



ViPNet PKI Client Android

Руководство пользователя

Версия продукта: 2.1

© АО «ИнфоТеКС», 2025

ФРКЕ.00175-02 34 04

Версия продукта 2.1

Этот документ входит в комплект поставки продукта ViPNet, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения АО «ИнфоТеКС».

ViPNet[®] является зарегистрированным товарным знаком АО «ИнфоТеКС».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

АО «ИнфоТеКС»

127083, Москва, улица Мишина, д. 56, стр. 2, этаж 2, помещение IX, комната 29

Телефон: +7 (495) 737-6192, 8 (800) 250-0260 — бесплатный звонок из России (кроме Москвы)

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение.....	6
О документе.....	6
Соглашения документа.....	6
О приложении	6
Комплект поставки.....	7
Системные требования.....	7
Лицензирование	8
Что нового в версии 2.1.....	9
Обратная связь.....	10
 Установка и запуск приложения.....	11
Установка, обновление с помощью магазина приложений	11
Установка, обновление с помощью файла *.apk.....	11
Первый запуск	11
 Управление сертификатами	13
Какие нужны сертификаты	13
Подключение токена к устройству.....	13
Подготовка личного сертификата и ключа ЭП	14
Получение сертификата.....	15
Установка сертификатов и CRL.....	17
Проверка сертификатов.....	19
Настройка автоматического обновления CRL.....	20
Экспорт сертификата в файл *.cer.....	21
Импорт сертификата и ключа ЭП из файла *.pfx	22
Удаление сертификатов	22
 Использование облачных сервисов ЭП.....	23
Настройка подключения к сервису	23
Подключение к сервису	24
Изменение настроек подключения к сервису	25
Смена пароля учетной записи пользователя	25
Удаление настроек подключения к сервису	26
 Подпись и зашифрование файлов.....	27

Требования к сертификатам для подписи и зашифрования	27
Подписание файла.....	27
Зашифрование файла	29
Работа с файлами, полученными от других пользователей	31
Проверка ЭП.....	31
Расшифрование файла	33
Подключение к сайтам, использующим TLS ГОСТ	35
Порядок настройки	35
Требования к сертификатам для работы по TLS ГОСТ	35
Настройка TLS-соединения	36
Установка корневого сертификата для TLS ГОСТ	37
Устройство с Android 11 или выше	37
Устройство с Android 10 или ниже	38
Настройка прокси-сервера.....	38
Включение TLS ГОСТ	39
Изменение настройки TLS-соединения	40
Подключение к сайту	41
Просмотр информации о TLS-соединениях	42
Служебные функции	44
Проверка целостности	44
Смена пароля хранилища сертификатов	44
Обновление лицензии.....	44
Сброс настроек приложения	45
Удаление приложения	45
Возможные неполадки	46
Заблокирована работа ViPNet PKI Client из-за нарушения целостности.....	46
Нет подключения к интернету	47
Не удастся войти в стороннее приложение	48
NFC-токен не обнаружен на устройстве	48
История версий.....	49
Что нового в версии 2.0.1	49
Что нового в версии 2.0	49
Что нового в версии 1.5	49
Что нового в версии 1.4	49

Что нового в версии 1.3	50
Что нового в версии 1.2	51
Что нового в версии 1.1	52
Термины и сокращения	53

Введение

О документе

Документ описывает настройку приложения ViPNet® PKI Client Android (далее — ViPNet PKI Client) и работу с ним.

Предполагается, что пользователь имеет общее представление об электронной подписи и сертификатах ключа проверки электронной подписи.

Соглашения документа

Обозначение	Описание
Название	Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки
Клавиша+Клавиша	Сочетание клавиш: нажмите первую клавишу и, не отпуская её, нажмите вторую
Меню > Команда	Последовательность элементов или действий
Код	Имя файла, путь, фрагмент кода или команда в командной строке



Примечание. В документе могут присутствовать снимки интерфейса из предыдущих версий продукта. Поэтому некоторые элементы интерфейса, которые не влияют на понимание текста, могут выглядеть не так, как в продукте.

О приложении

С помощью ViPNet PKI Client вы можете:

- Создать [запрос на сертификат](#) для передачи в удостоверяющий центр (далее — УЦ).
- Подписать файлы и проверить [ЭП](#) файлов.
- Зашифровать и расшифровать файлы.
- Подключиться к сайтам по TLS ГОСТ, в том числе с [аутентификацией пользователя](#).
Поддерживаемые версии [протокола TLS](#): 1.2, 1.3.
- Работать в облачном сервисе ЭП на базе [ViPNet PKI Service](#) версии 2.0 или выше: подписывать файлы, проверять ЭП файлов, расшифровывать файлы.

Вы можете выполнять операции с файлами из меню ViPNet PKI Client, а также из других приложений с помощью меню «Поделиться».

ViPNet PKI Client имеет интерфейс API, который разработчики могут использовать для встраивания TLS ГОСТ ViPNet PKI Client в свои приложения для Android.

ViPNet PKI Client использует российские криптографические алгоритмы:

- Алгоритм проверки ЭП: ГОСТ Р 34.10-2001 с вычислением хэш-функции по ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2012 с вычислением хэш-функции по ГОСТ Р 34.11-2012.
- Алгоритм создания ЭП: ГОСТ Р 34.10-2012 с вычислением хэш-функции по ГОСТ Р 34.11-2012.
- Алгоритм шифрования для TLS-соединений: ГОСТ 28147-89 и ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) «Магма» и «Кузнечик».
- Алгоритм шифрования для файлов: ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) «Магма» и «Кузнечик».

Комплект поставки

- Установочный файл ViPNet PKI Client for Android-<версия>.apk.
- AIDL-файлы `ITlsProxyService.aidl`, `ITlsProxyServiceListener.aidl` для работы с TLS ГОСТ ViPNet PKI Client.
- Серийный номер — получаете при приобретении [лицензии](#).
- Руководство пользователя в формате PDF.
- Руководство разработчика в формате PDF.

Системные требования

- ViPNet PKI Client можно установить на устройство с Android 9.0 или выше, которое работает на базе процессоров с архитектурой ARM, ARM64, x86 и x86_64, или на устройство с HarmonyOS.



Примечание. Поддержка HarmonyOS в текущей версии ViPNet PKI Client является экспериментальной.

-
- Для установки и обновления ViPNet PKI Client с помощью магазина приложений используйте RuStore, AppGallery и NashStore.
 - Для хранения сертификатов и ключей ЭП вы можете использовать токены — [Рутокен ЭЦП 3.0 NFC 3100](#) и [Смарт-карту Рутокен ЭЦП 3.0 NFC 3100](#).
 - Для подключения к сайтам по TLS ГОСТ используйте браузеры Atom, Chrome, Edge, Firefox, Яндекс.Браузер и Яндекс Лайт последних версий. Подключение с использованием других браузеров не гарантируется.

Лицензирование

Для использования ViPNet PKI Client необходимо активировать лицензию с помощью серийного номера или файла лицензии. Подробнее см. [Первый запуск](#).

Лицензирование с помощью серийного номера

Приобретите лицензию у [представителя ИнфоТеКС](#) и активируйте приложение с помощью полученного серийного номера.

Лицензирование с помощью файла

Получите файл лицензии в [ИнфоТеКС](#) и загрузите его в ViPNet PKI Client.

Лицензия содержит:

- Разрешенные для использования функции (все или некоторые из перечисленных):
 - TLS без аутентификации клиента — подключение к сайтам, использующим TLS ГОСТ с аутентификацией сервера;
 - TLS с аутентификацией клиента — подключение к сайтам, использующим TLS ГОСТ с взаимной аутентификацией сервера и клиента;
 - работа с облачными сервисами ЭП — хранение сертификатов и выполнение криптографических операций в облачном сервисе ViPNet PKI Service.
- Максимальную версию ViPNet PKI Client.
- Срок действия лицензии.

Если приложение активировано, всегда разрешены для использования функции:

- защита файлов: подписание, зашифрование, проверка ЭП, расшифрование;
- управление сертификатами.

Что нового в версии 2.1

- **Подписание файла несколькими равнозначными подписями**

В предыдущей версии ViPNet PKI Client вы могли подписать файл, который уже подписан другим лицом. При этом файл подписывался вместе с существующей подписью. Теперь вы можете подписать файл, не затрагивая подписи других лиц. Если файл содержит несколько подписей, каждая из них проверяется отдельно.

- **Поддержка XML-подписи**

Теперь вы можете создавать и проверять XML-подписи формата XAdES. При использовании облачного сервиса ViPNet PKI Service версии 2.3.0 или выше вы можете создавать ЭП с использованием облачного сертификата и проверять ЭП в облаке.

- **Новый способ лицензирования**

Добавлена возможность активации с помощью файла. Подробнее см. [Лицензирование](#).

- **Поддержка Android 14**

Изменения в предыдущих версиях см. в приложении [История версий](#).

Обратная связь

Контактная информация

- Единый многоканальный телефон:
+7 (495) 737-6192,
8 (800) 250-0-260 — бесплатный звонок из России (кроме Москвы).
- Служба поддержки: hotline@infotecs.ru.
Форма для обращения в службу поддержки через сайт.
Телеграм-канал поддержки: t.me/vhd21
Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.
- Отдел продаж: soft@infotecs.ru.

Дополнительная информация на сайте ИнфоТеКС

- [О продуктах ViPNet.](#)
- [О решениях ViPNet.](#)
- [Часто задаваемые вопросы.](#)
- [Форум пользователей продуктов ViPNet.](#)

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов ИнфоТеКС регулируется [политикой ответственного разглашения](#).

Установка и запуск приложения

Установка, обновление с помощью магазина приложений

- 1 Откройте [магазин приложений](#).
- 2 Найдите ViPNet PKI Client.
- 3 На экране с информацией о приложении нажмите **Установить** или **Обновить**.

Установка, обновление с помощью файла *.apk

- 1 Передайте установочный файл *.apk на устройство.
- 2 По умолчанию в Android запрещена установка приложений с помощью файлов *.apk. На время установки ViPNet PKI Client разрешите такую установку.
- 3 Запустите установочный файл и следуйте указаниям.
- 4 Для безопасности запретите установку приложений с помощью файлов *.apk.

Первый запуск

- 1 Убедитесь, что на устройстве есть доступ в интернет.
- 2 Примите условия лицензионного соглашения.
- 3 Следуйте указаниям на экране для создания последовательности случайных чисел.
- 4 Выберите способ активации лицензии.
- 5 Если у вас есть серийный номер:
 - 5.1 Введите номер телефона и серийный номер.
 - 5.2 Нажмите **Активировать лицензию**, вам будет отправлено СМС с кодом активации.
 - 5.3 Введите полученный код.
- 6 Если у вас есть файл лицензии:

- 6.1 Выберите файл лицензии в формате *.itcslic.
 - 6.2 Посмотрите состав лицензии и нажмите **Активировать лицензию**.
 - 6.3 Введите номер телефона.
 - 6.4 Нажмите **Продолжить**, вам будет отправлено СМС с кодом активации.
 - 6.5 Введите полученный код.
- 7 Задайте и подтвердите пароль хранилища сертификатов и ключей ЭП.



Внимание! Запомните пароль хранилища сертификатов. [Восстановить его нельзя](#).

Рисунок 1. Задание пароля хранилища сертификатов

- 8 Нажмите **Задать пароль**.
- 9 Следуйте указаниям на экране.

Управление сертификатами

Какие нужны сертификаты

- Личный сертификат — для подписи, расшифровки файлов, подключения к сайтам, использующим TLS ГОСТ. Получите его в УЦ [по запросу](#) и [установите в хранилище сертификатов](#).
- Сертификаты УЦ — для проверки личного сертификата. Получите их в УЦ и [установите в хранилище сертификатов](#).
- Сертификаты получателей — для зашифрования файлов. Запросите их у получателей файлов и [установите в хранилище сертификатов](#).

Для подтверждения действительности сертификатов могут использоваться:

- [Списки аннулированных сертификатов](#) (далее — CRL). Вы можете:
 - Настроить автоматическое получение CRL путем опроса [точек распространения CRL](#). URL для опроса содержатся в сертификатах, изданных УЦ, в поле **Точки распространения списков отзыва (CRL)**.
 - Получить CRL в УЦ и загрузить вручную.
- [Сервис онлайн-проверки статусов сертификатов по протоколу OCSP](#). В этом случае CRL не используются. Информация о поддержке сервиса содержится в сертификатах, изданных УЦ, в поле **Доступ к информации о центрах сертификации**.

Подключение токена к устройству

Если ваши сертификаты хранятся на токене, или вы хотите сохранить сертификаты и ключи на токен, подключите его к устройству:

- 1 В разделе **Настройки** нажмите  **Токены**.
- 2 Выберите магазин приложений и установите приложение «Панель управления Рутокен».



Внимание! Если приложение «Панель управления Рутокен» уже установлено, убедитесь, что его версия 1.10 или выше. Иначе вы не сможете подключить токен к устройству.

- 3 Вернитесь в ViPNet PKI Client и в разделе **Настройки** включите  **Токены**.
- 4 Подключите токен к устройству.

В разделе **Сертификаты** появятся сертификаты, хранимые на токене. Они будут отмечены значком .

Подготовка личного сертификата и ключа ЭП

Если нет сертификата и ключа ЭП

- 1 [Создайте запрос на сертификат.](#)
- 2 [Передайте запрос в УЦ.](#)
- 3 [Получите в УЦ:](#)
 - [личный сертификат;](#)
 - [корневой сертификат УЦ](#) и CRL;
 - [сертификаты и CRL вышестоящих УЦ](#) — если сертификат УЦ подписан вышестоящим УЦ.
- 4 [Установите полученные сертификаты и CRL.](#)

Если есть сертификат и ключ ЭП в файле *.pfx

- 1 [Импортируйте сертификат и ключ ЭП.](#)
- 2 [Установите сертификаты:](#)
 - [корневой сертификат УЦ](#) и CRL;
 - [сертификаты и CRL вышестоящих УЦ](#) — если сертификат УЦ подписан вышестоящим УЦ.

Если есть сертификат на токене

- 1 [Подключите токен к устройству.](#)
- 2 [Установите сертификаты:](#)
 - [корневой сертификат УЦ](#) и CRL;
 - [сертификаты и CRL вышестоящих УЦ](#) — если сертификат УЦ подписан вышестоящим УЦ.

Если вы хотите хранить сертификат в облачном сервисе ЭП

- 1 [Настройте подключение к облачному сервису ЭП.](#) В разделе **Сертификаты** появятся сертификаты, хранимые в облачном сервисе.
- 2 Если у вас нет сертификата в облачном сервисе ЭП или вам нужно его обновить:
 - 2.1 [Создайте запрос на сертификат с сохранением ключа ЭП в облачном сервисе ЭП.](#)
 - 2.2 [Получите сертификат в УЦ.](#)
 - 2.3 [Установите сертификат в облачный сервис ЭП.](#)

Получение сертификата

При создании запроса на сертификат создается [контейнер ключей](#). Этими ключами вы будете подписывать и расшифровывать файлы.

Перед созданием запроса определитесь с местом хранения контейнера ключей и при необходимости выполните предварительные настройки:

- Внутреннее хранилище — предварительные настройки не требуются.
- Облачный сервис ЭП — [подключитесь к облачному сервису ЭП](#).
- Токен — [подключите токен к устройству](#).

Чтобы получить сертификат:

- 1 В разделе **Сертификаты** справа вверху нажмите **+** > **Запрос на новый сертификат**.
- 2 Выберите шаблон запроса на сертификат.
- 3 На экране **Запрос на новый сертификат**:
 - 3.1 Выберите место для сохранения ключа ЭП. Если вы не подключились к облачному сервису ЭП или не подключили токен, ключ ЭП будет сохранен во внутреннем хранилище.

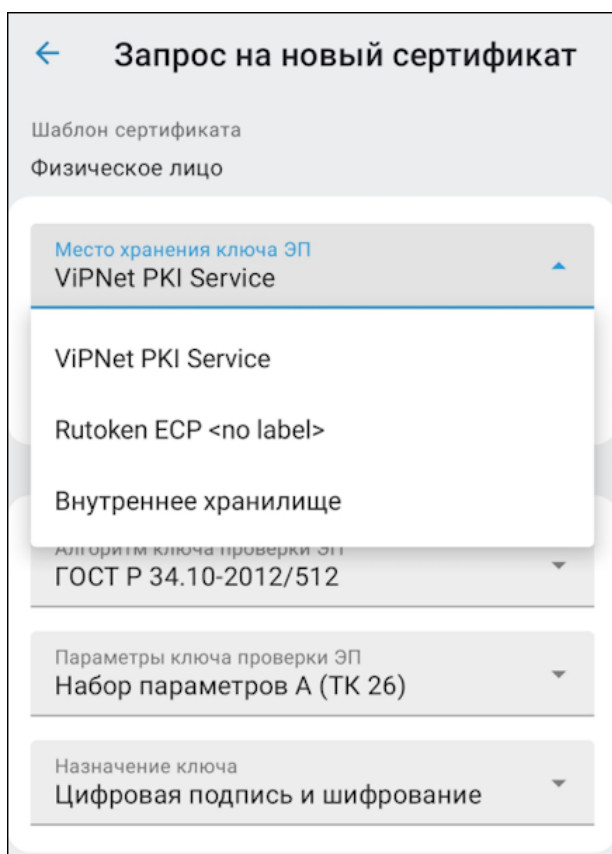


Рисунок 2. Выбор места хранения ключа ЭП

- 3.2 В поле **Идентификация заявителя** выберите способ установления личности при получении сертификата.

- 3.3 Выберите **Алгоритм ключа проверки ЭП** и **Параметры ключа проверки ЭП** или оставьте значения по умолчанию.
- 3.4 В поле **Назначение ключа** выберите операции, которые можно будет выполнять с использованием сертификата.
- 3.5 Заполните личные данные.

Запрос на новый сертификат

Шаблоны сертификата

Физическое лицо

Место хранения ключа ЭП
Внутреннее хранилище

Идентификация заявителя
Личное присутствие

Характеристики сертификата

Алгоритм ключа проверки ЭП
ГОСТ Р 34.10-2012/512

Параметры ключа проверки ЭП
Набор параметров А (ТК 26)

Назначение ключа
Цифровая подпись и шифрование

Владелец сертификата

Фамилия *
Иванов

Имя и отчество *
Иван Иванович

Общее имя *
Иванов Иван Иванович

Страна *
RU

СНИЛС *
12345678901

ИНН физического лица *
123456789012

Регион
Регион

Населенный пункт
Населенный пункт

Улица, дом
Улица, дом

Электронная почта
ivan@ivanov.ru

Создать запрос

Рисунок 3. Создание запроса на сертификат

- 3.6 Нажмите **Создать запрос**.
- 4 Выполните одно из действий:
- Если выбрали **Внутреннее хранилище** — введите пароль хранилища.
 - Если выбрали **<Имя облачного сервиса ЭП>** — приложение проверит связь с сервисом. Может потребоваться повторное подключение (например, если время сессии истекло).
 - Если выбрали **<Имя токена>** — [подключите токен к устройству](#) и введите ПИН.



Примечание. Если облачного сервиса нет в списке, [подключитесь к нему](#).

- 5 Если потребуется, разрешите доступ ViPNet PKI Client к файлам на устройстве. Для этого нажмите **Разрешить** и выберите файловый менеджер.
- 6 Сохраните или отправьте файл запроса.
- 7 Передайте запрос в УЦ.
- 8 Получите личный сертификат и корневой сертификат УЦ, а также при наличии сертификаты всех УЦ из цепочки и соответствующие CRL.
- 9 [Установите полученные сертификаты](#).

Установка сертификатов и CRL



Примечание. Устанавливать CRL вручную не нужно, если в УЦ используются точки распространения CRL или сервисы онлайн-проверки статусов сертификатов по протоколу OCSP, и [они доступны на устройстве](#).

- 1 Перенесите на устройство сертификаты и, если необходимо, CRL.
- 2 В разделе **Сертификаты** справа вверху нажмите **+** и в списке нажмите **Установить сертификат** или **Установить CRL**.
- 3 Выберите сертификат или CRL.
- 4 Ознакомьтесь с информацией о сертификате или CRL и нажмите **Импортировать**. CRL установится во внутреннее хранилище.
- 5 Для сертификата выберите место установки:
 - **Внутреннее хранилище** — сертификат установится во внутреннее хранилище.
 - **<Имя облачного сервиса ЭП>** — приложение проверит связь с сервисом. Может потребоваться повторное подключение (например, если время сессии истекло).
 - **<Имя токена>** — [подключите токен к устройству](#).



Примечание. Если вы [не подключились к облачному сервису ЭП](#) и [не подключили токен](#), сертификат будет установлен во внутреннее хранилище.

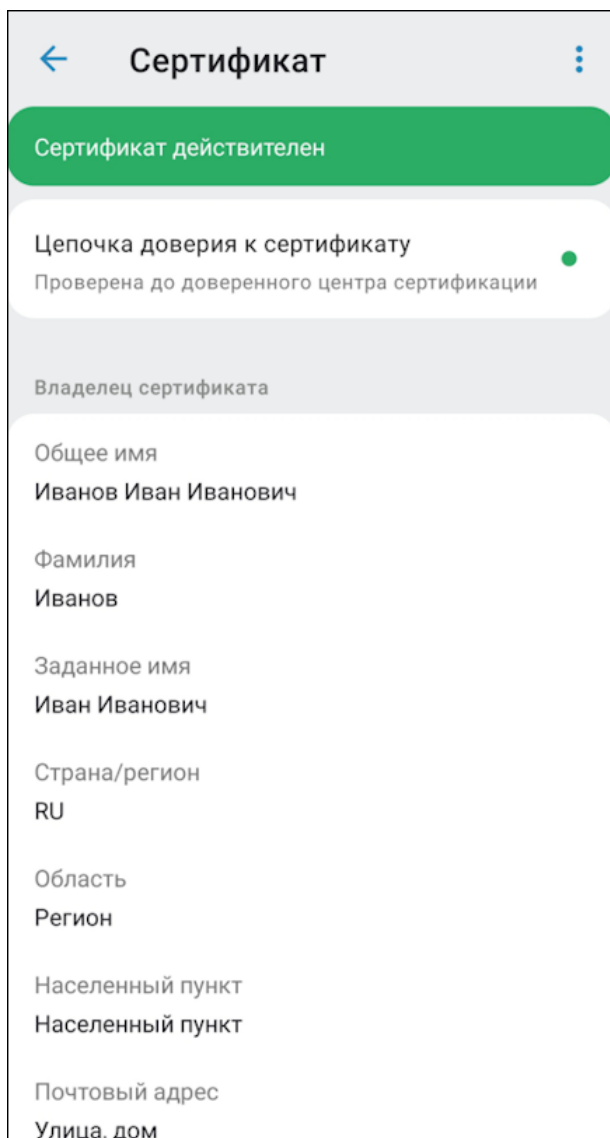


Рисунок 4. Просмотр информации об установленном сертификате

6 Повторите шаги 2–5 для следующего сертификата или CRL.



Примечание. Если после установки сертификата в строке с именем владельца появится значок , см. [Проверка сертификатов](#).

Проверка сертификатов

Недействительные сертификаты нельзя использовать для подписи и шифрования. При установке сертификата в ViPNet PKI Client автоматически проверяется, что сертификат **действителен**. Результат проверки отмечается значком напротив каждого сертификата:

-  — сертификат действителен.
-  — до окончания срока действия сертификата осталось менее 60 дней.
-  — сертификат недействителен.

Если сертификат недействителен, просмотрите и устраните причину:

- **Не найден сертификат издателя**
Получите в УЦ сертификат издателя и [установите его в хранилище](#).
- **Не найден CRL**
Получите в УЦ актуальный CRL и [установите его в хранилище](#).
- **Срок действия сертификата еще не наступил**
Дождитесь начала срока действия сертификата.
- **Срок действия сертификата истек**
[Получите новый сертификат](#) и [установите его в хранилище](#).
- **Срок действия CRL еще не наступил**
Дождитесь начала срока действия CRL.
- **Срок действия CRL истек**
Получите в УЦ актуальный CRL и [установите его в хранилище](#).
- **Сертификат аннулирован**
[Получите новый сертификат](#) и [установите его в хранилище](#).
- **В цепочке присутствует самоподписанный сертификат**
Получите корневой сертификат УЦ и [установите его в хранилище](#).
- **Ошибка ЭП сертификата**
Сертификат поврежден, получите новый сертификат.

Настройка автоматического обновления CRL



Примечание. Если в УЦ есть точки распространения CRL, и они доступны по сети, после установки сертификата УЦ CRL будут обновляться автоматически.

Если на вашем устройстве нет доступа к точкам распространения CRL, указанным в сертификате, и в вашей организации есть локальная точка распространения CRL, доступная по протоколу HTTP, настройте автоматическое обновление CRL из этой локальной точки:

- 1 У администратора вашей сети узнайте URL точки.
- 2 В разделе **Сертификаты** выберите сертификат УЦ и справа сверху нажмите  **CRL**.
- 3 В группе **Точки распространения CRL** нажмите **Добавить точку распространения**.
- 4 Введите URL точки и нажмите **Сохранить**.

Рисунок 5. Настройка автоматического обновления CRL



Примечание. Чтобы изменить или удалить точку, выберите ее и в меню нажмите 

Изменить или



Удалить.

Экспорт сертификата в файл *.cer

Чтобы экспортировать сертификат из ViPNet PKI Client (например, для передачи пользователю, от которого вы будете получать зашифрованные файлы):

- 1 В разделе **Сертификаты** выберите сертификат.
- 2 Справа сверху нажмите  > **Сохранить сертификат**.
- 3 Сохраните файл сертификата.

Импорт сертификата и ключа ЭП из файла *.pfx

- 1 Перенесите на устройство файл *.pfx, полученный в результате экспорта.
- 2 В разделе **Сертификаты** справа вверху нажмите  > **Установить сертификат**.
- 3 Выберите файл *.pfx.
- 4 Введите пароль файла, затем пароль хранилища.



Примечание. Если после установки сертификата в строке с именем владельца появится значок , см. [Проверка сертификатов](#).

Удаление сертификатов

Сертификаты с истекшим сроком действия и [аннулированные сертификаты](#) не удаляются автоматически. Но вы можете удалить их вручную:

- 1 В разделе **Сертификаты** выберите сертификат.
- 2 Справа вверху нажмите  > **Удалить**.
- 3 Подтвердите действие.

Использование облачных сервисов ЭП

Настройка подключения к сервису

Если в вашей организации используется ViPNet PKI Service, настройте подключение к нему. Это позволит создавать запросы на сертификаты, сохранять личные сертификаты и ключи ЭП в защищенном хранилище ViPNet PKI Service и использовать их для [подписи](#) и [расшифрования](#) файлов на любом устройстве с ViPNet PKI Client.

Чтобы настроить подключение к облачному сервису ЭП:

- 1 У оператора сервера подписи получите:
 - Адрес ViPNet PKI Service. Поддерживаемый протокол — HTTPS.
 - Имя и пароль учетной записи пользователя.
 - Корневой сертификат УЦ, в котором издан сертификат ViPNet PKI Service, а также все сертификаты цепочки и соответствующие CRL.
- 2 [Установите полученные сертификаты и CRL.](#)
- 3 В разделе **Настройки** нажмите  **Облачные сервисы.**
- 4 Включите  **Использовать облачные сервисы** и задайте:
 - Название облачного сервиса.
 - Адрес ViPNet PKI Service и порт 9441 в формате `https://<IP-адрес>:9441`.

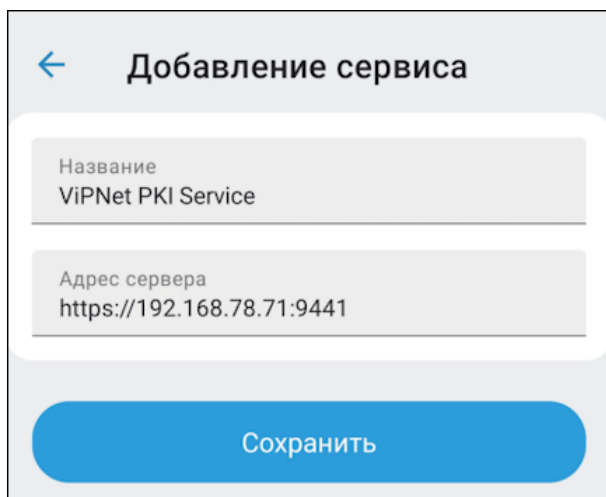


Рисунок 6. Настройка подключения к ViPNet PKI Service

- 5 Нажмите **Сохранить**.
- 6 Подключитесь к облачному сервису ЭП.

Подключение к сервису

- 1 В разделе **Настройки** нажмите  **Облачные сервисы**.
- 2 В списке выберите облачный сервис ЭП и нажмите **Подключить**.
- 3 Введите имя и пароль учетной записи пользователя.

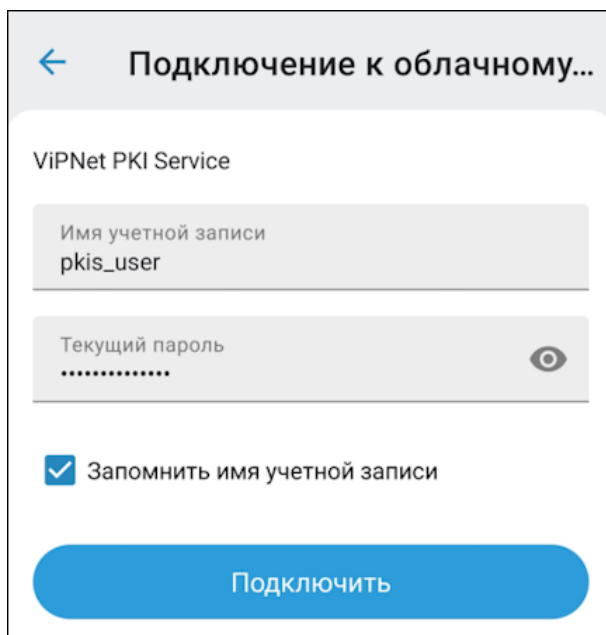


Рисунок 7. Подключение к облачному сервису ЭП

- 4 Нажмите **Подключить**.
- 5 Если вы подключаетесь впервые:

5.1 Введите разовый пароль, полученный у оператора сервера подписи, затем задайте и подтвердите постоянный.

5.2 Нажмите **Сменить пароль**.



Примечание. Если вы забыли постоянный пароль, обратитесь к оператору сервера подписи и получите новый разовый пароль.

В разделе **Сертификаты** появятся сертификаты, хранимые в облачном сервисе. Они будут отмечены значком .

Продолжительность сессии — 1 час. После этого потребуется повторное подключение.

Изменение настроек подключения к сервису

- 1 В разделе **Настройки** нажмите  **Облачные сервисы**.
- 2 Нажмите на облачный сервис ЭП.
- 3 Нажмите  **Изменить**.

Смена пароля учетной записи пользователя

Срок действия постоянного пароля учетной записи — 6 месяцев. По истечении этого срока при подключении к облачному сервису ЭП потребуется сменить пароль.

Чтобы сменить пароль до истечения этого срока:

- 1 В разделе **Настройки** нажмите  **Облачные сервисы**.
- 2 Нажмите на облачный сервис ЭП.
- 3 Нажмите  **Сменить пароль**.
- 4 Введите текущий пароль, затем задайте и подтвердите новый.
- 5 Нажмите **Сменить пароль**.

Удаление настроек подключения к сервису

- 1 В разделе **Настройки** нажмите  **Облачные сервисы**.
- 2 Нажмите на облачный сервис ЭП.
- 3 Нажмите  **Удалить**.

Подпись и зашифрование файлов

Требования к сертификатам для подписи и зашифрования

- Сертификат действителен.
- Личный сертификат, который используется для подписи, содержит значение **Цифровая подпись** в расширении **Использование ключа**.
- Сертификат получателя, который используется для зашифрования, содержит значение **Согласование ключей** в расширении **Использование ключа**.



Внимание! Если ваш сертификат или сертификат получателя не соответствует указанным требованиям, вы не сможете выбрать его для подписи или зашифрования.

Подписание файла

- 1 В разделе **Файлы** нажмите **Подписание файла**.
- 2 Выберите файл, который вы хотите подписать.
- 3 Выберите сертификат для подписи.



Примечание. Если сертификат находится в облачном сервисе ЭП, [подключитесь к нему](#). Если сертификат находится на токене, [подключите его к устройству](#).

- 4 Выберите **Тип подписи**:
 - **CAdES-подпись (прикрепленная)** — документ и подпись сохраняются в одном файле (выбрано по умолчанию);
 - **CAdES-подпись (открепленная)** — подпись сохраняется отдельно от подписываемого файла;
 - **XAdES-подпись (enveloped)** — XML-подпись, добавляется внутрь документа (для файлов формата XML).

Примечание.



- Максимальный размер файла для подписания прикрепленной или открепленной ЭП — 300 Мбайт, для подписания XAdES-подписью — 10 Мбайт.
 - Если сертификат хранится в облачном сервисе, то подписать файл XML-подписью вы можете только при использовании ViPNet PKI Service версии 2.3.0 или выше.
-

- 5 По умолчанию создаётся подпись, которая подтверждает предыдущие. Если необходимо подписать файл наравне с другими подписями, измените **Способ подписания**.

Подписать файл наравне с другими подписями можно только при использовании CAdES-подписи.

- 6 Чтобы добавить к ЭП подтверждение точного времени подписания файла:

6.1 Нажмите **Штамп времени** и включите  **Прикрепить штамп времени к подписи**.

6.2 Если сервера нет в списке:

6.2.1 Нажмите **Добавить TSP-сервер**.

6.2.2 Введите адрес [сервера штампов времени](#).

6.2.3 Нажмите **Добавить**.

6.3 Выберите сервер в разделе **TSP-серверы**.

6.4 Нажмите **Использовать**.

Рисунок 8. Подписание файла

- 7 Нажмите **Подписать** и введите пароль хранилища или ПИН токена.
- 8 В окне сообщения об успешном выполнении операции нажмите **Сохранить файл** или **Отправить файл**.



Примечание. По умолчанию к расширению файлов с прикрепленной ЭП добавляется *.sig, с открепленной — *.detached.sig. Не изменяйте эти расширения.

Зашифрование файла

- 1 В разделе **Файлы** нажмите **Зашифрование файла**.
- 2 Выберите файл, который хотите зашифровать.



Примечание. Максимальный размер файла для зашифрования — 300 Мбайт.

- 3 Выберите один или несколько сертификатов получателей.
- 4 Выберите алгоритм шифрования или оставьте значение по умолчанию.

← **Зашифрование файла**

Шифруемый файл

Текстовый документ.txt
161 байт

Выбрать другой файл

Сертификаты получателей

Петров Петр Петрович
CRYPTO-CA

Сергеев Сергей Сергеевич
Администратор сети 12101

Выбрать других получателей

Параметры шифрования

Алгоритм шифрования
ГОСТ 34.12-2018 Кузнечик

Зашифровать

Рисунок 9. Зашифрование файла

- 5 Нажмите **Зашифровать**.
- 6 В окне сообщения об успешном выполнении операции нажмите **Сохранить файл** или **Отправить файл**.



Примечание. К зашифрованным файлам добавляется расширение *.enc. Не изменяйте это расширение.

Работа с файлами, полученными от других пользователей

Если вы получили файл с расширением:

- *.sig, *.xml — [проверьте ЭП](#).
- *.enc — [расшифруйте](#).
- *.sig.enc, *.xml.enc — [расшифруйте](#), а затем [проверьте ЭП](#).

Проверка ЭП

- Если вы получили файл с расширением *.sig, использовалась [прикрепленная ЭП](#).
- Если вы получили документ и файл подписи с расширением *.sig или *.detached.sig, использовалась [открепленная ЭП](#).
- Если вы получили файл *.xml, использовалась XML-подпись.

Примечание.



- Максимальный размер файла для проверки прикрепленной и открепленной ЭП — 500 Мбайт.
- Максимальный размер XML-документа для проверки ЭП — 15 Мбайт.

-
- 1 В разделе **Файлы** нажмите **Проверка подписи**.
 - 2 Выберите файл, подпись которого вы хотите проверить. Если использовалась открепленная ЭП, выберите файл подписи, а затем в появившемся окне **Проверка подписи** выберите исходный файл.

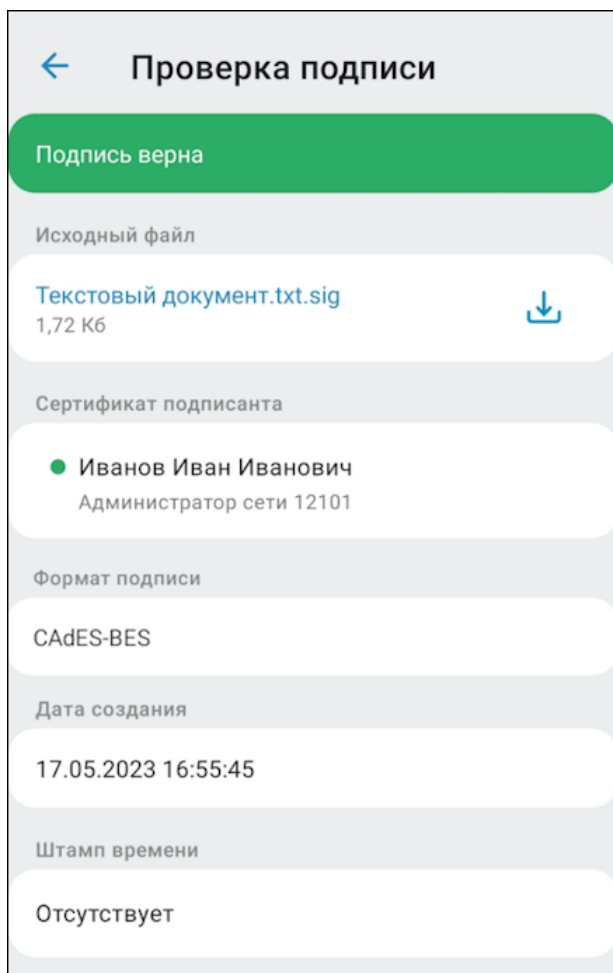


Рисунок 10. Результаты проверки ЭП

- 3 Вы можете проверить подпись в облачном сервисе ЭП. Для этого:
 - 3.1 Подключитесь к облачному сервису ЭП.
 - 3.2 Повторите шаги 1–2 для файла, подпись которого хотите проверить.
 - 3.3 Нажмите  Проверить в облачном сервисе.

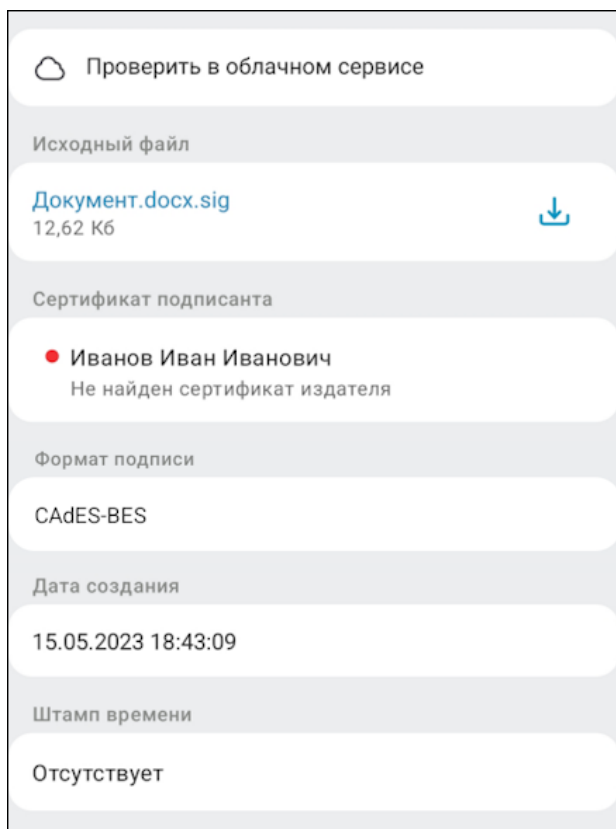


Рисунок 11. Проверка подписи в облачном сервисе

- 4 После проверки подписи вы можете:
 - 4.1 Сохранить подписанный файл, если использовалась прикрепленная ЭП. Для этого нажмите  напротив имени файла.
 - 4.2 Просмотреть информацию о сертификате подписанта. Для этого нажмите на название сертификата.

Расшифрование файла

- 1 Для расшифрования файла в облачном сервисе ЭП [подключитесь к нему](#).
- 2 В разделе **Файлы** нажмите **Расшифрование файла**.
- 3 Выберите файл, который хотите расшифровать.



Примечание. Максимальный размер файла для расшифрования — 500 Мбайт.

- 4 Выберите сертификат для расшифрования.
- 5 В зависимости от места хранения сертификата:
 - Внутреннее хранилище — введите пароль хранилища сертификатов.

- Облачный сервис ЭП — приложение проверит связь с сервисом. Может потребоваться повторное подключение (например, если время сессии истекло).
 - Токен — [подключите токен к устройству](#) и введите ПИН.
- 6 В окне сообщения об успешном выполнении операции нажмите **Сохранить файл** или **Отправить файл**.

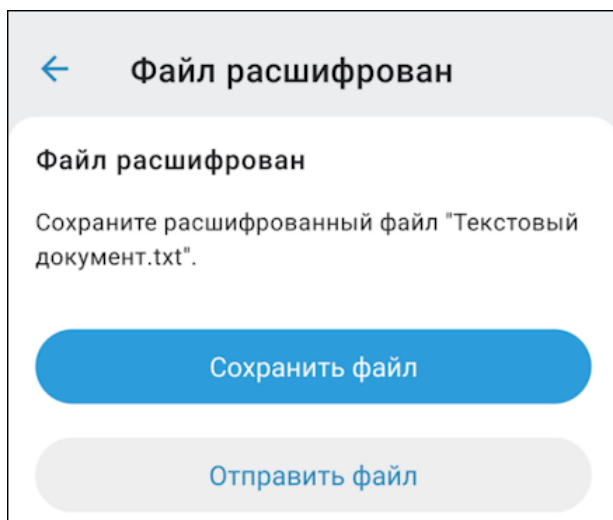


Рисунок 12. Расшифрование файла

Подключение к сайтам, использующим TLS ГОСТ

Порядок настройки

Действие	
1	Если на устройстве работает приложение ViPNet Client for Android или другой VPN-клиент, отключите его на время работы с сайтами
2	Чтобы подключаться к сайтам с аутентификацией пользователя, убедитесь, что ваш сертификат соответствует требованиям
3	Настройте TLS-соединение: • Установите корневой сертификат УЦ и соответствующие CRL; • Установите в хранилище устройства корневой сертификат, который будет использоваться для подключения по TLS ГОСТ; • Настройте прокси-сервер для вашего подключения к интернету.
4	Включите TLS ГОСТ
5	Выполните одно из действий: • отключите Wi-Fi, если вы используете мобильный интернет; • отключите мобильный интернет, если вы используете Wi-Fi.
6	Подключитесь к сайту
7	При необходимости просмотрите информацию о текущих TLS-соединениях

Требования к сертификатам для работы по TLS ГОСТ

Сертификат сервера

При подключении к сайту проверяется выполнение условий:

- [сертификат действителен](#);
- ЭП сертификата верна;

- адрес сайта соответствует адресу в сертификате;
- сертификат содержит значение **Проверка подлинности сервера** в расширении **Расширенное использование ключа**;
- сертификат содержит значения **Цифровая подпись**, **Шифрование ключей**, **Согласование ключей** (хотя бы одно из перечисленных) в расширении **Использование ключа**.



Внимание! Если не выполняется хотя бы одно из условий, соединение не будет установлено.

Сертификат пользователя

Для подключения к сайтам, использующим TLS ГОСТ с аутентификацией пользователя, нужен сертификат, для которого выполняются условия:

- [сертификат действителен](#);
- ЭП сертификата верна;
- сертификат содержит значение **Проверка подлинности клиента** в расширении **Расширенное использование ключа**;
- сертификат содержит значение **Цифровая подпись** и (или) **Согласование ключей** в расширении **Использование ключа**.



Внимание! Если не выполняется хотя бы одно из условий, вы не сможете выбрать сертификат при подключении к сайту, использующему TLS ГОСТ с аутентификацией пользователя.

Настройка TLS-соединения

- 1 В разделе **Соединение** нажмите **Настроить TLS-соединение**.



Примечание. Если у вас устройство с Android 13, разрешите ViPNet PKI Client отправлять уведомления.

- 2 Для настройки TLS-соединения:
 - 2.1 [Установите корневой сертификат УЦ и соответствующие CRL](#).
 - 2.2 Сохраните корневой сертификат для TLS ГОСТ.
 - 2.3 [Установите корневой сертификат для TLS ГОСТ в хранилище устройства](#).
 - 2.4 [Настройте прокси-сервер для вашего подключения к интернету](#).
- 3 Если настройки устройства выполнены, установите соответствующий флажок.

4 Нажмите **Продолжить**.

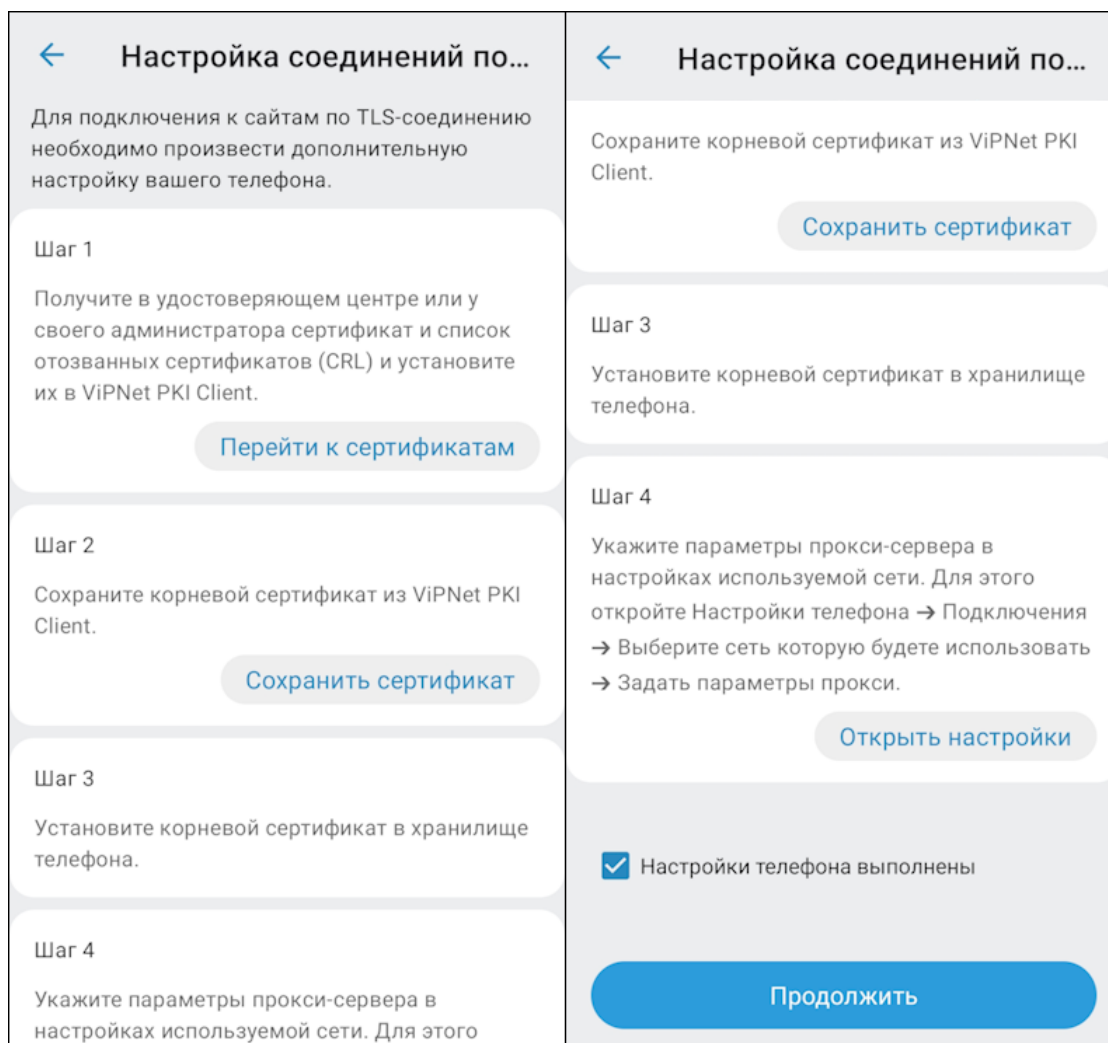


Рисунок 13. Настройка TLS-соединения

Установка корневого сертификата для TLS ГОСТ

Устройство с Android 11 или выше

- 1 Настройте блокировку экрана ПИНом, паролем, рисунком или с помощью биометрических данных. Блокировку нельзя отменить, пока сертификат установлен в Android.
- 2 [Сохраните корневой сертификат на устройстве.](#)
- 3 Установите корневой сертификат в Android:
 - 3.1 Перейдите в настройки устройства.

- 3.2 В поле **Поиск настроек** введите **Шифрование и учетные данные**.
- 3.3 Нажмите **Установка сертификатов > Сертификат центра сертификации**.
- 3.4 Согласитесь с установкой сертификата и подтвердите свою личность.
- 3.5 В файловом менеджере выберите файл сертификата.



Примечание. В зависимости от устройства установка корневого сертификата для TLS ГОСТ может отличаться.

Устройство с Android 10 или ниже

- 1 Настройте блокировку экрана ПИНом, паролем, рисунком или с помощью биометрических данных. Блокировку нельзя отменить, пока сертификат установлен в Android.
- 2 [Сохраните корневой сертификат на устройстве](#).
- 3 Установите корневой сертификат в Android:
 - 3.1 Откройте файловый менеджер и выберите файл сертификата.
 - 3.2 В списке приложений выберите **Установщик сертификатов**.
 - 3.3 Подтвердите свою личность.
 - 3.4 Введите имя сертификата и в качестве назначения выберите **VPN и приложения**.
 - 3.5 Нажмите **ОК**.



Примечание. В зависимости от устройства установка корневого сертификата для TLS ГОСТ может отличаться.

Настройка прокси-сервера

При подключении к сайтам ViPNet PKI Client выполняет роль прокси-сервера. Чтобы все соединения с сайтами проходили через приложение, задайте настройки прокси-сервера для вашего подключения к интернету.



Примечание. После настройки прокси-сервера интернет на устройстве может быть недоступен.

Я использую мобильный интернет

- 1 Перейдите в настройки устройства.

- 2 В поле **Поиск настроек** введите **Точки доступа** или **Имена точек доступа (APN)** и выберите используемую точку доступа.
- 3 В поле **Прокси-сервер** задайте IP-адрес — 127.0.0.1.
- 4 В поле **Порт** задайте порт, указанный в настройке TLS-соединения (по умолчанию задан порт 60000). Номера портов в настройках TLS-соединения и прокси-сервера должны быть одинаковыми.
- 5 Сохраните изменения.

Я использую Wi-Fi

- 1 Перейдите в **Настройки > Wi-Fi** и откройте расширенные настройки вашей сети Wi-Fi.
- 2 В поле **Прокси-сервер** выберите **Вручную** и задайте IP-адрес — 127.0.0.1 и порт, указанный в настройке TLS-соединения (по умолчанию задан порт 60000). Номера портов в настройках TLS-соединения и прокси-сервера должны быть одинаковыми.



Примечание. В зависимости от устройства настройка прокси-сервера может отличаться.

Включение TLS ГОСТ



Внимание! Если вы настроили локальный прокси-сервер для вашего подключения к интернету и не разрешили соединение по TLS ГОСТ, подключение к интернету будет недоступно.

Чтобы включить поддержку TLS-соединений по алгоритмам ГОСТ, в разделе **Соединение** нажмите **Разрешить**. Для отключения TLS ГОСТ нажмите **Запретить**.

Чтобы установить соединение по TLS ГОСТ при отсутствии доверия к сертификату сервера, на экране **Соединение** включите  **Разрешать небезопасные соединения**.

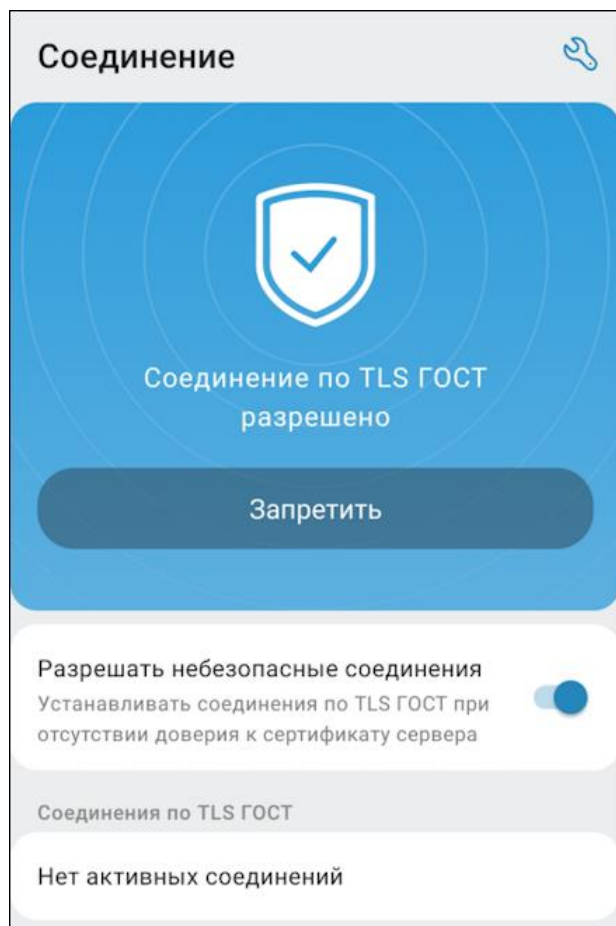


Рисунок 14. Включение TLS ГОСТ



Внимание! Подключайтесь к сайтам с недоверенными сертификатами, только если вы уверены в их безопасности. Иначе злоумышленники могут получить доступ к вашим личным данным.

Изменение настройки TLS-соединения

Если вам нужно заново сохранить корневой сертификат, ознакомиться с настройкой TLS-соединения или изменить порт:

- 1 В разделе **Соединение** справа сверху нажмите .
- 2 Для сохранения корневой сертификат нажмите **Корневой сертификат**.
- 3 Для повторного ознакомления с настройкой TLS-соединения нажмите **Как настроить**.
- 4 Для изменения порта нажмите **Порт** и задайте нужный (по умолчанию задан порт 60000).

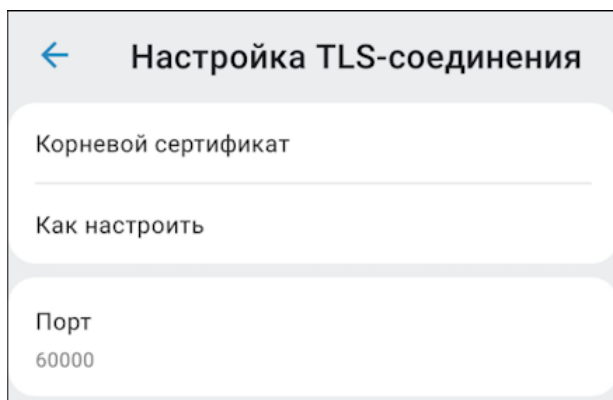


Рисунок 15. Изменение настройки TLS-соединения

Подключение к сайту



Внимание! Для гарантированного подключения к сайтам по TLS ГОСТ используйте браузеры Atom, Chrome, Edge, Firefox, Яндекс.Браузер и Яндекс Лайт последних версий.

Чтобы подключиться к сайту, использующему TLS ГОСТ, в браузере введите адрес сайта:

- Если для подключения не требуется аутентификация пользователя, соединение будет установлено. Сообщение о подключении появится на панели уведомлений.
- Если для подключения требуется аутентификация пользователя, выберите сертификат и введите пароль хранилища. Соединение будет установлено.



Внимание! При первом подключении с аутентификацией пользователя разрешите ViPNet PKI Client наложение поверх окон других приложений.

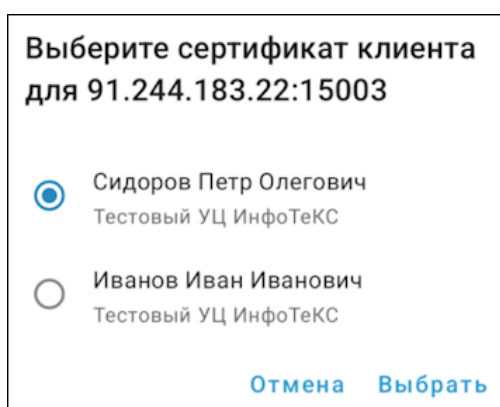


Рисунок 16. Выбор сертификата

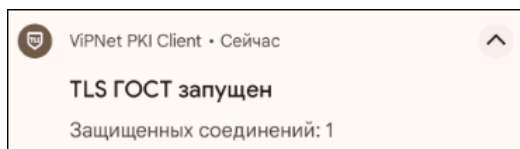
При первом подключении к сайту выбранный сертификат сохраняется в кеш, и при последующих подключениях к этому сайту в текущей сессии выбирать сертификат не требуется.

Если необходимо выбрать другой сертификат для подключения, удалите сертификат из кеша вручную. Для этого выключите, а затем [включите TLS ГОСТ](#).

Просмотр информации о TLS-соединениях

Для того, чтобы просмотреть подробные сведения о TLS-соединениях, выполните одно из действий:

- Смахните вниз от верхнего края экрана и нажмите на уведомление о включении TLS ГОСТ.



- В разделе **Соединение** в группе **Соединения по TLS ГОСТ** нажмите на список установленных соединений.

Будут отображены подробные сведения о соединениях:

- версия протокола TLS;
- алгоритм согласования ключей;
- алгоритм шифрования;
- имя владельца сертификата (для подключений с аутентификацией пользователя);
- причина отсутствия доверия к сертификату сервера.

TLS-соединения		
●	www.gosuslugi.ru:443 TLS 1.2 / ГОСТ 2012 - ГОСТ 89	10:21
●	91.244.183.22:15013 Иванов Иван Иванович TLS 1.3 / ГОСТ 2012 - Кузнечик(S)	10:21
●	login.mos.ru:443 В цепочке присутствует самоподписанный сертификат	10:22
●	static3.mos.ru:443 В цепочке присутствует самоподписанный сертификат	10:22
●	www.mos.ru:443 В цепочке присутствует самоподписанный сертификат	10:22

Рисунок 17. Сведения о TLS-соединениях

Чтобы просмотреть подробные сведения о сертификате сервера, нажмите на соединение в списке.

Служебные функции

Проверка целостности

Чтобы проверить целостность системных файлов и исполняемых файлов ViPNet PKI Client:

- 1 В разделе **Настройки** нажмите **Проверка целостности**.
- 2 Дождитесь окончания проверки.
- 3 При появлении предупреждения о нарушении целостности см. [Заблокирована работа ViPNet PKI Client из-за нарушения целостности](#).

Смена пароля хранилища сертификатов

Срок действия пароля хранилища сертификатов — 6 месяцев. По истечении этого срока при входе в приложение потребуется сменить пароль.

Чтобы сменить пароль до истечения этого срока:

- 1 В разделе **Настройки** нажмите **Смена пароля хранилища телефона**.
- 2 Введите текущий пароль, затем задайте и подтвердите новый.
- 3 Нажмите **Сменить пароль**.

Обновление лицензии

- 1 В разделе **Настройки** нажмите **Данные об активации**.
- 2 Нажмите  **Изменить**.
- 3 Выберите способ активации лицензии.
- 4 Если у вас есть серийный номер:
 - 4.1 Введите номер телефона и серийный номер.
 - 4.2 Нажмите **Активировать лицензию**, вам будет отправлено СМС с кодом активации.
 - 4.3 Введите полученный код.
- 5 Если у вас есть файл лицензии:
 - 5.1 Выберите файл лицензии в формате *.itcslic.

- 5.2 Посмотрите состав лицензии и нажмите **Активировать лицензию**.
- 5.3 Введите номер телефона.
- 5.4 Нажмите **Продолжить**, вам будет отправлено СМС с кодом активации.
- 5.5 Введите полученный код.

Сброс настроек приложения

Вам может потребоваться сбросить настройки приложения, удалить сертификаты и ключи ЭП без удаления приложения:

- Чтобы вернуть доступ к работе с приложением, если вы забыли пароль хранилища сертификатов.
- Чтобы удалить личную информацию, если вы передаете устройство другому пользователю.

Для этого:

- Запустите приложение, перейдите в раздел **Настройки**, нажмите **Удаление данных** и подтвердите действие.
- На устройстве перейдите в системные свойства приложения и нажмите **Удалить данные**.



Примечание. При удалении данных приложения лицензия не удаляется.

Для продолжения работы с приложением:

- 1 [Создайте хранилище сертификатов](#).
- 2 [Установите сертификаты](#).

Удаление приложения

При удалении приложения:

- Не удаляются подписанные и зашифрованные файлы.
- Удаляются сертификаты и ключи ЭП, которые вы установили.

Удалите приложение стандартными средствами Android.

Если вы [настраивали TLS-подключение к сайтам](#), после удаления приложения на устройстве не будет доступа в интернет. Для восстановления доступа [удалите из хранилища устройства установленный корневой сертификат](#) и [отключите использование прокси-сервера](#) для вашего подключения к интернету.

Возможные неполадки

Заблокирована работа ViPNet PKI Client из-за нарушения целостности

При запуске приложения или выполнении регламентной проверки могут появиться предупреждения о нарушении целостности:

- системных файлов;
- исполняемых файлов ViPNet PKI Client.

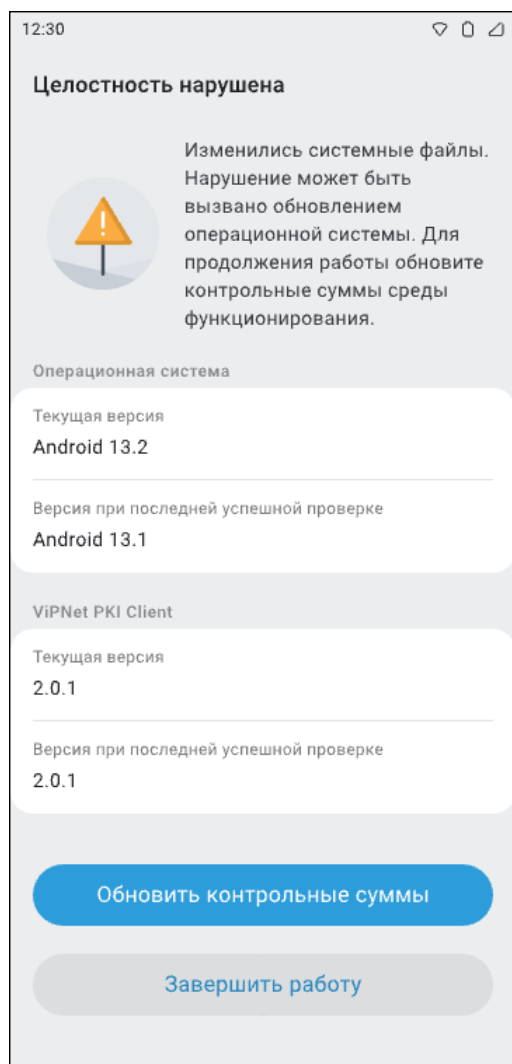


Рисунок 18. Предупреждение о нарушении целостности системных файлов

Нарушение целостности системных файлов может быть вызвано обновлением Android или системных компонентов, а также действиями посторонних лиц. Для продолжения работы после обновления нажмите **Обновить контрольные суммы**. Если вы не уверены в причине нарушения целостности, нажмите **Завершить работу**.

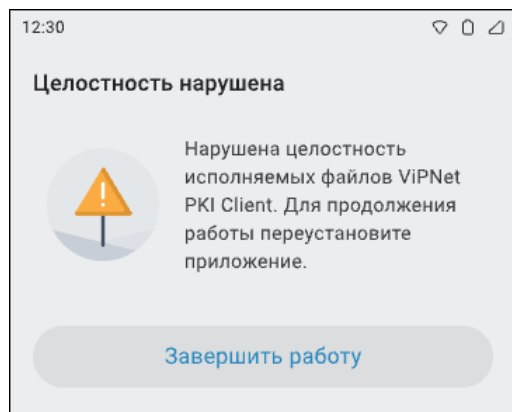


Рисунок 19. Предупреждение о нарушении целостности исполняемых файлов

Нарушение целостности исполняемых файлов может произойти в результате вмешательства посторонних лиц. При появлении предупреждения:

- 1 Нажмите **Завершить работу**.
- 2 Переустановите приложение.
- 3 Обратитесь в УЦ для аннулирования ваших личных сертификатов.

Нет подключения к интернету

При работе с сайтами в браузере может появиться ошибка:



Рисунок 20. Ошибка при подключении к интернету

Ошибка может возникнуть, если вы **настроили прокси-сервер** для вашего подключения к интернету, но **не включили TLS ГОСТ** в настройках приложения.

Выполните одно из действий:

- Если больше не требуется подключаться к сайтам, использующим TLS ГОСТ, **отключите использование прокси-сервера** для вашего подключения к интернету.

- [Включите TLS ГОСТ.](#)

Не удастся войти в стороннее приложение

Если у вас настроено подключение к сайтам, использующим TLS ГОСТ, при попытке войти в некоторые приложения может появиться сообщение о недоступности сервиса.

Воспользуйтесь сервисом через браузер, подключитесь к другой сети или выполните:

- 1 В настройках вашего подключения к интернету [отключите использование прокси-сервера](#).
- 2 [Отключите TLS ГОСТ](#).
- 3 Войдите в приложение.

NFC-токен не обнаружен на устройстве

Если при подключении NFC-токена устройство никак не реагирует, выполните одно из действий:

- Убедитесь, что устройство имеет NFC-модуль. Если да, выключите и включите NFC-модуль.
- [См. рекомендации](#).

История версий

Что нового в версии 2.0.1

- **Проверка целостности**

Добавлена возможность ручного запуска проверки целостности без перезапуска ViPNet PKI Client. Подробнее см. [Проверка целостности](#).

- **Изменение в лицензировании**

Теперь использовать ViPNet PKI Client можно только после приобретения лицензии (см. [Лицензирование](#)).

Что нового в версии 2.0

- Обновление пользовательского интерфейса ViPNet PKI Client
- Повышение стабильности работы TLS ГОСТ
- Увеличение максимальных размеров обрабатываемых файлов

Что нового в версии 1.5

- **Поддержка TLS 1.3**

Теперь поддерживается подключение к сайтам по протоколу TLS версии 1.3.

- **Возможность выбора параметров ключа проверки ЭП**

Теперь при создании запроса на сертификат вы можете выбрать [необходимые параметры ключа проверки ЭП](#).

- **Подключение к сервису облачной ЭП по протоколу HTTPS**

Теперь подключаться к ViPNet PKI Service можно только по протоколу HTTPS с указанием порта 9441.

Что нового в версии 1.4

- **Поддержка облачных сервисов ЭП**

Теперь, если в вашей организации используется облачный сервис ЭП на базе ViPNet PKI Service версии 2.0, вы можете подключиться к нему в приложении ViPNet PKI Client Android и подписывать, проверять подпись и расшифровывать файлы с помощью сертификатов, хранимых на нем.

- **Поддержка токенов и смарт-карт для ЭП**

Теперь вы можете подписывать файлы ЭП с помощью сертификатов на токенах, а также сохранять на токены сертификаты и ключи ЭП.

- **Поддержка сертификатов в формате PKCS #7**

Теперь вы можете [устанавливать сертификаты](#) из файлов в формате PKCS #7 (*.p7b). В этом формате обычно сохраняют сертификат пользователя вместе с корневым и промежуточными сертификатами УЦ, а также CRL. Поэтому при установке файлов такого формата ничего дополнительно устанавливать не нужно.

- **Темная тема интерфейса**

Добавлена возможность использовать темную тему интерфейса приложения. По умолчанию тема соответствует настройкам Android. Сменить тему можно в разделе **Настройки**.

- **Сервис для подключения к ресурсам, использующим TLS ГОСТ, из сторонних приложений**

Теперь разработчики сторонних приложений могут настроить взаимодействие с ViPNet PKI Client и в своих приложениях подключаться к ресурсам, использующим TLS ГОСТ. Подробнее см. документ «ViPNet PKI Client Android SDK. Руководство разработчика».

Что нового в версии 1.3

- **Новые алгоритмы шифрования файлов**

В предыдущей версии для шифрования файлов использовался алгоритм ГОСТ 28147-89. В новой версии были добавлены алгоритмы шифрования ГОСТ 34.12-2018 «Магма» и «Кузнечик», и теперь при зашифровании вы можете выбрать нужный алгоритм.

- **Предустановленные сертификаты УЦ**

Теперь для удобства в приложении предустановлены сертификаты аккредитованных удостоверяющих центров:

- Корневые:

- Головной удостоверяющий центр.
 - Минкомсвязи России.
 - IIT GOST Root CA (АО «ИнфоТеКс Интернет Траст»).
 - CryptoPro GOST Root CA (ООО «КРИПТО-ПРО»).

- Промежуточные:

- CryptoPro TLS CA (ООО «КРИПТО-ПРО»).

- **TLS ГОСТ с двусторонней аутентификацией и новые алгоритмы шифрования данных**

В предыдущей версии вы могли подключаться только к сайтам, использующим TLS ГОСТ с односторонней аутентификацией с шифрованием по алгоритму ГОСТ 28147-89. В новой версии добавлена возможность подключения к сайтам, использующим TLS ГОСТ с шифрованием по алгоритмам ГОСТ 34.12-2018 «Магма» и «Кузнечик», в том числе с двусторонней аутентификацией.

- **Взаимодействие с ViPNet PKI Client через API**

Добавлена возможность взаимодействия с ViPNet PKI Client через API. Это позволит разработчикам встраивать в приложения для ОС Android следующие функции:

- Заверение файла электронной подписью.
- Зашифрование и расшифрование файла.
- Проверка прикрепленной и открепленной электронной подписи.

- **Смена пароля хранилища сертификатов**

Теперь срок действия пароля хранилища сертификатов составляет 6 месяцев. По истечении этого срока для входа в приложение нужно сменить пароль. Также пароль можно сменить вручную, не дожидаясь окончания срока действия.

- **Поддержка сертификатов ГОСТ Р 34.10-2001**

Прекращена поддержка сертификатов ГОСТ Р 34.10-2001 для заверения электронной подписью и шифрования файлов, а также для подключения к сайтам, использующим TLS ГОСТ. Сертификаты ГОСТ Р 34.10-2001 могут использоваться только для проверки электронной подписи и расшифрования.

- **Английский язык приложения**

Начиная с версии 1.3, ViPNet PKI Client доступен на английском и русском языке. Язык приложения определяется языком ОС Android.

Что нового в версии 1.2

- **Изменилась политика использования приложения**

Теперь для использования приложения нужно приобрести [лицензию](#).

- **Добавлена возможность настройки автоматического обновления CRL**

Если в УЦ используются точки распространения CRL, вы можете [настроить автоматическое обновление CRL](#). Это позволит исключить обновление CRL вручную.

- **Добавлена поддержка проверки статуса сертификатов по протоколу OCSP**

Если УЦ используется сервис определения статуса сертификатов по сети и в изданных сертификатах содержится информация об адресах этих сервисов, установка CRL для таких УЦ не требуется.

- **Добавлена возможность подключения к сайтам по протоколу TLS с односторонней аутентификацией**

Теперь вы можете устанавливать защищенные TLS-соединения с односторонней аутентификацией с сайтами, использующими шифрование по алгоритмам ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 и ГОСТ 28147-89.

- **Изменения в интерфейсе**

- Добавлен раздел с настройками подключения к сайтам по протоколу TLS.

- Раздел **О программе** переименован в **О приложении** и перенесен отдельным пунктом в раздел **Настройки**.
- В пункт **О приложении** добавлена информация об активации.

Что нового в версии 1.1

- **Добавлена возможность шифрования и расшифрования файлов**

Теперь вы можете шифровать файлы с помощью сертификатов других пользователей, а также расшифровывать файлы, которые были зашифрованы с помощью вашего сертификата.

- **Добавлена возможность импорта сертификата и ключа электронной подписи из файла PFX**

В предыдущей версии для заверения файлов электронной подписью вы могли использовать только сертификаты, запрос на издание которых был создан в приложении ViPNet PKI Client. Это было неудобно, если у вас уже был сертификат и соответствующий ключ электронной подписи, установленные, например, на компьютере с ПК ViPNet PKI Client.

В новой версии вы можете экспортировать ваш сертификат и ключ электронной подписи в файл PFX, а затем [импортировать его на устройство](#).

- **Добавлена возможность подтверждения времени заверения файла электронной подписью**

В предыдущей версии была возможность только проверять штампы времени при проверке электронной подписи файлов, полученных от других пользователей.

В новой версии вы можете добавлять штамп времени при [заверении файлов электронной подписью](#).

- **Добавлена возможность удаления данных приложения**

В предыдущей версии удаление ключей электронной подписи было возможно только с помощью удаления приложения. Это было неудобно, например, если вы используете корпоративное устройство и вам нужно передать его другому сотруднику.

В новой версии для удаления ключей электронной подписи вы можете воспользоваться функцией удаления данных приложения. Подробнее см. раздел [Сброс настроек приложения](#).

Термины и сокращения

OCSP-сервер

Сервер в составе доверенного субъекта инфраструктуры открытых ключей, предоставляющего информацию о статусах сертификатов по запросам в режиме онлайн.

TLS (Transport Layer Security)

Криптографический протокол транспортного уровня для защищённой передачи данных между узлами в интернете. Использует асимметричные ключи, симметричное шифрование данных и коды аутентичности сообщений.

TSP (Time-Stamp Protocol)

Криптографический протокол, позволяющий создавать доказательство факта существования электронного документа на определённый момент времени. Подробнее см. [RFC 3161](#).

ViPNet PKI Service

Программно-аппаратный комплекс для выполнения криптографических операций по запросам пользователей, а также для создания и защищенного хранения ключей пользователей. Является средством криптографической защиты информации класса КВ и средством электронной подписи класса КВ2.

Аннулирование сертификата

Признание сертификата недействительным до истечения его срока действия (например, в случае компрометации соответствующего ключа электронной подписи).

Аутентификация

Процесс односторонней или двусторонней (взаимной) проверки подлинности между клиентом (пользователем) и системой (сервером), например, с использованием учётных данных или сертификатов ключей проверки электронной подписи.

Действительность сертификата

Сертификат, для которого выполняются условия:

- срок действия сертификата наступил и не истёк;
- сертификат не аннулирован;
- цепочка сертификатов полна, и все сертификаты цепочки действительны.

Запрос на сертификат

Документ с информацией, которая требуется для издания сертификата ключа проверки электронной подписи в удостоверяющем центре (владелец, срок действия, назначение сертификата и прочее).

Ключ электронной подписи (ключ ЭП)

Секретный (закрытый) ключ из пары асимметричных ключей, который представляет собой уникальную последовательность символов, предназначенную для создания электронной подписи.

Контейнер ключей

Файл или устройство, в котором хранятся ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи.

Корневой сертификат

Самоподписанный сертификат головного удостоверяющего центра. Используется для подписи сертификатов, издаваемых головным удостоверяющим центром, с целью обеспечения доверия к ним.

Открепленная подпись

Тип электронной подписи, при использовании которой электронная подпись файла помещается в отдельный контейнер. Для проверки такой электронной подписи требуется контейнер с электронной подписью и исходный файл.

Прикрепленная подпись

Тип электронной подписи, при использовании которой исходный файл и электронная подпись помещаются в один контейнер. Для проверки электронной подписи требуется только этот контейнер.

Список аннулированных сертификатов (CRL)

Список сертификатов, которые до истечения срока их действия были аннулированы или приостановлены администратором удостоверяющего центра и потому недействительны на момент, указанный в данном списке аннулированных сертификатов.

Точка распространения списков аннулированных сертификатов (CDP)

Хранилище, в которое удостоверяющий центр публикует актуальные списки аннулированных сертификатов. URL таких точек указываются в соответствующем расширении сертификатов, издаваемых удостоверяющим центром.

Удостоверяющий центр (УЦ)

Организация, уполномоченная издавать сертификаты ключа проверки электронной подписи для физических и юридических лиц, а также управлять жизненным циклом этих сертификатов.

Цепочка сертификатов

Иерархия сертификатов, в которой каждый сертификат подписан вышестоящим сертификатом вплоть до корневого (самоподписанного) сертификата. Наличие для сертификата полной цепочки действительных сертификатов подтверждает доверие к этому сертификату.

Электронная подпись (ЭП)

Созданная криптографической операцией дополнительная информация, с помощью которой можно подтвердить авторство и неизменность основной информации.