДАЁТ

- Любой браузер на любой платформе без плагинов, расширений или резидентных программ
- Нет аппаратных или программных СКЗИ
  - отсутствует логистика
  - существенное снижение затрат
  - кардинально снижаются требования к точкам распространения
- SaaS или самостоятельная инсталляция
- Любой УЦ, в том числе в составе SaaS
- Переход на новые стандарты (ГОСТы 2012-го года) без перевыдачи средств подписи

Как итог – полная мобильность

ЧТО В ИТОГЕ

- PayControl - усиленная неквалифицированная подпись
  - мобильно
  - безопасно
  - удобно
  - финансово эффективно

- DSS + myDSS – квалифицированная подпись
  - мобильно
  - масштабируемо на любые виды взаимодействия с клиентом
  - легитимно без оговорок

СПАСИБО ЗА ВНИМАНИЕ

Вопросы?