Криптография в банковских цифровых каналах

STCRYPT SAFETECH

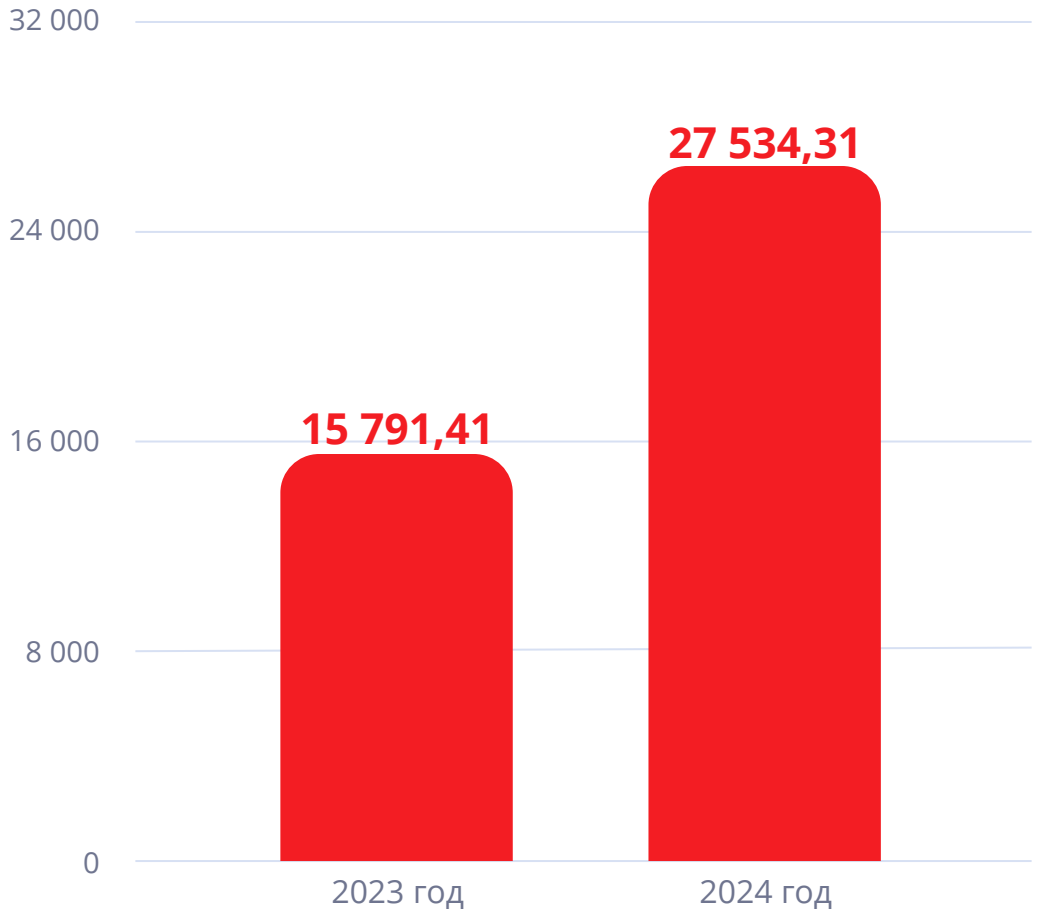
как способ борьбы с мошенничеством

Дарья Верестникова
Генеральный директор STCrypt
(SafeTech Group)

РусКрипто

Убытки от хищений в цифровых каналах

Объем операций, млн рублей



2024 !

Общий объем хищений за 2024 года: более 27 млрд рублей*

Объем хищений у ФЛ увеличился почти **в 2 раза**

Наибольший объем хищений осуществлялся с использованием ДБО

Доля возмещенных средств клиентам — **до 15,9 %**

* По данным с сайта Банка России cbr.ru

Основные схемы мошенничества с ПЭП и OTP-кодами

STCRYPT

Взлом аккаунтов

Использование слабых паролей и утечек данных для доступа к банковским приложениям. Разглашение данных для аутентификации в личные кабинеты самими клиентами

Троянские программы

Клиенты скачивают поддельные приложения или обновления, содержащие вредоносные программы–трояны, через которые крадут данные OTP-кодов из SMS/PUSH-сообщений

Подмена номера телефона

Мошенники перехватывают OTP-коды путем настройки переадресации SMS и звонков на свой номер или методом SIM-свопинг

Разглашение OTP-кода

Клиенты разглашают OTP-код под различными предлогами злоумышленников, не подозревая, что производят подтверждение операций, подписание кредитных договоров посредством ПЭП. Это приводит к финансовым последствия как для клиента, так и для банка

Оспаривание операций

Клиенты заявляют, что не совершали операций, подписанных ПЭП, что приводит к судебным разбирательствам

Фишинг

Клиенты вводят OTP-коды на поддельных сайтах или в приложениях

Чего не дают OTP-коды

STCRYPT

Нет отображения подписываемых данных

В соответствии с пунктом 2 статьи 12 63-ФЗ:

«При создании электронной подписи средства электронной подписи должны: **показывать** самостоятельно или с использованием программных, программно-аппаратных и технических средств, необходимых для отображения информации, подписываемой с использованием указанных средств, лицу, осуществляющему создание электронной подписи, **содержание информации, подписание которой производится**»

Нет контроля целостности подписываемых данных

Основные причины невозврата кредитов, взятых клиентами под влиянием злоумышленников

Недостаточность информации об условиях кредита в смс с кодом для подписания

Ненадлежащее выполнение банком всех возложенных на него обязательств

Юридическая простота оспаривания ПЭП (коды в сообщении) электронных документов

УИД 66RS0005-01-2023-003507-94

№ 88-5692/2024

Мотивированное определение составлено 09 апреля 2024 года

ОПРЕДЕЛЕНИЕ

г. Челябинск 02 апреля 2024 года

Судебная коллегия по гражданским делам Седьмого кассационного суда общей юрисдикции в составе: председательствующего Сафронова М.В.
судей Шведка Н.В., Федотенкова С.Н.
рассмотрела в открытом судебном заседании гражданское дело № 2-3895/2023 по иску Солодовникова Евгения Мергеновича к Акционерному обществу «Газпромбанк» о защите прав потребителя по кассационной жалобе Акционерного общества «Газпромбанк» на апелляционное определение судебной коллегии по гражданским делам Свердловского областного суда от 12 декабря 2023 года.

…представленные ответчиком доказательства направления на мобильное устройство истца кода для введения …сами по себе не свидетельствуют о принятии банком всех необходимых мер по обеспечению безопасности совершаемых операций

ОПРЕДЕЛИЛА:

апелляционное определение судебной коллегии по гражданским делам С
от 12 декабря 2023 года оставить без изменения, кассационную жалобу Акцион
банк» - без удовлетворения.

РЕШЕНИЕ

ИМЕНЕМ РОССИЙСКОЙ ФЕДЕРАЦИИ

08 декабря 2023 года г. Новосибирск

Заельцовский районный суд города Новосиб ир

в составе:
судьи Павлючик И.В.
При секретаре Чумакове Д.М.
рассмотрев в открытом судебном заседании гражданское дело по иску Б е
банк» о признании кредитного договора недействительным, освобождении от и с
кредитному договору, истории, возложении обязанности по внесению изменен ий

…из буквального содержания смс-сообщения, направленного истцу и содержащего коды для осуществления вышеуказанного перевода, не представляется возможным понять, что введением данного кода истец совершает распоряжение на перевод денежных средств определенному лицу на определенный счет…

ОПРЕДЕЛИЛА:

апелляционное определение судебной коллегии по гражданским делам Свердловского областного суда от 12 декабря 2023 года оставить без изменения, кассационную жалобу Акционерного общества «Газпром банк» - без удовлетворения.

Дело No 2-3388/2023

РЕШЕНИЕ

Именем Российской Федерации

Куйбышевский районный суд г. Омска в составе п1 председательствующего судьи Котельниковой О.В., с участием истца ФИО1, представителя истца ФИО7, при секретаре Попове А.А., помощнике судьи Смирновой П.В., рассмотрев 23 августа 2023 года в г. Омске в открытом судебном заседании гражданское дело по иску ФИО1 к Коммерческому банку <<Ренессанс Кредит>> (ООО) о признании кредитных договоров недействительными,

все действия по заключению кредитного договора,… и переводу денежных средств в другой банк совершены практически одномоментно - путем введения четырехзначного цифрового кода, направленного Банком смс-сообщением….

РЕШИЛ:

Исковые требования удовлетворить.
Признать недействительным кредитный договор No от ДД.ММ.ГГГГ, зак
санс Кредит>> (ООО) (ИНН 7744000126) и ФИО1 (ДД.ММ.ГГГГ г.р., паспорт 52
Признать недействительным договор о карте No от ДД.ММ.ГГГГ, заключ
Кредит>> (ООО) и ФИО1.
Признать недействительным договор о карте No от ДД.ММ.ГГГГ, заключ
Кредит>> (ООО) и ФИО1.
Взыскать с КБ <<Ренессанс Кредит>> (ООО) (ИНН 7744000126) госпош
в размере 900 руб.
Решение может быть обжаловано в апелляционном порядке в Омский о
ский районный суд г. Омска в течение месяца со дня принятия решения в окон
Судья подпись О.В. Котельникова

Председательствующий: Чекурда А.Г. Дело No 33-3493/2024

No 2-107/2024

55RS0002-01-2023-004 761-64

АПЕЛЛЯЦИОННОЕ ОПРЕДЕЛЕНИЕ

город Омск 13 июня 2024 г.

Судебная коллегия по гражданским делам Омского областного суда в составе:
председательствующего Лисовского В.Ю.,
судей Григорец Т.К., Лозовой Ж.А.,
при секретаре Ляхове Д.И.,
рассмотрела в судебном заседании дело по апелляционной жалобе представителя истца Колмогорова И.Н. - Большакова Н.Ю. на решение Куйбышевского районного суда города Омска от 1 апреля 2024 года по иску Колмогорова И. Н. к ПАО Банк ВТБ о признании кредитного договора недействительным, взыскании денежных средств.

…для совершения нескольких операций потребителем фактически получено одно SMS уведомление, что свидетельствует о нарушении как требований Закона РФ «О защите прав потребителей», Закона об электронной подписи.

Предоставляя возможность заключения кредитного договора дистанционным способом, предлагая к использованию мобильное приложение, банк обязан гарантировать клиенту, оплачивающему услуги банка, безопасность их выполнения.

ОПРЕДЕЛИЛА:

решение Куйбышевского районного суда города Омска от 1 апреля 2024 года отменить, принять по делу новое решение.
Исковые требования Колмогорова И. Н. к Банку ВТБ (ПАО) о признании кредитного договора недействительным, взыскании денежных средств в удовлетворить.
Признать недействительным кредитный договор от 18 ноября 2022 года No < ... > между Банком ВТБ (ПАО) (ИНН 7702070139) и Колмогоровым И. Н. (паспорт < ... >).
Взыскать с Банка ВТБ (ПАО) (ИНН 7702070139) в пользу Колмогорова И. Н. (паспорт < ... >) денежные средства в размере 182282, 12 руб., штраф в размере 91141,06 руб.
Взыскать с Банка ВТБ (ПАО) (ИНН 7702070139) в доход местного бюджета государственную пошлину в размере 5146 руб.
Апелляционное определение может быть обжаловано в Восьмой кассационный суд общей юрисдикции (г. Кемерово) в течение трёх месяцев со дня его вынесения путём подачи кассационной жалобы через суд первой инстанции - Куйбышевский районный суд города Омска.
Председательствующий
Судьи:
Мотивированное апелляционное определение изготовлено 17.06.2024.

ЦБ уже позаботился (851-П)

STCRYPT

В целях обеспечения целостности электронных сообщений и подтверждения их составления уполномоченным на это лицом кредитные организации должны обеспечивать реализацию мер по использованию:

- усиленной квалифицированной электронной подписи
- усиленной неквалифицированной электронной подписи
- СКЗИ реализующих функцию имитозащиты информации с аутентификацией отправителя сообщения

Все боятся реализовывать

- «Сложно реализовать»
- «Клиентам будет неудобно»
- «Все равно бизнес все сведет к SMS-коду, тогда зачем СКЗИ и ЭП»

Реализация 851-П с помощью УКЭП

STCRYPT

Средства электронной подписи для хранения ключей ЭП :

CSP + аппаратные
(USB-токены, смарт-карты)

Мобильные

В соответствии с пунктом 1 статьи 13 63-ФЗ:

При создании **квалифицированного** сертификата идентификация заявителя проводится:

- «при его личном присутствии»
- «с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата»
- «путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы»

Безопасно, но дорого

Реализация 851-П с помощью УНЭП

с выпуском неквалифицированных сертификатов

В соответствии с пунктом 1 статьи 13 63-ФЗ:

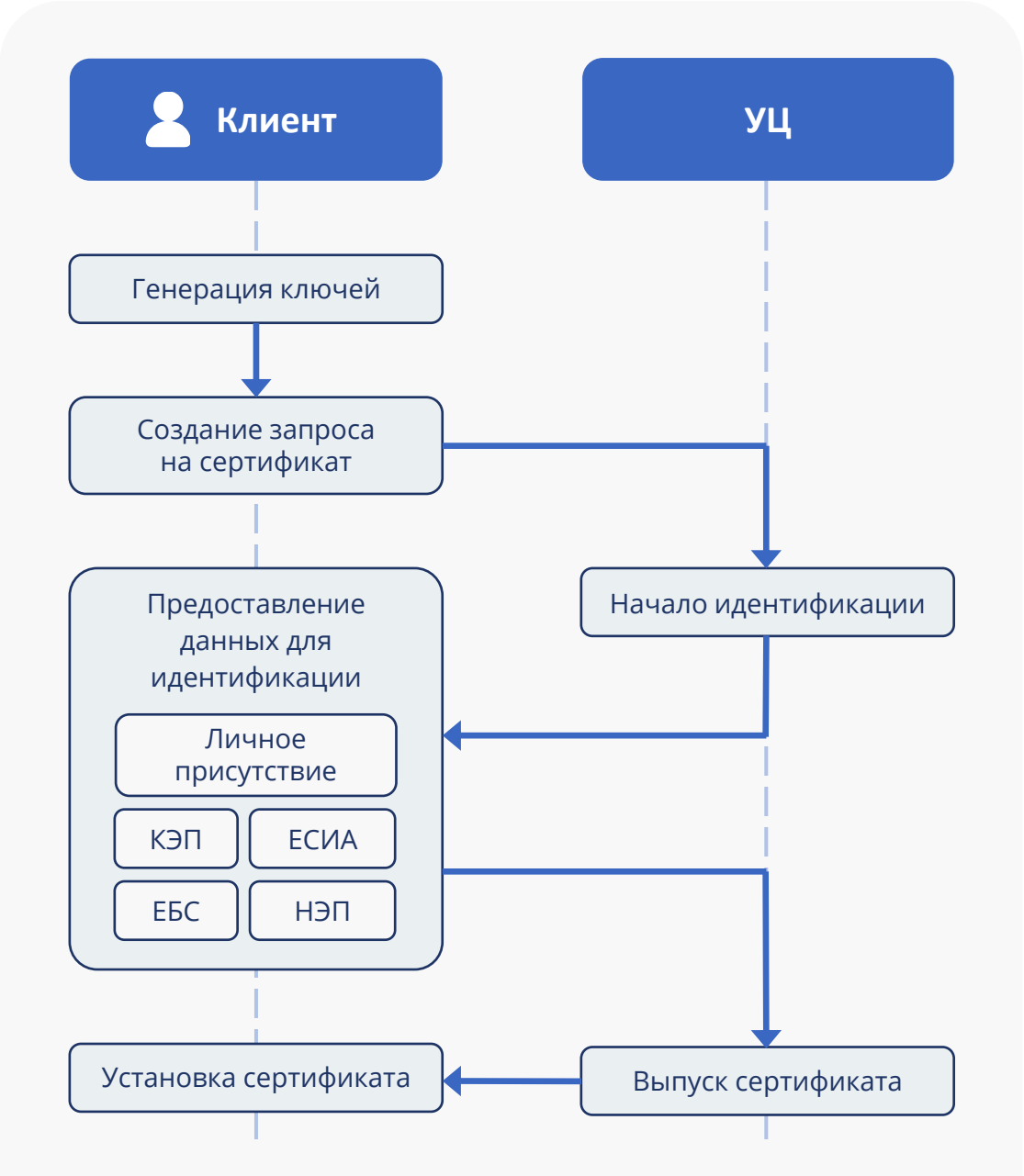
При создании **неквалифицированного** сертификата идентификация проводится:

- аналогично КЭП
- «с использованием простой электронной подписи, ключ которой получен при личной явке в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме» (Госуслуги: логин, пароль, OTP-код)
- «с использованием усиленной неквалифицированной электронной подписи, сертификат ключа проверки которой создан и используется в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг»

Дополнительно в соответствии с пунктом 1.2 статьи 13 63-ФЗ :

УЦ может создавать сертификаты ключей проверки неквалифицированной электронной подписи «при наличии действующего сертификата ключа проверки электронной подписи, который выдан тем же удостоверяющим центром» если «идентификация заявителя была проведена удостоверяющим центром одним из способов, указанных в пункте 1»

Создание ключей ЭП и выпуск неквалифицированного сертификата в мобильном приложении



Реализация 683-П с помощью УНЭП

без выпуска неквалифицированных сертификатов

В соответствии с пунктом 5.5 63-ФЗ:

«При использовании неквалифицированной электронной подписи сертификат ключа проверки электронной подписи может не создаваться, **если соответствие электронной подписи признакам неквалифицированной электронной подписи**, установленным настоящим Федеральным законом, **может быть обеспечено без использования сертификата ключа проверки электронной подписи»**

В соответствии с пунктом 5.3 63-ФЗ:

«Неквалифицированной электронной подписью является электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи
- **позволяет определить лицо, подписавшее электронный документ**
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания
- создается с использованием средств электронной подписи»

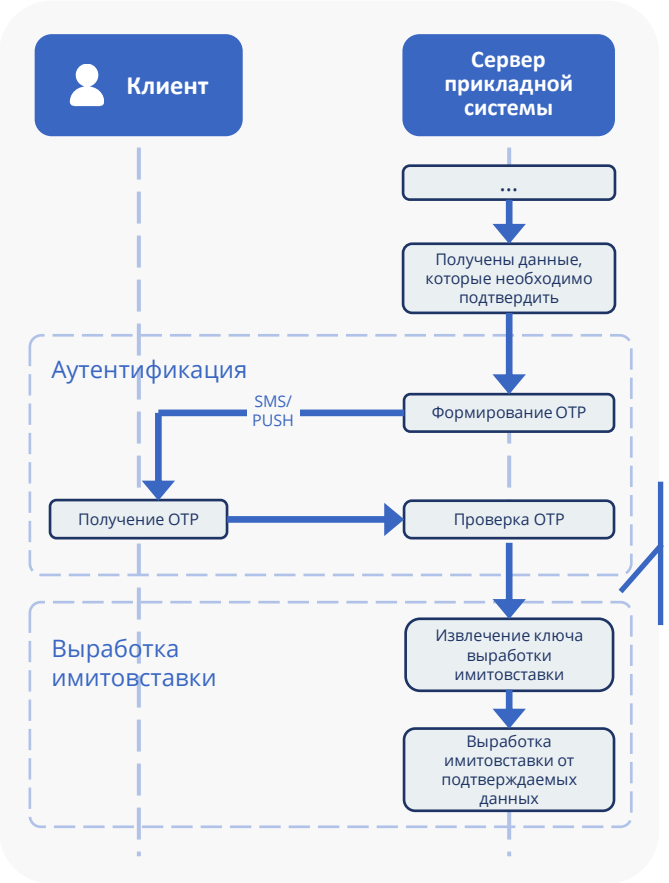
! Способ идентификации пользователя, который создает на своем средстве электронной подписи ключи неквалифицированной электронной подписи **без создания сертификата ключа проверки электронной подписи,** должен быть **СТРОГО** регламентирован соглашением об электронной подписи между банком и клиентом

Реализация 683-П с помощью СКЗИ, реализующих функцию имитозащиты информации с аутентификацией отправителя сообщения

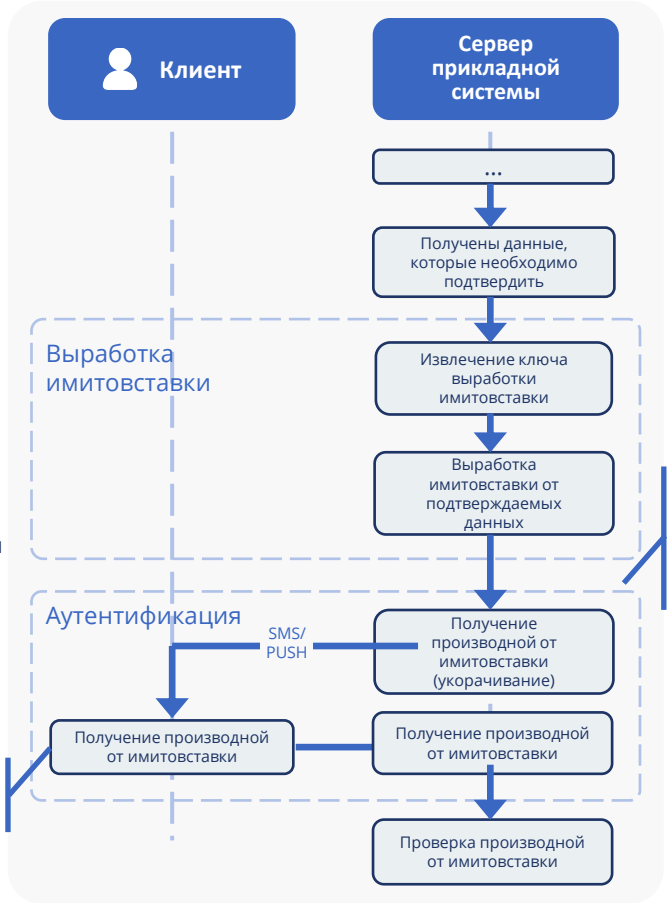
Должно использоваться СКЗИ, обеспечивающее аутентификацию отправителя + имитозащиту. Многие делают имитовставку на сервере.

НЕПРАВИЛЬНО

Имитовставка на Сервере



Функции аутентификации и выработки имитовставки не связанны



Функции аутентификации и выработки имитовставки не связанны

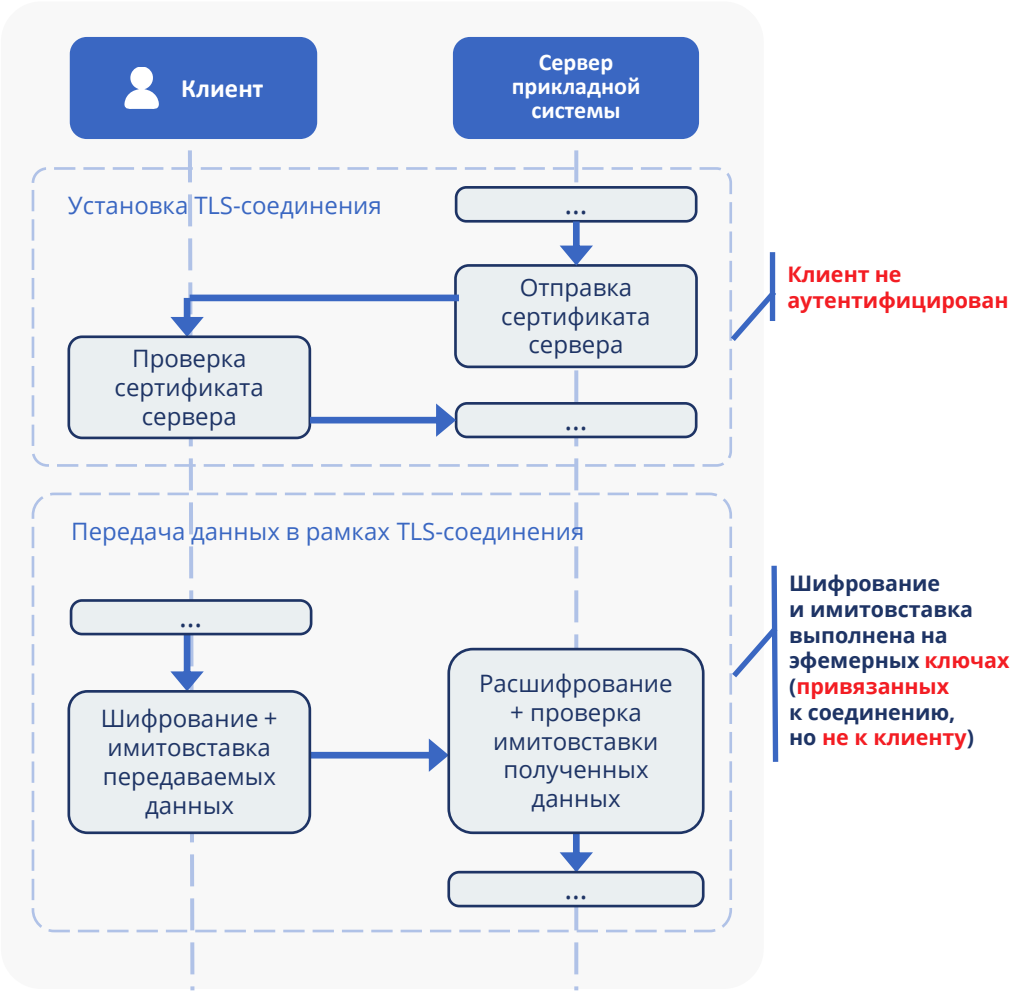
Выглядит как OTP

Реализация 683-П с помощью СКЗИ, реализующих функцию имитозащиты информации с аутентификацией отправителя сообщения

Должно использоваться СКЗИ, обеспечивающее аутентификацию отправителя + имитозащиту. Или односторонний TLS.

НЕПРАВИЛЬНО

Односторонний TLS



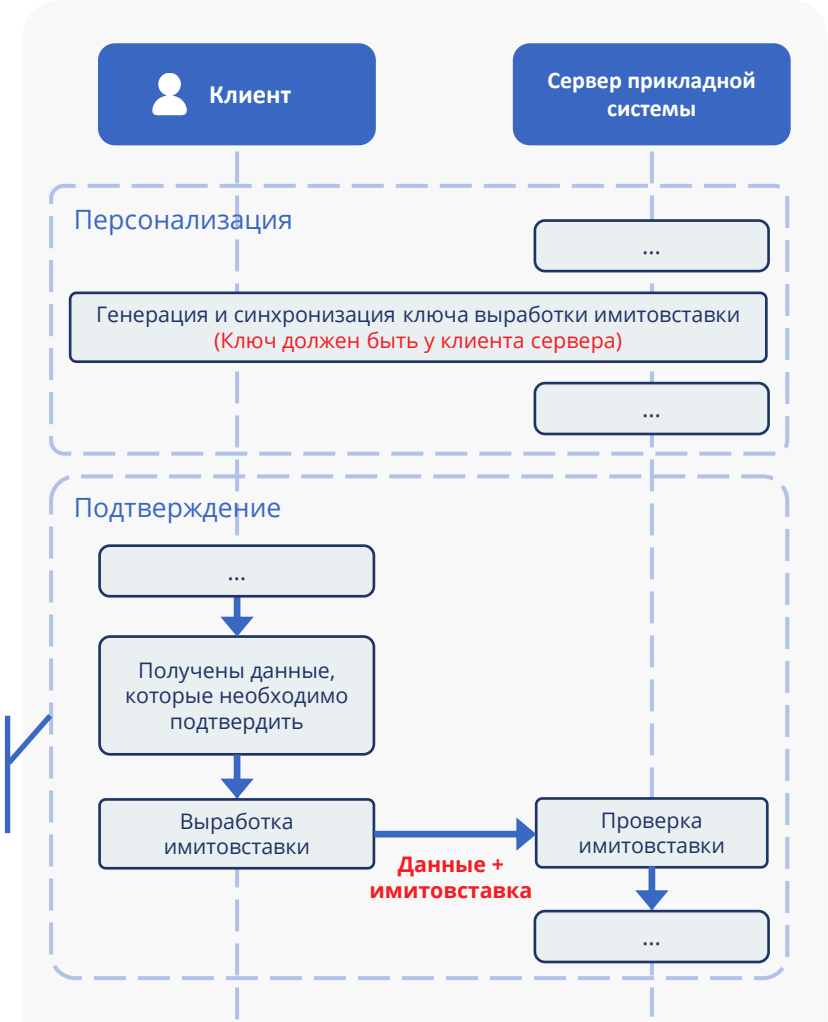
Аутентификация выполняется отдельно. Функции аутентификации и выработки/проверки имитовставки не связаны

Реализация 851-П с помощью СКЗИ, реализующих функцию имитозащиты информации с аутентификацией отправителя сообщения

Должно использоваться СКЗИ, обеспечивающее аутентификацию отправителя + имитозащиту

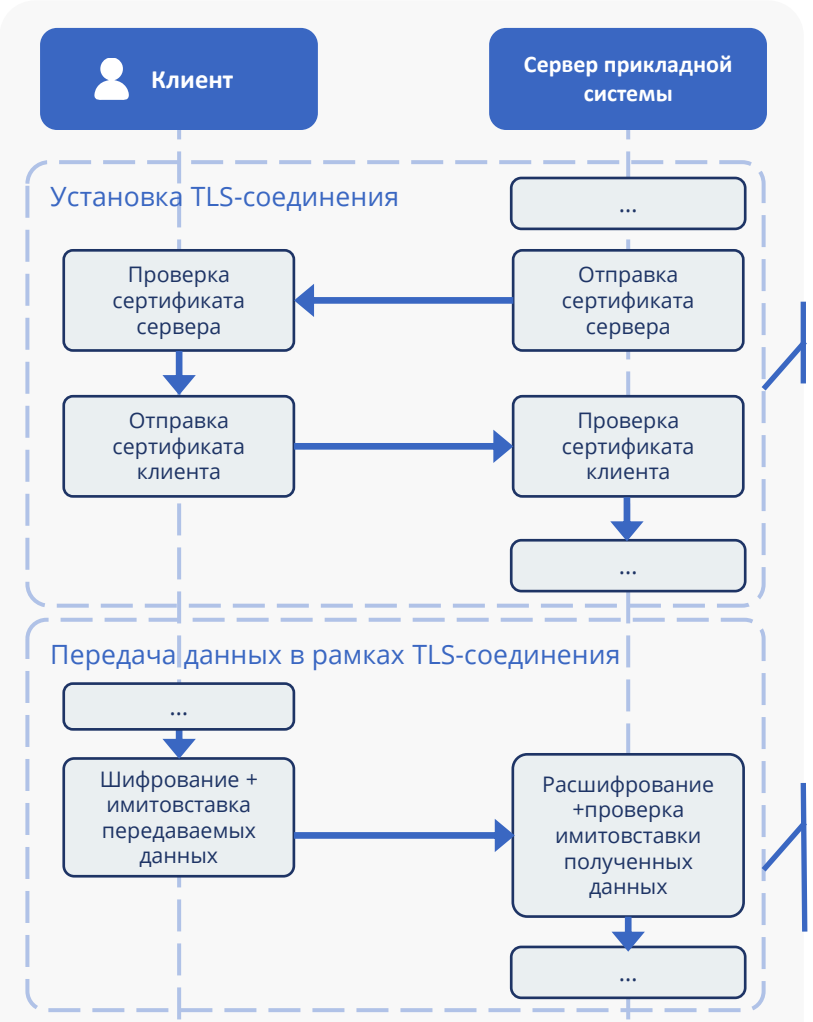
ПРАВИЛЬНО

Имитовставка на Клиенте



Клиент аутентифицирован по ключу выработки имитовставки

Двусторонний TLS



Криптографическая аутентификация

Имитовставка на ключах, связанных с ключами, использованных при аутентификации

Оставшиеся «узкие» места на практике

STCRYPT

На практике при удаленной идентификации:

1. **при создании неквалифицированных сертификатов проверки ключей ЭП**
2. **при генерации ключей неквалифицированной ЭП**
3. **при генерации ключей для выработки имитовставки**

в качестве дополнительного (или единственного) фактора аутентификации всегда **используется OTP-код в SMS**

Удобно, но мошенники их **ПЕРЕХВАТЫВАЮТ** способами, описанными ранее

Нужны вспомогательные меры

Два процесса, для которых необходимо ввести вспомогательные меры

STCRYPT

1 **«Первичная» генерация ключей ЭП и выпуск неквалифицированного сертификата** (если используется)

2 **«Перегенерация» ключей ЭП и перевыпуск неквалифицированного сертификата** (если используется) при смене устройства:

- при наличии существующих ключей ЭП на другом устройстве
- при отсутствии существующих ключей ЭП на другом устройстве (утерян доступ к устройству или мобильное приложение удалено)

Часто:
реализуют только сценарий «первичной» генерации и не предусматривают использование ранее созданных ключей

Результат:
упрощение процедуры «первичной» генерации

Последствия:
увеличение фрода и снижение доверия к СКЗИ как к способу защиты от мошенничества

Вспомогательные меры для «первичной» генерации

STCRYPT

Дополнительно проверять клиента

Минимальный срок использования ДБО и отсутствие жалоб на мошенничество:

- Клиент должен активно использовать мобильное ДБО **не менее 5 дней**
- **Клиент должен совершить хотя бы одну доверенную операцию**
- У клиента не должно быть обращений в банк по поводу фрода, взлома или подозрительных операций за последние **5 дней** (опционально)

В течение этих 5 дней (опционально) необходимо использовать повышенные меры информирования

клиентов о совершении операций, производить дополнительную аутентификацию совершаемых операций:

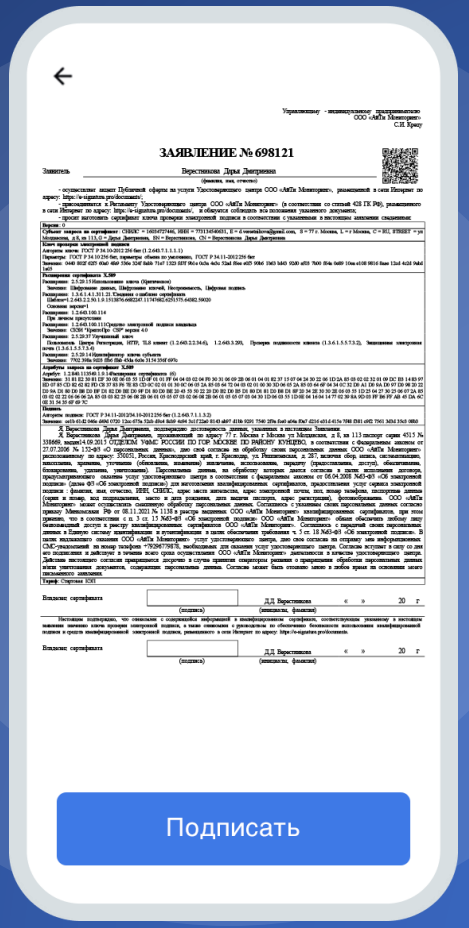
- Информировать о создании ЭП на устройстве
- Запрашивать дополнительные кодовые слова при совершении операций
- Брать клиента на дополнительный контроль системами антифрода

Дополнить юридическую доказательную базу - нивелировать «риск первой операции»

Можно усилить доказательство принадлежности ключей ЭП с помощью уже совершенной доверенной операции:

Если данными ключами ЭП была подписана хоть одна операция, от которой пользователь не отказывается - значит он совершал эту операцию и, значит, ключи ЭП принадлежат ему

Вспомогательные меры при «перегенерации»



Подписывать запрос на генерацию ключей ЭП/выпуск сертификата уже существующими ключами ЭП на другом устройстве

! Важно: проверять геопозицию

- в случае расхождения геопозиции следует блокировать доступ в ДБО и уведомлять клиента согласно требованиям 161-ФЗ
- в иных случаях — осуществлять «первичный» путь

Вспомогательные меры
(при сохранении данных в учетных записях Apple и Google)

STCRYPT

1. На мобильном устройстве доверенного «чистого» пользователя **генерируется «секрет»**
2. Данный «секрет» **регистрируется на банковском сервере** в качестве дополнительной информации
3. Данный «секрет» вместе со служебной информацией мобильного приложения **сохраняется в аккаунте Apple/Google**
4. При генерации ключей ЭП или выпуске неквалифицированного сертификата, получение данного секрета приложением из учетной записи Apple и Google и его совпадение с «секретом», зарегистрированном в Банке, **позволит дать дополнительную информацию о доверии к данному пользователю**

!

Важно!

В рамках работы в российском правовом поле опираться на безопасность учетных записей Apple и Google невозможно, **но хуже не будет**

Выводы

- СКЗИ — это не «страшно» и не «сложно» для пользователя
- Если внедрять СКЗИ «с умом», значительно повысится безопасность и снизятся риски и для клиента, и для Банка
- Реализация «фиктивного» соответствия требованиям регулятора может ухудшить ситуацию с мошенничеством
- Вспомогательные меры защиты обязательны для повышения безопасности и упрощения клиентского пути

Спасибо за внимание!

STCRYPT

stcrypt.ru

+7 (495) 120-99-09

info@safe-tech.ru