Цифровые технологии

КриптоАРМ Подпись и шифрование

Документация продукта

Релиз v7.3

> Архивная документация. Актуальный релиз: v7.4

Исходная документация на CryptoARM.ru

Редакция от 26.11.2026

Правообладатель и разработчик
ООО «Цифровые технологии»

Содержание

Документация ... 4

Общие сведения

- О продукте ... 5
- Криптопровайдеры и стандарты ... 11
- Глоссарий ... 14

Установка

- Установка на Windows ... 21
- Установка на Linux ... 34
- Установка на macOS ... 49
- Активация лицензии ... 55

Начало работы

- Быстрый старт ... 61
- Интерфейс приложения ... 65
- Общие настройки ... 70
- Уведомления и журнал событий ... 75
- Проверка обновлений ... 82

Документы

- Обзор операций и выбор мастера ... 86
- Профили подписи ... 93
- Подпись и шифрование ... 100
- Проверка и расшифрование ... 117
- Подпись и защита PDF ... 130
- Настройки подписи и шифрования ... 143
- Контекстное меню Проводника и открытие файлов ... 158
- Выполнение операций в командной строке ... 165

Сертификаты

- Раздел «Сертификаты» ... 182
- Установка сертификатов ... 192
- Создание запроса и самоподписанного сертификата ... 197
- Экспорт и удаление сертификатов ... 204

Контейнеры и списки отзыва 208
Группы сертификатов 214

OpenPGP

О разделе OpenPGP 218
Создание и импорт сертификатов 223
Действия с сертификатами 229
Экспорт и резервное копирование 235

API

Описание и возможности API 239
Приложение и пользователь 247
Транспорт и доверие 251
Команда signAndEncrypt 256
Команда certificates 271
Команда certrequests 276
Команда diagnostics 282
Команда startView 286
Лимиты, статусы и ошибки 288

Открыть статью на сайте

Документация КриптоАРМ Подпись и шифрование

КриптоАРМ версии «Подпись и шифрование» — программа для создания и проверки электронной подписи, шифрования файлов и управления сертификатами на Windows, Linux и macOS.

С чего начать

- О продукте — возможности, лицензирование и системные требования.
- Установка на Windows, Linux или macOS.
- Активация лицензии — ввод серийного номера после установки.
- Быстрый старт — первоначальная настройка и первая операция.

Разделы документации

- **Общие сведения** — назначение продукта, поддерживаемые криптопровайдеры и глоссарий.
- **Установка** — установка на поддерживаемых операционных системах и активация лицензии.
- **Начало работы** — интерфейс приложения, общие настройки, уведомления и журнал событий, проверка обновлений.
- **Документы** — подпись и шифрование, проверка и расшифрование, защита PDF, профили подписи, командная строка.
- **Сертификаты** — установка, создание запроса, экспорт и удаление, контейнеры и списки отзыва, группы.
- **OpenPGP** — создание и импорт, действия с сертификатами, экспорт и резервное копирование.
- **API** — описание и возможности, команды signAndEncrypt, certificates, certrequests, diagnostics, startView, а также лимиты, статусы и ошибки.

Поиск и навигация

- **Используйте боковое меню** слева для перехода между разделами.
- **Следите за перекрёстными ссылками** в статьях — они ведут на связанные темы.

Открыть статью на сайте

КриптоАРМ Подпись и шифрование — приложение для электронной подписи и защиты документов

КриптоАРМ версии Подпись и шифрование — это программное обеспечение для создания и проверки электронной подписи, шифрования файлов и управления сертификатами.

КриптоАРМ предназначен для юридически значимого электронного документооборота между организациями, государственными органами и частными лицами, а также для защиты конфиденциальных данных.

Документация описывает версию **«Подпись и шифрование»**, предназначенную для работы с файлами на компьютере пользователя. Защиту электронной переписки обеспечивает версия **«Защищенная почта»**: она дополнительно включает почтовый клиент, подпись и шифрование сообщений по S/MIME, а её лицензия действует и в этой версии.

Порядок первоначальной настройки и выполнения первой операции описан в инструкции Быстрый старт.

Содержание:

- Основные возможности КриптоАРМ
- Совместимость и условия эксплуатации
- Лицензирование
- Системные требования
- Поддерживаемые операционные системы
- Смотрите также

Основные возможности КриптоАРМ

КриптоАРМ предоставляет полный набор инструментов для работы с электронной подписью, сертификатами и шифрованием данных.

Электронная подпись

- создание электронной подписи произвольных файлов;
- проверка электронной подписи;
- создание присоединённой и отсоединённой электронной подписи;
- создание соподписей;
- поддержка стандартов электронной подписи CAdES-BES, CAdES-T, CAdES-X Long Type 1, CAdES-A;
- подпись и проверка подписи с машиночитаемой доверенностью (МЧД);

- формирование отчётов о проверке электронной подписи в формате PDF;
- снятие и объединение электронных подписей.

Подпись документов формата PDF

- подписание и сертификация документов формата PDF;
- поддержка встроенной подписи по стандарту PAdES с видимым или невидимым штампом;
- разметка областей размещения подписей и подписантов;
- добавление текстовых и графических элементов;
- преобразование документов в форматы PDF/A-2b и PDF/A-3b.

Шифрование и расшифрование данных

- шифрование и расшифрование файлов;
- поддержка стандарта PKCS#7;
- шифрование данных для одного или нескольких получателей;
- шифрование данных по группам сертификатов;
- поддержка алгоритмов ГОСТ 28147-89, ГОСТ Р 34.12-2015 «Магма» и «Кузнечик», AES-256-CBC, DES3-CBC;
- автоматическое удаление исходных файлов после шифрования (при настройке).

Архивирование данных

- архивирование файлов перед выполнением операций подписи и шифрования;
- упаковка результатов в один архив или в отдельный архив на каждый файл.

Управление сертификатами и ключами

- отображение сертификатов и связанных с ними закрытых ключей;
- проверка корректности сертификатов с построением цепочки доверия;
- создание запросов на сертификаты и самоподписанных сертификатов;
- импорт, экспорт и удаление сертификатов, в том числе в формате PKCS#12;
- печать карточки сертификата со сведениями о владельце, издателе, сроке действия и отпечатке;
- работа с ключевыми контейнерами и аппаратными ключевыми носителями при использовании поддерживаемых криптопровайдеров;
- импорт, просмотр и экспорт списков отзыва сертификатов (CRL);
- объединение сертификатов в группы для быстрого выбора получателей шифрования.

Сертификаты и ключи OpenPGP

- создание, импорт и экспорт сертификатов OpenPGP;
- подключи подписи и шифрования, отзыв ключа и подключа;
- заверение чужих сертификатов (сеть доверия);
- резервное копирование закрытого ключа;
- постквантовые схемы подписи и шифрования.

Автоматизация и интеграции

- профили подписи — сохранённые наборы настроек операции;
- контекстное меню Проводника Windows и быстрые действия Finder с профилями;
- командная строка (CLI) для скриптов и систем обмена документами;
- внешний API для вызова операций из веб-сервисов и локальных приложений.

Журналирование и уведомления

- ведение журнала событий;
- просмотр, фильтрация и сортировка событий;
- экспорт журнала в файл формата CSV;
- уведомления о результате операции.

Совместимость и условия эксплуатации

Стандарты операций и криптопровайдеры

Приложение выполняет операции по двум независимым стандартам — **X.509** и **OpenPGP**. У каждого стандарта собственные сертификаты, форматы файлов и профили подписи. Активный стандарт задаётся настройкой **«Стандарт операций по умолчанию»** в разделе **Настройки → Криптопровайдеры** и определяет содержимое разделов **«Сертификаты»**, **«Подпись и шифрование»** и **«Проверка и расшифрование»**, а также стандарт, применяемый в контекстном меню Проводника.

По умолчанию выбран стандарт **X.509**: он применяется в юридически значимом документообороте по 63-ФЗ и при обмене документами с государственными органами и контрагентами. Стандарт **OpenPGP** предназначен для обмена внутри команд и сообществ, в которых приняты ключи OpenPGP, и поддерживает сеть доверия и постквантовые схемы.

Криптографические вычисления выполняет криптопровайдер, соответствующий стандарту и алгоритмам операции:

1. **Встроенная библиотека OpenSSL** — стандарт X.509:

- реализует криптографические операции по международным стандартам: RSA, ECDSA, AES и др.;
- не поддерживает российские криптографические алгоритмы ГОСТ;

1. **КриптоПро CSP (версии 5.0 и выше)** — стандарт X.509 с использованием российских алгоритмов ГОСТ (ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ 28147-89 и др.); необходим для:

- работы с сертификатами, выданными по российским стандартам ГОСТ;
- создания электронной подписи, отвечающей требованиям законодательства РФ;

- использования аппаратных ключевых носителей;

1. **Встроенный провайдер OpenPGP** — стандарт OpenPGP: выполняет все операции стандарта, включая постквантовые схемы подписи и шифрования.

Отдельно устанавливается только КриптоПро CSP. Подробнее — в инструкции Криптопровайдеры в КриптоАРМ.

> 💡 **Примечание**: мастер **«Подпись и защита PDF»** работает только со стандартом X.509.

Поддерживаемые ключевые носители

При использовании криптопровайдера КриптоПро CSP поддерживается работа с аппаратными ключевыми носителями:

- Рутокен ЭЦП 3.0 (форм-факторы указаны в формуляре на Рутокен ЭЦП 3.0);
- JaCarta,
- ESMART,
- ФОРОС,
- АНГАРА.

Актуальный список поддерживаемых носителей приведён в формуляре криптопровайдера КриптоПро CSP.

Лицензирование

Общая информация о лицензиях

Для выполнения криптографических операций с алгоритмами ГОСТ требуется лицензия.

Не требуют лицензии:

- проверка электронной подписи и штампов времени, просмотр сведений о проверке и печатная форма;
- шифрование без подписи;
- снятие подписи и объединение подписей;
- просмотр, импорт, экспорт и удаление сертификатов;
- операции с сертификатами встроенного провайдера OpenSSL;
- все операции OpenPGP;
- архивирование.

Доступны следующие варианты лицензии:

- **Пробная лицензия**
- **Лицензия на рабочее место**

Состояние лицензии — её тип, статус и оставшийся срок — показано в разделе **Настройки → О программе**. Порядок активации описан в инструкции Активация лицензии.

> 💡 **Примечание**: лицензия КриптоАРМ не заменяет лицензию КриптоПро CSP. Лицензии CSP, TSP Client и OCSP Client устанавливаются отдельно — см. Лицензии КриптоПро.

Пробная лицензия

При первом запуске КриптоАРМ автоматически активируется **30-дневная пробная лицензия**, которая позволяет ознакомиться со всеми функциями продукта и протестировать работу криптографических операций с алгоритмами ГОСТ.

Если для знакомства со всеми возможностями КриптоАРМ недостаточно ознакомительного периода, вы можете получить дополнительную лицензию, написав в техническую поддержку support@trusted.ru.

Лицензия на рабочее место

Локальная лицензия устанавливается на конкретное рабочее место и используется для выполнения операций непосредственно в приложении.

Особенности:

- Привязана к устройству пользователя
- Требует ввода лицензионного ключа
- Работает независимо от внешних сервисов
- Может быть **годовой** и **бессрочной**

Приобрести лицензии можно в официальном интернет-магазине cryptoarm.ru.

- КриптоАРМ версии Подпись и шифрование, годовая
- КриптоАРМ версии Подпись и шифрование, бессрочная

Этому приложению подходит и лицензия версии **«Защищенная почта»**: она включает подпись и шифрование документов.

- КриптоАРМ версии Защищенная почта, годовая
- КриптоАРМ версии Защищенная почта, бессрочная

Системные требования

Минимальные и рекомендуемые системные требования приведены в таблице ниже.

Компонент	Минимальная конфигурация	Рекомендуемая конфигурация
Процессор	x86-64, 1.0 ГГц	x86-64, 2.0 ГГц+
ОЗУ	2 ГБ	4 ГБ+
Дисковое пространство	500 МБ	5 ГБ+
Дисплей	1024×768	1920×1080+

Для macOS выпускаются сборки под оба типа процессоров — Intel и Apple Silicon.

Поддерживаемые операционные системы

Клиентские операционные системы

- Windows 10 и выше
- Astra Linux Special Edition 1.8
- Альт Рабочая станция 11
- РЕД ОС 8
- Ubuntu 20.04 и выше
- macOS 14 и выше

Серверные операционные системы

- Windows Server 2016 и выше
- Альт Сервер 11
- Astra Linux Server
- Ubuntu Server 20.04 и выше
- РЕД ОС «Сервер»

Контекстное меню Проводника доступно в Windows, быстрые действия Finder — в macOS; в Linux меню файлового менеджера нет.

Смотрите также

- Криптопровайдеры в КриптоАРМ — обзор поддерживаемых криптопровайдеров в КриптоАРМ.
- Глоссарий — термины электронной подписи простыми словами.
- Быстрый старт — первоначальная настройка и выполнение первой операции.
- Установка на Windows — руководство по установке КриптоАРМ на Windows.
- Установка на Linux — руководство по установке КриптоАРМ на Linux.
- Установка на macOS — руководство по установке КриптоАРМ на macOS.

Открыть статью на сайте

Криптопровайдеры в КриптоАРМ

В приложении КриптоАРМ реализована поддержка как российских стандартов ГОСТ через КриптоПро CSP, так и международных алгоритмов через встроенную библиотеку OpenSSL. Операции по стандарту OpenPGP выполняет встроенный провайдер OpenPGP. Эта статья поможет разобраться в их отличиях и выбрать нужный для ваших задач.

В инструкции также описано, где посмотреть состояние провайдеров. Выбор стандарта операций и установка лицензий КриптоПро описаны в инструкции Общие настройки.

Содержание:

- Что такое криптопровайдер
- Особенности в российском сегменте
- Поддерживаемые криптопровайдеры в КриптоАРМ
- Раздел «Криптопровайдеры»
- Инструкции по установке КриптоПро CSP

Что такое криптопровайдер

Криптопровайдер (CSP — Cryptography Service Provider) — это специализированный программный модуль, интегрируемый в операционную систему, который обеспечивает выполнение криптографических операций и управление криптографической инфраструктурой.

Криптопровайдер выполняет ключевые функции:

- генерация и хранение криптографических ключей;
- создание и проверка электронной подписи (ЭП);
- шифрование и расшифрование данных;
- обеспечение целостности и подлинности информации;
- работа с аппаратными ключевыми носителями (токены, смарт-карты).

Принцип работы криптопровайдера

Криптопровайдер выступает посредником между:

1. **операционной системой**, предоставляющей интерфейсы безопасности;
2. **пользовательскими приложениями**, которым необходима защита данных и электронная подпись;
3. **аппаратными средствами**, такими как токены и смарт-карты.

Приложения обращаются к криптопровайдеру через стандартизированные интерфейсы, что позволяет унифицировать работу с различными криптопровайдерами и аппаратными устройствами.

Особенности в российском сегменте

В России использование встроенных криптопровайдеров Windows **не допускается** для работы с государственными органами и юридически значимыми документами, так как они **не сертифицированы ФСБ России** как средства криптографической защиты информации, соответствующие российским криптографическим стандартам ГОСТ. Сертификация обязательна для СКЗИ, используемых в государственных системах и для работы с юридически значимыми документами.

При работе с государственными органами или в ситуациях, требующих применения сертифицированных СКЗИ, необходимо использовать решения, прошедшие сертификацию ФСБ России и поддерживающие российские криптоалгоритмы (ГОСТ Р 34.10-2012 для электронной подписи, ГОСТ Р 34.11-2012 для хеширования, ГОСТ 28147-89 для шифрования и др.).

Для работы с российскими алгоритмами ГОСТ в приложении КриптоАРМ используется **КриптоПро CSP** — криптопровайдер СКЗИ, разработанный компанией «КриптоПро».

Поддерживаемые криптопровайдеры в КриптоАРМ

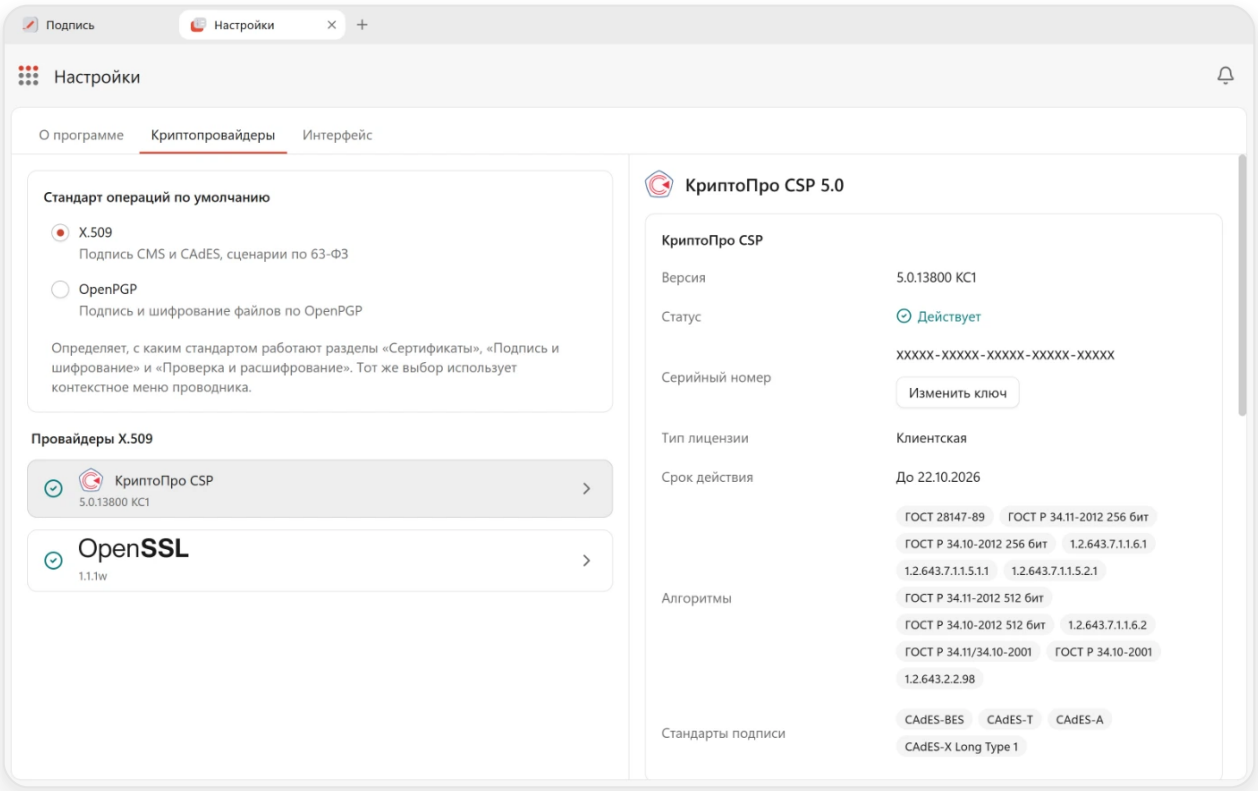
В приложении КриптоАРМ реализована поддержка трёх криптопровайдеров:

- **Российские алгоритмы ГОСТ** — через криптопровайдер **КриптоПро CSP**, который обеспечивает создание квалифицированной электронной подписи, работу с сертификатами ГОСТ, ключевыми контейнерами и аппаратными ключевыми носителями.
- **Международные алгоритмы** — через встроенную библиотеку **OpenSSL**, используемую для криптографических операций по международным стандартам: RSA, ECDSA, AES, 3DES.
- **Стандарт OpenPGP** — через встроенный **провайдер OpenPGP**, который выполняет все операции стандарта, включая постквантовые схемы подписи и шифрования.

> 🔍 Более подробная информация о поддерживаемых криптопровайдерах, их возможностях и совместимых ключевых носителях доступна в основной статье: КриптоАРМ Подпись и шифрование.

Раздел «Криптопровайдеры»

Состояние провайдеров показывает раздел **Настройки → Криптопровайдеры**.



Слева — список провайдеров, справа — сведения о выбранном.

Для **КриптоПро CSP** показаны версия, статус лицензии, её серийный номер, тип и срок действия, а также доступные алгоритмы и стандарты подписи. Статус принимает значения **«Действует»**, **«Недоступен»**, **«Истекла»** и **«Не удалось определить»**; если провайдер не установлен, в списке слева он помечен как **«Не установлен»**.

Для **OpenSSL** показаны версия, алгоритмы и стандарты подписи, для **OpenPGP** — статус, алгоритмы подписи и шифрования, постквантовые схемы.

Инструкции по установке КриптоПро CSP

- Windows
- macOS
- Linux

Смотрите также

- О продукте — возможности и требования приложения.
- Активация лицензии — лицензия КриптоАРМ.
- Общие настройки — стандарт операций, лицензии КриптоПро и настройки интерфейса.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Глоссарий терминов КриптоАРМ

Содержание:

- Сертификаты
- Подпись и шифрование
- OpenPGP
- Смотрите также

Сертификаты

Сертификат электронной подписи

Электронный документ, который подтверждает владение ключом электронной подписи и принадлежность открытого ключа указанному в сертификате владельцу.

Сертификат усиленной квалифицированной электронной подписи (УКЭП)

Выпускает только аккредитованный удостоверяющий центр. Документ, подписанный УКЭП, действителен для любой организации или ведомства.

Самоподписанный сертификат

Сертификат, изданный самим пользователем, без обращения к удостоверяющему центру. Подходит для тестирования приложения и внутренних задач, но не для юридически значимого документооборота.

Открытый ключ

Ключ проверки электронной подписи. Содержит уникальный код, с помощью которого можно проверить подлинность электронной подписи, а также используется для шифрования в адрес владельца. Сертификат открытого ключа содержит сведения о подписанте (ФИО, СНИЛС и др.), об удостоверяющем центре, который выдал сертификат, и срок действия ключа.

Закрытый ключ

Секретный уникальный набор символов, который формируется криптопровайдером. Закрытый ключ необходим для формирования электронной подписи и для расшифрования, хранится в зашифрованном виде — как правило, на носителе (токене). Доступ к закрытому ключу имеет только владелец.

Запрос на сертификат

Электронный документ, который содержит данные владельца и открытый ключ и передаётся в удостоверяющий центр для получения сертификата электронной подписи.

Ключевой контейнер

Способ хранения закрытых ключей. Кроме ключей, он содержит служебную информацию, необходимую для обеспечения криптографической защиты ключей, их целостности и т. п. Физическое представление ключевого контейнера зависит от типа ключевого носителя: флеш-накопитель, жёсткий диск, смарт-карта, реестр.

Статус сертификата электронной подписи

Информация о действительности сертификата.

Удостоверяющий центр (УЦ)

Доверенная организация, которая имеет право выпускать сертификаты электронной подписи юридическим и физическим лицам.

Корневой сертификат

Цифровой документ, в котором содержится информация об удостоверяющем центре. Корневые сертификаты выдаются только организациям и могут иметь разный уровень. В Российской Федерации главный корневой сертификат принадлежит Министерству цифрового развития. На основе этого сертификата Минцифры России выдаёт удостоверяющим центрам собственные сертификаты, подписывая их своим корневым сертификатом.

Промежуточный сертификат

Сертификат удостоверяющего центра, выпущенный вышестоящим центром. Занимает среднее звено цепочки доверия.

Сертификат другого пользователя

Сертификат, принадлежащий другому пользователю. Предназначен для шифрования документов в его адрес.

Список отзыва сертификатов (CRL)

Подписанный удостоверяющим центром список сертификатов, которые он пометил как отозванные.

OCSP

Протокол проверки статуса сертификата в режиме реального времени — альтернатива загрузке полного списка отзыва.

Цепочка сертификации (цепочка доверия)

Иерархическая последовательность сертификатов. Для квалифицированных сертификатов электронной подписи она, как правило, состоит из трёх звеньев: верхнее — корневой сертификат, среднее — сертификат удостоверяющего центра, конечное — сертификат пользователя. Если цепочку построить не удалось, подпись считается непроверенной.

Отпечаток (thumbprint)

Хэш сертификата, которым его удобно однозначно называть — например, при выборе сертификата в командной строке.

Подпись и шифрование

Электронная подпись (ЭП)

Информация в электронно-цифровой форме для определения и подтверждения личности автора подписи.

Усиленная неквалифицированная электронная подпись (УНЭП)

Цифровой аналог собственноручной подписи. Применяется, если стороны заключили соглашение об этом или так указано в законе. В таких случаях документы, подписанные от руки или с помощью УНЭП, имеют равную юридическую силу.

Усиленная квалифицированная электронная подпись (УКЭП)

Цифровой аналог собственноручной подписи. Ей можно подписывать любые документы без предварительной договорённости с другой стороной.

Криптопровайдер

Провайдер криптографических услуг — специализированный программный модуль или набор модулей, предоставляющих средства шифрования и расшифрования данных, электронной подписи, а также генерации и хранения ключей.

Профили подписи в КриптоАРМ

Заранее подготовленные наборы настроек, которые можно применять для выполнения подписи, архивирования и шифрования. Профили переключаются одним щелчком и попадают в контекстное меню Проводника на Windows.

Алгоритмы подписи

Криптографические алгоритмы, которые используются для создания электронной подписи.

Алгоритмы шифрования

Криптографические алгоритмы, которые используются для шифрования файлов.

Присоединённая подпись

Подпись, в процессе создания которой формируется специальный контейнер, где находятся и подписываемый документ, и сама подпись. Исходный документ извлекается операцией снятия подписи.

Отсоединённая подпись

Файл подписи формируется и хранится отдельно от подписываемого документа. Для проверки нужны оба файла.

Соподпись

Ещё одна подпись, добавленная в существующий файл подписи. Все подписи равноправны и относятся к одному документу.

Формат подписи CAdES

Стандарт усовершенствованной электронной подписи. Такую подпись можно прикрепить к любому типу файла: текстовым документам (`.doc`, `.docx`), электронным таблицам (`.xls`, `.xlsx`), изображениям (`.jpg`, `.png`, `.gif`) и PDF-файлам. Подписи CAdES создаются сертификатами КриптоПро; сертификатом встроенного провайдера OpenSSL подпись создаётся в базовом формате CMS.

Стандарт подписи CAdES-BES (Basic Electronic Signature)

Основной и простейший формат электронной подписи, описываемый в стандарте CAdES. Обеспечивает базовую проверку подлинности данных и защиту их целостности: в подпись вложены сведения о подписанте.

Стандарт подписи CAdES-T (Timestamp)

Формат электронной подписи, в которую автоматически добавляется штамп времени на подпись. Требует адреса службы TSP.

Стандарт подписи CAdES-X Long Type 1

Формат электронной подписи, в которую вложены штамп времени и полные сведения о сертификатах и списках отзыва. Позволяет проверить подпись и после того, как сертификат истечёт.

Стандарт подписи CAdES-A (Archival)

Формат электронной подписи на основе CAdES-X Long Type 1, дополненный архивными штампами времени. Предназначен для долговременного хранения.

Штамп времени (TSP)

Подписанное службой времени подтверждение того, что данные существовали в определённый момент.

Машиночитаемая доверенность (МЧД)

Аналог бумажной доверенности в электронном виде. Она создаётся в формате XML, который позволяет компьютеру прочитать её содержание и подтвердить полномочия того, кто подписал документ от имени организации.

Шифрование в адрес получателя

Файл шифруется на открытых ключах из сертификатов получателей. Расшифровать его сможет только владелец соответствующего закрытого ключа.

keyAgreement

Отметка в сертификате, разрешающая использовать его для обмена ключами при шифровании. Приложение может требовать её у сертификатов получателей — см. Общие настройки.

PAdES

Формат, при котором подпись встраивается в PDF-документ. Встроенная подпись позволяет подписывать электронные документы без изменения формата файла и без создания отдельного файла подписи, как это происходит при использовании присоединённой и отсоединённой подписи. Результат остаётся PDF-файлом, который получатель может проверить.

Видимая подпись PDF-документа

Встроенная подпись, которая отображается на странице документа в виде штампа.

Невидимая подпись PDF-документа

Встроенная подпись, которая визуально на страницах не видна.

Сертификация PDF-документа

Позволяет защитить PDF-документ от изменений путём его подписания электронной подписью с указанием типа изменений, разрешённых для документа. Сертифицирующая подпись должна быть первой в документе.

Область для штампа подписи в PDF-документе

Область на странице PDF-документа, размеченная для видимой подписи. В неё помещает свою подпись следующий подписант.

Произвольная область в PDF-документе

Область для графического изображения или текста. В области можно разместить свой комментарий, статус или отметку о конфиденциальности документа.

Печатная копия со штампом

Копия документа с нарисованным штампом подписи, но без криптографической подписи. Предназначена для печати и визуального контроля.

Конвертация PDF-документа

Преобразование документа к архивному профилю PDF/A-2b или PDF/A-3b. При конвертации удаляются скрипты, формы и прочие элементы, влияющие на безопасность и целостность документа.

OpenPGP

Сертификат OpenPGP

Открытый ключ OpenPGP с идентификаторами пользователя, подключами и заверениями.

Подключ

Дополнительная ключевая пара внутри сертификата OpenPGP, выделенная под конкретную задачу — подпись или шифрование. Подключ можно отозвать, не отзывая сертификат целиком.

Заверение (сертификация)

Подпись, которой один владелец подтверждает принадлежность чужого сертификата его владельцу. Из заверений складывается сеть доверия.

Достоверность и доверие

Достоверность отвечает на вопрос «подтверждена ли принадлежность сертификата владельцу», доверие — «насколько мы полагаемся на заверения этого владельца».

Отзыв

Публикуемое владельцем объявление о том, что сертификат или подключ больше не следует использовать.

ASCII armor

Текстовое представление двоичных данных OpenPGP (файлы `.asc`). Удобно для передачи в теле письма или в мессенджере.

Смотрите также

- О продукте — возможности приложения.
- Криптопровайдеры в КриптоАРМ — какие провайдеры выполняют операции.
- Обзор операций — какой мастер выбрать для задачи.

Открыть статью на сайте

Пошаговая установка КриптоАРМ на Windows

В этом разделе описано, как установить КриптоАРМ на ОС Windows. Вы узнаете, как подготовить систему, установить КриптоАРМ и КриптоПро CSP, а также где найти инструкции по активации лицензий.

Содержание:

- Подготовка к установке
- Установка КриптоАРМ
- Установка КриптоПро CSP
- Активация лицензий
- Обновление
- Удаление КриптоАРМ
- Смотрите также

Подготовка к установке

Перед установкой

1. **Проверьте наличие прав администратора.** Приложение устанавливается для всех пользователей компьютера, поэтому требуются права администратора.
2. **Проверьте разрядность системы.** Приложение поставляется в сборке x64 и требует 64-разрядной Windows 10 или новее.

> 💡 Установщик КриптоАРМ содержит недостающие компоненты — Microsoft Visual C++ Runtime и КриптоПро ЭЦП Runtime (CAdES).

Скачивание установочных файлов

Дистрибутив КриптоАРМ

Скачайте установочный файл с официальных источников:

- Официальный сайт КриптоАРМ
- Сайт компании-разработчика Trusted.ru

Файл установщика называется `cryptoarm-sign-<версия>-win-x64.exe`.

Дистрибутив КриптоПро CSP (при использовании ГОСТ-алгоритмов)

> ⚠️ **Примечание**: КриптоАРМ можно использовать без установки КриптоПро CSP, если ваши сценарии работы не требуют выполнения криптографических операций с алгоритмами ГОСТ.

Скачайте дистрибутив КриптоПро CSP с официального сайта компании ООО «КРИПТО-ПРО» или используйте компакт-диск.

Чтобы загрузить дистрибутив КриптоПро CSP из официального источника:

1. Перейдите на официальный сайт КриптоПро.
2. Пройдите регистрацию или авторизацию.
3. Откроется страница продукта КриптоПро CSP.
4. Нажмите **Скачать**.
5. Ознакомьтесь и согласитесь с лицензионным соглашением.
6. Скачайте дистрибутив в соответствии с установленной операционной системой и её разрядностью.

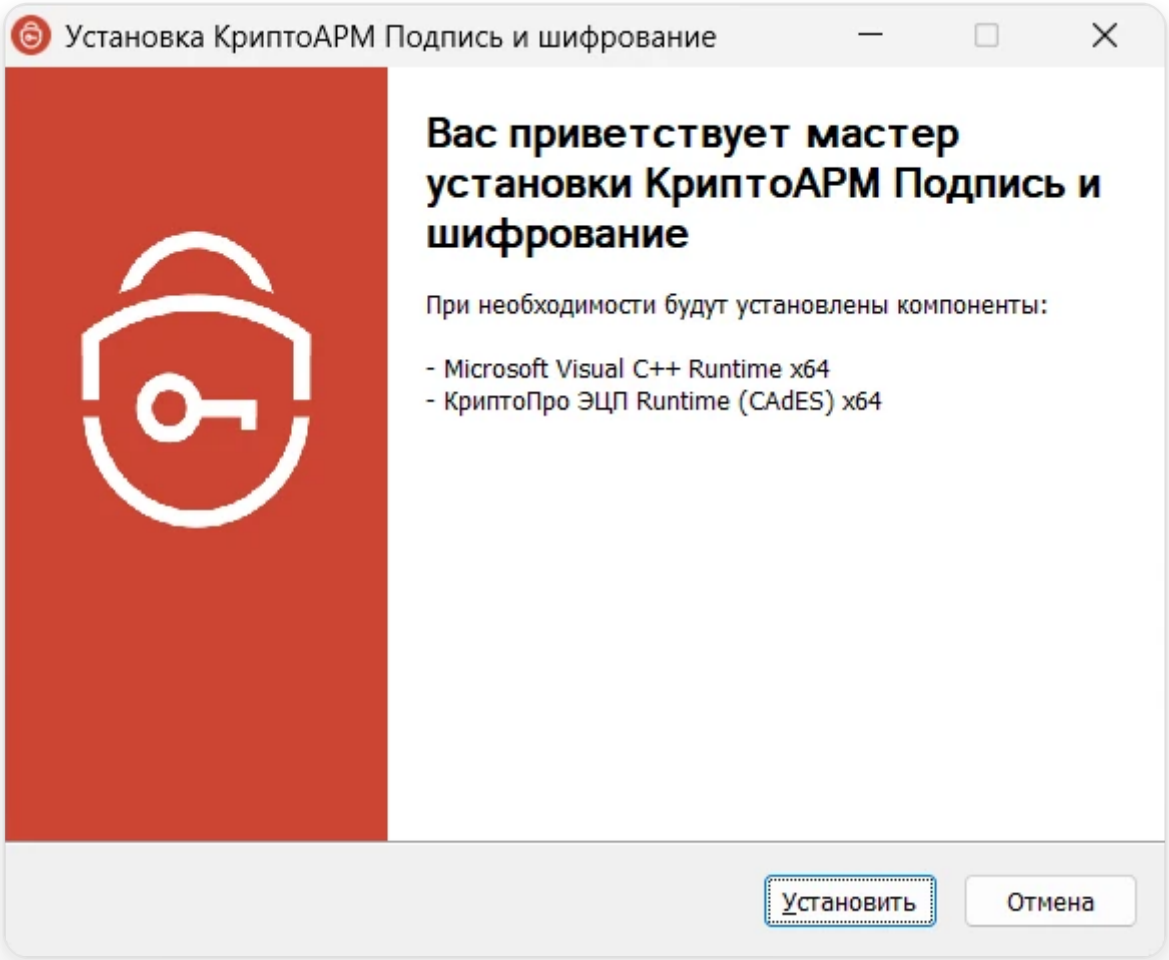
> ⚠️ **Требования к версии**: КриптоАРМ поддерживает КриптоПро CSP версии 5.0 и выше.

Установка КриптоАРМ

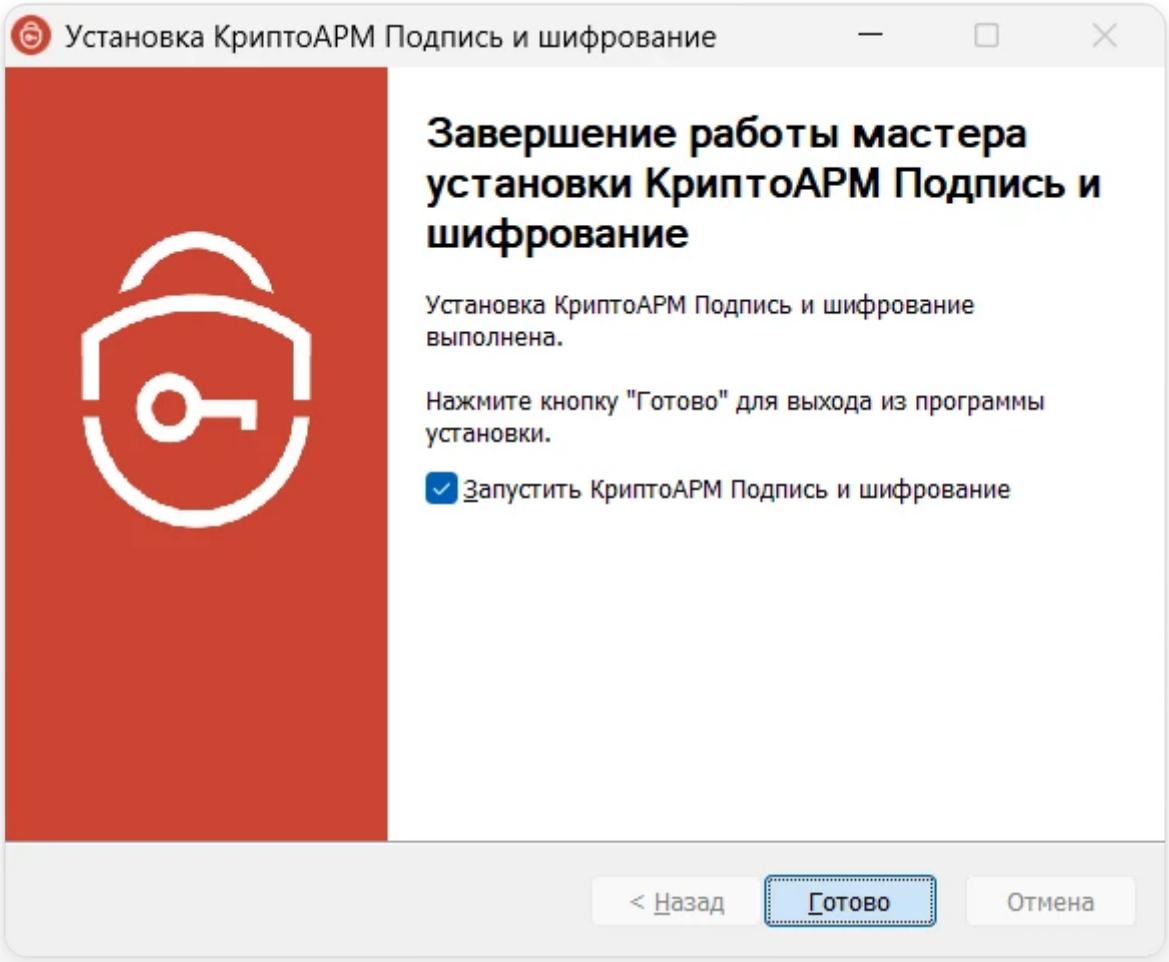
1. Запустите скачанный файл установщика.

2. Откроется страница приветствия. На ней перечислены компоненты, которые будут установлены при необходимости:

- Microsoft Visual C++ Runtime x64,
- КриптоПро ЭЦП Runtime (CAdES) x64.



1. Нажмите **Установить** и дождитесь окончания установки.
2. Закройте окно установки по кнопке **Готово**. Отметка **Запустить КриптоАРМ Подпись и шифрование** включена: снимите её, если открывать приложение сейчас не нужно.



> 💡 **Примечание**: установщик не задаёт вопросов о языке и каталоге. Язык окон он берёт из языка системы, а приложение ставит для всех пользователей в `C:\Program Files\cryptoarm-sign`.

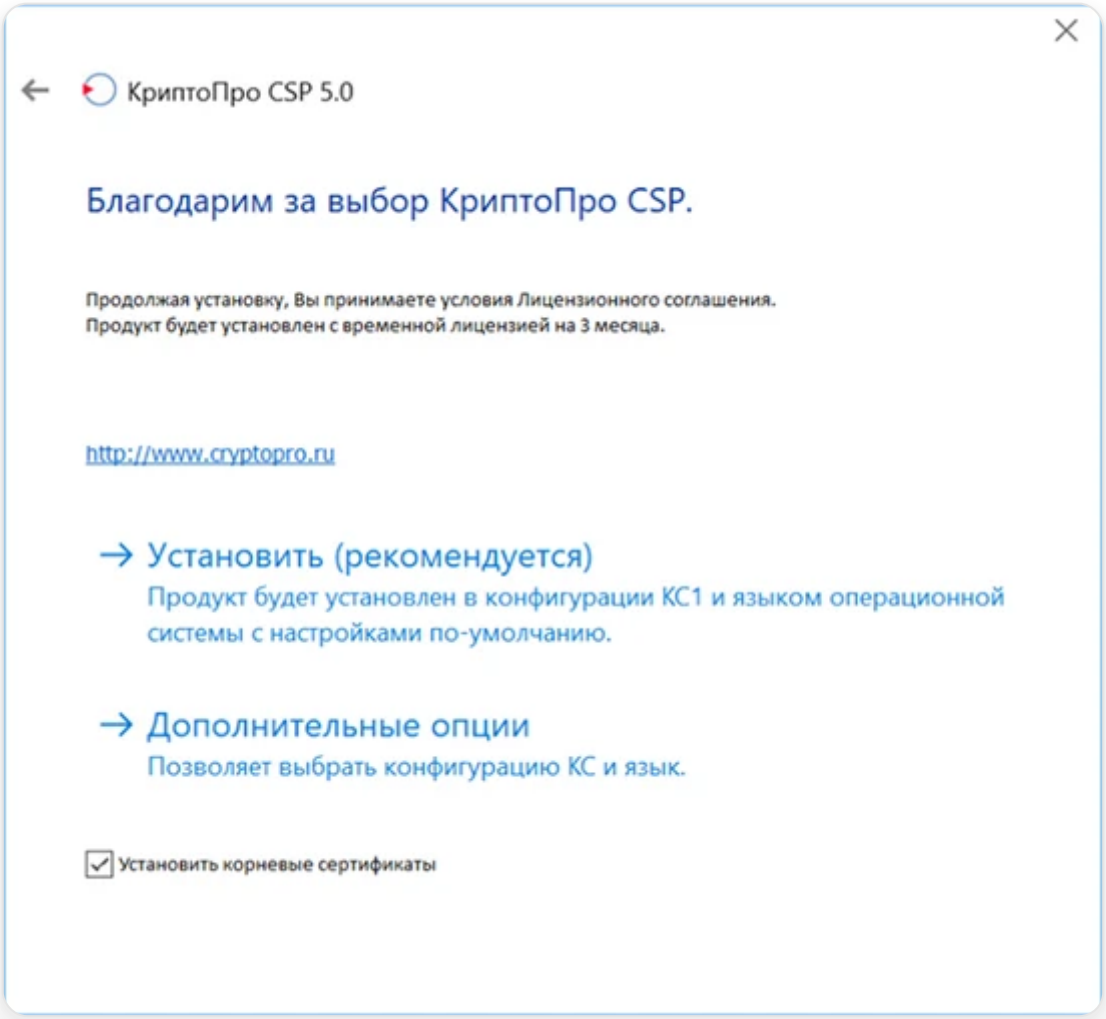
Установка КриптоПро CSP

КриптоПро CSP в дистрибутив КриптоАРМ не входит и устанавливается отдельно. Он нужен, чтобы подписывать и расшифровывать файлы ГОСТ-сертификатами и работать с аппаратными носителями.

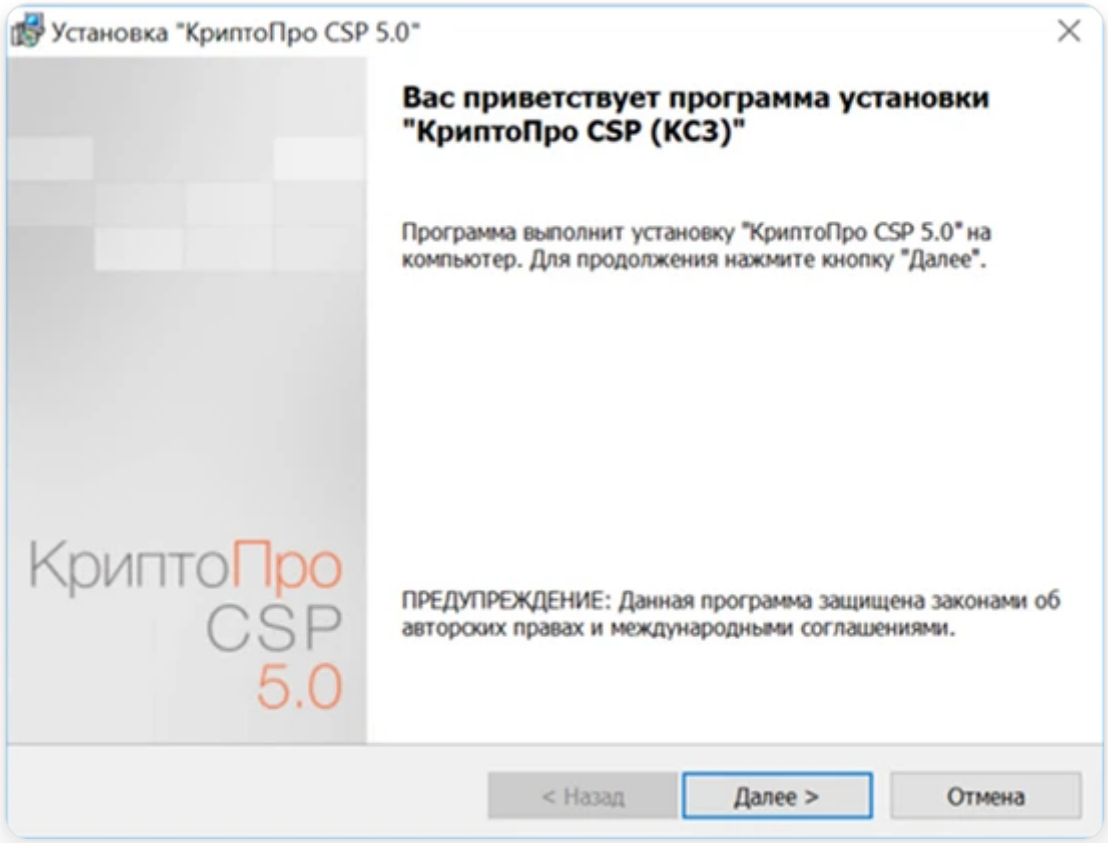
1. Запустите скачанный дистрибутив КриптоПро CSP. Если используется компакт-диск, в стартовом меню диска выберите систему и язык установки.



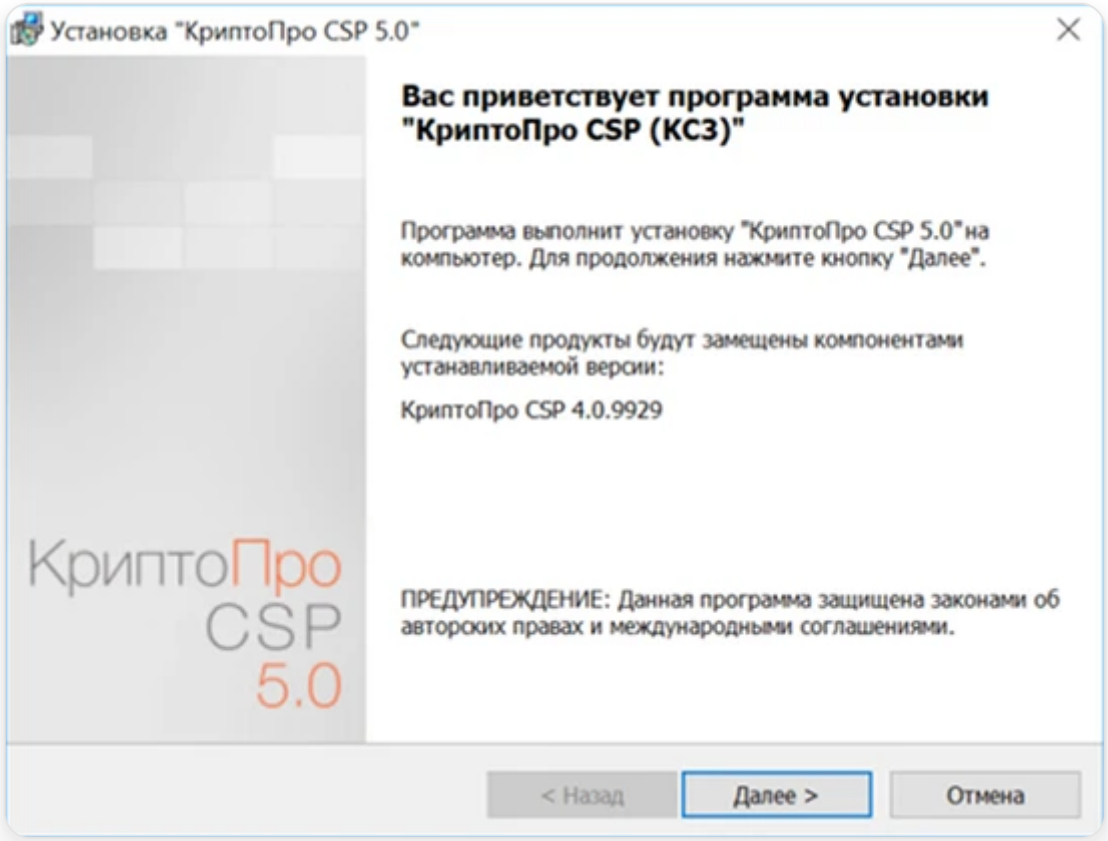
1. Откроется приветственное окно мастера установки КриптоПро CSP. Для изменения уровня класса защиты или языка установки нажмите кнопку **Дополнительные опции**.



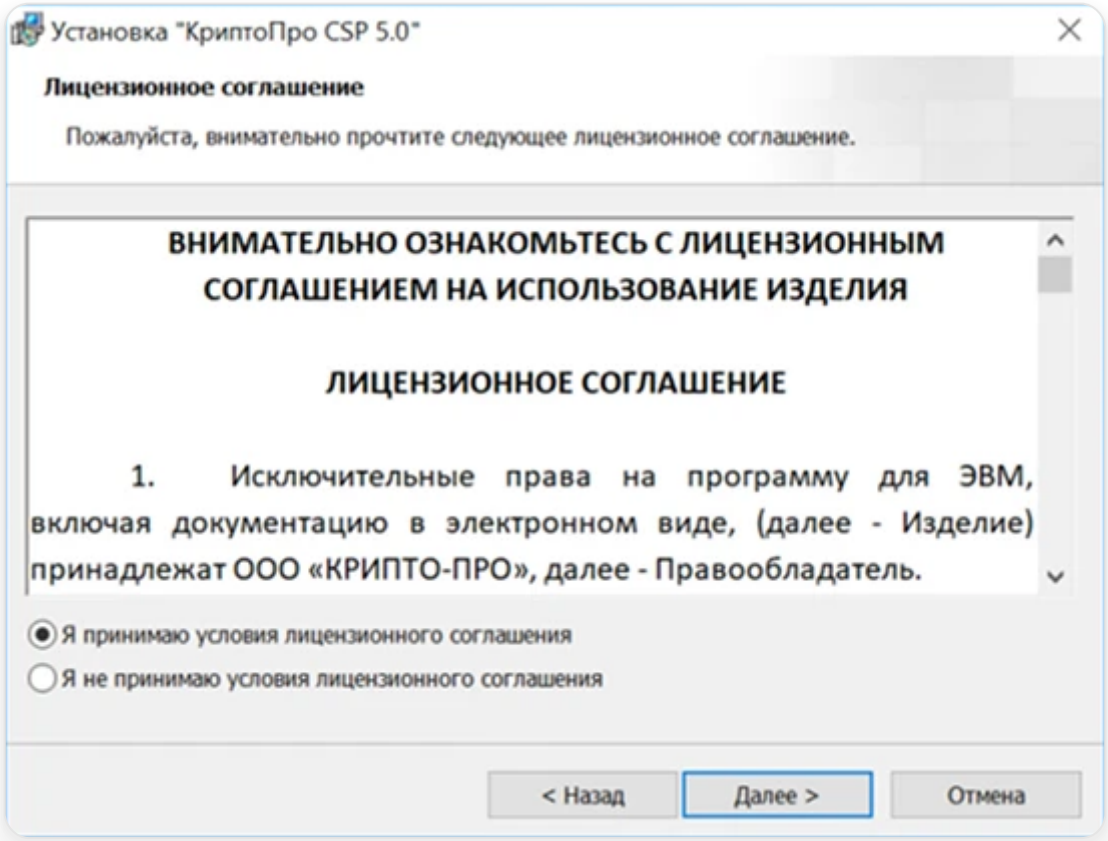
1. Последующая установка производится в соответствии с сообщениями, выдаваемыми программой установки. В процессе установки будет предложено зарегистрировать дополнительные считыватели ключевой информации, дополнительные датчики случайных чисел или настроить криптопровайдер на использование дополнительной защиты. Для продолжения установки нажмите **Далее**.



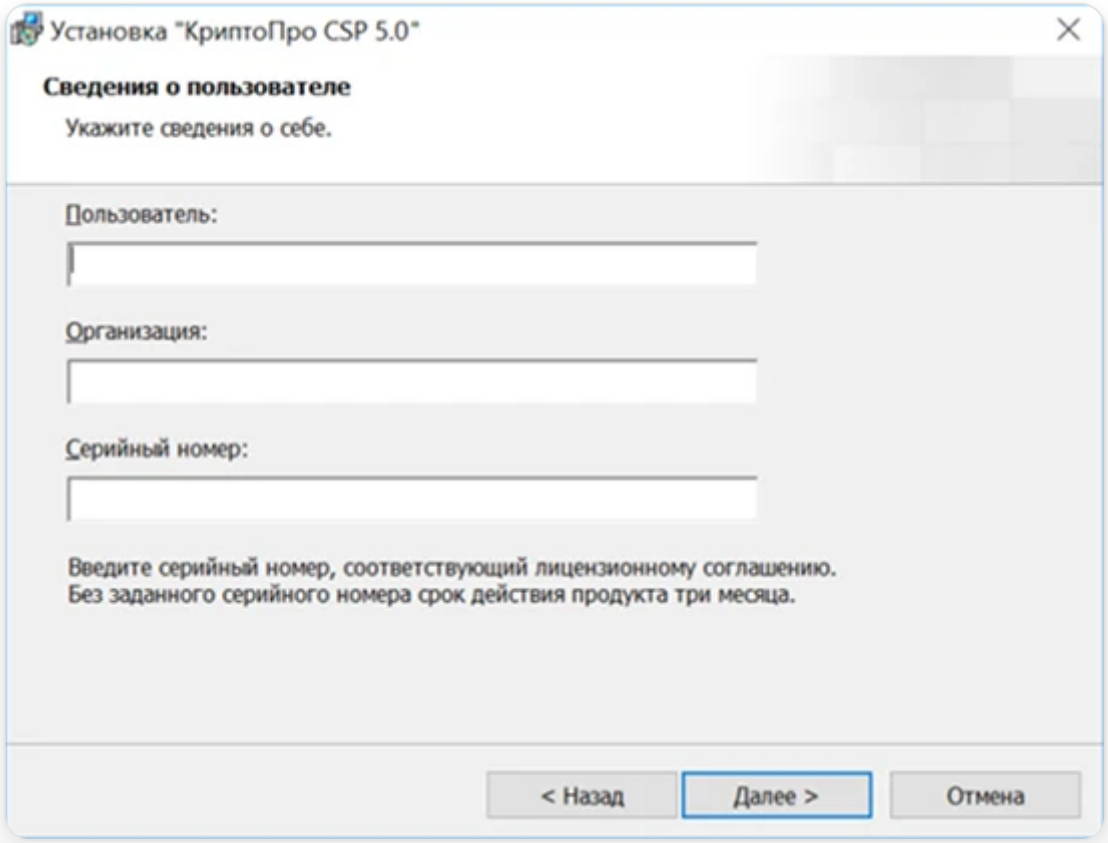
1. Если в системе была установлена более ранняя версия КриптоПро CSP, то в окне установки появится информация о текущей версии. Для продолжения установки нажмите **Далее**.



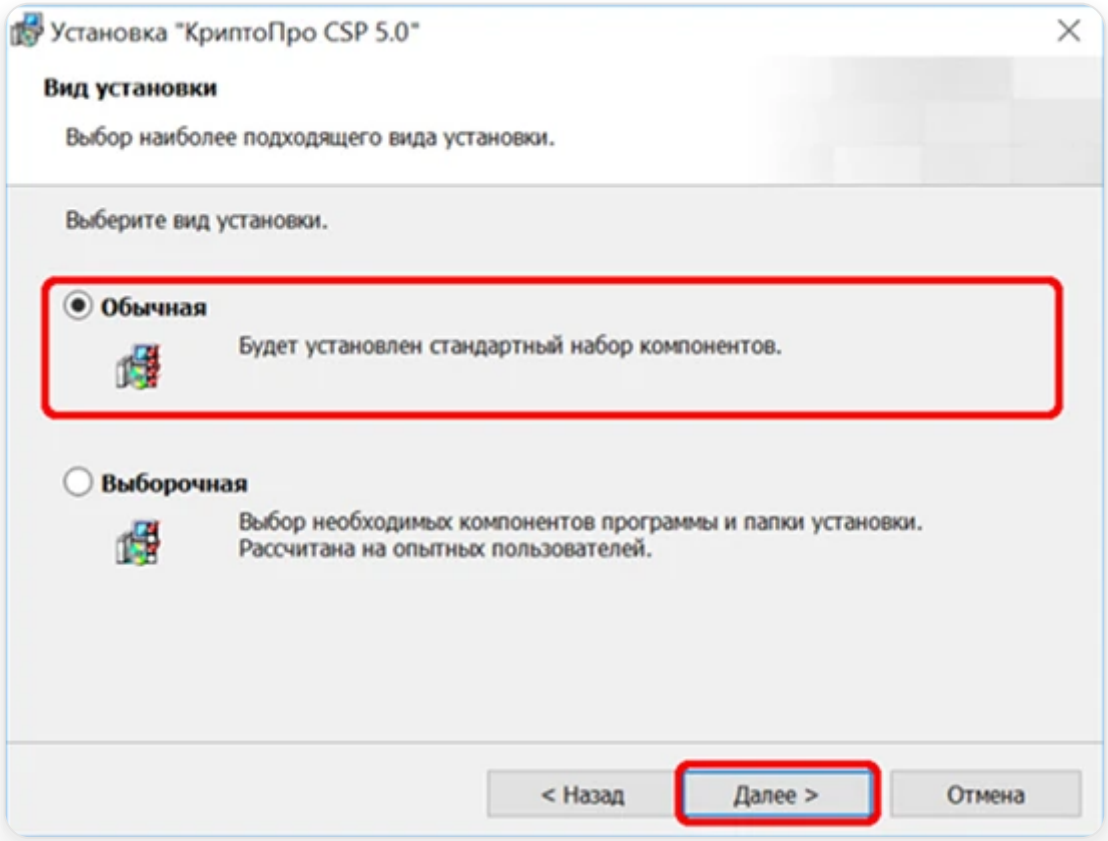
1. Внимательно ознакомьтесь с лицензионным соглашением. Выберите опцию **Я принимаю условия лицензионного соглашения** и нажмите **Далее** для продолжения установки.



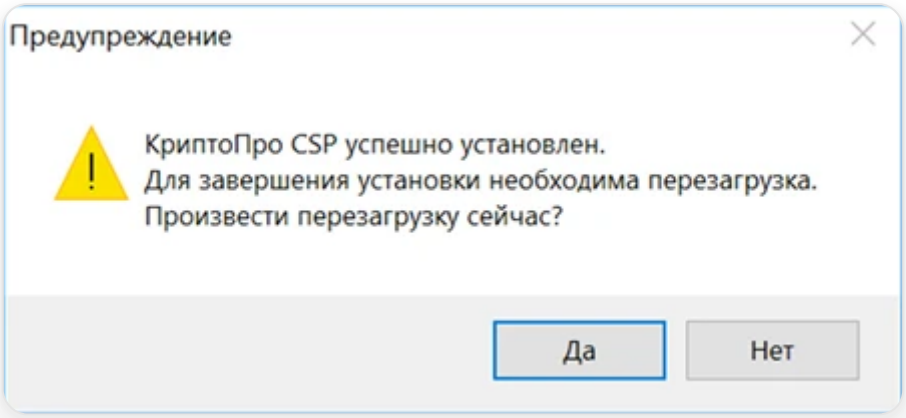
1. В окне сведений о пользователе можно ввести данные о пользователе, организации и серийный номер лицензии. Эти данные можно ввести позже в процессе работы с программой. Для продолжения установки нажмите **Далее**.



1. Выберите тип установки — **Обычная** (стандартный набор компонентов) и нажмите **Далее**.



1. Дождитесь окончания установки.
2. После успешной установки криптопровайдера выполните перезагрузку системы.



Активация лицензий

Для выполнения криптографических операций с алгоритмами ГОСТ необходимо активировать лицензию КриптоАРМ.

Инструкции по активации лицензий:

- Активация лицензии КриптоАРМ — ввод лицензионного ключа приложения;
- Лицензии КриптоПро — только при использовании CSP. Установка серийных номеров КриптоПро CSP, TSP Client и OCSP Client через интерфейс КриптоАРМ.

При первом запуске КриптоАРМ автоматически активируется **30-дневная пробная лицензия**, которая позволяет полностью ознакомиться со всеми возможностями приложения и протестировать работу криптографических операций с российскими алгоритмами ГОСТ.

При первой установке криптопровайдера КриптоПро CSP может быть активирована ознакомительная лицензия (обычно сроком до 90 дней).

> 💡 Пробный период КриптоАРМ и ознакомительная лицензия КриптоПро CSP действуют независимо друг от друга.

Обновление

Приложение само проверяет наличие новой версии и обновляется с вашего одобрения: в разделе **Настройки → О программе** появляется строка «Доступна версия», а установка запускается кнопкой **Установить и перезапустить** — см. Проверка обновлений.

Новую версию можно поставить и вручную — тем же установщиком поверх предыдущей. Настройки, профили и журнал сохраняются.

Удаление КриптоАРМ

Через стандартный интерфейс Windows

1. Откройте **Параметры Windows** → **Приложения** (или **Панель управления** → **Программы и компоненты**).
2. Найдите в списке **КриптоАРМ Подпись и шифрование**.
3. Нажмите **Удалить**.
4. Дождитесь завершения процесса.

При удалении программа снимает свои регистрации в системе, а ярлык приложения исчезает из меню **Пуск**.

Очистка остаточных файлов

Каталог данных приложения при удалении не стирается. Удалите его вручную, если необходимо полностью очистить систему:

```
%APPDATA%\cryptoarm-sign
```

> ⚠️ **Важно**: в каталоге данных находятся зашифрованные закрытые ключи OpenPGP. Удаляйте его, только если сохранили резервные копии ключей.

Смотрите также

- Активация лицензии — ввод лицензионного ключа.
- Быстрый старт — подготовка к первой операции.
- Контекстное меню Проводника — операции без открытия приложения.
- Криптопровайдеры в КриптоАРМ — какие провайдеры выполняют операции.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Пошаговая установка КриптоАРМ на Linux

В этом разделе описано, как установить КриптоАРМ на ОС Linux из пакетов `.deb` и `.rpm`. Вы узнаете, как подготовить систему, установить КриптоАРМ и КриптоПро CSP, а также где найти инструкции по активации лицензий.

Содержание:

- Подготовка к установке
- Установка КриптоАРМ
- Установка КриптоПро CSP
- Активация лицензий
- Обновление
- Удаление КриптоАРМ
- Смотрите также

Подготовка к установке

Перед установкой

Права администратора

Проверьте наличие прав суперпользователя (`root`) или возможности использовать `sudo`. Для установки КриптоАРМ и связанных компонентов требуются соответствующие привилегии на компьютере.

Скачивание установочных файлов

Дистрибутив КриптоАРМ

Скачайте установочный файл КриптоАРМ с официальных источников:

- Официальный сайт КриптоАРМ
- Сайт компании-разработчика Trusted.ru

Выберите пакет по системе управления пакетами вашего дистрибутива:

Файл	Дистрибутивы
`cryptoarm-sign_<версия>_amd64.deb`	Astra Linux, Ubuntu и другие системы с `apt`
`cryptoarm-sign-<версия>.x86_64.rpm`	Альт, РЕД ОС, РОСА и другие системы с rpm

Дистрибутив КриптоПро CSP (при использовании ГОСТ-алгоритмов)

> ⚠️ **Примечание**: КриптоАРМ можно использовать без установки КриптоПро CSP, если ваши сценарии работы не требуют выполнения криптографических операций с алгоритмами ГОСТ.

Скачайте дистрибутив КриптоПро CSP с официального сайта компании ООО «КРИПТО-ПРО» или используйте компакт-диск.

Чтобы загрузить дистрибутив КриптоПро CSP из официального источника:

1. Перейдите на официальный сайт КриптоПро.
2. Пройдите регистрацию или авторизацию.
3. Откроется страница продукта КриптоПро CSP.
4. Нажмите **Скачать**.
5. Ознакомьтесь и согласитесь с лицензионным соглашением.
6. Скачайте дистрибутив в соответствии с установленной операционной системой и её разрядностью.

> ⚠️ **Требования к версии**: КриптоАРМ поддерживает КриптоПро CSP версии 5.0 и выше.

Для создания подписей со штампом времени или усовершенствованной подписи необходимо установить библиотеки поддержки модулей TSP и OCSP. Дистрибутив КриптоПро CSP не содержит пакетов TSP и OCSP. Эти модули доступны в составе КриптоПро ЭЦП SDK для Linux, который необходимо скачать отдельно.

Установка КриптоАРМ

Установка DEB-пакета

Через терминал

1. Откройте терминал.
2. Выполните команду для установки пакета:

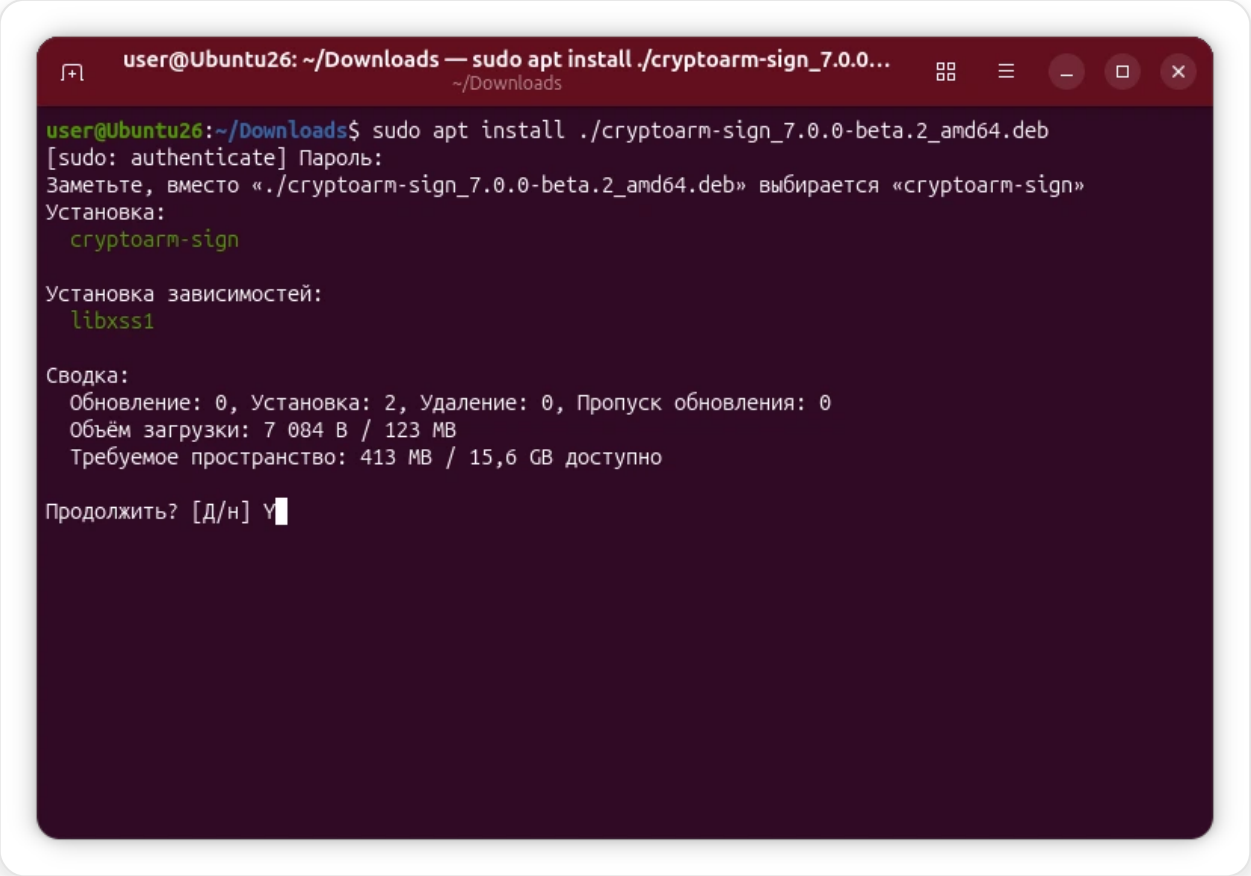
- Если вы находитесь в той же папке, что и пакет:

```
sudo apt install ./cryptoarm-sign_<версия>_amd64.deb
```

- Если пакет находится в другой папке:

```
sudo apt install /{путь_до_файла}/cryptoarm-sign_<версия>_amd64.deb
```

1. Введите пароль администратора, а когда `apt` покажет список устанавливаемых пакетов — подтвердите установку: `Д` (`Y`) и **Enter**.

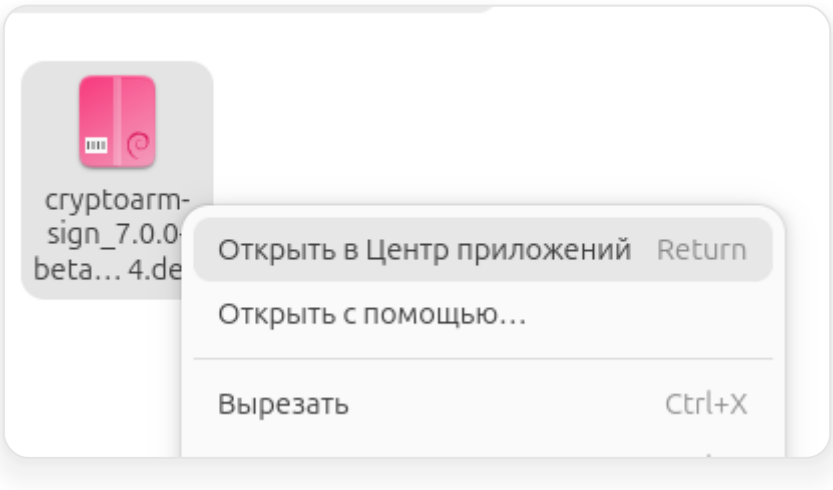


1. Дождитесь окончания установки.

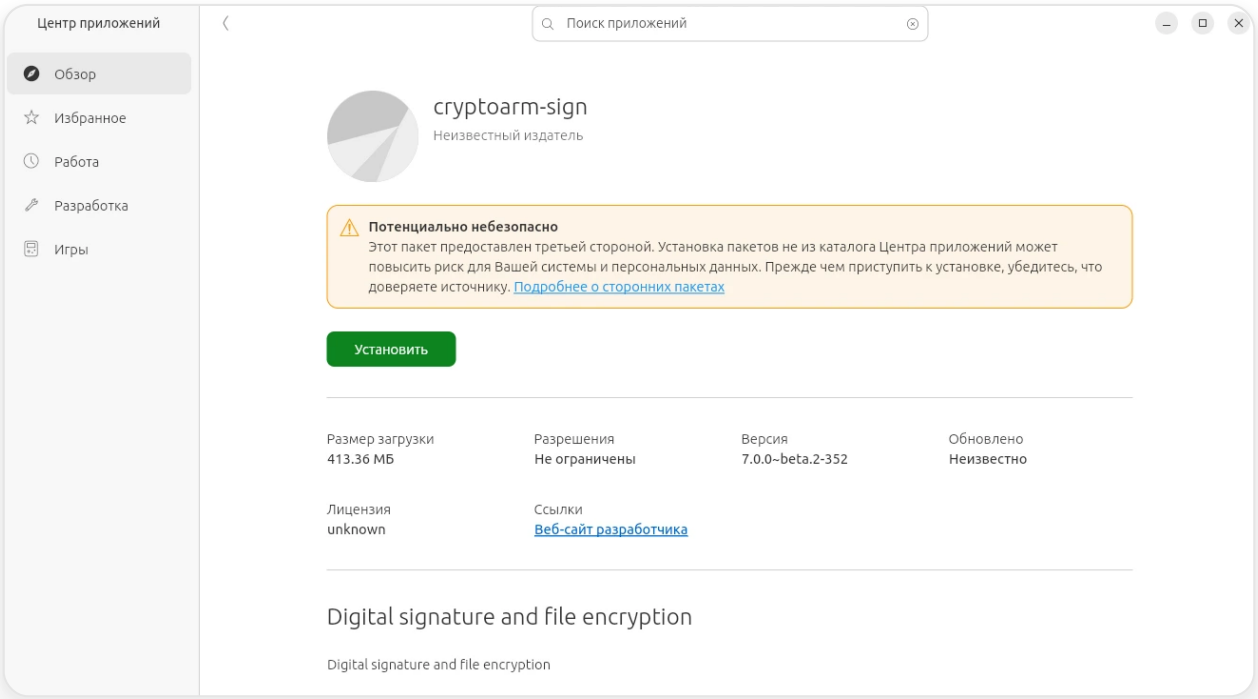
> 💡 **Примечание**: `apt` устанавливает пакет вместе с недостающими зависимостями. Команда `sudo dpkg -i` тоже установит приложение, но зависимости придётся доустанавливать отдельно командой `sudo apt install -f`.

Через графический интерфейс

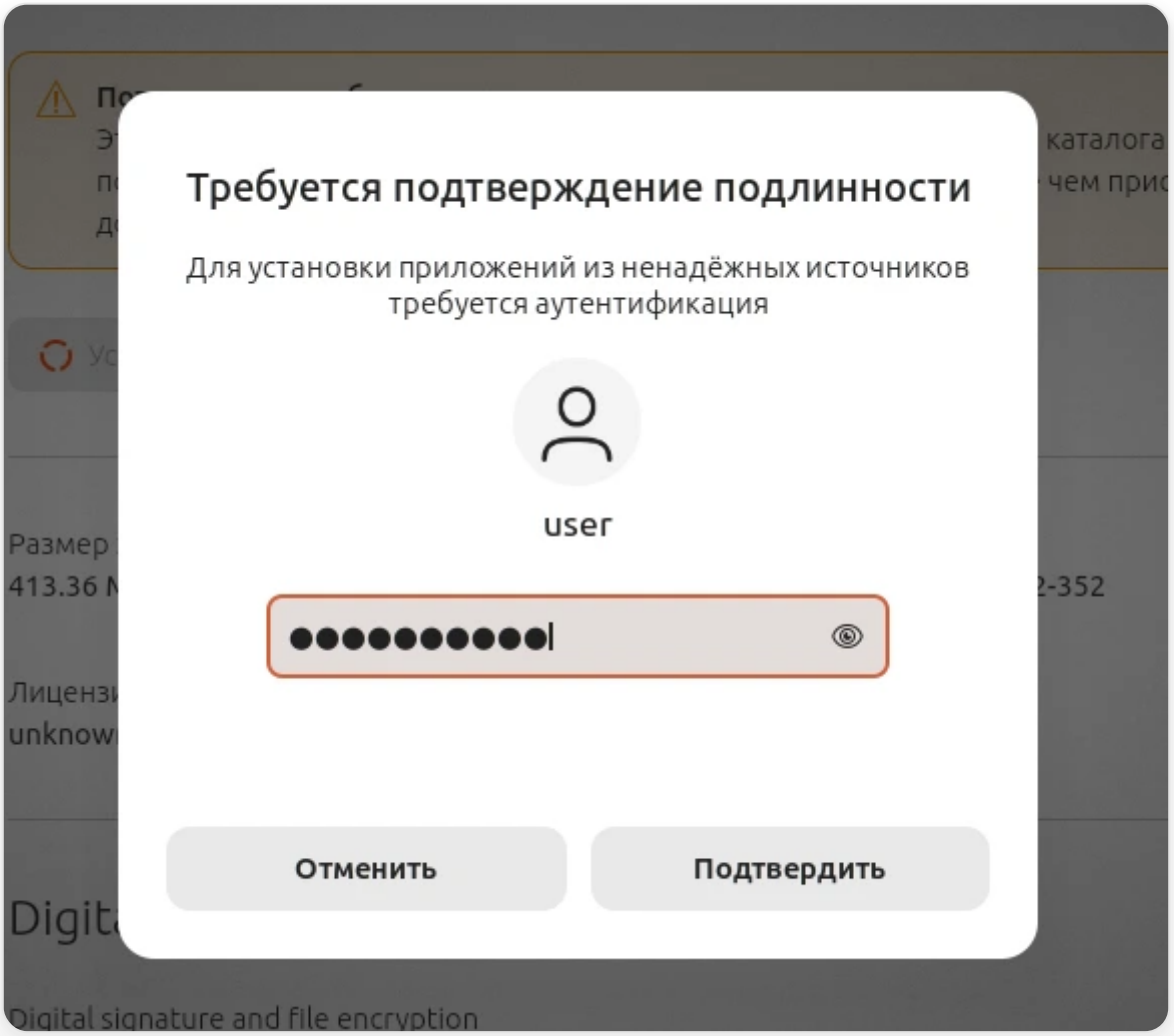
1. Дважды щёлкните по файлу `.deb` или откройте его через установщик пакетов — например, в Ubuntu это Центр приложений.



1. Нажмите **Установить**.



1. При необходимости укажите пароль администратора.



1. Дождитесь окончания установки и закройте окно установщика.

Установка RPM-пакета

Через терминал

1. Откройте терминал.
2. Выполните команду для установки пакета:

- Если вы находитесь в той же папке, что и пакет:

```
sudo apt-get install ./cryptoarm-sign-<версия>.x86_64.rpm # Альт
sudo dnf install ./cryptoarm-sign-<версия>.x86_64.rpm     # РЕД ОС, РОСА и другие системы
с dnf
```

- Если пакет находится в другой папке:

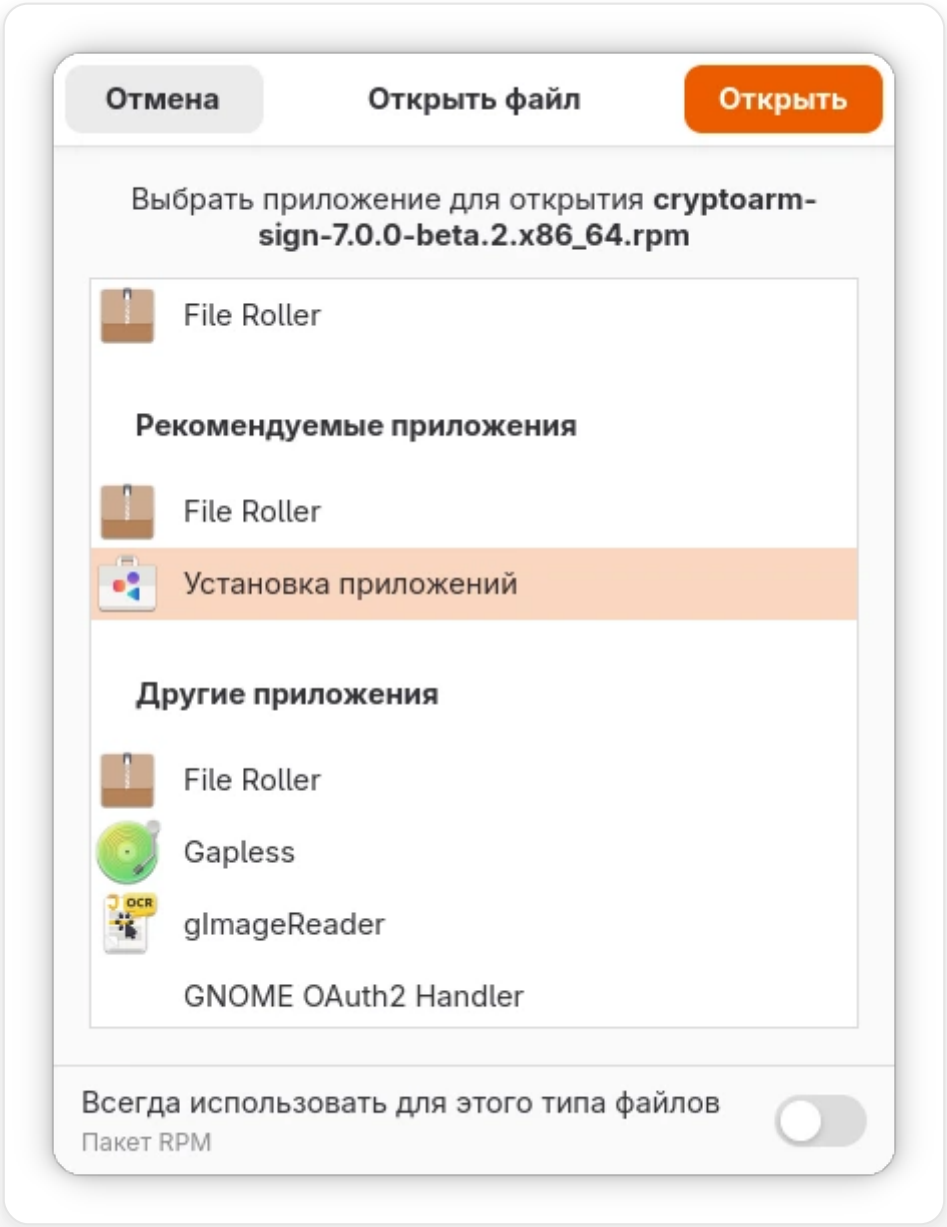
```
sudo apt-get install /{путь_до_файла}/cryptoarm-sign-<версия>.x86_64.rpm # Альт
sudo dnf install /{путь_до_файла}/cryptoarm-sign-<версия>.x86_64.rpm     # РЕД ОС, РОСА
```

1. Дождитесь окончания установки.

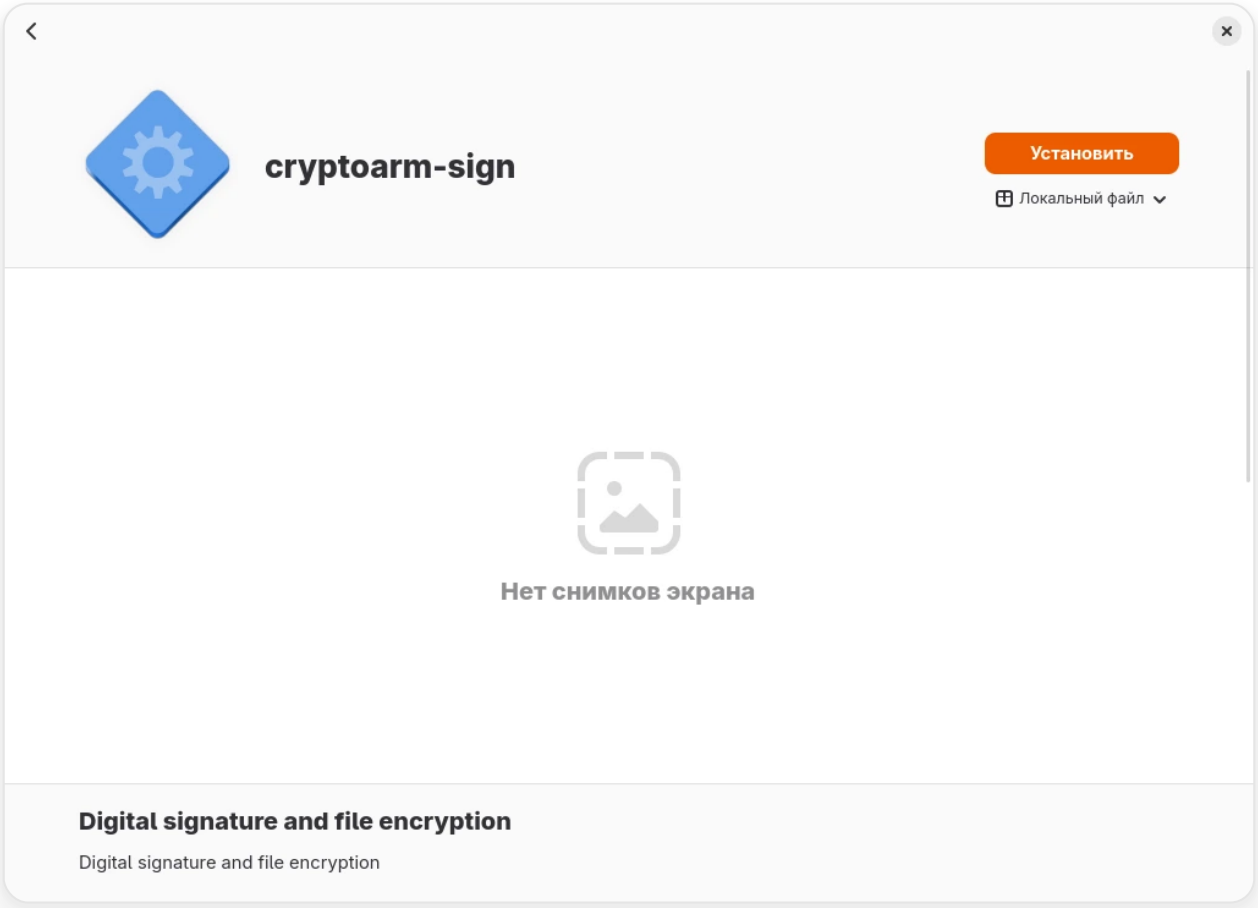
> 💡 **Примечание**: если менеджера пакетов в системе нет, пакет ставится командой `sudo rpm -i ./cryptoarm-sign-<версия>.x86_64.rpm`. Она не подтягивает зависимости: при сообщении о недостающих библиотеках установите их средствами дистрибутива и повторите команду.

Через графический интерфейс

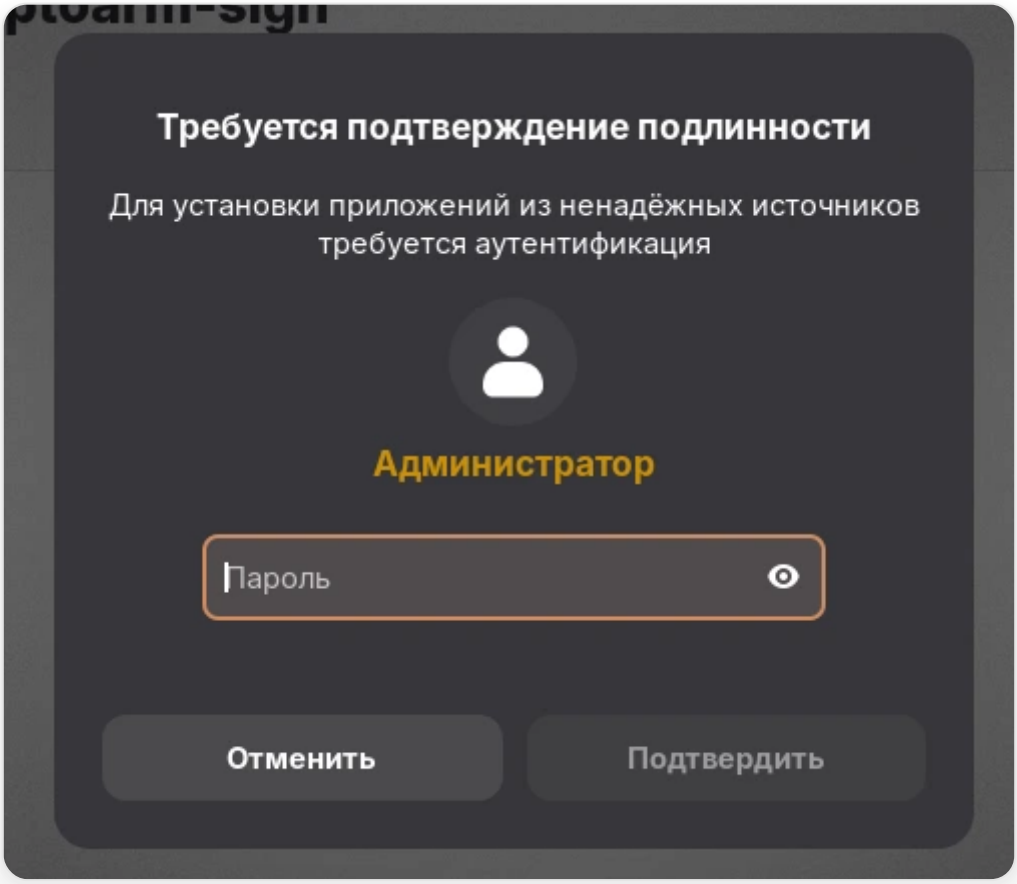
1. Откройте установочный файл `.rpm` через установщик пакетов — например, в Альт это «Установка приложений».



1. Нажмите на кнопку **Установить**.



1. При необходимости укажите пароль администратора.



1. Дождитесь окончания установки.

После установки

По умолчанию приложение устанавливается в каталог `/opt/CryptoARM Sign and Encrypt/` и появляется в меню системы под именем **КриптоАРМ Подпись и шифрование**. Запустить его можно и из терминала:

```
"/opt/CryptoARM Sign and Encrypt/cryptoarm-sign"
```

Установка КриптоПро CSP

1. Если дистрибутив скачан в формате `.tgz`, его необходимо распаковать. Сделать это можно двумя способами — через графический интерфейс или в терминале.

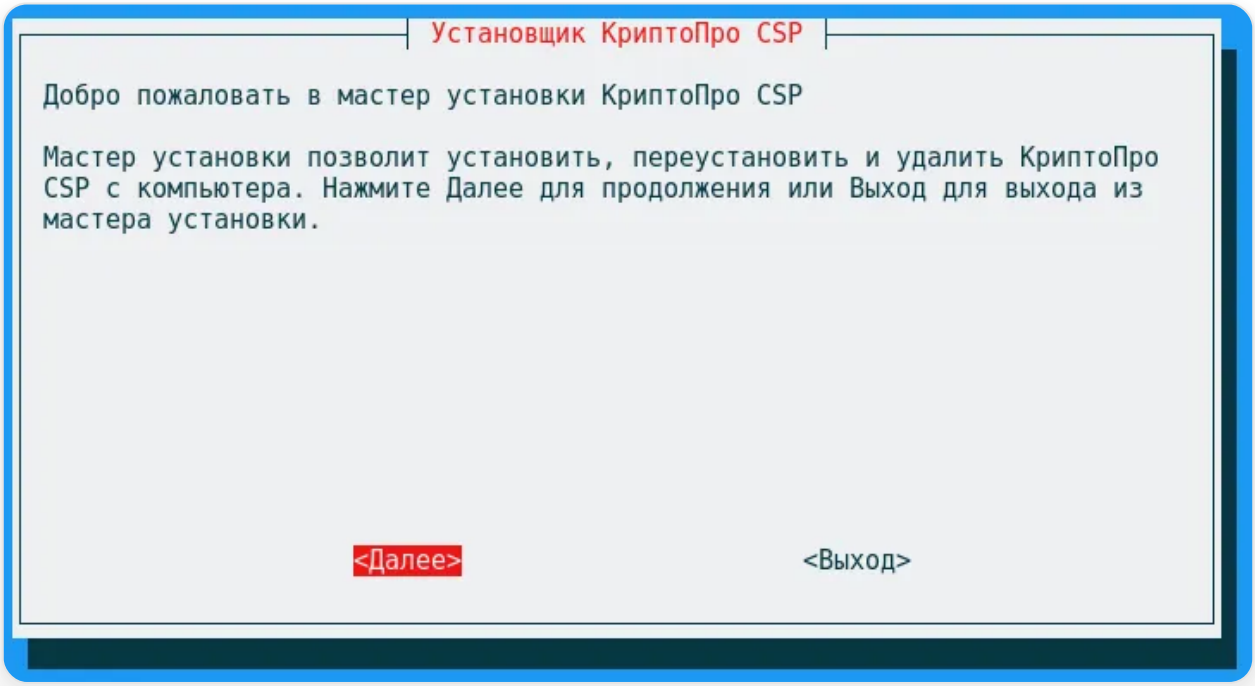
- Найдите архив в файловом менеджере и нажмите на него правой кнопкой мыши. Выберите пункт **Распаковать в эту папку** / **Извлечь здесь**.
- Выполните команду в терминале:

```
tar -xzf имя_пакета.tgz # Распаковка в текущую директорию
tar -xzf имя_пакета.tgz -C /{путь_до_файла}/ # Распаковка в указанную директорию
```

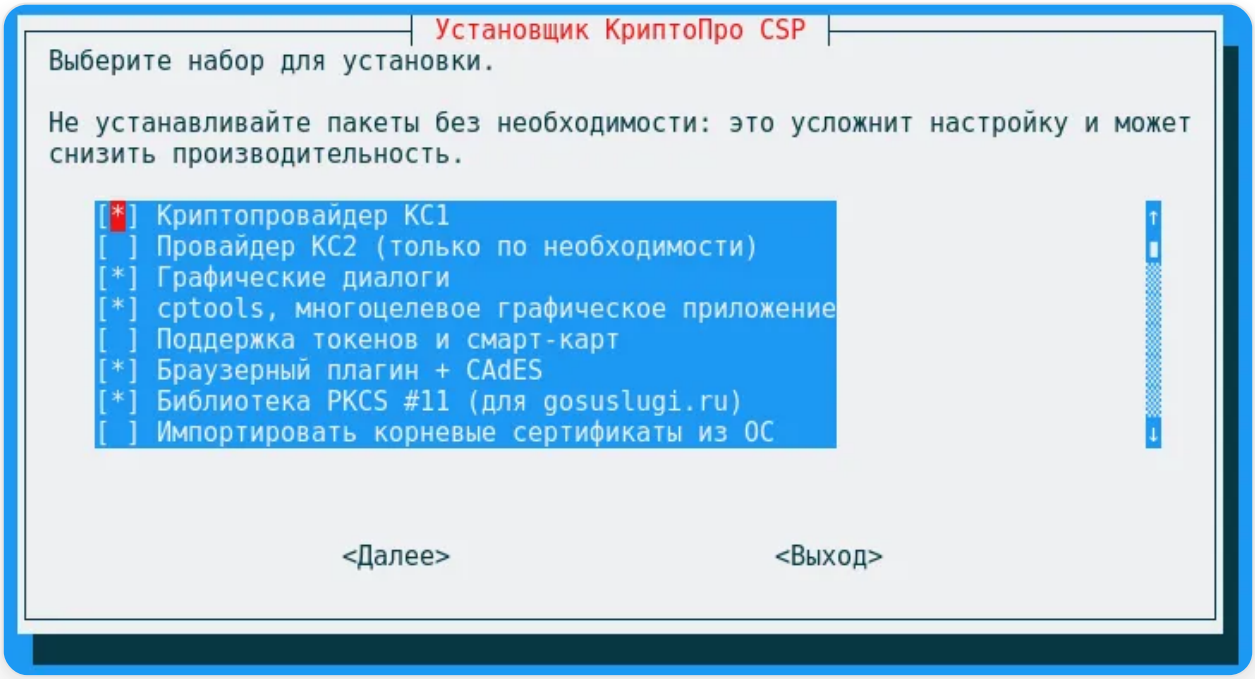
1. Запустите установщик по команде:

```
/{путь_до_файла}/install_gui.sh # Запуск графического установщика
/{путь_до_файла}/install.sh # Без графического установщика
```

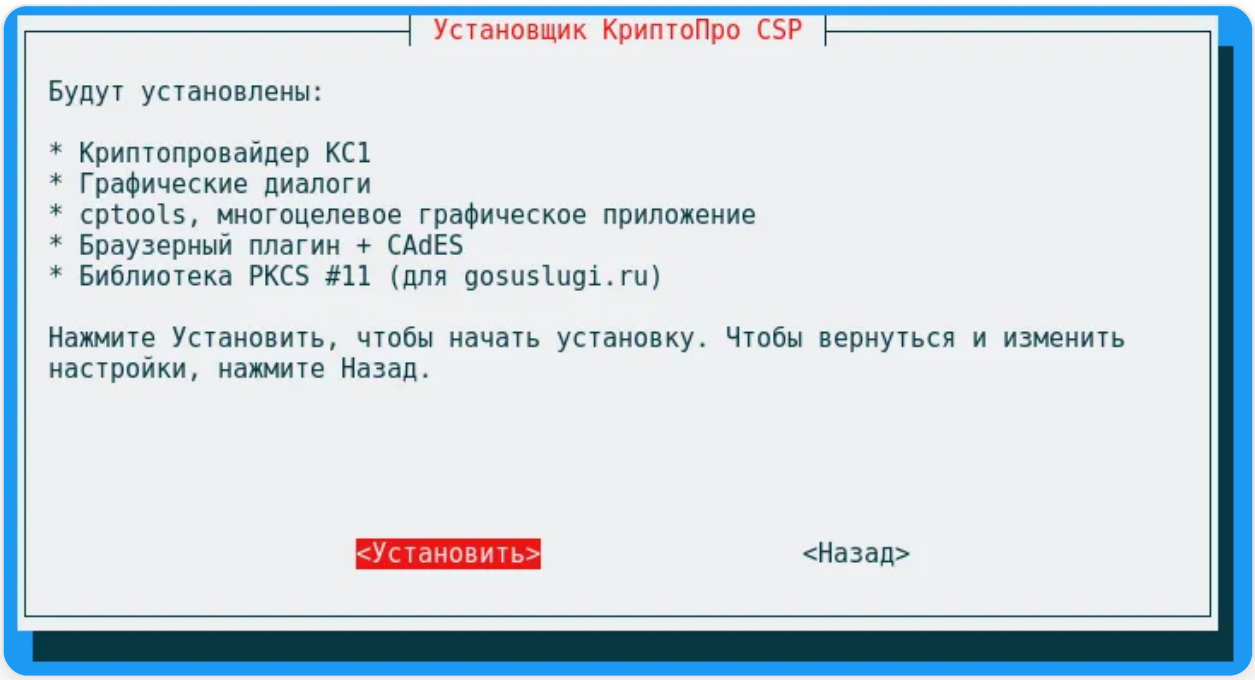
1. Если запущена графическая установка, нажмите **Далее** в открывшемся окне.



1. Выберите все дополнительные пакеты, кроме «Провайдер КС2», и снова нажмите **Далее**.



1. Подтвердите установку и дождитесь её окончания.



1. Закройте установщик.

> 📌 По умолчанию CSP устанавливается в `/opt/cprocsp/`.

После установки КриптоПро CSP перезапустите КриптоАРМ, чтобы приложение увидело провайдер.

Установка пакета для графического интерфейса ввода пароля

Для работы с контейнерами закрытых ключей требуется ввод пароля.

Установите пакет для графического интерфейса диалога ввода пароля, запустив в терминале команду:

```
sudo dpkg -i /<путь_до_файла>/cprocsp-rdr-gui-<...>.deb
```

Установка пакетов для работы с ключевыми носителями

> ⚠️ **Примечание**: для работы с ключевыми носителями в deb-based системе должны быть установлены библиотека `libccid` не ниже 1.3.11, пакеты `pcscd` и `libpcsclite1`.

1. Установите пакеты и драйверы для работы с ключевыми носителями с помощью команд в терминале:

```
sudo dpkg -i <путь_до_файла>/cprocsp-rdr-pcsc-<...>.deb
```

1. Для ключевого носителя **Рутокен**:

```
sudo dpkg -i <путь_до_файла>/cprocsp-rdr-rutoken-<...>.deb
sudo dpkg -i <путь_до_файла>/ifd-rutokens_<...>.deb
```

1. Для ключевого носителя **JaCarta**:

```
sudo dpkg -i <путь_до_файла>/cprocsp-rdr-jacarta-<...>.deb
```

1. Для ключевого носителя **ESMART**:

```
sudo dpkg -i <путь_до_файла>/cprocsp-rdr-esmart-<...>.deb
```

Установка модулей TSP и OCSP

Для создания подписи со штампом времени или усовершенствованной подписи необходимо установить библиотеки поддержки модулей TSP и OCSP:

1. Скачайте КриптоПро ЭЦП SDK 2.0.
2. Распакуйте архив.
3. Установите пакет:

```
sudo dpkg -i <путь_до_файла>/cprocsp-pki-<версия>-amd64-cades.deb
```

> 💡 Для создания обычной подписи без штампа времени установка этих модулей не обязательна.

Установка лицензий КриптоПро через терминал

> 💡 Установить лицензии можно и в приложении — см. Лицензии КриптоПро.

1. Откройте терминал.
2. Введите лицензию КриптоПро CSP командой:

```
sudo /opt/cprocsp/sbin/amd64/cpconfig -license -set <серийный_номер>
```

1. Введите лицензию на модуль TSP командой:

```
sudo /opt/cprocsp/bin/amd64/tsputil license -s <серийный_номер>
```

1. Введите лицензию на модуль OCSP командой:

```
sudo /opt/cprocsp/bin/amd64/ocsputil license -s <серийный_номер>
```

> ⚠️ **Примечание**: серийный номер вводится с учётом регистра символов.

Активация лицензий

Для выполнения криптографических операций с алгоритмами ГОСТ необходимо активировать лицензию КриптоАРМ.

Инструкции по активации лицензий:

- Активация лицензии КриптоАРМ — ввод лицензионного ключа приложения;
- Лицензии КриптоПро — только при использовании CSP. Установка серийных номеров КриптоПро CSP, TSP Client и OCSP Client через интерфейс КриптоАРМ.

При первом запуске КриптоАРМ автоматически активируется **30-дневная пробная лицензия**, которая позволяет полностью ознакомиться со всеми возможностями приложения и протестировать работу криптографических операций с российскими алгоритмами ГОСТ.

При первой установке криптопровайдера КриптоПро CSP может быть активирована ознакомительная лицензия (обычно сроком до 90 дней).

> 💡 Пробный период КриптоАРМ и ознакомительная лицензия КриптоПро CSP действуют независимо друг от друга.

Обновление

Приложение само проверяет наличие новой версии и обновляется с вашего одобрения: в разделе **Настройки → О программе** появляется строка «Доступна версия», а установка запускается кнопкой **Установить и перезапустить** — см. Проверка обновлений.

Новую версию можно поставить и вручную — той же командой, что и первую установку: пакет заменит предыдущую версию. Настройки, профили и журнал сохраняются.

Удаление КриптоАРМ

DEB-пакеты

1. Откройте терминал.
2. Выполните команду:

```
sudo apt remove cryptoarm-sign        # удаление приложения
sudo dpkg -P cryptoarm-sign           # полное удаление с настройками пакета
```

RPM-пакеты

1. Откройте терминал и при необходимости переключитесь на `root`.
2. Выполните команду:

```
sudo dnf remove cryptoarm-sign        # системы с dnf
sudo rpm -e cryptoarm-sign            # удаление только приложения
```

Очистка остаточных файлов

Каталог данных приложения при удалении не стирается. Удалите его вручную, если необходимо полностью очистить систему:

```
rm -rf ~/.config/cryptoarm-sign
```

> ⚠️ **Важно**: в каталоге данных находятся зашифрованные закрытые ключи OpenPGP. Удаляйте его, только если сохранили резервные копии ключей.

Смотрите также

- Активация лицензии — ввод лицензионного ключа.
- Быстрый старт — подготовка к первой операции.
- Выполнение операций в командной строке — работа без графического интерфейса.
- Криптопровайдеры в КриптоАРМ — какие провайдеры выполняют операции.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Пошаговая установка КриптоАРМ на macOS

В этом разделе описано, как установить КриптоАРМ на ОС macOS. Вы узнаете, как выбрать сборку под свой процессор, установить КриптоАРМ и КриптоПро CSP, а также где найти инструкции по активации лицензий.

Инструкция актуальна для macOS 14 (Sonoma) и новее.

Содержание:

- Скачивание установочных файлов
- Установка КриптоАРМ
- Установка КриптоПро CSP
- Активация лицензий
- Обновление
- Удаление КриптоАРМ
- Смотрите также

Скачивание установочных файлов

Дистрибутив КриптоАРМ

Скачайте установочный файл КриптоАРМ с официальных источников:

- Официальный сайт КриптоАРМ
- Сайт компании-разработчика Trusted.ru

Дистрибутив поставляется в формате `.dmg` и представляет собой образ диска с приложением. Образов два — по типу процессора:

Файл	Для каких компьютеров
`cryptoarm-sign-<версия>-mac-arm64.dmg`	Apple Silicon (M1 и новее)
`cryptoarm-sign-<версия>-mac-x64.dmg`	Intel

Тип процессора показан в меню → **Об этом Mac**.

Дистрибутив КриптоПро CSP (при использовании ГОСТ-алгоритмов)

> ⚠️ **Примечание**: КриптоАРМ можно использовать без установки КриптоПро CSP, если ваши сценарии работы не требуют выполнения криптографических операций с алгоритмами ГОСТ.

Скачайте дистрибутив КриптоПро CSP с официального сайта компании ООО «КРИПТО-ПРО» или используйте компакт-диск.

Чтобы загрузить дистрибутив КриптоПро CSP из официального источника:

1. Перейдите на официальный сайт КриптоПро.
2. Пройдите регистрацию или авторизацию.
3. Откроется страница продукта КриптоПро CSP.
4. Нажмите **Скачать**.
5. Ознакомьтесь и согласитесь с лицензионным соглашением.
6. Скачайте дистрибутив в соответствии с установленной операционной системой и её разрядностью.

> ⚠️ **Требования к версии**: КриптоАРМ поддерживает КриптоПро CSP версии 5.0 и выше.

Для создания подписей со штампом времени или усовершенствованной подписи необходимо установить библиотеки поддержки модулей TSP и OCSP. Дистрибутив КриптоПро CSP не содержит пакетов TSP и OCSP. Эти модули доступны в составе КриптоПро ЭЦП SDK для macOS, который необходимо скачать отдельно.

Установка КриптоАРМ

1. Откройте скачанный файл `.dmg` двойным щелчком.
2. В открывшемся окне перетащите значок приложения в папку **Applications**.



1. Извлеките образ из бокового меню Finder.
2. Запустите приложение из папки **Программы** или через Launchpad.

> 💡 **Примечание**: приложение подписано и заверено Apple.

После установки

Ярлык приложения появляется в **Launchpad**, а само приложение — в каталоге **Программы (Applications)**.

После первого запуска в контекстном меню Finder, в подменю **Быстрые действия**, появляются команды **КриптоАРМ —** для подписи, проверки и расшифрования файлов — см. Быстрые действия Finder.

Установка КриптоПро CSP

1. Распакуйте загруженный дистрибутив `.tgz`.
2. Откройте образ диска `.dmg` двойным кликом.
3. Запустите установочный пакет `.pkg` двойным кликом.
4. Если появится предупреждение «Программа загружена из интернета», выберите **Открыть**.
5. Нажмите **Продолжить**, ознакомьтесь с лицензией и примите условия.
6. Выберите все необходимые пакеты и нажмите **Продолжить → Установить**.

7. После завершения закройте мастер установки.

> 📌 По умолчанию CSP устанавливается в `/Applications/CryptoPro_ECP.app`. Если вы выбрали другой каталог, используйте его в последующих командах терминала.

После установки КриптоПро CSP перезапустите КриптоАРМ, чтобы приложение увидело провайдер.

Установка модулей TSP и OCSP

Для создания подписей со штампом времени или усовершенствованной подписи необходимо установить библиотеки поддержки модулей TSP и OCSP:

1. Скачайте КриптоПро ЭЦП SDK 2.0.
2. Установите пакет `.pkg`, следуя шагам установщика.

> 💡 Для создания обычной подписи без штампа времени установка этих модулей не обязательна.

Активация лицензий на модули TSP и OCSP через терминал

> 💡 Рекомендуемый способ активации — через интерфейс КриптоАРМ, см. Лицензии КриптоПро. Терминал нужен только там, где графический интерфейс недоступен.

1. Откройте терминал и введите команды.

Если вы используете стандартный путь установки (`/Applications/CryptoPro_ECP.app`), команды будут:

```
sudo /Applications/CryptoPro_ECP.app/Contents/MacOS/bin/tsputil license -s <серийный_номер>
sudo /Applications/CryptoPro_ECP.app/Contents/MacOS/bin/ocsputil license -s <серийный_номер>
```

- Замените серийный номер на ваш приобретённый.
- Если CSP установлен в другой каталог, замените путь на соответствующий.

1. После ввода команды система попросит пароль пользователя macOS.
2. Проверьте статус лицензий по команде:

```
/Applications/CryptoPro_ECP.app/Contents/MacOS/bin/tsputil license
/Applications/CryptoPro_ECP.app/Contents/MacOS/bin/ocsputil license
```

Активация лицензий

Для выполнения криптографических операций с алгоритмами ГОСТ необходимо активировать лицензию КриптоАРМ.

Инструкции по активации лицензий:

- Активация лицензии КриптоАРМ — ввод лицензионного ключа приложения;
- Лицензии КриптоПро — только при использовании CSP. Установка серийных номеров КриптоПро CSP, TSP Client и OCSP Client через интерфейс КриптоАРМ.

При первом запуске КриптоАРМ автоматически активируется **30-дневная пробная лицензия**, которая позволяет полностью ознакомиться со всеми возможностями приложения и протестировать работу криптографических операций с российскими алгоритмами ГОСТ.

При первой установке криптопровайдера КриптоПро CSP может быть активирована ознакомительная лицензия (обычно сроком до 90 дней).

> 💡 Пробный период КриптоАРМ и ознакомительная лицензия КриптоПро CSP действуют независимо друг от друга.

Обновление

Приложение само проверяет наличие новой версии и обновляется с вашего одобрения: в разделе **Настройки → О программе** появляется строка «Доступна версия», а установка запускается кнопкой **Установить и перезапустить** — см. Проверка обновлений.

Вручную новая версия ставится так же, как в первый раз: закройте приложение и замените его в папке **Программы** содержимым нового образа. Настройки, профили и журнал сохраняются.

Удаление КриптоАРМ

Закрытие приложения

1. Перед удалением убедитесь, что КриптоАРМ не запущен.
2. Закройте все окна программы и завершите её сочетанием `⌘ + Q`.

Удаление приложения

1. Откройте каталог **Программы (Applications)**.
2. Найдите **КриптоАРМ Подпись и шифрование** (`CryptoARM Sign and Encrypt.app`).
3. Перетащите приложение в **Корзину (Trash)**.

Удаление файлов конфигурации и данных пользователя

Каталог данных приложения при удалении не стирается. Для полной очистки системы удалите его вручную:

1. Откройте **Finder** → **Переход** → **Переход к папке...** (или `⇧ + ⌘ + G`).
2. Введите следующие пути и удалите соответствующие файлы:

- `~/Library/Application Support/cryptoarm-sign` — настройки, журнал, логи и база сертификатов и ключей OpenPGP;
- `~/Library/Preferences/ru.cryptoarm.sign.plist` — служебные параметры окна;
- workflow в `~/Library/Services` — команды подменю «Быстрые действия» Finder: «Проверить и расшифровать», «Открыть для...» и профили. Удалять их вручную не обязательно: первый же выбор такого пункта после удаления приложения уберёт их все и сообщит об этом уведомлением.

> ⚠️ **Важно**: в каталоге данных находятся зашифрованные закрытые ключи OpenPGP. Удаляйте его, только если сохранили резервные копии ключей.

Смотрите также

- Активация лицензии — ввод лицензионного ключа.
- Быстрый старт — подготовка к первой операции.
- Криптопровайдеры в КриптоАРМ — какие провайдеры выполняют операции.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Инструкция по активации лицензий КриптоАРМ и КриптоПро CSP

В этой инструкции вы узнаете, как активировать лицензии на **КриптоАРМ** и **КриптоПро CSP**, а также на дополнительные модули **TSP Client** и **OCSP Client** через интерфейс приложения КриптоАРМ. Здесь же описано, как перенести лицензию КриптоАРМ на другое рабочее место и где посмотреть состояние всех лицензий.

Содержание:

- Лицензия КриптоАРМ
- Лицензия КриптоПро CSP
- Проверка статуса лицензии
- Смотрите также

Лицензия КриптоАРМ

Лицензия КриптоАРМ требуется для подписи и расшифрования файлов сертификатами с ГОСТ-алгоритмами. Какие операции обходятся без неё и какие бывают виды лицензий — в разделе Лицензирование.

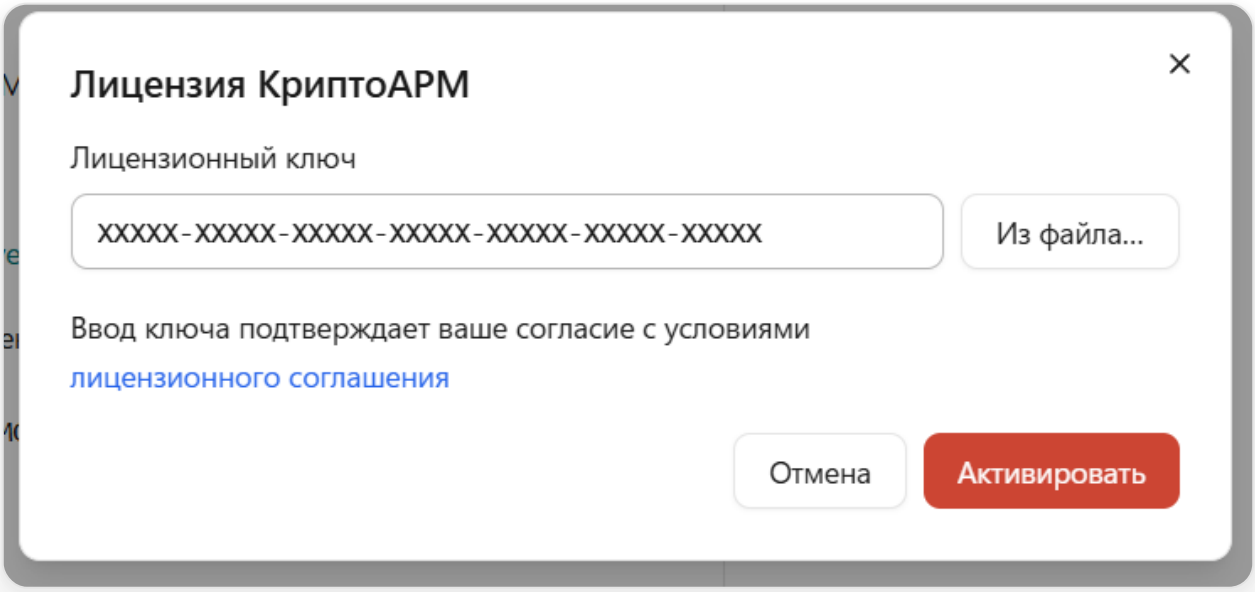
Приложению подходят ключи двух версий КриптоАРМ: **«Подпись и шифрование»** и **«Защищенная почта»**.

Если ключ уже установлен в программе КриптоАРМ Защищенная почта, вводить его повторно не нужно: приложение прочитает его само.

При первом запуске приложение автоматически создаёт пробную лицензию на 30 дней.

Активация лицензии КриптоАРМ

1. Перейдите в раздел **Настройки** → вкладка **О программе**.
2. В блоке **Данные о лицензии** нажмите **Ввести ключ**.
3. В открывшемся окне **Лицензия КриптоАРМ** введите или вставьте лицензионный ключ в формате `XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`. Ключ также можно активировать **Из файла...**.



1. Нажмите **Активировать** и дождитесь завершения активации.

Если активация прошла успешно, статус лицензии обновится автоматически.

Лицензия действует для всех пользователей компьютера, поэтому при активации система запросит подтверждение прав администратора.

Если подтверждение отменить, приложение сохранит ключ только для текущего пользователя: лицензия будет работать, но другие пользователи этого компьютера её не увидят. В журнале появится запись **«Лицензия активирована только для текущего пользователя»**. Чтобы установить её для всех, повторите активацию и подтвердите права.

Перенос лицензии КриптоАРМ на другое устройство

Лицензия на рабочее место привязана к устройству, поэтому перед активацией на новом компьютере её снимают со старого.

1. Перейдите в раздел **Настройки** → вкладка **О программе**.
2. При необходимости скопируйте лицензионный ключ из блока **Данные о лицензии** — он понадобится при активации на новом устройстве.
3. Нажмите **Удалить лицензию** и подтвердите удаление в окне запроса.

Удаляется только лицензия этого приложения — лицензии других приложений КриптоАРМ не изменятся.

Дальше активируйте лицензию на новом устройстве по инструкции по активации.

> 💡 **Примечание**: удаление самого приложения лицензию с рабочего места не снимает — после переустановки ключ вводить заново не нужно.

Лицензия КриптоПро CSP

Лицензия КриптоАРМ не заменяет лицензии КриптоПро: серийные номера **КриптоПро CSP**, **КриптоПро TSP Client** и **КриптоПро OCSP Client** устанавливаются отдельно. Все три вводятся в интерфейсе КриптоАРМ — переходить в отдельные утилиты КриптоПро не требуется.

Продукт	Для чего нужен
КриптоПро CSP	Любые операции с алгоритмами ГОСТ
КриптоПро TSP Client	Штампы времени: стандарты CAdES-T, CAdES-X Long Type 1 и CAdES-A
КриптоПро OCSP Client	Доказательства статуса отзыва в подписи: стандарты CAdES-X Long Type 1 и CAdES-A

Стандарту CAdES-BES эти лицензии не нужны.

Активация лицензии КриптоПро CSP

1. Перейдите в раздел **Настройки** → вкладка **Криптопровайдеры** → провайдер **КриптоПро CSP**.
2. В карточке **КриптоПро CSP** нажмите **Ввести ключ** (или **Изменить ключ**, если лицензия уже установлена).
3. Введите серийный номер и нажмите **Установить**.

Лицензия устанавливается для всех пользователей компьютера, поэтому потребуется подтверждение прав администратора. Если активация прошла успешно, статус лицензии обновится автоматически.

Если лицензии нет, в карточке продукта доступны ссылки **Купить лицензию КриптоПро CSP**, **Купить лицензию КриптоПро TSP Client 2.0** и **Купить лицензию КриптоПро OCSP Client 2.0**.

Возможные ошибки установки:

Сообщение	Что это значит	Что сделать
Введите 25 символов латиницей и цифрами	Серийный номер введён с ошибкой	Проверьте номер: 25 символов группами по пять
Ключ не соответствует выбранному продукту	Номер выдан для другого продукта КриптоПро	Вводите номер в карточке того продукта, для которого он куплен
Установка отменена или не предоставлены права администратора	Запрос прав администратора был отклонён	Повторите установку и подтвердите запрос системы
Не удалось установить лицензию	Установка не завершилась	Повторите установку; причина записана в журнале

Сообщение	Что это значит	Что сделать
Лицензия записана, но её действие не удалось подтвердить	Провайдер не подтвердил установленную лицензию	Перезапустите приложение и проверьте статус
Компонент управления лицензиями КриптоПро недоступен	На компьютере нет компонента, через который приложение ставит лицензии	Установите лицензию средствами КриптоПро — например, через терминал

Активация лицензии на модули TSP и OCSP

> 💡 Модули **КриптоПро TSP Client** и **КриптоПро OCSP Client** лицензируются отдельно и активируются так же, как лицензия КриптоПро CSP.

1. Перейдите в раздел **Настройки** → вкладка **Криптопровайдеры** → провайдер **КриптоПро CSP**.
2. Нажмите **Ввести ключ** в карточке **КриптоПро TSP Client** или **КриптоПро OCSP Client**.
3. Введите серийный номер и нажмите **Установить**.

Номера продуктов различаются началом: у TSP Client он начинается с `TA`, у OCSP Client — с `0A`, у КриптоПро CSP — с цифры. Если номер выдан другому продукту, приложение откажет в установке.

Активация через терминал

Лицензии КриптоПро можно установить и вне приложения:

- через **Инструменты КриптоПро** (графический интерфейс, если он установлен);
- через **терминал (командную строку)** — актуально в первую очередь для Linux.

Подробные инструкции по активации через терминал:

- Активация лицензий КриптоПро в Linux через терминал
- Активация лицензий на модули TSP и OCSP в macOS через терминал

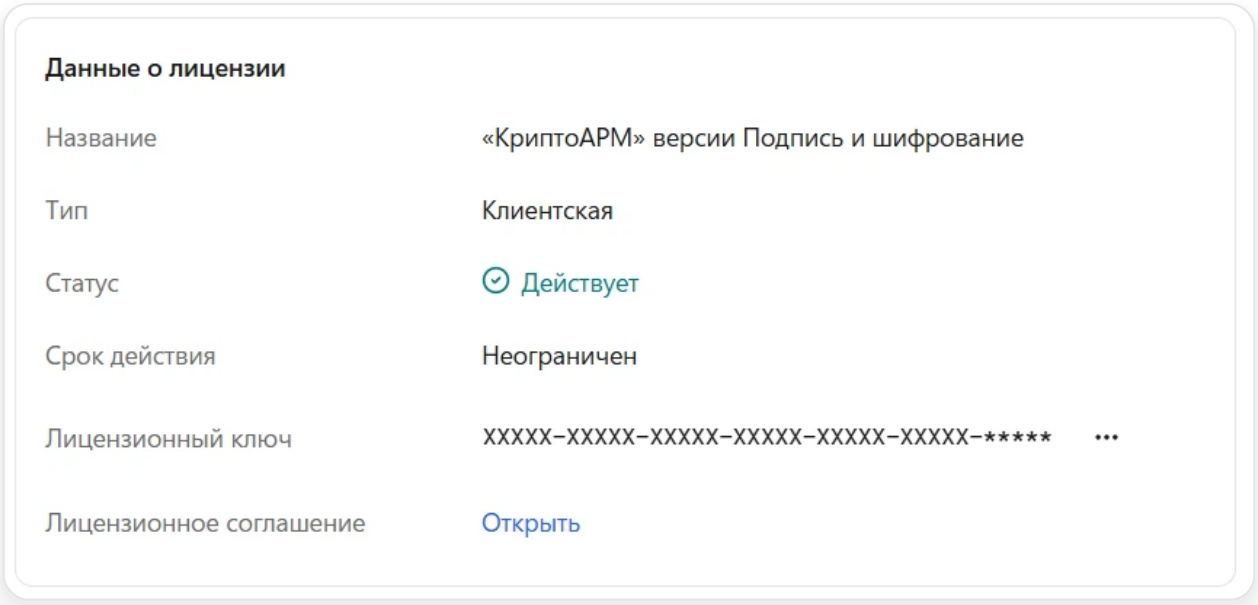
> 💡 Рекомендуется использовать активацию через КриптоАРМ, если нет необходимости выполнять настройку вручную или работать в среде без графического интерфейса.

Проверка статуса лицензии

КриптоАРМ

Откройте **Настройки → О программе**. Блок **Данные о лицензии** содержит:

Поле	Значение
Название	Продукт, для которого выдан ключ
Тип	«Клиентская» или «Серверная»
Статус	«Действует», «Пробная», «Не установлена», «Истекла», «Недействительна», «Другая редакция», «Скомпрометирована» или «Ошибка проверки»
Срок действия	«Неограничен» либо количество оставшихся дней
Лицензионный ключ	Установленный ключ



Статус **«Действует»** означает, что все операции доступны. При статусах **«Не установлена»**, **«Истекла»** и **«Недействительна»** введите новый ключ.

КриптоПро CSP и модули

Откройте **Настройки → Криптопровайдеры** и выберите **КриптоПро CSP**. В карточках продуктов показаны статус, серийный номер, тип лицензии и срок её действия — как для самого провайдера, так и для модулей TSP Client и OCSP Client.

Если сведения о лицензии прочитать не удалось, статус будет **«Не удалось определить»**: на компьютере нет компонента КриптоПро, через который приложение читает лицензии. Операциям это не мешает — их по-прежнему выполняет сам провайдер.

Если активация не удалась или операция отклонена из-за лицензии, причина записывается в журнал — см. Уведомления и журнал событий.

Смотрите также

- О продукте — какие операции требуют лицензии.
- Общие настройки — лицензии КриптоПро CSP, TSP и OCSP.
- Быстрый старт — подготовка к первой операции.
- Уведомления и журнал событий — где смотреть причину отказа операции.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Начало работы в КриптоАРМ

Это пошаговое руководство поможет вам быстро подготовить КриптоАРМ к работе. Вы узнаете, как добавить сертификат подписи, подписать и проверить документ, зашифровать файл для получателя. Всё необходимое для старта собрано в одном месте, чтобы вы могли сразу приступить к работе.

Приложение готово к работе сразу после установки: настраивать его перед первой подписью не нужно. Понадобятся только документ и ваш сертификат электронной подписи — обычно он на токене или флеш-накопителе, выданных удостоверяющим центром.

Содержание:

- Общие подготовительные шаги
- Работа с документами
- Если что-то пошло не так
- Что настроить дальше
- Работа по стандарту OpenPGP
- Смотрите также

Общие подготовительные шаги

Некоторые действия универсальны и необходимы для любого сценария.

Добавьте сертификат подписи

Сертификат используется для создания электронной подписи.

Подключите токен или флеш-накопитель с ключом, откройте раздел **Сертификаты** и выберите **Личные сертификаты**. Если ваш сертификат в списке — всё готово, переходите к работе с документами.

Если список пуст:

Откуда у вас сертификат	Что сделать
На токене, флеш-накопителе или в реестре	Установите сертификат из контейнера
Файлом `.pfx` или `.p12` с паролем	Импортируйте его вместе с закрытым ключом
Сертификата ещё нет	Получите его в удостоверяющем центре — при необходимости создайте запрос
Нужно просто попробовать программу	

Откуда у вас сертификат	Что сделать
	Создайте самоподписанный сертификат — для юридически значимого документооборота он не подходит

Добавьте сертификаты получателей

Чтобы шифровать документы в чей-то адрес, нужен сертификат получателя: он присылает его сам, закрытый ключ при этом не передаётся.

- Импортируйте сертификат другого пользователя — он попадёт в раздел **Сертификаты → Других пользователей**;
- Объедините сертификаты в группу — если шифруете постоянному кругу адресатов.

Работа с документами

Шаг 1. Подпишите документ

1. Откройте раздел **«Подпись и шифрование»**.
2. Перетащите документ в окно раздела — или нажмите **Добавить файлы**.
3. Нажмите **Далее**.
4. В блоке **Операции** отметьте **Подписать**.
5. В блоке **Личная подпись** выберите свой сертификат.
6. Нажмите **Выполнить** и подтвердите операцию.
7. Введите ПИН-код токена или пароль закрытого ключа, если приложение их запросит.

Результат: рядом с исходным документом появится файл подписи — по умолчанию с расширением `.sig`. В списке результатов будет статус **«Успешно»**, а исходный документ останется нетронутым.

Остальные параметры уже заполнены рабочими значениями — для первой подписи их можно оставить как есть. Если принимающая сторона требует определённый формат подписи, задайте его в настройках подписи и шифрования.

Заданные параметры хранятся в профиле подписи. Первый профиль приложение создаёт само — см. Профили подписи.

Подробное описание шага — в инструкции Подпись и шифрование файлов.

Шаг 2. Проверьте подпись

1. Откройте раздел **«Проверка и расшифрование»**.
2. Перетащите в окно созданный файл подписи.

Проверка запускается сама. В столбце **Статус** должно появиться **«Подпись действительна»**.

Шаг 3. Зашифруйте файл для получателя

Зашифрованный файл сможет открыть только тот, для кого он предназначен.

1. Добавьте файл в раздел **«Подпись и шифрование»** и нажмите **Далее**.
2. В блоке **Операции** отметьте **Зашифровать** и выберите получателей из ранее импортированных сертификатов.
3. Нажмите **Выполнить**.

Как открыть присланный подписанный файл

Если вам прислали файл `.sig`, `.p7s`, `.sgn` или `.enc`, дважды щёлкните по нему: откроется КриптоАРМ, проверит подпись и при необходимости расшифрует файл.

- Если пришли **два файла** — документ и подпись отдельно, — положите их в одну папку и откройте файл подписи. Приложение найдёт документ само; см. Отсоединённая подпись.
- Чтобы достать из файла подписи исходный документ, воспользуйтесь снятием подписи.
- Чтобы получить бумажный экземпляр с отметкой о подписи, создайте печатную форму со штампом.

Готово! Теперь вы можете подписывать, шифровать и проверять файлы в разделах **«Подпись и шифрование»** и **«Проверка и расшифрование»**.

Если что-то пошло не так

Что происходит	Что проверить
В разделе «Сертификаты» пусто	Подключён ли токен; установлен ли **КриптоПро CSP** — без него сертификаты ГОСТ не видны (как проверить)
Сертификаты есть, но не те, что нужны	Переключите профиль доверия: ГОСТ-сертификаты показывает «Российская Федерация», RSA и ECDSA — «Открытая криптография»
Приложение сообщает об отсутствии лицензии	Активируйте лицензию — она нужна для подписи и расшифрования сертификатами ГОСТ
Подпись не проходит проверку	Почему подпись не проходит проверку
Операция прервалась, причина неизвестна	Откройте журнал событий — там записана причина отказа

Что настроить дальше

Всё перечисленное необязательно — приложение работает и без этого.

- Профили подписи — готовые наборы настроек подписи, шифрования и архивирования. Один профиль уже создан, дополнительные добавляются вручную и переключаются одним щелчком.
- Команды в контекстном меню Проводника — подписывать файлы, не открывая приложение (только Windows).
- Сохранение результатов — куда складывать подписанные и зашифрованные файлы.
- Тема, язык и сворачивание в трей.
- Уведомления и журнал событий — где смотреть результат и причину отказа.
- Проверка обновлений.

Работа по стандарту OpenPGP

OpenPGP — отдельный стандарт со своими ключами; для документооборота по 63-ФЗ не подходит. Выбирайте его, только если так принято у ваших корреспондентов.

1. В разделе **Настройки → Криптопровайдеры** выберите **«Стандарт операций по умолчанию» → OpenPGP**.
2. Создайте сертификат OpenPGP или импортируйте существующий.
3. Сохраните резервную копию закрытого ключа — восстановить его иначе невозможно.
4. Импортируйте открытые ключи корреспондентов и при необходимости заверьте их.
5. Подписывайте и шифруйте файлы в том же разделе **«Подпись и шифрование»** — см. Особенности OpenPGP.

Смотрите также

- Общие настройки — инструкция по настройке приложения КриптоАРМ.
- Интерфейс приложения — как устроено окно и вкладки.
- Установка сертификатов — руководство по установке сертификатов в КриптоАРМ.
- Обзор операций и выбор мастера — какой раздел выбрать под задачу.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

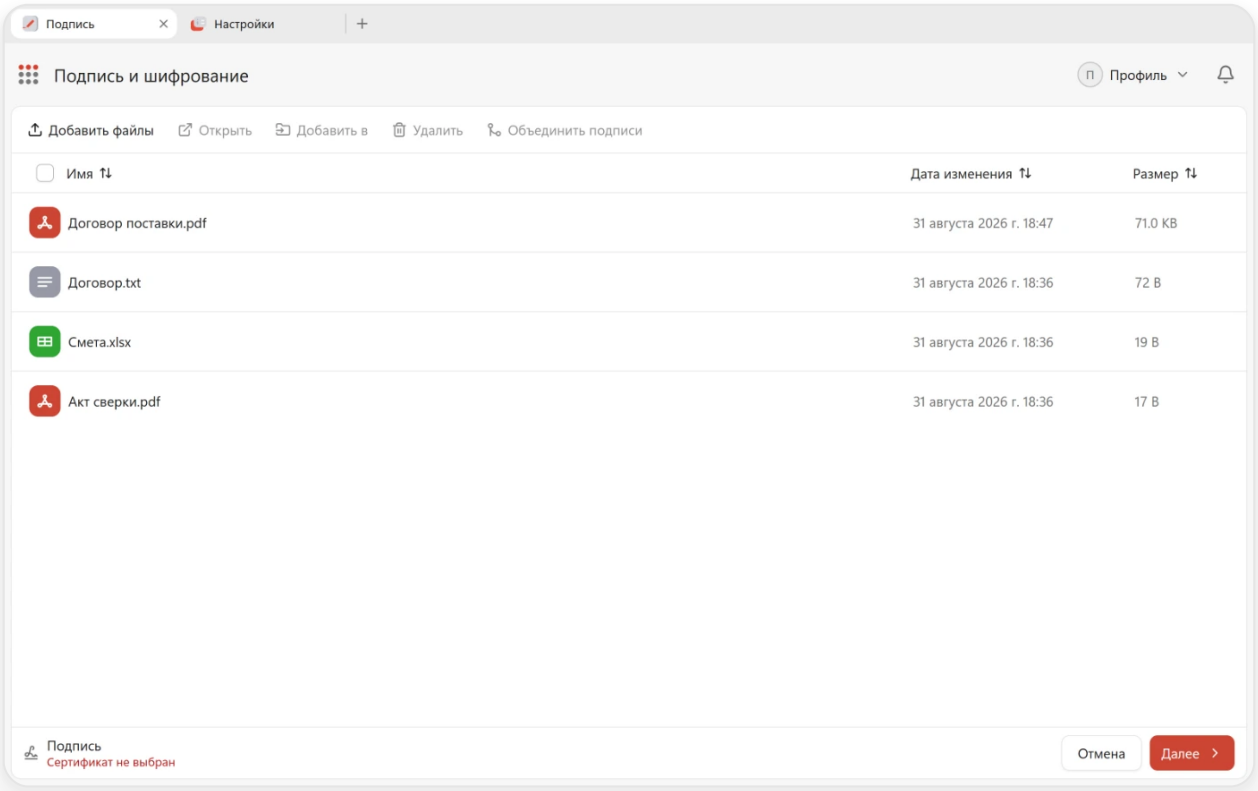
Интерфейс КриптоАРМ

Разделы приложения открываются во вкладках. Несколько разделов можно держать открытыми одновременно и переключаться между ними: начатая операция при этом не сбрасывается.

Содержание:

- Из чего состоит окно
- Разделы приложения
- Работа с вкладками
- Поиск
- Настройка столбцов
- Центр уведомлений
- Работа из трея
- Смотрите также

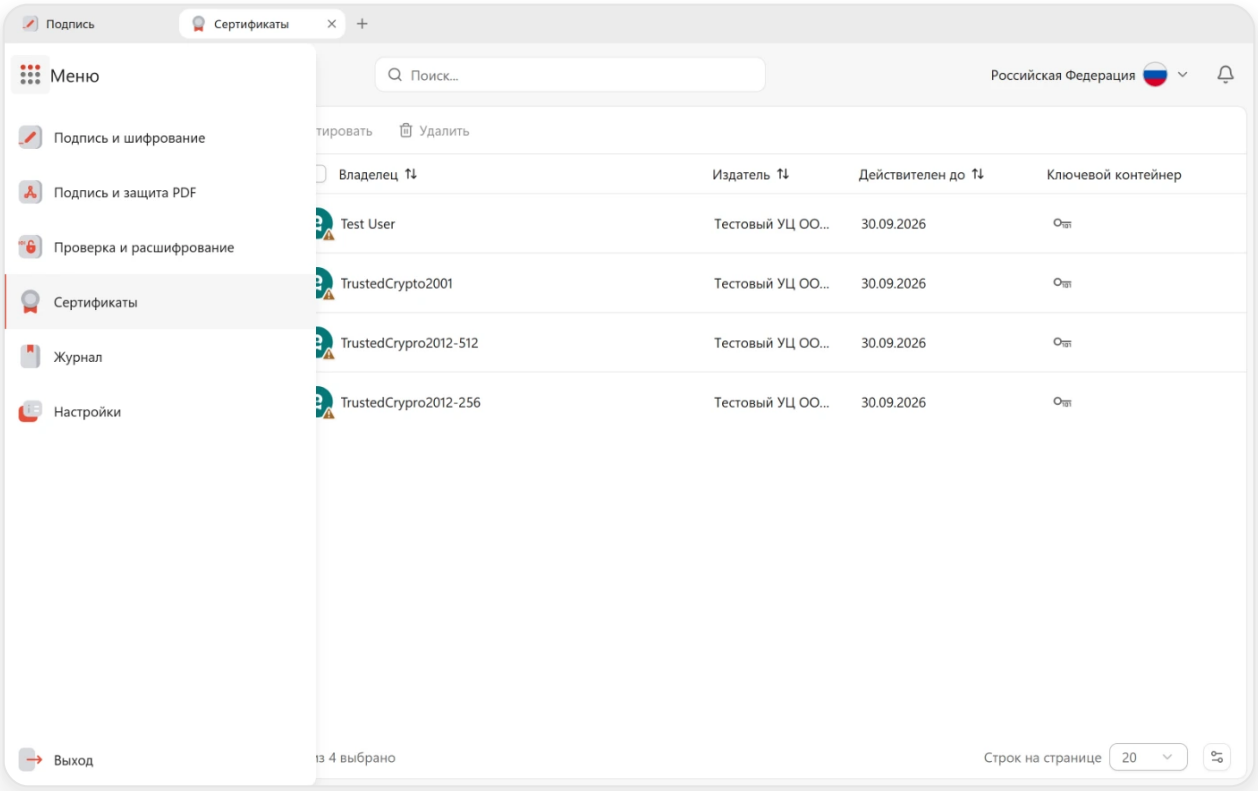
Из чего состоит окно



Элемент	Назначение
Меню — кнопка слева вверху	Открывает список разделов приложения
Строка вкладок	Открытые разделы; здесь же кнопка новой вкладки
Заголовок	Название текущего раздела и его собственные элементы управления
Поиск	Фильтрация содержимого текущего раздела
Колокольчик	Центр уведомлений

Разделы приложения

Нажмите кнопку **Меню** в левом верхнем углу.



Раздел	Что делает
Подпись и шифрование	Подпись, архивирование и шифрование файлов
Подпись и защита PDF	Мастер работы с одним PDF-документом
Проверка и расшифрование	Проверка подписи, расшифрование, отчёты, снятие подписи

Раздел	Что делает
Сертификаты	Сертификаты, контейнеры, списки отзыва, запросы, группы
Журнал	События приложения
Настройки	Оформление, криптопровайдеры, лицензия, обновления
Выход	Завершение работы приложения

Выбор раздела открывает его в новой вкладке или переключает на уже открытую.

> 💡 **Примечание**: содержимое разделов **«Сертификаты»**, **«Подпись и шифрование»** и **«Проверка и расшифрование»** зависит от настройки «Стандарт операций по умолчанию» — X.509 или OpenPGP.

Работа с вкладками

- **Новая вкладка** — кнопка + в строке вкладок: щелчок открывает раздел **«Подпись и шифрование»**, а правый щелчок показывает список разделов, чтобы сразу открыть нужный.
- **Переключение** — щелчок по вкладке.
- **Закрытие** — крестик на вкладке.
- **Прокрутка** — стрелки по краям строки, когда вкладок больше, чем помещается.

Контекстное меню вкладки (правая кнопка мыши) содержит команды:

- **Закрыть вкладку**,
- **Закрыть другие вкладки**,
- **Закрыть вкладки справа**,
- **Закрыть все вкладки**.

Вкладки редактирования — например, **«Редактирование профиля»** или **«Создание сертификата»** — открываются рядом с обычными и закрываются после сохранения.

Поиск

Поиск в заголовке фильтрует содержимое текущего раздела: сертификаты, записи журнала, файлы операции.

Строка поиска очищается автоматически при переключении между разделами списка сертификатов: разделы ищут по разным полям.

Настройка столбцов

Таблицы сертификатов, контейнеров, списков отзыва, запросов и журнала показывают не все сведения сразу: лишние столбцы можно скрыть, нужные — вернуть и расставить в удобном порядке.

Список **Столбцы** открывает правый щелчок по заголовкам таблицы или стрелка справа в строке заголовков — она появляется при наведении указателя.

- **Показать или скрыть столбец** — переключатель в его строке.
- **Поменять порядок** — перетащите строку за значок слева или нажмите Alt+↑ / Alt+↓ (на macOS — ⌥+↑ / ⌥+↓).
- **По умолчанию** — вернуть исходный набор и порядок.

Первый столбец называет строку, поэтому его скрыть нельзя: в списке он стоит первым с неактивным переключателем. Настройки запоминаются для каждой таблицы отдельно.

Центр уведомлений

Кнопка с колокольчиком открывает центр уведомлений. В нём собраны ошибки и предупреждения, которые вы могли пропустить: то, что уже видно на месте, например статус файла в таблице, сюда не попадает.

Доступные действия:

- **Прочитать всё** — снять отметку о непрочитанном со всех уведомлений;
- **Очистить** — убрать все уведомления из панели;
- **Скрыть** — убрать одно уведомление;
- **Открыть журнал** — перейти к полному списку событий.

Подробнее — в инструкции Уведомления и журнал событий.

Работа из трея

Если в разделе **Настройки → Общие** включена настройка **«Сворачивать программу в трей при закрытии окна»**, закрытие окна не завершает работу приложения: значок остаётся в области уведомлений.

Меню значка содержит команды **Открыть** и **Выход**.

Такой режим удобен, когда операции запускаются из контекстного меню Проводника: приложение уже загружено и выполняет их быстрее.

Смотрите также

- Быстрый старт — что настроить перед первой операцией.
- Общие настройки — тема, язык, поведение окна.
- Уведомления и журнал событий — где смотреть результат операции.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Общие настройки КриптоАРМ

Раздел **Настройки** состоит из трёх вкладок: **О программе**, **Криптопровайдеры** и **Общие**. В этой инструкции описаны настройки криптопровайдеров и вкладка **Общие**: оформление, поведение в системе и служебные возможности.

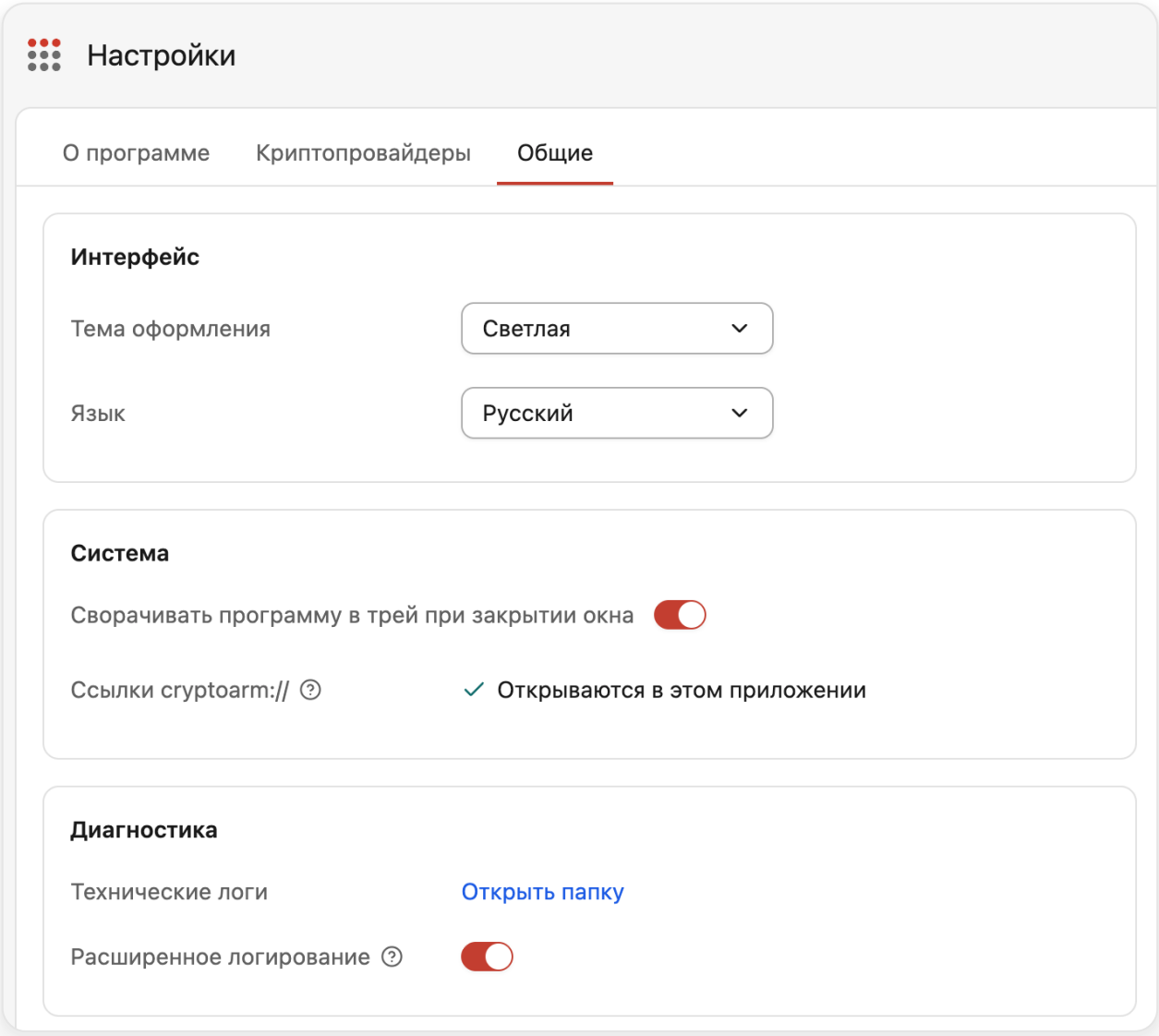
Содержание:

- Настройка темы
- Язык интерфейса
- Сворачивание в трей при закрытии окна
- Стандарт операций по умолчанию
- Ограничение использования сертификатов по атрибуту KeyAgreement
- Технические логи
- Смотрите также

Настройка темы

Откройте **Настройки → Общие** и в блоке **Интерфейс** выберите значение в поле **Тема оформления**:

- **Светлая**,
- **Тёмная**,
- **Системная** — тема следует за настройкой операционной системы.



Язык интерфейса

Поле **Язык** в том же блоке переключает язык интерфейса. Доступны русский, английский, немецкий, испанский, французский и итальянский.

При первом запуске язык определяется по языку системы.

Сворачивание в трей при закрытии окна

Настройка **«Сворачивать программу в трей при закрытии окна»** в блоке **Система** той же вкладки определяет, что происходит при закрытии окна:

- **включена** — приложение продолжает работать, значок остаётся в области уведомлений; открыть окно снова можно из меню значка;

- **выключена** — закрытие окна завершает работу приложения.

Как управлять программой, когда она свёрнута в трей:

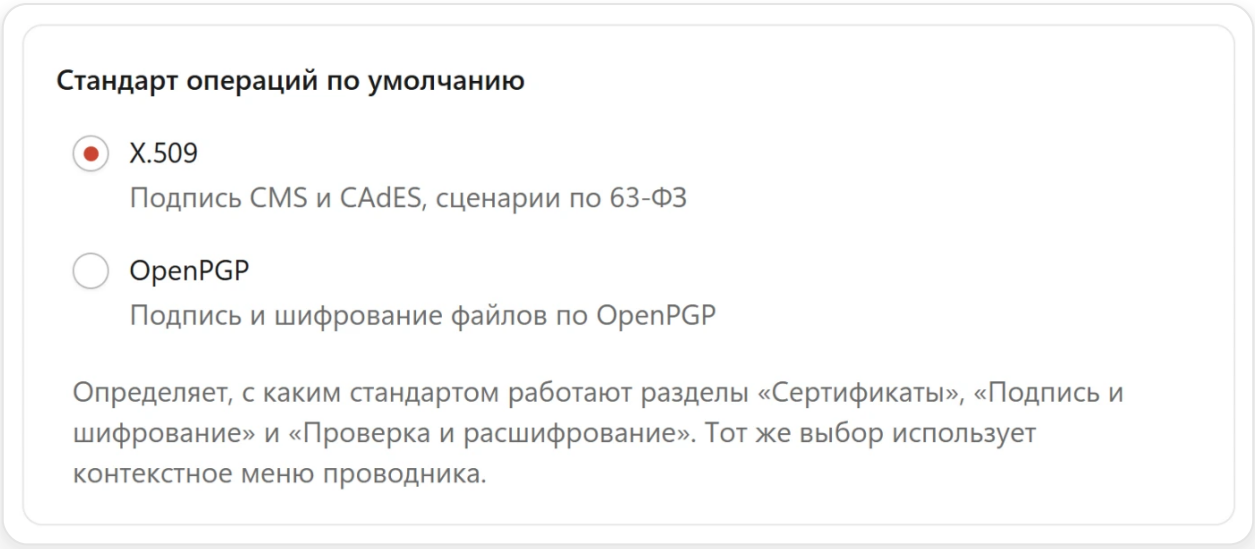
- **Развернуть окно** — щёлкните по значку в области уведомлений; на macOS щелчок открывает меню значка, в котором нужно выбрать **Открыть**.
- **Полностью выйти из программы** — щёлкните по значку правой кнопкой и выберите **Выход**.

Включённая настройка ускоряет операции из контекстного меню Проводника: приложение уже загружено.

Стандарт операций по умолчанию

Настройка **«Стандарт операций по умолчанию»** во вкладке **Криптопровайдеры** переключает всё приложение между двумя стандартами:

- **X.509** — подпись CMS и CAdES, сценарии по 63-ФЗ;
- **OpenPGP** — подпись и шифрование файлов по OpenPGP.



Выбор определяет содержимое разделов **«Сертификаты»**, **«Подпись и шифрование»** и **«Проверка и расшифрование»**. Тот же выбор используют контекстное меню Проводника и быстрые действия Finder для команд проверки и расшифрования.

> 💡 **Примечание**: профили подписи хранятся отдельно для каждого стандарта — переключение не изменит настройки профилей другого стандарта.

Ограничение использования сертификатов по атрибуту KeyAgreement

Зачем нужна проверка

Атрибут **KeyAgreement** (согласование ключей) в расширении **keyUsage** сертификата указывает, что сертификат может использоваться для безопасного обмена ключами при выполнении операций шифрования.

В КриптоАРМ доступна настройка, позволяющая ограничить использование сертификатов:

- при включённой проверке операции выполняются только для сертификатов, содержащих атрибут **KeyAgreement**;
- при отключённой проверке допускается использование сертификатов с атрибутом **keyEncipherment**, даже если атрибут **KeyAgreement** отсутствует.

По умолчанию проверка атрибута **KeyAgreement** отключена. Включайте её, если этого требует регламент организации.

> ⚠️ Настройка доступна только при использовании криптопровайдера КриптоПро CSP.

Включение проверки KeyAgreement

1. Перейдите в раздел **Настройки** → вкладка **Криптопровайдеры**.
2. Нажмите на панель **КриптоПро CSP**.
3. В блоке **Дополнительно** активируйте настройку **Проверять флаг keyAgreement**.

Технические логи

Приложение ведёт служебные записи о своей работе. Они нужны только технической поддержке, когда та разбирает нештатную ситуацию; персональных данных и путей к вашим файлам в них нет.

Блок **Диагностика** в разделе **Настройки → Общие** содержит строку **Технические логи** с кнопкой **Открыть папку** — по ней открывается каталог с файлами, которые просит прислать поддержка, — и переключатель **Расширенное логирование**.

> 💡 **Примечание**: включайте расширенное логирование только по просьбе поддержки и выключайте после — оно заметно увеличивает объём файлов.

Смотрите также

- Криптопровайдеры в КриптоАРМ — какие провайдеры выполняют операции.
- Интерфейс приложения — вкладки, поиск и уведомления.
- Проверка обновлений — как узнать о новой версии.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Как работать с журналом событий и уведомлениями КриптоАРМ

В этом разделе описано, как пользоваться уведомлениями и журналом событий: узнавать результат операции сразу, возвращаться к пропущенным сообщениям, отбирать записи фильтрами и передавать журнал в службу поддержки.

Содержание:

- Уведомления
- Всплывающие уведомления
- Центр уведомлений
- Системные уведомления
- Журнал событий
- Открытие журнала
- Столбцы журнала
- Детали записи
- Поиск и фильтрация
- Экспорт журнала
- Очистка журнала
- Смотрите также

Уведомления

Приложение сообщает о событиях на трёх уровнях: всплывающее уведомление, центр уведомлений и журнал.

Всплывающие уведомления

Результат действия показывается всплывающим сообщением в углу окна: «Сертификат успешно импортирован», «Сохранён 1 файл», «Не удалось сохранить файлы».

Сообщение исчезает само: об успехе — через несколько секунд, а ошибки, предупреждения и сообщения с кнопкой действия держатся дольше, чтобы их успели прочитать. Пока указатель над сообщением, оно не исчезает. Если вы его пропустили, откройте центр уведомлений или журнал.

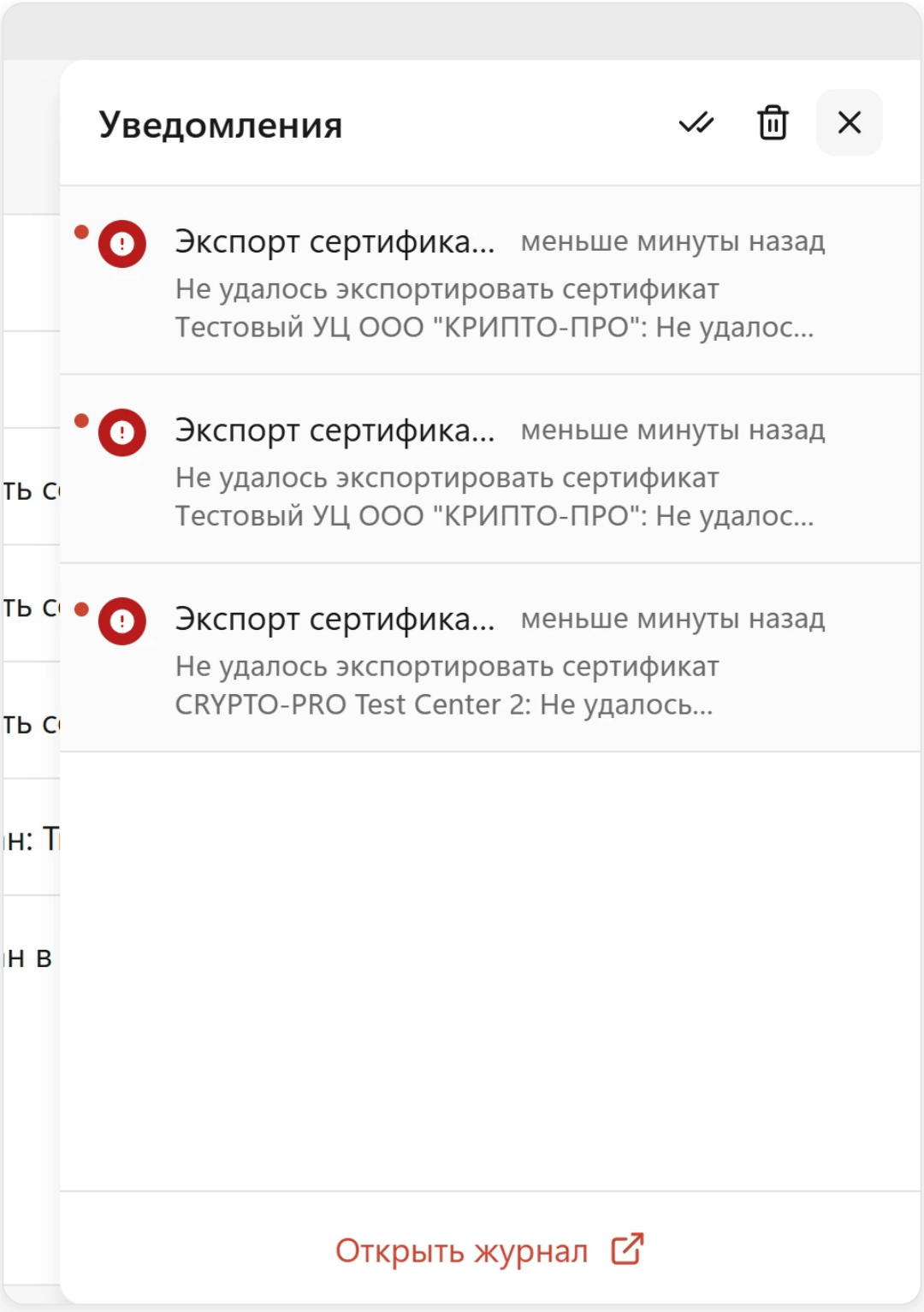
Если результат уже виден там, где вы работаете, — например, статус файла в таблице разделов **«Подпись и шифрование»** и **«Проверка и расшифрование»**, — ни всплывающего сообщения, ни уведомления в центре нет. То же для операций, запущенных не из окна

приложения: результат операции из контекстного меню показывает системное уведомление, а операции, запущенной другой программой через API или командную строку, — сама эта программа. Событие всё равно записывается в журнал.

Если система не умеет показывать уведомления, ошибка операции из контекстного меню попадает в центр уведомлений: другого места, где её видно, нет.

Центр уведомлений

Кнопка с колокольчиком в заголовке окна открывает панель уведомлений.



Доступные действия:

Действие	Что делает
Прочитать всё	Снимает отметку о непрочитанном со всех уведомлений
Очистить	Убирает все уведомления из панели

Действие	Что делает
Скрыть	Убирает одно уведомление
Открыть журнал	Открывает раздел «Журнал»

Если новых сообщений нет, панель показывает **«Нет новых уведомлений»**.

> 💡 **Примечание**: очистка панели уведомлений не удаляет записи журнала.

Системные уведомления

Операции, запущенные из контекстного меню Проводника или быстрых действий Finder, могут выполняться без окна приложения. Их результат сообщает системное уведомление.

Щелчок по такому уведомлению открывает папку с полученным файлом. Подробнее — в инструкции Контекстное меню Проводника.

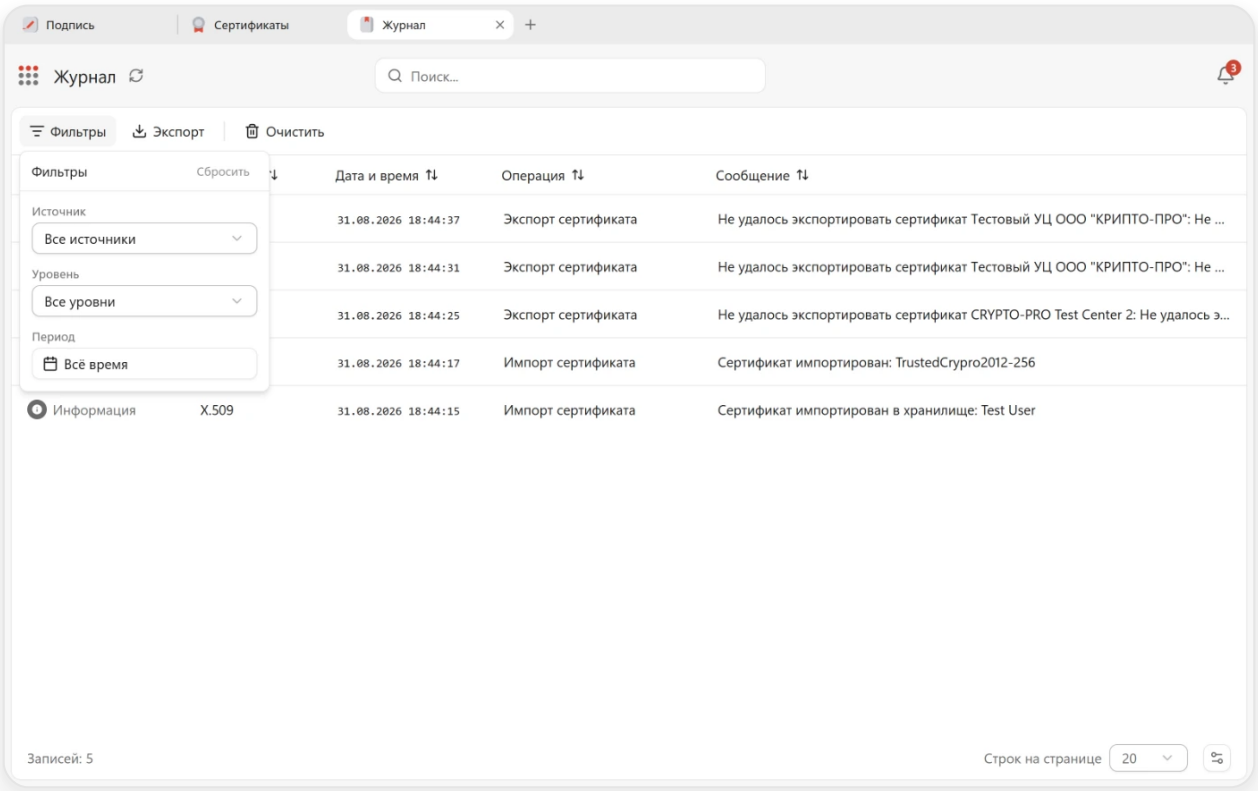
Журнал событий

Журнал фиксирует значимые действия и ошибки приложения и используется для разбора сбоев и передачи данных в службу поддержки.

Открытие журнала

- **Из бокового меню**: нажмите кнопку **Меню** и выберите раздел **Журнал**.
- **Из центра уведомлений**: нажмите кнопку с колокольчиком и выберите **Открыть журнал**.

Столбцы журнала



Столбец	Содержание
Уровень	«Информация», «Предупреждение» или «Ошибка»
Источник	«Приложение», «X.509» или «OpenPGP»
Дата и время	Когда произошло событие
Операция	Подпись, проверка подписи, шифрование, расшифрование, импорт сертификата, лицензия и другие
Сообщение	Что произошло

Набор и порядок столбцов можно поменять — см. Настройка столбцов.

Журнал ведётся для пользователя: в нём записан смысл события. Технические причины отказов пишутся в лог для поддержки — см. Технические логи.

Детали записи

Разверните запись, чтобы увидеть параметры события. Состав полей зависит от операции:

- **Файл**, **Путь к файлу**, **Количество** — над чем выполнялась операция;
- **Сертификат**, **Подписант**, **Отпечаток**, **Серийный номер**, **Издатель** — каким сертификатом;

- **Стандарт подписи**, **Алгоритм**, **Формат** — с какими параметрами;
- **Получатели** — для шифрования;
- **Профиль** — если операция запускалась по профилю;
- **Контейнер**, **Хранилище**, **Провайдер** — для операций с сертификатами и контейнерами;
- **Ошибка** и **Диагностика** — для неуспешных операций.

Поиск и фильтрация

Кнопка **Фильтры** открывает панель отбора записей.

Период:

- **Сегодня**,
- **7 дней**,
- **30 дней**,
- **Всё время**,
- **Произвольный период** — с указанием дат; после выбора нажмите **Применить**.

Уровень: «Все уровни», «Информация», «Предупреждение», «Ошибка».

Источник: «Все источники», «Приложение», «X.509», «OpenPGP».

Кнопка **Сбросить** снимает все фильтры.

Поиск в заголовке окна отбирает записи по тексту сообщения и деталям.

Экспорт журнала

1. Нажмите **Экспорт** над таблицей.
2. Укажите имя и расположение файла.
3. Дождитесь сообщения **«Журнал успешно экспортирован»**. Кнопка **Показать** в нём открывает папку с файлом.

Журнал сохраняется в файл CSV — его можно открыть в табличном редакторе и передать в техническую поддержку. В файл попадают записи, которые видны с текущими фильтрами.

> 💡 **Примечание**: если под фильтрами нет ни одной записи, кнопка **Экспорт** недоступна.

Очистка журнала

1. Нажмите **Очистить** над таблицей.
2. Подтвердите действие в окне **«Очистка журнала»**.

> ⚠️ **Важно**: очистка удаляет все записи журнала без возможности восстановления. Если история нужна, сначала выполните экспорт.

Сама очистка тоже записывается в журнал — записью **«Журнал очищен»**.

Смотрите также

- Интерфейс приложения — где находится центр уведомлений.
- Общие настройки — технические логи и расширенное логирование.
- Проверка и расшифрование — подробные результаты проверки подписи.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Как выполнить обновление КриптоАРМ

Обновления КриптоАРМ приносят не только новые функции, но и улучшают безопасность, совместимость с операционными системами и общую производительность. В этой инструкции описано, как проверить наличие обновлений и установить актуальную версию приложения.

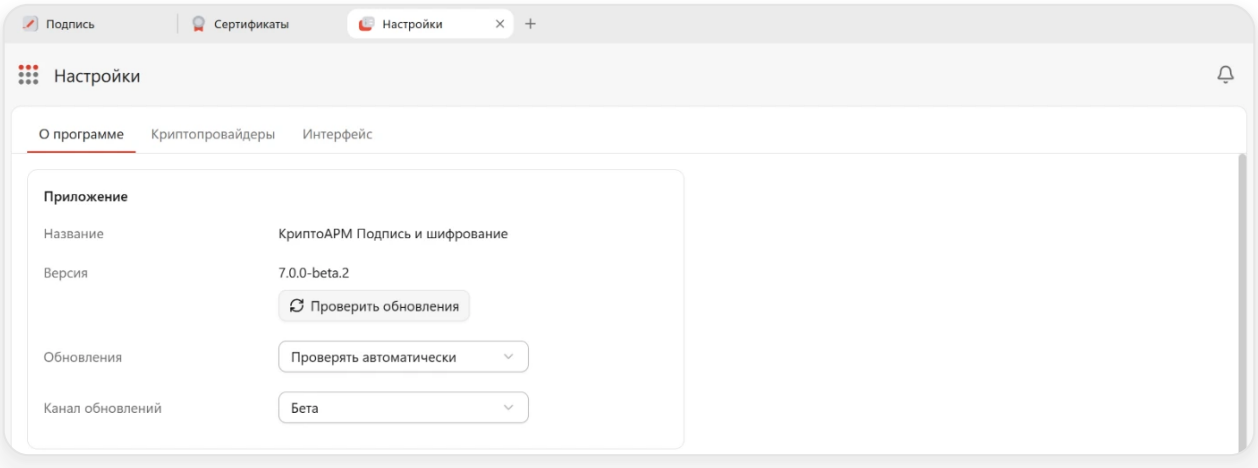
Приложение проверяет обновления само и загружает их по вашей команде. Установку всегда запускаете вы.

Содержание:

- Автоматическая проверка
- Ручная проверка обновлений
- Установка обновления
- Режимы обновления
- Предварительные версии
- Что делать, если обновление не обнаруживается
- Смотрите также

Автоматическая проверка

Приложение обращается к серверу обновлений в фоне и проверяет наличие более свежей версии. Состояние показано в строке **Версия** раздела **Настройки → О программе**.



Пока обновление предложено, загружается или готово к установке, у пункта **«Настройки»** в боковом меню горит точка.

Ручная проверка обновлений

Вы можете в любой момент инициировать проверку вручную.

1. Откройте раздел **Настройки** → вкладка **О программе**.
2. В строке **Версия** нажмите **Проверить обновления**.

Установка обновления

1. Когда появилась строка **«Доступна версия X.Y.Z»**, нажмите **Скачать**. В режиме «Загружать автоматически» этот шаг приложение делает само.
2. Дождитесь строки **«Версия X.Y.Z готова к установке»**.
3. Нажмите **Установить и перезапустить**.

Приложение закроется, установит новую версию и запустится снова.

Настройки, профили подписи, журнал и база сертификатов при обновлении сохраняются.

> 📌 При обновлении приложения лицензия останется действующей. Повторная активация после обновления не нужна.

Режимы обновления

Режим задаётся настройкой **Обновления** в разделе **Настройки → О программе**.

Режим	Что делает приложение
Загружать автоматически	Проверяет и скачивает обновление само, установку запускаете вы
Проверять автоматически	Проверяет само, загрузку и установку запускаете вы. Значение по умолчанию
Проверять вручную	Не проверяет в фоне; работает только кнопка **Проверить обновления**

Установка ни в одном режиме не выполняется без вашего участия.

Предварительные версии

В КриптоАРМ можно настроить получение предварительных версий. Такие версии содержат новые возможности, находящиеся в тестировании, и могут работать нестабильно.

Настройка **Канал обновлений** в разделе **Настройки → О программе** выбирает, какие версии предлагать:

- **Стабильный** — обычные выпуски;
- **Бета** — предварительные версии с новыми возможностями до их общего выпуска.

Канал первого запуска соответствует установленной сборке. Дальше выбор остаётся за вами.

Чтобы вернуться с беты, выберите канал **Стабильный**: приложение предложит перейти на стабильную версию, даже если её номер ниже установленной.

> 💡 **Примечание**: предварительные версии выходят чаще и предназначены для проверки новых возможностей. Для рабочих мест, где важна предсказуемость, оставляйте стабильный канал.

Что делать, если обновление не обнаруживается

Иногда проверка не показывает новую версию, даже если вы знаете о её выходе.

Проблема	Решение
Отсутствует подключение к интернету	Проверьте соединение и повторите попытку
Брандмауэр или антивирус блокирует обращение к серверу обновлений	Добавьте КриптоАРМ в исключения или временно отключите защиту
Используется прокси-сервер	Убедитесь, что в системе настроены параметры прокси
Выбран стабильный канал, а новая версия — предварительная	Переключите канал обновлений на **Бета** и повторите проверку
Установлена самая свежая версия	Номер текущей версии показан в строке **Версия** раздела **О программе**

Сообщения об ошибках:

Сообщение	Что это значит	Что сделать
Не удалось получить обновление	Приложение не смогло связаться с сервером обновлений	Проверьте подключение к интернету и настройки прокси, затем нажмите **Проверить обновления**
Не удалось установить версию X.Y.Z	Установка не запустилась — например, был отклонён запрос прав администратора	Нажмите **Установить и перезапустить** ещё раз и подтвердите запрос системы

Если обновиться через приложение не удаётся, установите новую версию поверх текущей обычным установщиком — см. Установка на Windows, Установка на Linux или Установка на macOS.

> 🚨 Если ни одно из решений не помогло, обратитесь в техническую поддержку: support@trusted.ru.

Смотрите также

- Общие настройки — остальные настройки приложения.
- Активация лицензии — состояние лицензии в том же разделе.
- Установка на Windows — руководство по установке КриптоАРМ на Windows.
- Установка на Linux — руководство по установке КриптоАРМ на Linux.
- Установка на macOS — руководство по установке КриптоАРМ на macOS.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Обзор операций КриптоАРМ и выбор мастера

В этом разделе описано, как работать с документами в КриптоАРМ: создавать подписи по стандартам CAdES и PAdES, шифровать файлы и выбирать подходящий мастер для конкретной задачи.

Этот обзор поможет быстро сориентироваться в возможностях КриптоАРМ и перейти к нужному сценарию работы.

Содержание:

- Основные операции
- Электронная подпись в КриптоАРМ
- Особые операции с подписью
- Выбор мастера
- Смотрите также

Основные операции

В КриптоАРМ все действия с документами выполняются в виде операций — последовательных процессов, которые позволяют создавать электронные подписи, шифровать файлы, проверять подписи и расшифровывать защищённые данные.

Операции выполняются с помощью специальных мастеров — пошаговых интерфейсов, которые позволяют решать задачи. В рамках одной операции можно выполнять одну или несколько задач одновременно:

- создание электронной подписи,
- архивирование и шифрование документов,
- проверку подписей и расшифрование.

Операция	Что делает	Где выполняется
Подписать	Создаёт электронную подпись файлов	«Подпись и шифрование», «Подпись и защита PDF»
Архивировать	Упаковывает файлы в ZIP	«Подпись и шифрование»
Зашифровать	Шифрует файлы в адрес получателей	«Подпись и шифрование»
Проверить подпись		«Проверка и расшифрование», «Подпись и защита PDF»

Операция	Что делает	Где выполняется
	Проверяет подпись, цепочку доверия, отзыв и штампы времени	
Расшифровать	Расшифровывает файлы вашим сертификатом	«Проверка и расшифрование»
Снять подпись	Извлекает исходный документ из присоединённой подписи	«Проверка и расшифрование»
Объединить подписи	Собирает несколько отсоединённых подписей в один файл	«Подпись и шифрование»

Параметры операций можно сохранить в профиле подписи, чтобы в дальнейшем применять готовые настройки без повторной ручной конфигурации.

Порядок выполнения

В разделе **«Подпись и шифрование»** можно выбрать сразу несколько операций. Они выполняются последовательно:

```
Подписать → Архивировать → Зашифровать
```

Примеры сочетаний:

- **Подписать** — на выходе файл подписи (или подписанный PDF);
- **Подписать + Зашифровать** — подпись, затем шифрование результата;
- **Подписать + Архивировать + Зашифровать** — подпись, упаковка в ZIP, шифрование архива;
- **Зашифровать** — только шифрование исходных файлов.

Выбранные операции и их параметры видны в сводке над списком файлов до запуска.

Электронная подпись в КриптоАРМ

Электронная подпись используется для подтверждения подлинности, целостности и юридической значимости электронных документов.

Приложение КриптоАРМ позволяет создавать подписи со стандартами:

- **CAdES** — для любых файлов (DOCX, XLSX, XML и других типов данных);
- **PAdES** — для PDF-документов с возможностью видимого штампа подписи.

Выбор стандарта подписи зависит от типа документа, требований к его хранению и способа проверки подписи.

Ниже приведено краткое сравнение стандартов электронной подписи:

Стандарт	Для каких файлов	Тип подписи	Визуальный штамп
CAdES	Любые (docx, xlsx, pdf, xml и др.)	Отсоединённая / присоединённая	Нет (кроме печатной формы)
PAdES	Только PDF	Встроенная	Да / нет

Подпись со стандартом CAdES

CAdES используется для подписания файлов любых форматов. Уровень стандарта определяет, что вложено в подпись помимо неё самой и как долго её потом можно проверить: чем ниже строка в таблице, тем дольше подпись остаётся проверяемой — и тем больше для неё требуется.

Стандарт	Зачем нужен	Что требуется
CAdES-BES	Базовая подпись документа: кроме самой подписи в неё вложены сведения о подписанте	—
CAdES-T	Добавляет отметку точного времени от независимой службы — подтверждает, что документ подписан именно тогда, а не задним числом	Адрес службы TSP
CAdES-X Long Type 1	Подпись останется проверяемой и после того, как сертификат истечёт: внутрь вложены доказательства, что на момент подписания он действовал	Адрес службы TSP
CAdES-A	Архивная подпись для долгосрочного хранения: её можно перепроверять годами, даже когда сертификат давно недействителен	Адрес службы TSP

Если принимающая сторона не назвала стандарт, оставьте тот, что уже выбран в профиле подписи, — менять его без требования не нужно. Как выбрать стандарт и указать службу штампов времени, описано в инструкции Настройки подписи и шифрования.

> 💡 **Примечание**: подписи CAdES создаются только сертификатами КриптоПро. Сертификатом встроенного провайдера OpenSSL подпись создаётся в базовом формате **CMS** — приложение выбирает его само, и поле выбора стандарта в этом случае недоступно.

Подпись CAdES может быть:

- **присоединённой** — подпись и документ объединяются в один файл;
- **отсоединённой** — подпись сохраняется отдельно (обычно с расширением `.p7s` или `.sig`), при этом исходный документ не изменяется.

Такой подход позволяет выбрать оптимальный вариант хранения и передачи документов в зависимости от требований процесса.

Печатная форма

Для PDF-документов, подписанных обычной подписью (CAdES или CMS), доступно создание печатной формы.

Печатная форма — это копия документа с визуальным отображением штампа подписи. В ней отсутствует электронная подпись и криптографические данные.

> ⚠️ **Примечание**: печатная форма предназначена только для визуального ознакомления и подтверждения факта подписания. Она не обладает юридической силой, так как не содержит электронной подписи.

Печатные формы можно создавать:

- при выполнении подписи — вариант **«Обычная подпись + печатная копия»** (см. Подпись и шифрование файлов);
- при просмотре сведений о подписи (см. Печатная форма со штампом).

Подпись со стандартом PAdES

PAdES — стандарт электронной подписи для PDF-документов. Подпись встраивается непосредственно в PDF-файл без изменения его формата и без создания отдельного файла подписи.

Документ остаётся обычным PDF и может быть открыт в любом просмотрщике.

Подпись PAdES может быть:

- **видимой** — отображается в виде штампа на странице;
- **невидимой** — не отображается визуально, но полностью доступна для проверки.

Сертифицирующая подпись PDF

Сертифицирующая подпись — это особый тип электронной подписи, применяемый к PDF-документу до внесения в него других подписей. Она не только подтверждает авторство и целостность документа, но и устанавливает правила его дальнейшего использования.

В отличие от обычной подписи, сертифицирующая подпись позволяет контролировать, какие изменения разрешены после подписания, а любые неразрешённые модификации приводят к утрате валидности подписи.

При сертификации документа определяется перечень допустимых действий, например установка подписи в заранее размеченные области для подписантов и изменение оформления произвольной области.

Все действия, не включённые в список разрешённых, приведут к тому, что сертифицирующая подпись станет недействительной при проверке.

> ⚠ **Примечание**: поставить сертифицирующую подпись может только первый подписант — см. Сертифицировать документ.

Конвертация в формат PDF/A

PDF/A — международный стандарт (ISO 19005) для долгосрочного архивирования PDF-документов; он обеспечивает их корректное воспроизведение на любых устройствах в будущем.

КриптоАРМ поддерживает конвертацию в форматы:

- **PDF/A-2b** — обеспечивает базовую стабильность для долгосрочного хранения;
- **PDF/A-3b** — позволяет добавлять структурированные данные и прикреплённые файлы без нарушения стандартов.

При конвертации выполняется удаление или отключение элементов, которые могут нарушить отображение документа или повлиять на его безопасность: скриптов (JavaScript), мультимедиа, 3D-объектов и интерактивных форм, внешних ссылок на ресурсы, а также шифрования и парольной защиты.

> ⚠ **Примечание**: конвертация доступна только для неподписанных документов и выполняется совместно с подписью документа — см. Конвертировать в формат PDF/A.

Особые операции с подписью

Соподпись

Если добавить в раздел «Подпись и шифрование» существующий файл подписи и выполнить подпись, ваша подпись будет добавлена в этот же файл. Так документ подписывают несколько человек.

Объединение подписей

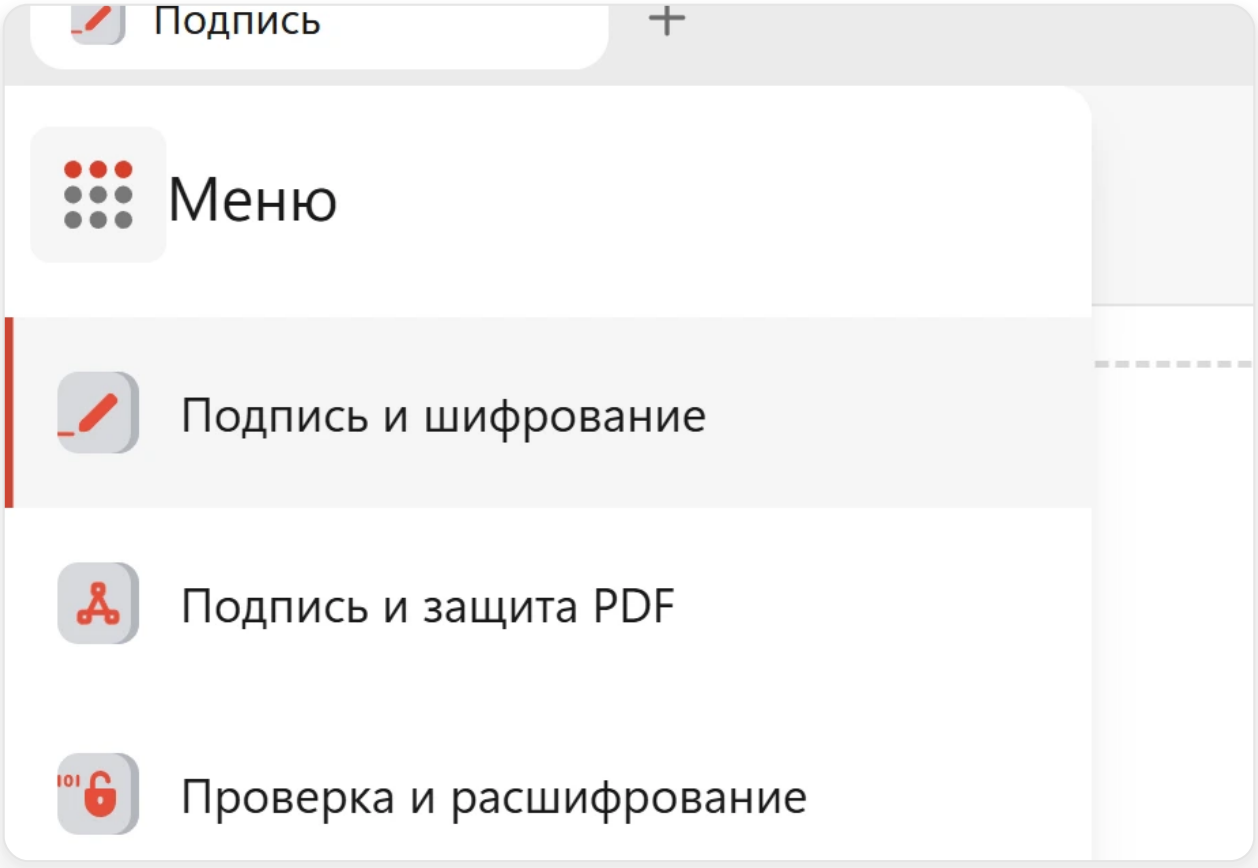
Несколько отсоединённых подписей одного документа можно собрать в один файл подписи — кнопка **Объединить подписи** на панели инструментов.

Снятие подписи

Из присоединённой подписи можно извлечь исходный документ — в разделе «Проверка и расшифрование».

Выбор мастера

Выбор мастера в КриптоАРМ зависит от типа документа и выполняемой операции. Ниже приведено краткое описание основных мастеров и сценариев их использования.



- Подпись и шифрование — предназначен для групповой работы с файлами. Позволяет подписывать и шифровать несколько документов одновременно, создавать архивы и использовать стандарты CAdES и PAdES. Настройки берутся из активного профиля подписи.
- Подпись и защита PDF — оптимален для работы с одним PDF-документом. Предоставляет инструменты просмотра, проверки подписей, разметки областей, подготовки мест для других подписантов и добавления новых подписей в одном интерфейсе.
- Проверка и расшифрование — используется для работы с файлами, содержащими электронные подписи и (или) зашифрованные данные. После загрузки файла приложение автоматически определяет его тип и производит доступные действия: проверку электронной подписи, расшифрование данных или обе операции одновременно.

Задача / Сценарий	Рекомендуемый мастер	Почему
Подписать / зашифровать **много файлов** сразу	Подпись и шифрование	Групповая обработка, CAdES и PAdES, архивы, шифрование
Работать с **одним PDF**: просмотр, разметка областей, несколько подписантов	Подпись и защита PDF	Встроенный просмотрщик, разметка, сертификация, PDF/A
Проверить подпись / расшифровать документ	Проверка и расшифрование	Автоматически определяет тип файла и предлагает действия
Добавить ещё одну подпись к уже подписанному файлу	Подпись и шифрование или Подпись и защита PDF	Зависит от формата исходного файла

> 💡 **Примечание**: файлы можно передать из одного раздела в другой кнопкой **Добавить в** на панели инструментов — например, отправить только что подписанный PDF в мастер PDF или в проверку.

Смотрите также

- Профили подписи — сохранение параметров операций в профилях для повторного использования.
- Подпись и шифрование — руководство по созданию электронных подписей и шифрованию файлов.
- Проверка и расшифрование — проверка подписей и расшифрование документов.
- Подпись и защита PDF — работа с PDF: просмотр, разметка областей, добавление подписей и сертифицирующая подпись.
- Настройки подписи и шифрования — справочник всех параметров.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Создание и управление профилем подписи

Профиль подписи в КриптоАРМ — это готовый шаблон настроек для операций с документами: какие действия выполнять, каким сертификатом, в каком формате и куда сохранять результат. Используйте профили, чтобы применять нужные параметры в один клик, экономя время на ручной настройке.

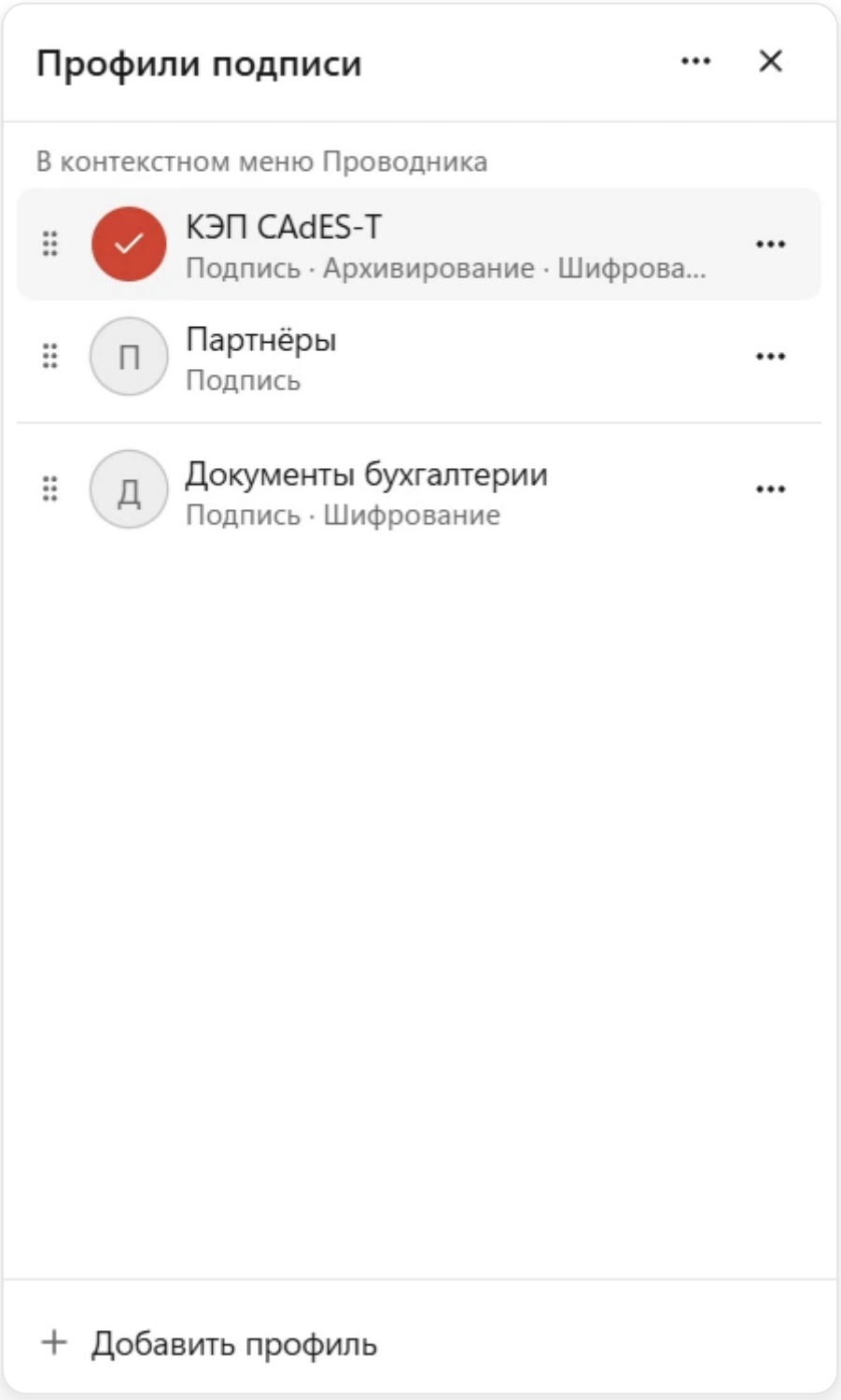
В этом руководстве вы узнаете, как создавать и настраивать профили подписи.

Содержание:

- Где находятся профили
- Создание профиля подписи
- Переключение между профилями подписи
- Редактирование настроек профиля подписи
- Сохранение настроек в мастере «Подпись и шифрование»
- Порядок профилей
- Профили в контекстном меню Проводника
- Удаление профилей подписи
- Экспорт и импорт профилей подписи
- Смотрите также

Где находятся профили

Профили доступны в мастерах **«Подпись и шифрование»** и **«Подпись и защита PDF»**. Имя активного профиля показано в верхней части раздела; щелчок по нему открывает панель **«Профили подписи»**.



💡 **Примечание**: профили хранятся отдельно для X.509 и для OpenPGP. Панель показывает профили того стандарта, который выбран настройкой «Стандарт операций по умолчанию».

При первом открытии раздела приложение создаёт профиль само: для X.509 он называется **«Профиль»**, для OpenPGP — **«Профиль PGP»**. Настройки, заданные в мастере, сохраняются в активный профиль, поэтому создавать профиль перед первой операцией не нужно.

Профиль есть всегда: последний профиль удалить нельзя — операции выполняются только под профилем.

Создание профиля подписи

> 💡 **Совет**: начните с профилей для самых частых операций, затем постепенно добавляйте специализированные настройки по мере необходимости.

1. Откройте раздел **«Подпись и шифрование»**.
2. Щёлкните по имени активного профиля.
3. Внизу панели нажмите **Добавить профиль**.
4. Откроется вкладка **«Редактирование профиля»**.
5. В блоке **Общие настройки** укажите **Название профиля**.
6. В блоке **Операции** укажите, какие действия нужно выполнить с документом. Можно выбрать одну операцию или несколько сразу: при сочетании **Подписать + Архивировать + Зашифровать** документ сначала подписывается, затем результат упаковывается в архив, а архив шифруется для выбранных получателей.
7. Задайте остальные параметры — см. Настройки подписи и шифрования.
8. Нажмите **Сохранить**.

Появится сообщение **«Профиль «...» создан»**, и вкладка редактирования закроется.

Переключение между профилями подписи

Активный профиль автоматически применяется в мастерах подписи и шифрования. Чтобы переключить профиль, откройте мастер **«Подпись и шифрование»** или **«Подпись и защита PDF»**, щёлкните по имени активного профиля и выберите нужный в списке. Настройки применятся сразу.

Под названием каждого профиля показан состав его операции — например, «Подпись · Шифрование». Если операции не выбраны, вместо состава отображается **«Операции не выбраны»**: такой профиль выполнить нельзя.

Редактирование настроек профиля подписи

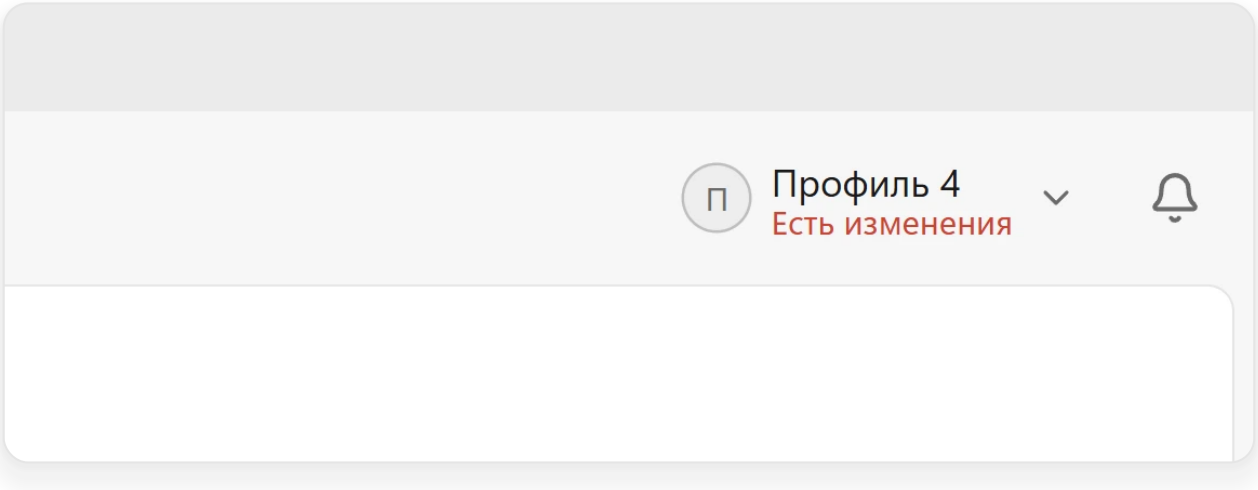
1. Откройте панель профилей.

2. Нажмите кнопку меню в строке профиля и выберите **Редактировать**.
3. Измените настройки и нажмите **Сохранить изменения**.

Профиль откроется в отдельной вкладке, поэтому редактирование не мешает работе в других разделах.

Сохранение настроек в мастере «Подпись и шифрование»

Настройки можно менять прямо перед выполнением операции. Если текущие параметры отличаются от сохранённых в профиле, рядом с его именем появляется отметка **«Есть изменения»**.



Доступны два действия:

- **Сохранить изменения** — записать параметры в текущий профиль;
- **Сохранить как новый профиль** — создать профиль с этими параметрами, не изменяя исходный.

Если изменения не сохранять, они действуют до переключения профиля.

> ⚠️ **Важно**: сохранение изменений в текущем профиле отменить нельзя — прежние настройки будут заменены новыми. Если они ещё нужны, заранее сохраните профиль в файл.

Порядок профилей

Профили в списке можно перетаскивать мышью за область захвата в строке. Порядок сохраняется и используется в том числе в контекстном меню Проводника (порядок быстрых действий Finder задаёт сама система).

Профили в контекстном меню Проводника

> 💡 **Примечание**: раздел относится к Windows и macOS. На macOS та же настройка называется **Показывать в быстрых действиях Finder**, а раздел панели — **«В быстрых действиях Finder»**. На Linux настройки нет.

Профиль можно вывести в контекстное меню Проводника — тогда операция запускается прямо из меню файла.

1. Откройте панель профилей.
2. Нажмите кнопку меню в строке профиля.
3. Включите **Показывать в меню Проводника**.

Профили, выведенные в меню, собираются в панели в отдельный раздел **«В контекстном меню Проводника»** и идут в меню в том же порядке.

Ограничения:

Сообщение	Что это значит	Что сделать
В профиле нет операции	В профиле не выбрано ни одного действия — выполнять нечего	Отметьте в профиле подпись, шифрование или архивирование
Меню заполнено: 10 профилей	В меню уже выведено десять профилей	Выключите ненужный профиль, чтобы освободить место

Подробнее о работе меню — в инструкции Контекстное меню Проводника.

Удаление профилей подписи

1. Откройте панель профилей.
2. Нажмите кнопку меню в строке профиля и выберите **Удалить**.
3. Подтвердите действие.

> ⚠️ **Важно**: удаление профиля нельзя отменить — профиль будет полностью удалён из приложения. Последний оставшийся профиль удалить нельзя: операции выполняются только под профилем.

Экспорт и импорт профилей подписи

Экспорт профиля подписи позволяет сохранить настройки в файл для резервного копирования, переноса на другой компьютер или передачи коллегам. Файл сохраняется с расширением `.pcarm-profile`; при импорте принимаются также файлы `.json`.

Экспорт профиля в файл

1. Откройте панель профилей.
2. Нажмите кнопку меню в строке профиля и выберите **Сохранить в файл**.
3. Укажите имя и расположение файла.

Экспорт всех профилей

1. Откройте панель профилей.
2. Нажмите кнопку **Ещё** в заголовке панели.
3. Выберите **Сохранить все в файл**.

Импорт профиля из файла

1. Откройте панель профилей.
2. Нажмите кнопку **Ещё** в заголовке панели.
3. Выберите **Импортировать из файла** и укажите файл.

После импорта появится сообщение о количестве добавленных профилей. Если часть записей в файле некорректна, они будут пропущены с сообщением **«Пропущено N некорректных профилей»**.

> 💡 **Примечание**: профиль хранит идентификатор сертификата. Если на новом рабочем месте этого сертификата нет, выберите в профиле другой сертификат подписи.

Смотрите также

- Настройки подписи и шифрования — справочник всех параметров профиля.
- Подпись и шифрование — как выполнить операцию.
- Контекстное меню Проводника — запуск профиля из Проводника.

- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Подпись и шифрование файлов

В этой инструкции вы научитесь подписывать и шифровать документы в КриптоАРМ с помощью мастера **Подпись и шифрование**. С его помощью вы легко подпишете несколько документов одновременно, защитите их шифрованием и выполните смешанные операции — например, сначала подпись, а затем шифрование.

Содержание:

- Что потребуется
- Работа с пошаговым мастером
- Подпись со стандартом CAdES
- Подпись со стандартом PAdES
- Подпись с машиночитаемой доверенностью
- Добавление соподписи
- Объединение подписей
- Шифрование
- Подпись и шифрование за одну операцию
- Действия в мастере
- Результат операции
- Особенности OpenPGP
- Возможные ошибки
- Смотрите также

Что потребуется

- **Сертификат подписи с закрытым ключом** — то есть ваш собственный сертификат: подписать можно только тем, ключ от которого есть у вас. Как его получить: установка сертификата, создание сертификата OpenPGP.
- **Сертификаты получателей** — если файлы шифруются. Их импортируют заранее и при необходимости объединяют в группу.
- **КриптоПро CSP и действующая лицензия КриптоАРМ** — для операций с ГОСТ-сертификатами. Проверить и то, и другое можно в разделе **Настройки**: криптопровайдеры, лицензия.
- **Доступ в интернет к службе штампов времени** — только если выбран стандарт подписи CAdES-T, CAdES-X Long Type 1 или CAdES-A. Адрес службы уже указан в настройках, менять его не требуется.

Работа с пошаговым мастером

Мастер **Подпись и шифрование** состоит из нескольких последовательных шагов:

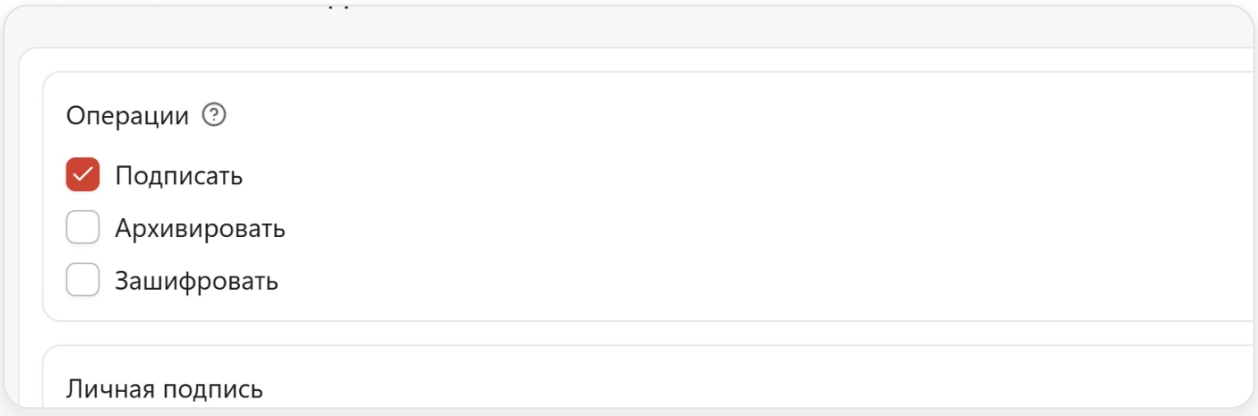
1. **Файлы** — добавьте документы.
2. **Настройки** — проверьте состав операции и её параметры.
3. **Подтверждение** — убедитесь, что выполняется именно то, что нужно.
4. **Результат** — заберите файлы, откройте их или передайте дальше.

Над списком файлов показана сводка операции: какие действия выполняются, каким сертификатом и для кого шифруются файлы.

> 💡 **Примечание**: если в профиле выключена настройка **«Показывать эти настройки перед выполнением»**, шаг настроек пропускается и операция сразу переходит к подтверждению.

Подпись со стандартом CAdES

1. Добавьте файлы в мастер — см. Добавление документов.
2. Выберите профиль подписи или оставьте активный — см. Профили подписи.
3. Нажмите **Далее**.
4. В блоке **Операции** отметьте **Подписать**.



1. В блоке **Личная подпись** укажите:

- **Сертификат подписи** — сертификат с закрытым ключом;
- **Стандарт подписи** — CAdES-BES, CAdES-T, CAdES-X Long Type 1 или CAdES-A; для сертификата встроенного провайдера OpenSSL поле показывает **CMS** и недоступно для изменения;
- **Машиночитаемая доверенность** — при подписании по доверенности.

> 💡 **Примечание**: для CAdES-T, CAdES-X Long Type 1 и CAdES-A нужно указать адрес службы штампов времени (TSP) — см. Служба штампов времени.

1. При необходимости раскройте **Настройки подписи** и измените:

- **Вид подписи** — присоединённая или отсоединённая;
- **Формат файла подписи** — `.sig`, `.p7s`, `.sgn`, `.sign`, `.bin`, `.pem`;
- **Данные в подписи** — сертификат владельца, цепочка без корневого или все сертификаты цепочки;
- **Кодировка подписи** — DER или BASE-64.

1. Проверьте блок **Сохранение результатов**: куда сохранять файлы и как их именовать.
2. Нажмите **Выполнить**.
3. Подтвердите операцию и при необходимости введите PIN-код или пароль закрытого ключа.

По завершении в списке появятся строки результатов со статусом **«Успешно»** или **«Ошибка»**. Готовые файлы сохраняются туда, куда указывает блок **Сохранение результатов**.

Подробное описание каждого параметра — в инструкции Настройки подписи и шифрования.

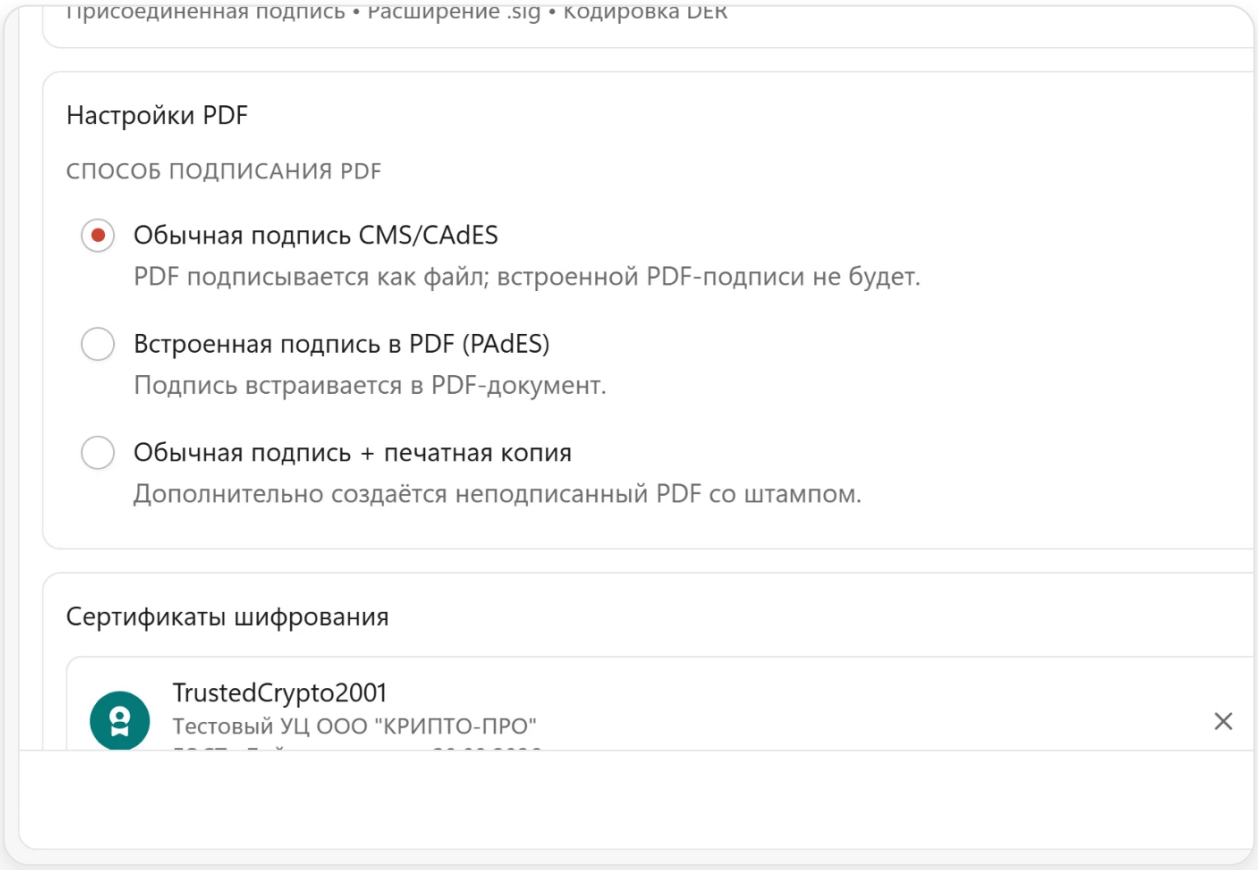
Подпись со стандартом PAdES

Для PDF-файлов в блоке **Настройки PDF** выбирается **способ подписания**:

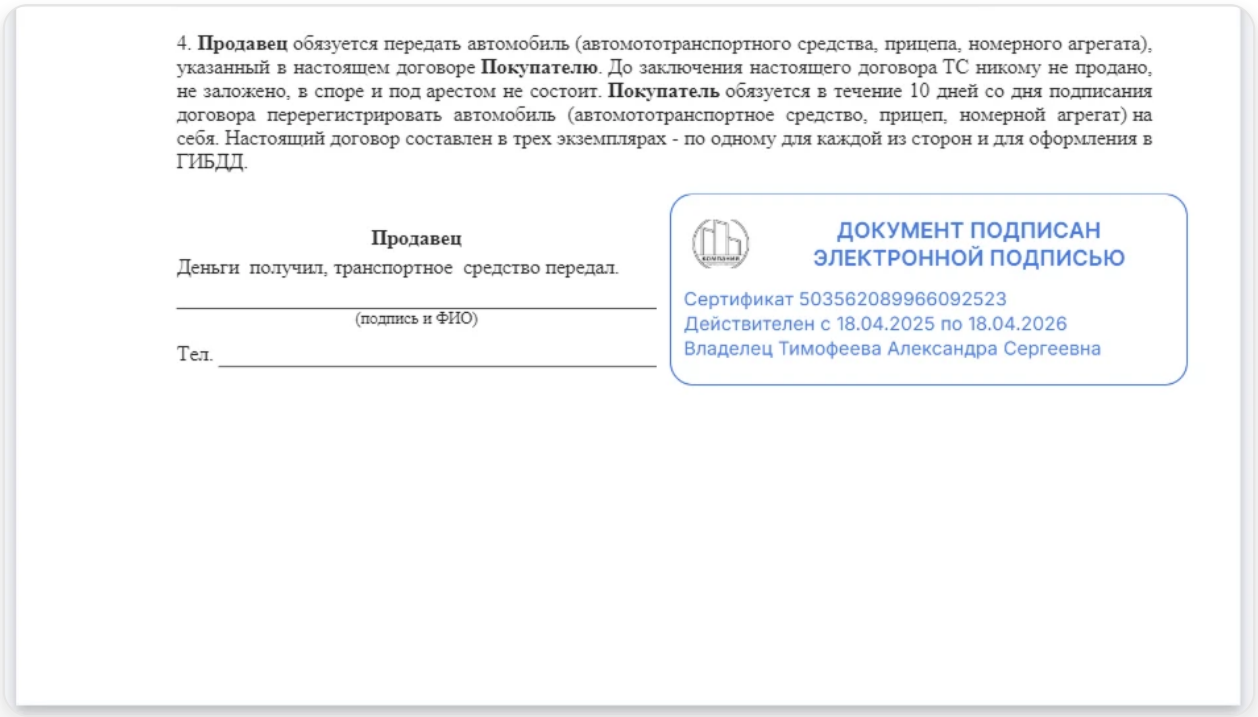
Способ	Результат
Обычная подпись CMS/CAdES	PDF подписывается как файл, создаётся отдельный файл подписи
Встроенная подпись в PDF (PAdES)	Подпись помещается внутрь документа, результат остаётся PDF
Обычная подпись + печатная копия	Файл подписи плюс отдельный неподписанный PDF со штампом

Для встроенной подписи дополнительно доступны:

- **Подготовка PDF** — преобразование в PDF/A-2b или PDF/A-3b перед подписанием;
- **Сертификация** — сертифицирующая подпись с разрешениями на последующие изменения;
- **Визуальное оформление** — видимый штамп подписи, его оформление и положение на странице.



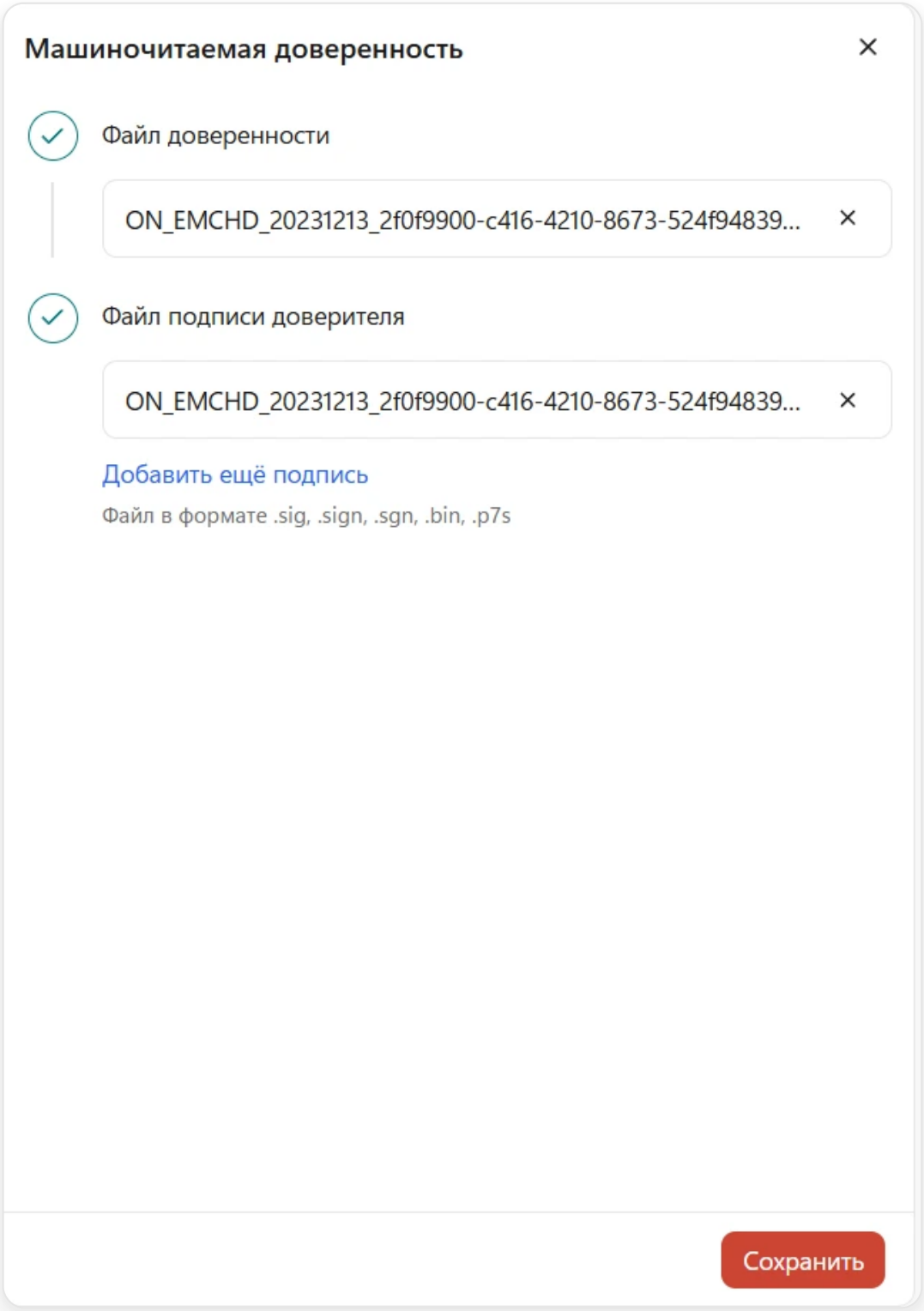
Пример визуализации штампа подписи:



> 💡 **Совет**: если важно, где именно на странице встанет подпись, или документ подписывают несколько человек, используйте мастер Подпись и защита PDF.

Подпись с машиночитаемой доверенностью

1. В блоке **Личная подпись** нажмите на поле **Машиночитаемая доверенность**.
2. Нажмите **Добавить доверенность** и выберите XML-файл МЧД.
3. Нажмите **Добавить файл подписи** и выберите подпись доверителя — файл `.sig`, `.sign`, `.sgn`, `.bin` или `.p7s`. Подписей может быть несколько: следующую добавляет ссылка **Добавить ещё подпись**.
4. Нажмите **Добавить**. Если доверенность в операции уже была и вы её заменяете, кнопка называется **Сохранить**.



В поле **Машиночитаемая доверенность** появятся номер доверенности, имя XML-файла и число приложенных подписей.

Проверку доверенности приложение выполняет в фоне, а её результат показывает только тогда, когда он мешает операции, — в окне подтверждения:

Вопрос в окне подтверждения	Когда появляется
Проверка МЧД ещё не завершена. Использовать доверенность при подписи?	Проверка не успела закончиться
МЧД не прошла проверку: срок действия, подписи доверенности или ИНН представителя требуют внимания. Использовать доверенность при подписи?	Истёк срок, подписи доверенности недействительны или ИНН не совпадают

Подписать всё равно можно — решение остаётся за вами.

Полные сведения о доверенности — номер, срок действия, ИНН доверителя и представителя, статус подписей и применимость к сертификату — показываются при проверке подписи, см. Проверка соответствия МЧД сертификату подписи.

Чтобы убрать доверенность из операции, откройте то же поле и нажмите **Убрать**.

Добавление соподписи

Соподпись — добавление дополнительной электронной подписи к документу, который уже содержит одну или несколько подписей. Статус такого документа считается действительным только при действительности всех подписей.

Если исходный документ содержит присоединённую подпись, соподпись тоже делают присоединённой, чтобы все подписи хранились в одном файле; для отсоединённой подписи — наоборот.

Чтобы добавить свою подпись к уже подписанному документу, добавьте в раздел **файл подписи** и выполните операцию подписи. Ваша подпись будет добавлена в тот же файл.

Файлы подписи X.509 и подписанные PDF проверяются сразу после добавления: значок файла в списке показывает, действительна ли подпись, а подробности открываются в панели сведений по щелчку на файле. Полную проверку с отчётом выполняет раздел **Проверка и расшифрование** — туда файлы передаются кнопкой **Добавить в**.

> ⚠️ **Важно**: если результат сохраняется рядом с исходным файлом, файл подписи будет перезаписан. Приложение предупреждает об этом в окне подтверждения.

Объединение подписей

Несколько отсоединённых подписей одного документа можно собрать в один файл:

1. Добавьте файлы подписей в раздел.

2. Выделите две или более подписи.
3. Нажмите **Объединить подписи** на панели инструментов.

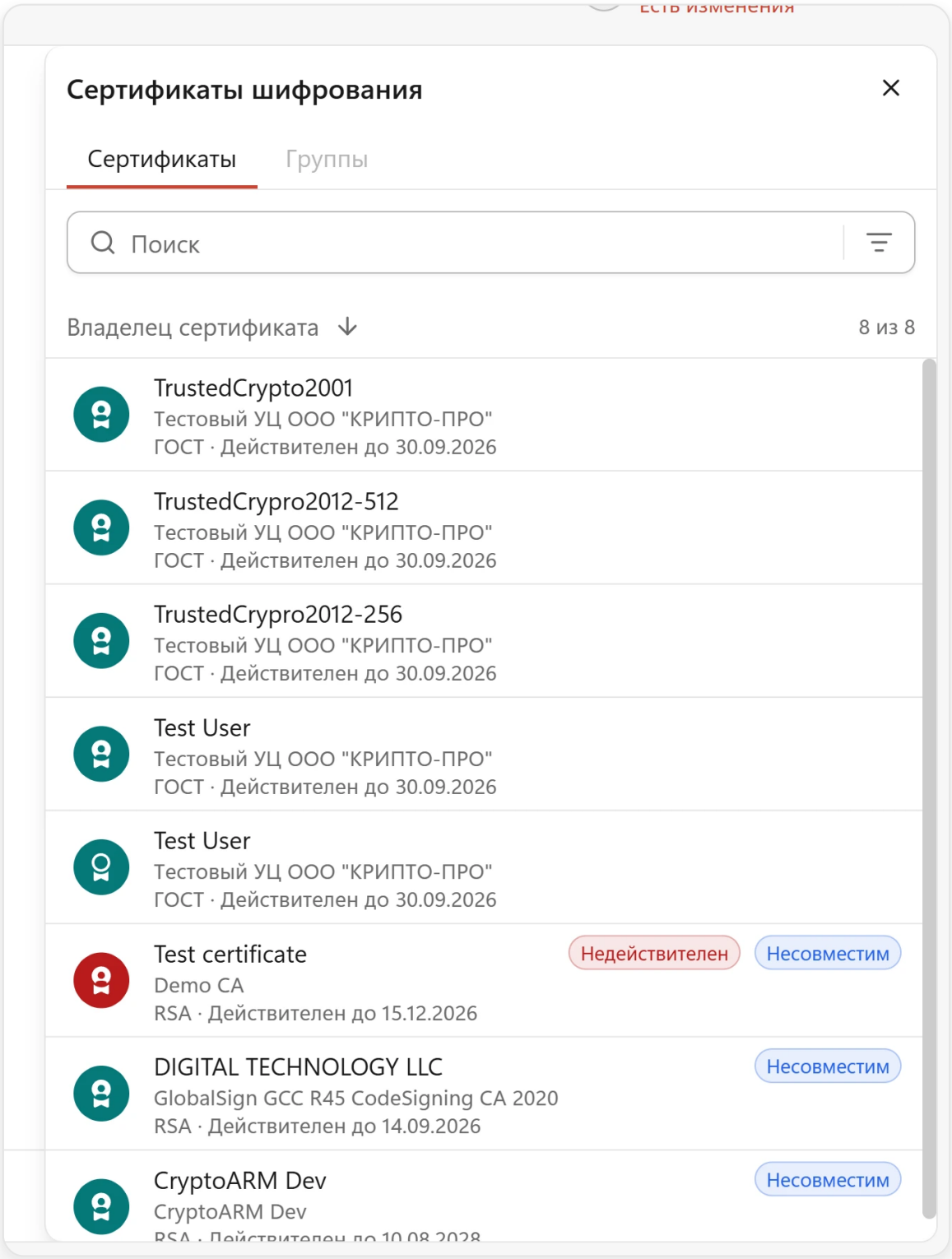
Исходные файлы остаются без изменений, а новый файл получает суффикс `_joined_<количество>_signs` и сохраняется в папке первой подписи из списка.

Если выделена одна подпись, появится сообщение **«Выберите две или более подписи»**.

Шифрование

Для шифрования файла понадобится открытый ключ получателя: вы выбираете сертификаты получателей, приложение шифрует данные в их адрес, а расшифровать их сможет только владелец соответствующего закрытого ключа.

1. Добавьте файлы и нажмите **Далее**.
2. В блоке **Операции** отметьте **Зашифровать**.
3. В блоке **Сертификаты шифрования** нажмите **Добавить сертификаты** и выберите получателей.



Выбирать можно как отдельные сертификаты, так и группы сертификатов.

1. При необходимости раскройте **Настройки шифрования** и укажите алгоритм, формат и кодировку результата.
2. Нажмите **Выполнить** и подтвердите операцию.

По завершении рядом с исходными файлами (или в указанной папке) появятся зашифрованные файлы, а в списке — строки результатов со статусом **«Успешно»**.

> ⚠️ **Важно**: настройка **«Удалить исходные файлы после шифрования»** удаляет исходники после успешного шифрования. Восстановить их можно будет только расшифрованием. Перед запуском такой операции приложение отдельно предупредит об этом в окне подтверждения.

Расшифровать файл сможет только владелец закрытого ключа одного из указанных сертификатов. Добавьте в получатели свой сертификат, если файл понадобится вам самим.

Подпись и шифрование за одну операцию

Отметьте в блоке **Операции** несколько действий сразу. Они выполняются по порядку:

```
Подписать → Архивировать → Зашифровать
```

Дополнительная операция **Архивировать** упаковывает результат в ZIP. Настройка **«Отдельный архив на каждый файл»** создаёт по архиву на файл; без неё все файлы попадают в один архив.

Состав операции виден в сводке над списком файлов до запуска и повторяется в окне подтверждения.

Действия в мастере

Некоторые действия универсальны и нужны для выполнения любой операции.

Запуск мастера

Мастер **Подпись и шифрование** открывается:

- из бокового меню — пункт **Подпись и шифрование**;
- кнопкой + в строке вкладок (правый щелчок открывает список разделов);
- из другого раздела — кнопкой **Добавить в** на панели инструментов;
- на Windows — командой **Открыть для подписи и шифрования…** в контекстном меню Проводника.

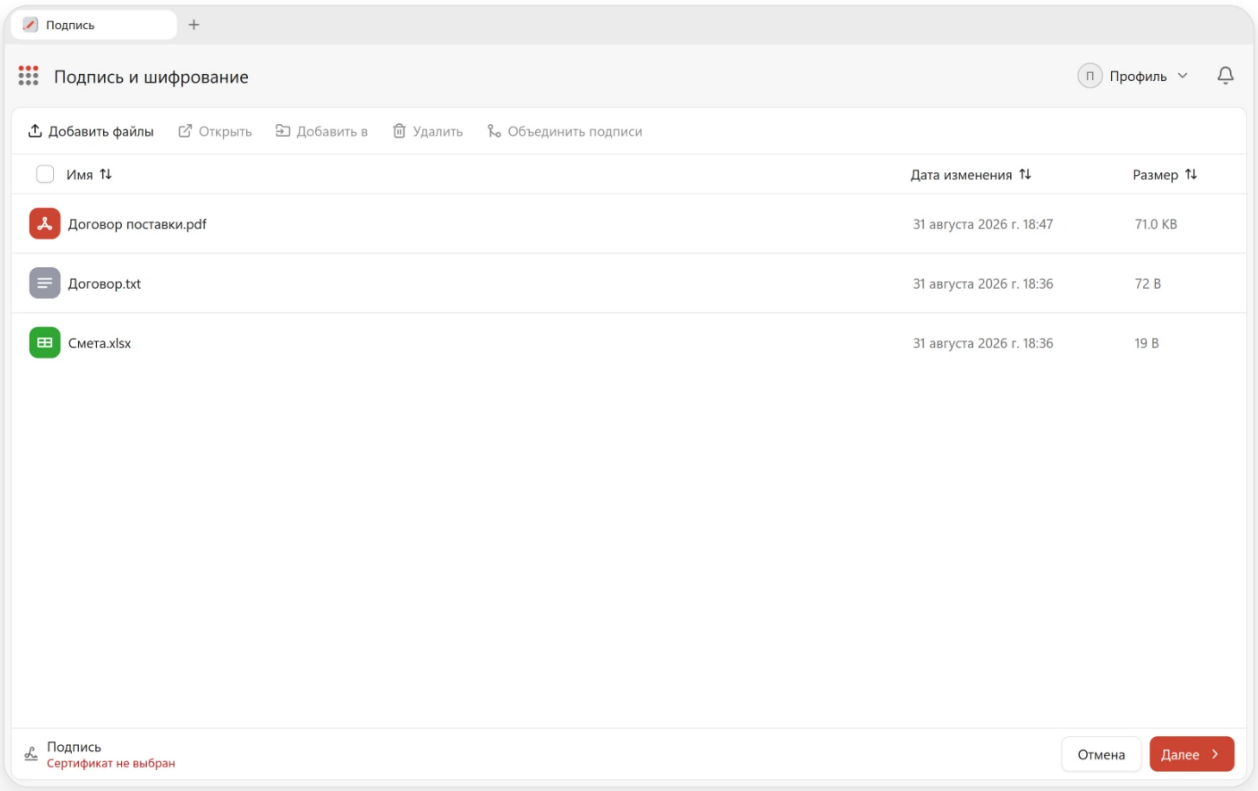
Мастер открывается в новой вкладке.

Добавление документов

Способы добавить файлы:

- перетащите их в окно раздела;

- нажмите **Добавить файлы** на панели инструментов;
- в пустом разделе нажмите на область **«Перетащите файлы сюда»**;
- передайте файлы из другого раздела кнопкой **Добавить в**;
- на Windows выберите файлы в Проводнике и воспользуйтесь командой **Открыть для подписи и шифрования...**.



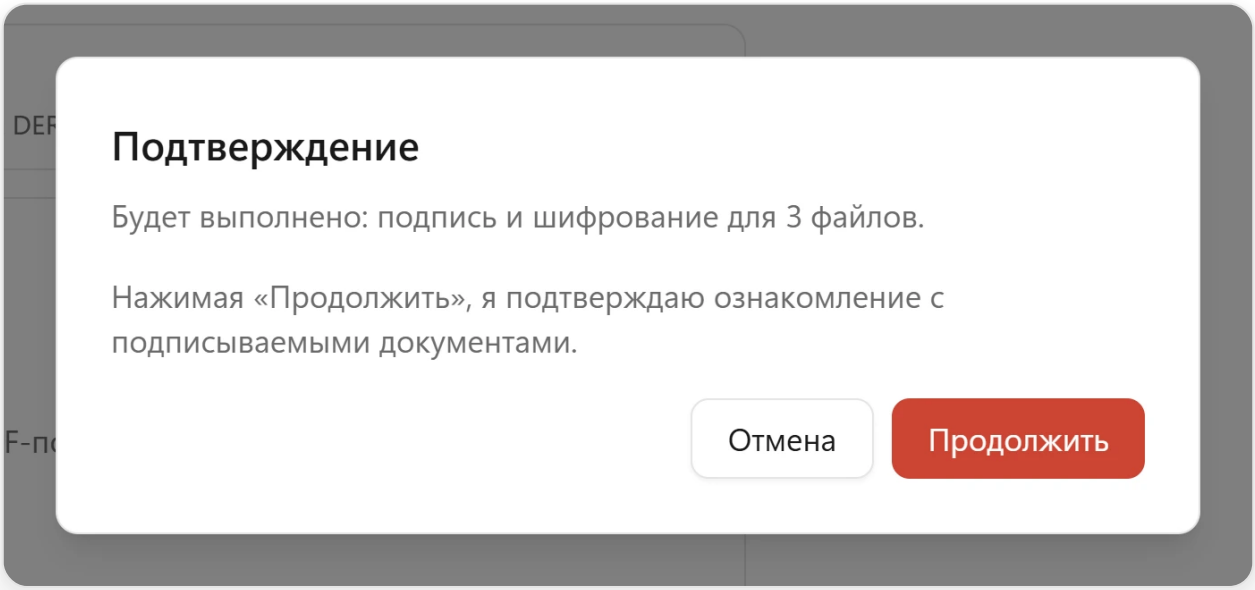
При перетаскивании папки в список попадают файлы из неё. За один раз можно добавить не более **1000** файлов — при превышении появится сообщение **«Файлы не добавлены»** с указанием количества.

Для каждого файла в списке показаны имя, размер, дата изменения и статус. Выделите строку, чтобы увидеть подробные сведения о файле.

Кнопка **Удалить** убирает выделенные файлы из списка, **Удалить все** — очищает список. Сами файлы на диске при этом не изменяются.

Подтверждение операции

Перед выполнением открывается окно **«Подтверждение»**.



В нём указаны:

- состав операции и количество файлов;
- предупреждения — удаление исходных файлов, перезапись PDF или файла подписи, недействительный сертификат, несовместимые сертификаты шифрования, замечания к МЧД;
- строка о том, что нажатием кнопки вы подтверждаете ознакомление с подписываемыми документами.

Кнопки:

- **Изменить настройки** — вернуться к параметрам операции;
- **Продолжить** — запустить операцию;
- **Отмена** — отказаться.

Дальше приложение при необходимости запросит PIN-код закрытого ключа или пароль ключа OpenPGP.

Результат операции

Во время выполнения в сводке подсвечивается текущий этап и число обработанных файлов, а в списке у каждого файла меняется статус: «Подписание», «Архивирование», «Шифрование», «Готово», «Ошибка».

По завершении:

- в списке остаются строки результатов со статусом **«Успешно»** или **«Ошибка»**;
- выделите строку, чтобы увидеть вкладки **«Файл»** и **«Результат»** со сведениями об исходном и полученном файле;

- отдельного всплывающего сообщения нет: итог виден в самом списке и записывается в журнал.

Действия на панели инструментов:

Действие	Что делает
Открыть	Открывает выбранные файлы средствами системы
Показать	Открывает папку с файлом
Добавить в	Передаёт файлы в другой раздел — проверку, мастер PDF или новую операцию
Удалить	Убирает строки из списка

> 💡 **Примечание**: при открытии сразу нескольких файлов приложение спросит подтверждение.

Особенности OpenPGP

Если выбран стандарт операций **OpenPGP**, набор настроек другой:

- в блоке **Подпись** указываются **сертификат подписи** и, при наличии нескольких, **подключ для подписи**;
- **вид подписи** — присоединённая или отсоединённая;
- в расширенных настройках доступен **хэш-алгоритм** (по умолчанию — по алгоритму ключа);
- в блоке **Шифрование** выбираются получатели: сертификаты и группы;
- настройка **ASCII armor (.asc)** сохраняет результат в текстовом виде;
- архивирование выполняется в формате TAR внутри операции.

Пароль закрытого ключа запрашивается перед выполнением подписи.

Возможные ошибки

Приложение показывает в списке результатов короткое сообщение, а техническую причину отказа записывает в журнал событий — там же виден текст криптопровайдера.

> ⚠️ **Примечание**: коды ошибок (`0x...`) приходят от криптопровайдера КриптоПро CSP.

Предупреждения перед запуском

Эти сообщения появляются на шаге настроек: пока они не сняты, операция не запускается.

Предупреждение	Что это значит	Что сделать
Выберите сертификат подписи	Не указано, каким сертификатом подписывать	Выберите сертификат в блоке **Личная подпись**
Требуется закрытый ключ	Выбран чужой сертификат — подписать им нельзя	Выберите свой сертификат из раздела **Личные**
Срок действия закрытого ключа истёк. Подписание невозможно: выберите другой сертификат или получите новый	Ключ выбранного сертификата больше не действует	Выберите другой сертификат или получите новый в удостоверяющем центре
Выбранный сертификат недействителен. Использовать сертификат?	Сертификат просрочен либо для него не построена цепочка доверия	Решение за вами: такую подпись принимающая сторона может не принять
Выберите сертификат шифрования	Не указано, для кого шифровать файлы	Добавьте получателей в блоке **Сертификаты шифрования**
Выберите сертификат шифрования, совместимый с алгоритмом шифрования	Сертификат получателя не подходит выбранному алгоритму	Выберите другого получателя или измените алгоритм шифрования
Укажите адрес службы штампов времени (TSP)	Выбранный стандарт подписи требует отметки времени	Укажите адрес службы — см. Служба штампов времени
Укажите адрес прокси / **Укажите порт прокси**	Для обращения к службе TSP включён прокси, но он не настроен	Заполните адрес и порт прокси-сервера
Укажите номер страницы PDF от 1	Для штампа подписи указана несуществующая страница	Проверьте количество страниц и укажите существующий номер
Укажите папку для сохранения результата / **Укажите существующую папку**	Папка для результатов не задана или была удалена	Проверьте блок **Сохранение результатов**
Файлы не добавлены	За один раз можно добавить не больше 1000 файлов	Добавьте файлы частями

Общие ошибки

Код ошибки	Ошибка	Рекомендуемые действия
—	**Не удалось подписать файл**	1. Проверьте права доступа к папке, указанной для сохранения результатов

Код ошибки	Ошибка	Рекомендуемые действия
		2. Освободите место на диске 3. Точная причина записана в журнале
—	**Для операций подписи и расшифрования с использованием ГОСТ алгоритмов требуется лицензия КриптоАРМ**	1. Приобретите лицензию КриптоАРМ 2. Активируйте лицензию в настройках программы
`0x0000065b`	**Проверьте наличие действующей лицензии на КриптоПро CSP**	Установите лицензию КриптоПро CSP
`0xc2100140`	**Проверьте наличие действующей лицензии на КриптоПро TSP Client**	Приобретите и установите лицензию TSP Client
`0xc2110140`	**Проверьте наличие действующей лицензии на КриптоПро OCSP Client**	Приобретите и установите лицензию OCSP Client
—	**Модуль CAdES недоступен**	Переустановите КриптоАРМ: КриптоПро ЭЦП Runtime (CAdES) входит в установщик
—	**Для CAdES-T укажите адрес службы штампов времени (TSP)**	Укажите адрес службы в настройках операции
—	**CAdES недоступен для SYSTEM/RSA сертификата / CMS недоступен для CryptoPro/GOST сертификата**	Стандарт подписи не подходит сертификату — оставьте тот, который приложение подставляет само
—	**Сертификат подписи не найден / Сертификат подписи должен быть личным / У сертификата подписи нет закрытого ключа**	Носитель отключён или сертификат сменился — выберите его заново в блоке **Личная подпись**
—	**Не удалось прочитать файл МЧД / Файл МЧД не является корректным XML**	1. Проверьте целостность файла машиночитаемой доверенности 2. Запросите корректную версию файла
—	**Неверный пароль**	Пароль закрытого ключа OpenPGP не подошёл — проверьте раскладку и регистр
—	**Не удалось создать архив / Нет файлов для архивирования**	1. Проверьте права доступа к папке результатов 2. Убедитесь, что список файлов не пуст

Код ошибки	Ошибка	Рекомендуемые действия
—	**Не удалось открыть файл**	Файл результата не открылся во внешней программе: проверьте, что он не удалён и что для его типа назначено приложение

Ошибки при подписании PDF (PAdES и печатная копия)

Ошибка	Описание	Рекомендуемые действия
Не удалось подписать PDF-файл	Документ не удалось подписать встроенной подписью	1. Уменьшите размер штампа или сдвиньте его ближе к центру страницы 2. Проверьте, что документ не защищён от изменений
Файл не является корректным PDF-документом	Файл повреждён или это не PDF	Запросите у отправителя исправную версию документа
Для PAdES-подписи выберите файл PDF	Встроенная подпись выбрана для файла другого формата	Подпишите такой файл обычной подписью CMS/CAdES
Сертификационная подпись должна быть первой подписью PDF	В документе уже есть подписи, поверх них сертифицировать нельзя	Сертифицируйте исходную неподписанную версию документа
Не удалось преобразовать PDF в PDF/A	Документ не поддаётся конвертации выбранным способом	Измените режим в блоке **Подготовка PDF** или подпишите документ без конвертации
Не удалось заменить исходный PDF подписанным	Файл занят другой программой или защищён от записи	Закройте документ и повторите операцию
Не удалось создать печатную копию PDF со штампом	Печатную копию сформировать не удалось	1. Проверьте номер страницы для штампа 2. Уменьшите размер штампа
Для печатной копии со штампом выберите файл PDF	Печатная копия создаётся только для PDF	Уберите этот способ подписания для файлов других форматов

Ошибки при шифровании

Ошибка	Рекомендуемые действия
Не удалось зашифровать файл	1. Проверьте права доступа к папке, указанной для сохранения результатов 2. Освободите место на диске
Сертификат получателя не найден	Сертификат удалён из хранилища — выберите получателя заново в блоке **Сертификаты шифрования**

Смотрите также

- Настройки подписи и шифрования — подробное описание всех параметров.
- Профили подписи — как сохранить настройки для повторного применения.
- Проверка и расшифрование — обратные операции.
- Подпись и защита PDF — точная разметка подписи в документе.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Проверка подписи и расшифрование файлов

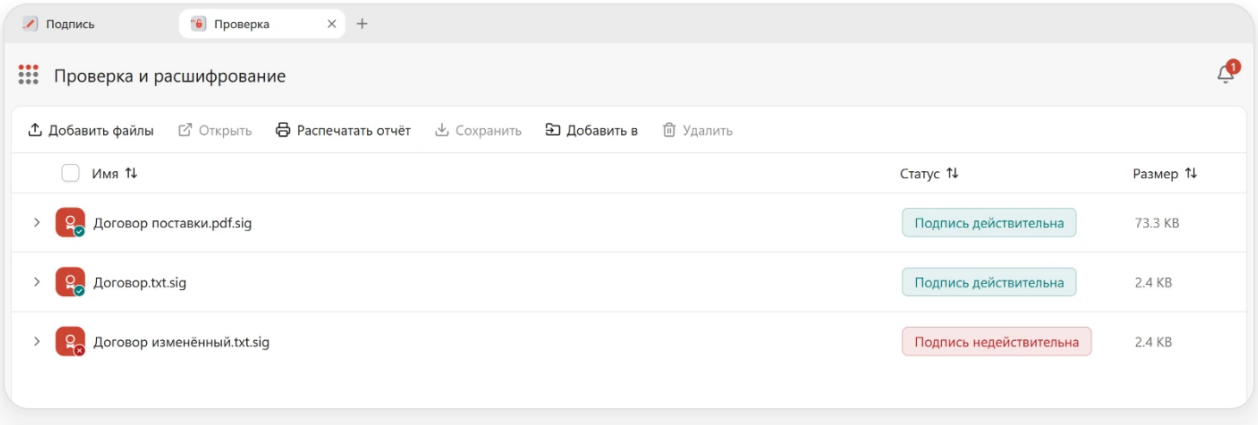
В этой инструкции вы научитесь работать с разделом **«Проверка и расшифрование»**. Вы сможете проверить электронную подпись и просмотреть её подробные сведения, снять подпись с документа, чтобы получить исходный файл, а также расшифровать зашифрованные файлы.

Содержание:

- Проверка подписи
- Снятие подписи с документа
- Расшифрование документа
- Действия в мастере
- Возможные ошибки
- Смотрите также

Проверка подписи

1. Откройте раздел **«Проверка и расшифрование»** (см. Запуск мастера).
2. Добавьте файлы (см. Добавление документов).
3. Проверка запускается автоматически сразу после добавления файлов.
4. Результат появится в столбце **Статус**, а на значке файла — отметка о результате проверки.



Возможные статусы:

Статус	Значение
Подпись действительна	Подпись верна, сертификат и цепочка проверены

Статус	Значение
Подпись недействительна	Проверка не прошла — см. сведения о подписи
Подпись не проверена	Проверку не удалось выполнить — например, не импортирован открытый ключ подписанта
Нет исходного файла	Не найден документ отсоединённой подписи — см. Отсоединённая подпись
Подписей не найдено	В файле нет электронной подписи
Расшифрован	Файл был зашифрован и успешно расшифрован
Обработка...	Файл ещё проверяется или расшифровывается
Ошибка	Проверить или расшифровать файл не удалось

Приложение само определяет, что делать с файлом: проверить подпись, расшифровать или и то, и другое. Тип операции берётся из содержимого файла.

> 💡 **Примечание**: по какому стандарту идёт проверка — X.509 или OpenPGP — определяет настройка «Стандарт операций по умолчанию». Если файл не подходит выбранному стандарту, появится сообщение **«Формат файла не поддерживается выбранным стандартом операций»**.

Отсоединённая подпись

Отсоединённая подпись хранится отдельным файлом, рядом с документом, поэтому для проверки нужен и сам документ. Приложение находит его по имени — в папке с подписью или среди файлов, добавленных в мастер: для `договор.pdf.sig` это `договор.pdf`. Если подходящих файлов несколько, приложение просит указать документ.

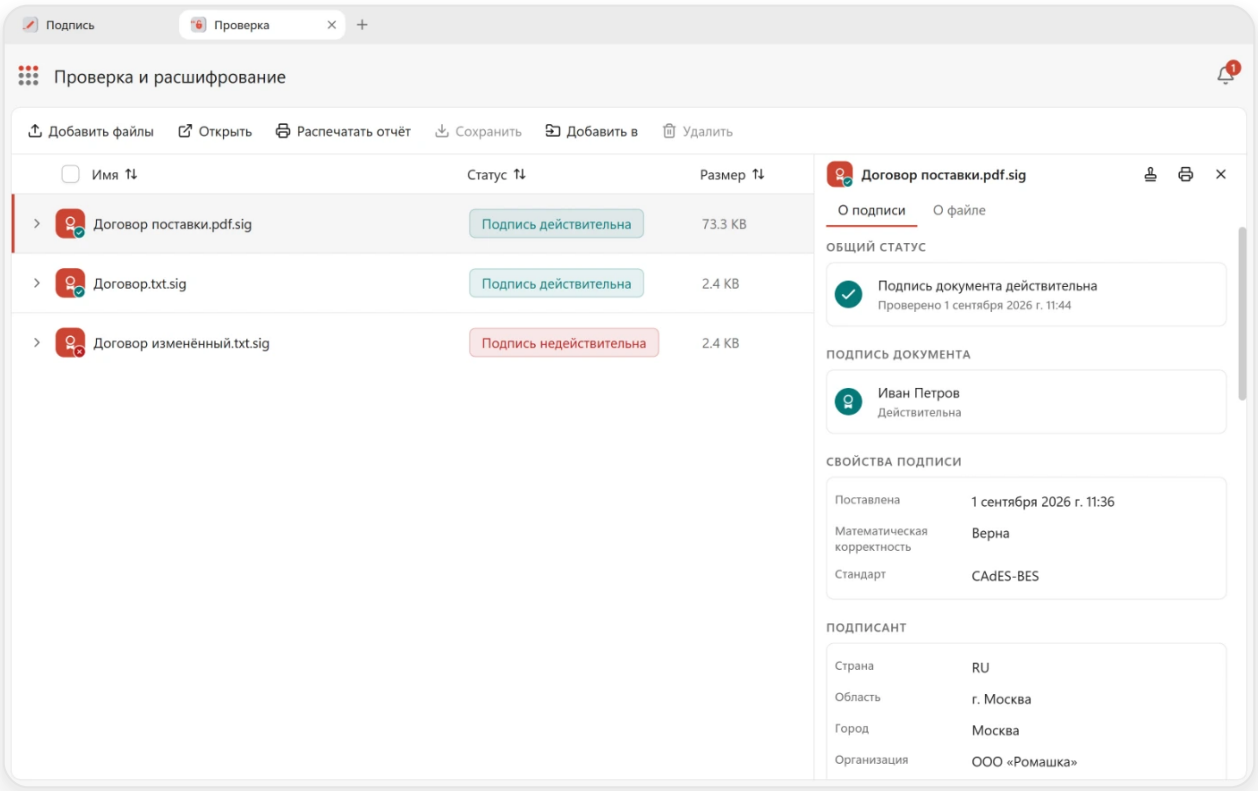
Если документ не найден, в столбце **Статус** появится **«Нет исходного файла»**, а в сведениях о подписи — **«Проверка отсоединённой подписи невозможна»**. Добавьте документ в мастер — подпись проверится заново. Или нажмите кнопку поиска файла рядом со статусом либо **Указать путь к исходному файлу** в сведениях и выберите документ вручную.

Просмотр сведений о подписи документа

Чтобы просмотреть сведения о подписи документа:

1. Выполните шаги из инструкции Проверка подписи.
2. Выделите файл в списке.
3. В правой части окна откроется панель сведений с двумя вкладками:

- **О файле** — имя, размер, расположение, даты;
- **О подписи** — результат проверки.



Для каждой подписи показаны:

Блок	Содержание
Общий статус	Действительна подпись или нет
Подписант	Владелец сертификата, издатель, серийный номер, отпечаток
Свойства подписи	Стандарт подписи, дата и время создания, алгоритм и хэш-алгоритм
Сертификат подписанта	Статус сертификата и его действительность на момент подписания
Цепочка сертификации	Действительна цепочка или нет
Статус отзыва	Результат проверки на отзыв
Штампы времени	Штампы времени, встроенные в подпись

Отдельно отмечаются предупреждения: **«Срок действия сертификата истёк на момент создания подписи»**, **«Сертификат ещё не вступил в силу на момент создания подписи»**, **«Срок действия закрытого ключа истёк на момент создания подписи»**.

Если подпись математически верна, но не проходит по политике доверия, показывается пояснение **«Подпись математически корректна, но сертификат или политика доверия недействительны»**.

> 💡 Просмотреть сведения о подписи можно не только в разделе **«Проверка и расшифрование»**, но и в результатах операции в разделе **«Подпись и шифрование»** — панель сведений там та же.

Просмотр сведений о подписи документа с соподписями

1. Выполните шаги из инструкции Просмотр сведений о подписи документа для файла, содержащего соподписи.
2. В панели сведений появится блок **«Подписи документа»** с их количеством.
3. Выберите подпись, сведения о которой нужно просмотреть.
4. Отобразится подробная информация по выбранной подписи.

Статус файла складывается из статусов всех подписей: он остаётся **«Подпись действительна»**, только если действительны все подписи, иначе файл получает статус **«Подпись недействительна»**.

Просмотр сведений о штампе времени

Если подпись создана по стандартам CAdES-T, CAdES-X Long Type 1 или CAdES-A, в сведениях появляется блок **«Штампы времени»**.

1. Выполните шаги из инструкции Просмотр сведений о подписи документа.
2. Выберите нужный штамп в блоке **«Тип штампа»**: **на данные**, **на подпись**, **на доказательства** или **архивный**.
3. Отобразится подробная информация по выбранному штампу: время штампа, имя и сертификат службы TSP, статус подписи штампа и хэш-алгоритм.

Для усовершенствованных подписей доступны дополнительные блоки с данными проверки статуса:

- блок **«Сертификат службы OCSP»** содержит сертификат, которым подписан ответ OCSP;
- блок **«Ответ службы OCSP»** содержит сам ответ с подтверждением статуса сертификата, время подписи ответа и время следующего обновления.

Статус отзыва сертификата

Блок **«Статус отзыва»** показывает, проверялся ли сертификат подписанта на отзыв и каким способом:

Источник	Значение
Список отзыва CRL	Использован список отзыва
Встроенный OCSP-ответ	Ответ службы OCSP, вложенный в подпись
Online OCSP	Обращение к службе OCSP во время проверки

Источник	Значение
Статус CAdES	Результат встроенной проверки CAdES

Возможные результаты: **«Сертификат не отозван»**, **«Сертификат отозван»** (с причиной и временем отзыва), **«Статус отзыва не проверен»**, **«Статус отзыва неизвестен»**.

Проверка подписей PDF

Для PDF со встроенной подписью дополнительно проверяется сертификация документа. В сведениях появляется блок **«Сертификация PDF»**:

- **Сертификация действительна** или **Сертификация нарушена**;
- **Разрешения сертификации** — что было разрешено после сертифицирующей подписи;
- количество изменений, нарушивших разрешения.

> 💡 **Совет**: подписи PDF удобно смотреть в мастере Подпись и защита PDF — он показывает, где именно на странице стоит каждая подпись.

Почему подпись не проходит проверку

Причина недействительности указана в сведениях о подписи. По ней видно, можно ли исправить положение на вашем рабочем месте или документ придётся запросить заново.

Причина	Можно ли исправить	Что сделать
«Криптографическая проверка не прошла — данные были изменены»	Нет — изменён документ	Запросите у отправителя оригинал документа и подпись к нему: содержимое изменилось после подписания
«Сертификат подписанта отозван»	Нет — сертификат недействителен	Запросите документ, подписанный действующим сертификатом
«Срок действия сертификата истёк на момент создания подписи»	Нет — сертификат недействителен	Подпись создана недействительным сертификатом: запросите документ, подписанный действующим
«На момент проверки срок действия сертификата истёк»	Иногда	Если подпись содержит штамп времени (CAdES-T и выше), она остаётся проверяемой. Для подписи без штампа момент подписания подтвердить невозможно — запросите документ с усовершенствованной подписью

Причина	Можно ли исправить	Что сделать
«Не удалось построить цепочку для сертификата, которым подписано сообщение»	Да	Импортируйте корневой и промежуточные сертификаты удостоверяющего центра, выпустившего сертификат подписанта, и повторите проверку
«Ошибка проверки сертификата цепочки на отзыв», **«Статус отзыва не проверен»**	Да	Импортируйте актуальный список отзыва или обеспечьте доступ к службе OCSP
«Подпись математически корректна, но сертификат или политика доверия недействительны»	Да, если причина в цепочке	Проверьте цепочку и статус отзыва в сведениях: сама подпись верна, но сертификату нет доверия
«Сертификат использует неподдерживаемый алгоритм или криптопровайдер»	Да	Для ГОСТ-подписей установите КриптоПро CSP и перезапустите приложение. Инструкции по установке: Windows, macOS, Linux
«Формат файла не поддерживается выбранным стандартом операций»	Да	Переключите стандарт операций: файл OpenPGP не проверяется по стандарту X.509 и наоборот
«Нарушены разрешения сертификации» (PDF)	Нет — изменён документ	В сертифицированный документ внесли изменения, запрещённые сертифицирующей подписью. Запросите исходную версию

> 💡 **Примечание**: недействительная подпись остаётся в списке вместе со сведениями — её можно включить в отчёт о проверке и передать отправителю как описание проблемы.

Снятие подписи с документа

Из присоединённой подписи можно извлечь исходный документ.

1. Откройте раздел **«Проверка и расшифрование»** (см. Запуск мастера).
2. Добавьте файлы (см. Добавление документов).
3. После добавления документов запустится автоматическая проверка подписи.
4. Нажмите стрелку слева от имени файла — команда **«Открыть содержимое»**.
5. Статус файла сменится на **«Снятие подписи»**, а извлечённый документ появится вложенной строкой.
6. Выполните нужное действие с документом — например, сохраните его (см. Сохранение результатов).

Той же стрелкой открывается содержимое зашифрованного файла и содержимое архива.

> 💡 **Примечание**: снять подпись можно только с присоединённой подписи. При отсоединённой подписи оригинал документа и так находится в отдельном файле.

Расшифрование документа

1. Откройте раздел **«Проверка и расшифрование»** (см. Запуск мастера).
2. Добавьте файлы (см. Добавление документов).
3. После добавления файлов запустится автоматическое расшифрование и проверка подписи, если она есть.
4. Если потребуется, укажите ПИН-код или пароль закрытого ключа:

- для сертификатов X.509 приложение запрашивает **ПИН-код закрытого ключа**. Одно окно закрывает все файлы, которым нужен этот же ПИН-код;
- для OpenPGP запрашивается **пароль закрытого ключа**.

Если пароль или ПИН-код введён неверно, появится сообщение **«Неверный ПИН-код, попробуйте ещё раз»** или **«Неверный пароль, попробуйте ещё раз»**.

1. Расшифрованный файл появится вложенной строкой под зашифрованным, а в столбце **Статус** отобразится **«Расшифрован»**.

В сведениях о файле показан блок **«Зашифровано для»** — список получателей. Ваш собственный сертификат отмечен как **«Ваш сертификат»**, скрытые получатели — как **«Скрытый получатель»**.

Если подходящего закрытого ключа нет, файл получит статус ошибки: расшифровать его на этом рабочем месте нельзя.

При успешном расшифровании исходные файлы не изменяются, а результат готовится во временном хранилище. Чтобы оставить его на диске, сохраните файлы — см. Сохранение результатов.

Действия в мастере

Некоторые действия универсальны и необходимы для выполнения любой операции.

Запуск мастера

Раздел **«Проверка и расшифрование»** можно открыть следующими способами:

- из бокового меню: нажмите кнопку **Меню** и выберите **Проверка и расшифрование**;

- из строки вкладок: нажмите + правой кнопкой мыши и выберите раздел;
- из другого раздела: выделите файлы и нажмите **Добавить в** → **Проверка и расшифрование**;
- двойным щелчком по файлу подписи или зашифрованному файлу в проводнике — см. Открытие файлов двойным щелчком;
- из контекстного меню Проводника Windows — см. Контекстное меню Проводника.

Добавление документов

Добавьте документы одним из способов:

- перетащите один или несколько файлов в окно приложения;
- нажмите **Добавить файлы** и выберите их на диске.

> 💡 **Совет**: в мастер можно перетаскивать не только файлы, но и папки — все файлы из вложенных папок тоже будут добавлены. За один раз добавляется не больше 1000 файлов; если их больше, появится сообщение **«Файлы не добавлены»** — добавьте их частями.

Проверка соответствия МЧД сертификату подписи

При проверке подписи выполняется дополнительная проверка данных владельца сертификата подписи и представителя, указанного в машиночитаемой доверенности. Сравнение идёт по реквизиту ИНН.

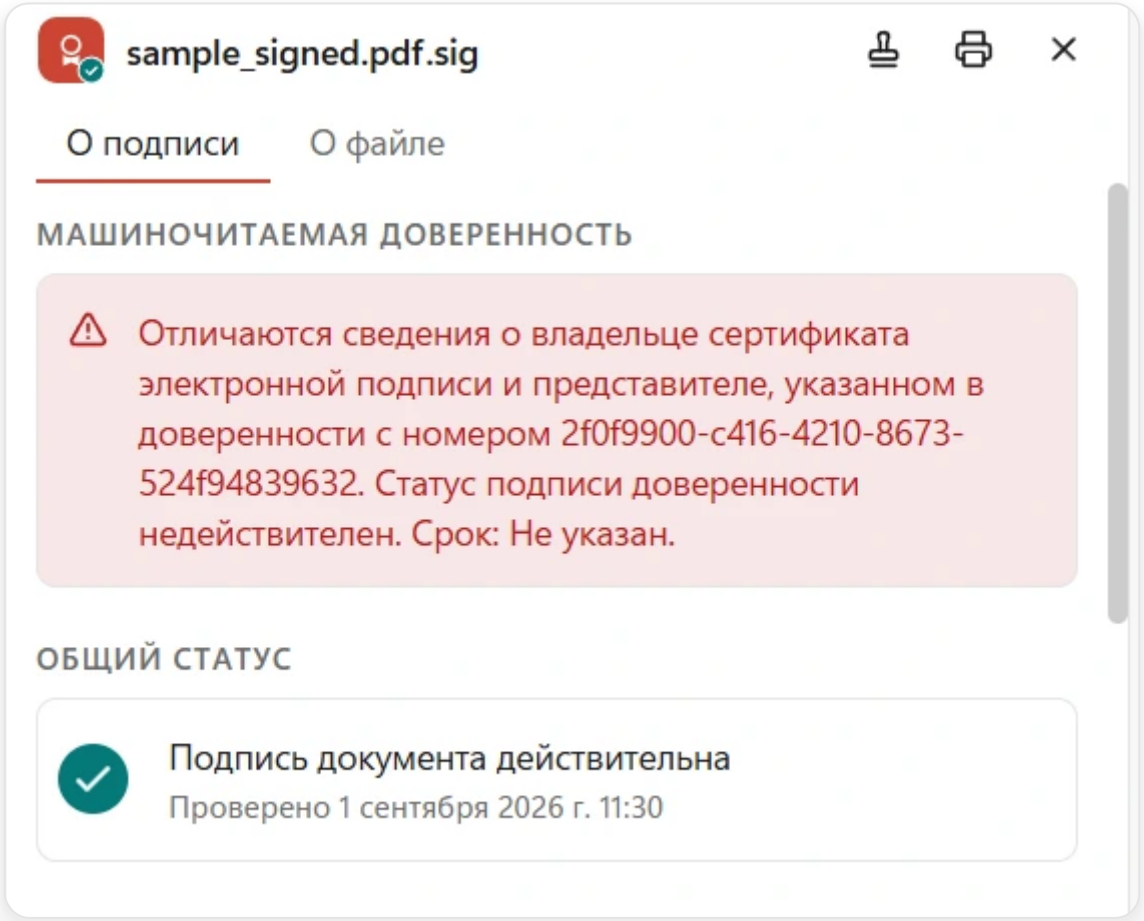
Если к подписи приложена МЧД, в панели сведений появляется вкладка **«О доверенности»**. В ней показаны:

- номер доверенности и её формат;
- срок действия и его статус: **Действует**, **Истёк**, **Ещё не действует**;
- ИНН доверителя, ИННФЛ и ИННЮЛ представителя;
- статус подписей доверенности: **Действительны** или **Требуют внимания**;
- применимость доверенности к сертификату подписанта;
- ссылка **Проверить на сайте ФНС** — переход к записи в реестре.

Результат сравнения показан в блоке **«Применимость»**:

Результат	Значение
Совпадают сведения о владельце сертификата электронной подписи и представителе, указанном в доверенности	ИНН представителя совпадает с сертификатом
Отличаются сведения о владельце сертификата электронной подписи и представителе, указанном в доверенности	ИНН представителя не совпадает с сертификатом

Результат	Значение
В МЧД не найден ИННФЛ представителя / В сертификате не найден ИННФЛ	Сравнивать не по чему — проверка не выполнена



⚠️ **Примечание**: если в подписи найдено несколько доверенностей, появится сообщение **«Найдено несколько доверенностей. Выберите МЧД для проверки применимости»** — выберите нужную вручную.

Отчёт о проверке подписи

Отчёт — это документ с результатами проверки, пригодный для печати и передачи.

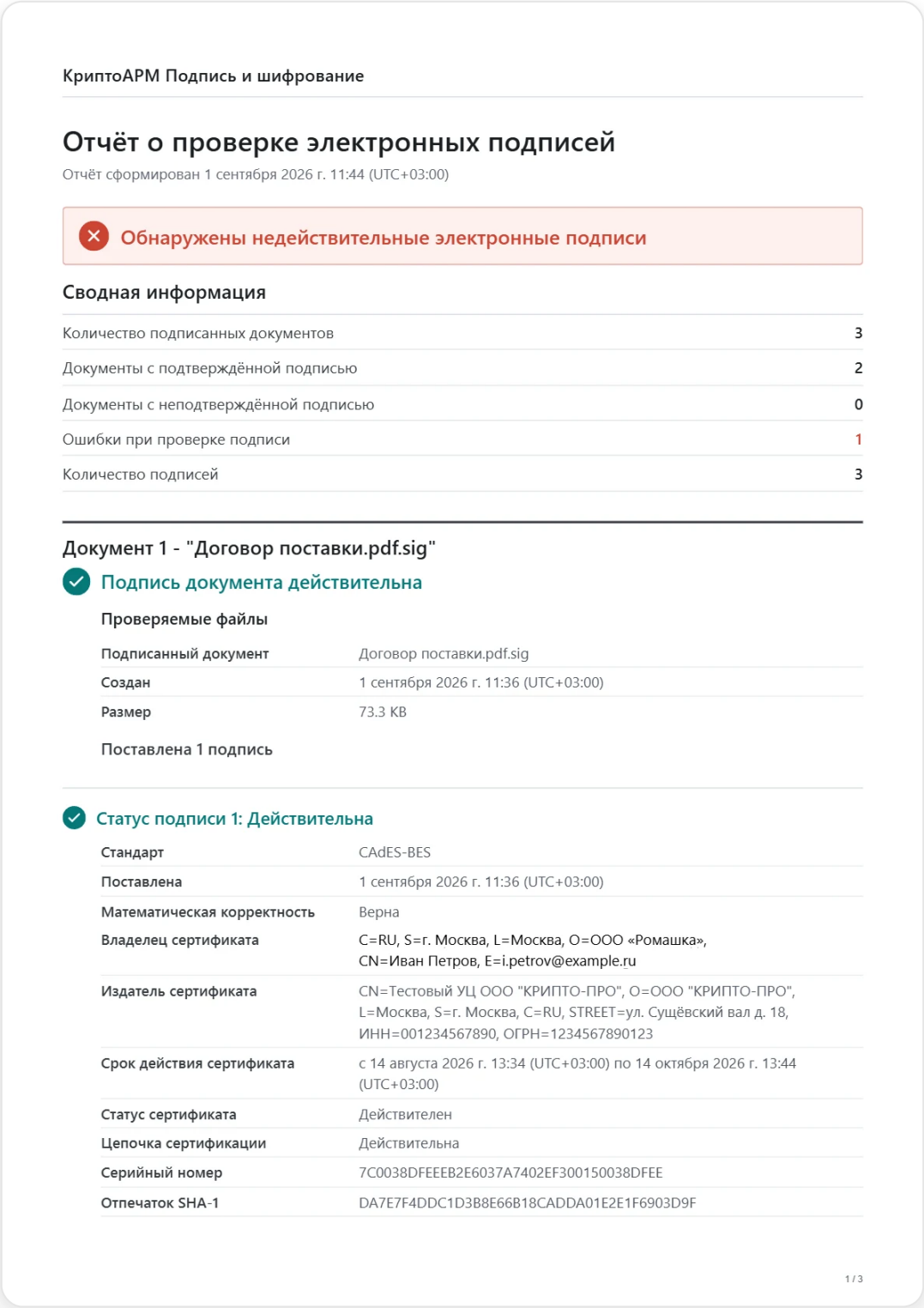
1. Выделите файлы, по которым нужен отчёт.
2. Нажмите **Распечатать отчёт** на панели инструментов или в панели сведений о подписи.
3. Откроется окно с отчётом о проверке электронной подписи.

Отчёт содержит:

- сводную информацию: количество документов, подписей, подтверждённых и неподтверждённых подписей, ошибок;

- общий вывод: **«Все электронные подписи действительны»**, **«Обнаружены недействительные электронные подписи»** или **«Не для всех электронных подписей удалось определить статус»**;
- по каждому документу — статус каждой подписи и сведения о подписанте;
- дату формирования отчёта.

Отчёт можно распечатать или сохранить на устройство.



КриптоАРМ Подпись и шифрование

Отчёт о проверке электронных подписей

Отчёт сформирован 1 сентября 2026 г. 11:44 (UTC+03:00)

Обнаружены недействительные электронные подписи

Сводная информация

Количество подписанных документов	3
Документы с подтверждённой подписью	2
Документы с неподтверждённой подписью	0
Ошибки при проверке подписи	1
Количество подписей	3

Документ 1 - "Договор поставки.pdf.sig"

Подпись документа действительна

Проверяемые файлы

Подписанный документ	Договор поставки.pdf.sig
Создан	1 сентября 2026 г. 11:36 (UTC+03:00)
Размер	73.3 KB

Поставлена 1 подпись

Статус подписи 1: Действительна

Стандарт	CAdES-BES
Поставлена	1 сентября 2026 г. 11:36 (UTC+03:00)
Математическая корректность	Верна
Владелец сертификата	C=RU, S=г. Москва, L=Москва, O=ООО «Ромашка», CN=Иван Петров, E=i.petrov@example.ru
Издатель сертификата	CN=Тестовый УЦ ООО "КРИПТО-ПРО", O=ООО "КРИПТО-ПРО", L=Москва, S=г. Москва, C=RU, STREET=ул. Сущёвский вал д. 18, ИНН=001234567890, ОГРН=1234567890123
Срок действия сертификата	с 14 августа 2026 г. 13:34 (UTC+03:00) по 14 октября 2026 г. 13:44 (UTC+03:00)
Статус сертификата	Действителен
Цепочка сертификации	Действительна
Серийный номер	7C0038DFEEEB2E6037A7402EF300150038DFEE
Отпечаток SHA-1	DA7E7F4DDC1D3B8E66B18CADDA01E2E1F6903D9F

1 / 3

Такой же отчёт можно получить из контекстного меню Проводника и из командной строки.

Создание печатной формы

Для подписанного PDF-документа доступно создание печатной формы — копии документа с графическим штампом подписи. Подробнее о печатных формах читайте в инструкции Обзор операций.

Если документ содержит **несколько подписей**, в печатной форме будут отображены **все подписи** — для каждой формируется отдельный штамп.

Чтобы создать печатную форму:

1. Выполните шаги из инструкции Просмотр сведений о подписи документа.
2. Нажмите кнопку **Печатная форма со штампом** в панели сведений.

Появится сообщение **«Создана печатная форма: ...»**, а рядом с подписанным документом — файл печатной формы.

Печатная форма предназначена для печати и визуального контроля: криптографической подписи в ней нет.

> 🚨 Печатную форму можно создать и при подписании PDF-документа — см. Подпись со стандартом PAdES.

Сохранение результатов

Расшифрованные файлы и документы, извлечённые из подписи, сначала готовятся во временном хранилище — так исходные файлы не изменяются.

Чтобы сохранить их:

1. Выделите нужные строки.
2. Нажмите **Сохранить** на панели инструментов.
3. Укажите папку.

Появится сообщение с количеством сохранённых файлов.

Кнопка **Открыть файл** открывает содержимое средствами системы. Если файл был зашифрован, откроется временная копия — приложение предупредит об этом сообщением **«Открыта временная копия — изменения не сохранятся в исходный файл»**.

Возможные ошибки

Технические подробности отказа записываются в журнал событий.

Ошибки при проверке подписи

Ошибка	Рекомендуемые действия
Не удалось открыть файл	1. Проверьте наличие и доступность файла 2. Повторите добавление файла в мастер
Файл ещё обрабатывается — повторите после завершения	Дождитесь окончания проверки и повторите действие
Не найден исходный файл для отсоединённой подписи	Добавьте в мастер исходный файл или нажмите **Указать путь к исходному файлу** и выберите документ
Не удалось проверить подпись	1. Проверьте, что файл подписи не повреждён 2. Причина отказа записана в журнале
Не удалось получить результат проверки электронной подписи	Повторите добавление файла; если ошибка повторяется, обратитесь в техническую поддержку
Сертификат подписанта не найден	Попросите сертификат у отправителя и импортируйте его
Не удалось проверить штамп времени	Проверьте доступ к службе штампов времени и повторите проверку
Формат файла не поддерживается для проверки или расшифрования	В файле нет ни подписи, ни зашифрованных данных — проверьте, тот ли файл добавлен
Файл не содержит данных OpenPGP	Переключите стандарт операций на X.509
Архив защищён паролем, распаковка невозможна	Распакуйте архив сторонней программой и добавьте файлы в мастер
Архив повреждён или не является ZIP-файлом	Запросите у отправителя исправную версию архива

Ошибки при снятии подписи

Ошибка	Рекомендуемые действия
Снятие подписи доступно только для совмещённой подписи	При отсоединённой подписи оригинал документа и так находится в отдельном файле
Не удалось снять подпись	1. Проверьте, что файл подписи не повреждён 2. Причина отказа записана в журнале
Не удалось открыть файл	1. Проверьте наличие и доступность файла 2. Повторите добавление файла в мастер

Ошибки при расшифровании

Ошибка	Рекомендуемые действия
Не удалось расшифровать файл	1. Убедитесь, что среди ваших сертификатов есть тот, для которого файл зашифрован 2. Проверьте, подключён ли носитель с закрытым ключом
Требуется PIN сертификата расшифрования / **Неверный ПИН-код, попробуйте ещё раз**	Введите ПИН-код закрытого ключа; проверьте раскладку клавиатуры и регистр символов
Неверный пароль, попробуйте ещё раз	Пароль закрытого ключа OpenPGP не подошёл — проверьте раскладку и регистр
Для операций подписи и расшифрования с использованием ГОСТ алгоритмов требуется лицензия КриптоАРМ	1. Приобретите лицензию КриптоАРМ 2. Активируйте лицензию в настройках программы
Проверьте наличие действующей лицензии на КриптоПро CSP	Установите лицензию КриптоПро CSP

Смотрите также

- Подпись и шифрование — обратные операции.
- Подпись и защита PDF — просмотр подписей в документе.
- Раздел «Сертификаты» — установка сертификатов подписантов и цепочек.
- Списки отзыва — импорт CRL для проверки отзыва.
- Активация лицензии — лицензии КриптоАРМ и КриптоПро CSP.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Подпись и защита PDF

В этой инструкции вы научитесь работать с мастером **«Подпись и защита PDF»**. Он работает с одним документом: показывает страницы, позволяет разметить, где встанет подпись, подготовить места для других подписантов, сертифицировать документ, преобразовать его в PDF/A и проверить уже поставленные подписи.

Содержание:

- Что потребуется
- Просмотр PDF-документа
- Создание подписи PDF-документа
- Сертифицирующая подпись PDF-документа
- Создание подписи с конвертацией в PDF/A
- Создание подписи в размеченной области
- Проверка подписи PDF-документа
- Действия в мастере
- Возможные ошибки
- Смотрите также

> 💡 **Совет**: для подписи нескольких PDF-документов сразу удобнее мастер Подпись и шифрование. Он выполняет групповые операции подписи, архивирования и шифрования и работает как со стандартом CAdES, так и с PAdES.

Что потребуется

- **Документ PDF** — мастер работает с одним документом за раз.
- **Сертификат подписи с закрытым ключом** — личный сертификат X.509. Мастер работает только по стандарту X.509: встроенной подписи PDF в OpenPGP не существует.
- **КриптоПро CSP и действующая лицензия КриптоАРМ** — для подписи ГОСТ-сертификатом.
- **Компонент КриптоПро ЭЦП Runtime (CAdES)** — на Windows его ставит установщик приложения. Если компонент отсутствует, список сертификатов подписи будет пуст с пояснением **«(модуль CAdES недоступен)»**.

Просмотр PDF-документа

Чтобы открыть PDF-документ для просмотра:

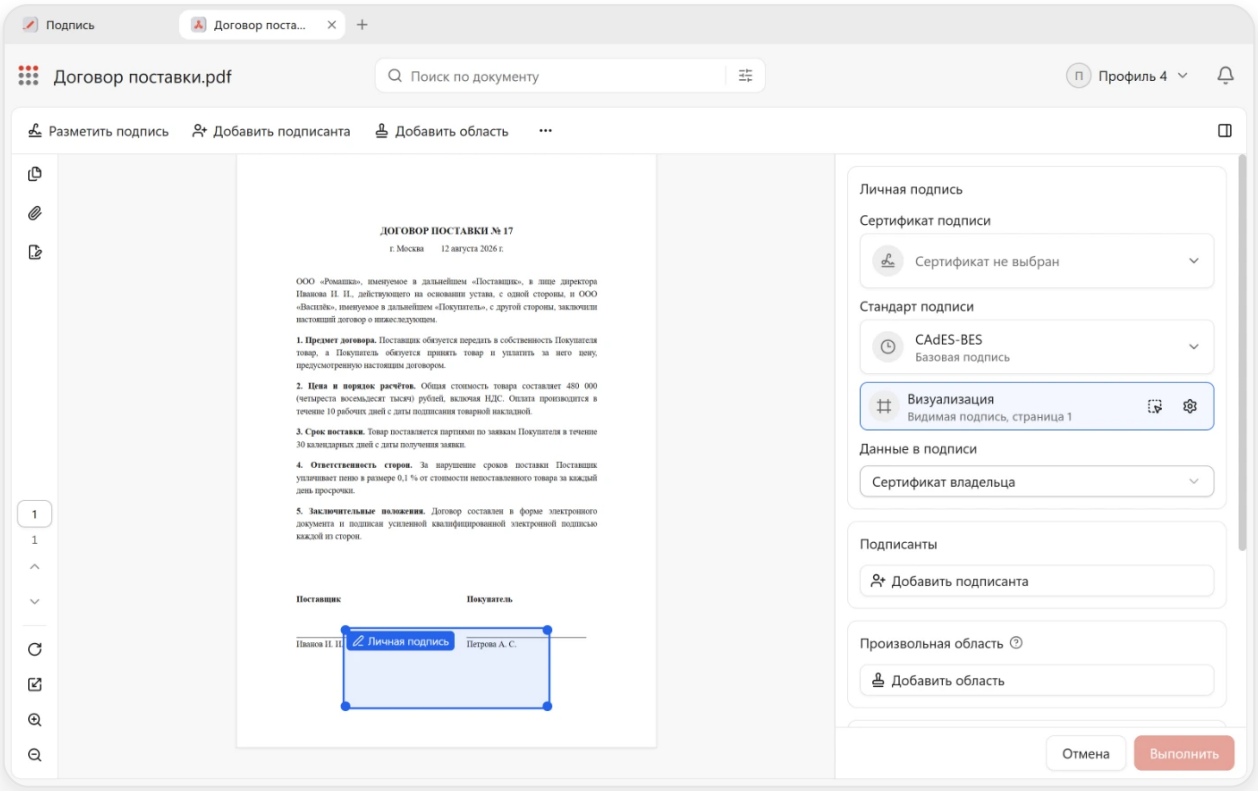
1. Откройте мастер (см. Запуск мастера).

2. Добавьте в мастер PDF-документ (см. Добавление документа).

После загрузки документ будет открыт для просмотра.

Если в документе есть подписи, приложение автоматически запустит их проверку (см. Проверка подписи PDF-документа).

Инструменты просмотра



Панель действий

Кнопка	Функция
Настройки подписи	Открывает боковую панель с настройками подписи и разметкой мест
Распечатать документ	Печать документа
Распечатать отчёт	Отчёт о проверке подписей документа
Сохранить как...	Создание копии файла
Показать в папке	Открытие расположения файла
Открыть другой документ	Замена текущего документа

Панель управления просмотром

Элемент	Функция
Навигация по страницам	Листание и переход к странице по номеру
Масштабирование	**Увеличить**, **Уменьшить** и свой масштаб
Режим отображения	**По ширине**, **Страница целиком**, **Реальный размер**
Поворот страниц	Поворот вправо на 90°
Поиск по тексту	Поиск по документу с параметрами **С учётом регистра** и **Целые слова**

> ⚠️ **Примечание**: поворот страниц не изменяет исходный файл — только режим просмотра.

Слово, разорванное переносом по дефису, ищется так, как оно записано в файле; буквы е и ё поиск считает одинаковыми.

Боковое меню навигации

- **Страницы** — панель с миниатюрами страниц. При выборе миниатюры выполняется переход к нужной странице документа.
- **Вложения** — список файлов, вложенных в документ. Любое вложение можно сохранить на диск командой **Сохранить как...**; если вложений нет, панель показывает **«Вложений нет»**.
- **Подписи** — подписи документа, их статус и подготовленные места для подписантов.

Все три раздела на месте всегда: если в документе нет вложений или подписей, раздел сообщает об этом.

Создание подписи PDF-документа

Чтобы подписать PDF-документ:

1. Откройте мастер и добавьте документ (см. Запуск мастера и Добавление документа).
2. Нажмите **Настройки подписи** на панели действий — в правой части окна появится панель настроек. По умолчанию используются параметры активного профиля подписи.
3. В блоке **Личная подпись** укажите:

- **Сертификат подписи** — сертификат с закрытым ключом;
- **Стандарт подписи** — CAdES-BES, CAdES-T, CAdES-X Long Type 1 или CAdES-A; для сертификата встроенного провайдера OpenSSL поле показывает **CMS** и недоступно для изменения;

- **Данные в подписи** — какие сертификаты вложить в подпись.

1. Проверьте строку **Визуализация**: где именно встанет подпись. При необходимости разметьте её заново (см. Разметка области для штампа подписи).
2. При необходимости добавьте и настройте:

- подписантов (см. Подписанты),
- произвольную область (см. Произвольная область).

1. При необходимости в блоке **Защита документа** настройте параметры защиты:

- включите **Сертифицировать документ** для создания сертифицирующей подписи,
- включите **Конвертировать в формат PDF/A**, чтобы привести документ к архивному профилю.

> ⚠️ **Примечание**: поставить сертифицирующую подпись может только первый подписант.

1. Нажмите **Выполнить**.
2. Перед началом подписания появится окно **«Подтверждение»** (см. Подтверждение операции). Нажмите **Выполнить**, чтобы подтвердить ознакомление с подписываемым документом.
3. Если на закрытый ключ задан ПИН-код, введите его в появившемся окне.

Выполнение операции занимает определённое время и зависит от объёма документа и производительности устройства. По завершении появится сообщение **«Документ подписан»**, а документ откроется в режиме просмотра и проверки подписи.

Подпись встраивается внутрь документа (PAdES): результат остаётся обычным PDF-файлом, который откроется в любой программе просмотра.

Сертифицирующая подпись PDF-документа

Сертифицирующая подпись — это особый тип электронной подписи, который не только подтверждает авторство и целостность документа, но и накладывает ограничения на дальнейшие изменения. Подробнее читайте в инструкции Обзор операций и выбор мастера.

Чтобы подписать PDF-документ сертифицирующей подписью:

1. Откройте мастер, добавьте документ и задайте настройки подписи по аналогии с инструкцией Создание подписи PDF-документа.
2. В блоке **Защита документа** включите **Сертифицировать документ**.
3. Нажмите **Выполнить** и завершите операцию обычным порядком.

После такой подписи в документе разрешены заполнение форм и добавление подписей — уровень разрешений задан приложением и не настраивается.

> 💡 **Примечание**: сертифицирующая подпись должна быть первой в документе. Если документ уже подписан, настройка недоступна — появится пояснение **«Документ уже подписан: сертифицирующая подпись должна быть первой»**.

Если документ уже сертифицирован, мастер учитывает его разрешения и говорит об этом в панели:

Сообщение панели	Что доступно
Документ сертифицирован: вносить изменения запрещено	Документ открывается только для чтения
Документ сертифицирован: подписи разрешены, произвольные области — нет	Можно подписывать, произвольную область — нельзя

Команды разметки, запрещённые сертификацией, недоступны, а подсказка объясняет причину — отказ приходит до подписания, а не после ввода ПИН-кода.

Создание подписи с конвертацией в PDF/A

PDF/A — архивный профиль формата: документ приводится к виду, пригодному для длительного хранения. При конвертации выполняется удаление или отключение элементов, которые могут нарушить отображение документа или повлиять на его безопасность. К таким элементам относятся скрипты (JavaScript), мультимедиа (аудио, видео), 3D-объекты и интерактивные формы, внешние ссылки на ресурсы, а также шифрование и парольная защита.

> 🔐 **Важно**: если вы конвертируете документ формата **PDF/A-3b** в **PDF/A-2b**, все вложенные файлы внутри документа будут удалены, потому что формат **PDF/A-2b** не поддерживает встроенные объекты.

Чтобы подписать PDF-документ с конвертацией в PDF/A:

1. Откройте мастер, добавьте документ и задайте настройки подписи по аналогии с инструкцией Создание подписи PDF-документа.
2. В блоке **Защита документа** включите **Конвертировать в формат PDF/A** и укажите дополнительные настройки:

- **Формат PDF/A** — **PDF/A-2b** или **PDF/A-3b**;
- **Если при конвертации возникнут ошибки** — **Преобразовать страницы с ошибками в изображения** или **Преобразовать все страницы в изображения**;
- **Разрешение изображений (DPI)** — для страниц, которые будут преобразованы в изображения; допустимый диапазон 70–300;

- **Безопасный режим** — ограничивает параллельную обработку страниц и снижает расход памяти на больших документах.

1. Нажмите **Выполнить** и завершите операцию обычным порядком.

> ⚠️ **Важно**: преобразование переписывает документ целиком, поэтому оно недоступно, как только в документе есть хоть одно поле подписи — подписанное или подготовленное. Переключатель недоступен, а подсказка поясняет: **«Преобразование перепишет документ: подписи и подготовленные места будут потеряны»**.

Создание подписи в размеченной области

Если документ содержит подготовленные места для подписантов, подпись можно поставить в любое из них. Все подготовленные места отображаются в разделе **Подписи** бокового меню.

Чтобы поставить подпись в размеченную область:

1. Откройте мастер и добавьте документ (см. Запуск мастера и Добавление документа).
2. Откройте в боковом меню раздел **Подписи**.
3. Нажмите **Поставить подпись** на свободном месте либо дважды щёлкните по самому прямоугольнику на странице.
4. Строка **Визуализация** покажет **«В подготовленное место „...“»**.
5. Задайте настройки подписи и завершите операцию по инструкции Создание подписи PDF-документа.

Размер и положение подготовленного места заданы документом и не меняются: в свойствах места приложение поясняет это строкой **«Размер и положение заданы документом — здесь их не изменить»**.

Проверка подписи PDF-документа

Чтобы проверить подписи PDF-документа:

1. Откройте мастер и добавьте документ (см. Запуск мастера и Добавление документа).
2. После загрузки документа автоматически запустится проверка подписей.

Общий результат показан полосой над страницами. В ней через · перечислены факты о документе:

- **Все подписи документа действительны**;
- **N подписей из M недействительны**;
- **сертификация нарушена** — документ изменяли вопреки запрету сертифицирующей подписи;

- **N мест ожидают подписи**.

Статус каждой подписи виден в разделе **Подписи** бокового меню: **Действительна** или **Недействительна**. Сертифицирующая подпись помечена отдельно словом **«Сертифицирующая»**.

Кнопка **Распечатать отчёт** формирует отчёт о проверке подписей документа.

> 💡 **Примечание**: если второй подписант поставил **видимую** подпись в подготовленное место сертифицированного документа, проверка может сообщить о нарушенной сертификации, хотя сам документ корректен. Это ограничение проверки: невидимая подпись в то же место и подпись в собственное новое место сертификацию сохраняют.

Просмотр сведений о подписи PDF-документа

Чтобы просмотреть сведения о подписи документа:

1. Выполните шаги из инструкции Проверка подписи PDF-документа.
2. Откройте в боковом меню раздел **Подписи** и выберите нужную подпись.
3. В панели появится блок **Сведения о подписи**: подписант, время подписания, статус сертификата и цепочки, штампы времени.

Пока сведения загружаются, показывается строка **«Получаем сведения о подписи...»**; если получить их не удалось — **«Не удалось получить сведения о подписи»**.

Действия в мастере

Некоторые действия универсальны и необходимы для выполнения любой операции.

Запуск мастера

Мастер **«Подпись и защита PDF»** можно открыть следующими способами:

- из бокового меню: нажмите кнопку **Меню** и выберите **Подпись и защита PDF**;
- из строки вкладок: нажмите + правой кнопкой мыши и выберите раздел;
- из другого раздела: выделите PDF-документ и нажмите **Добавить в** → **Подпись и защита PDF**.

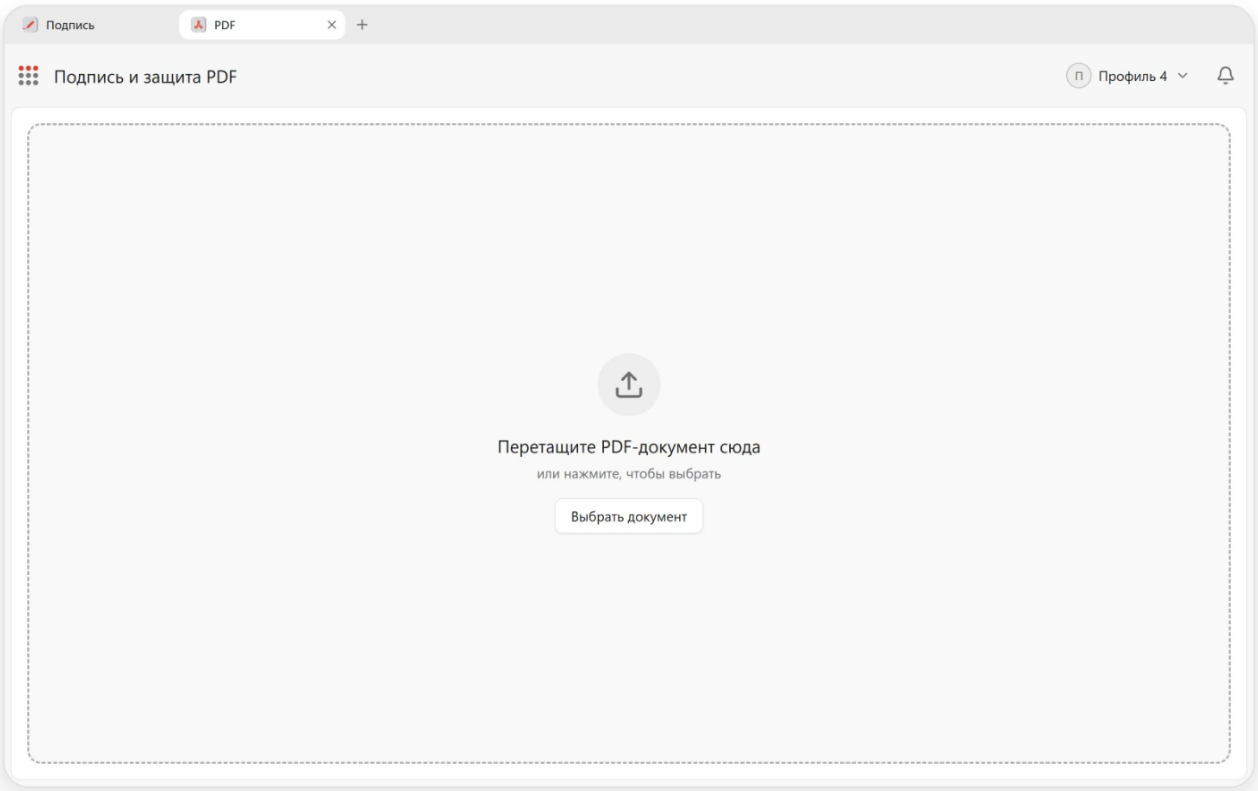
После выполнения любого из этих действий мастер откроется в новой вкладке.

Добавление документа

Добавьте документ в мастер одним из способов:

- перетащите PDF в окно приложения;

- нажмите **Выбрать документ** и укажите файл на диске.



После загрузки документ будет открыт для просмотра.

> 💡 **Примечание**: мастер открывает только файлы PDF и работает с одним документом. Если выбрано несколько файлов, откроется первый PDF из выбранных — об этом сообщит строка **«Открыт первый PDF из выбранных — за раз открывается один документ»**.

Разметка области для штампа подписи

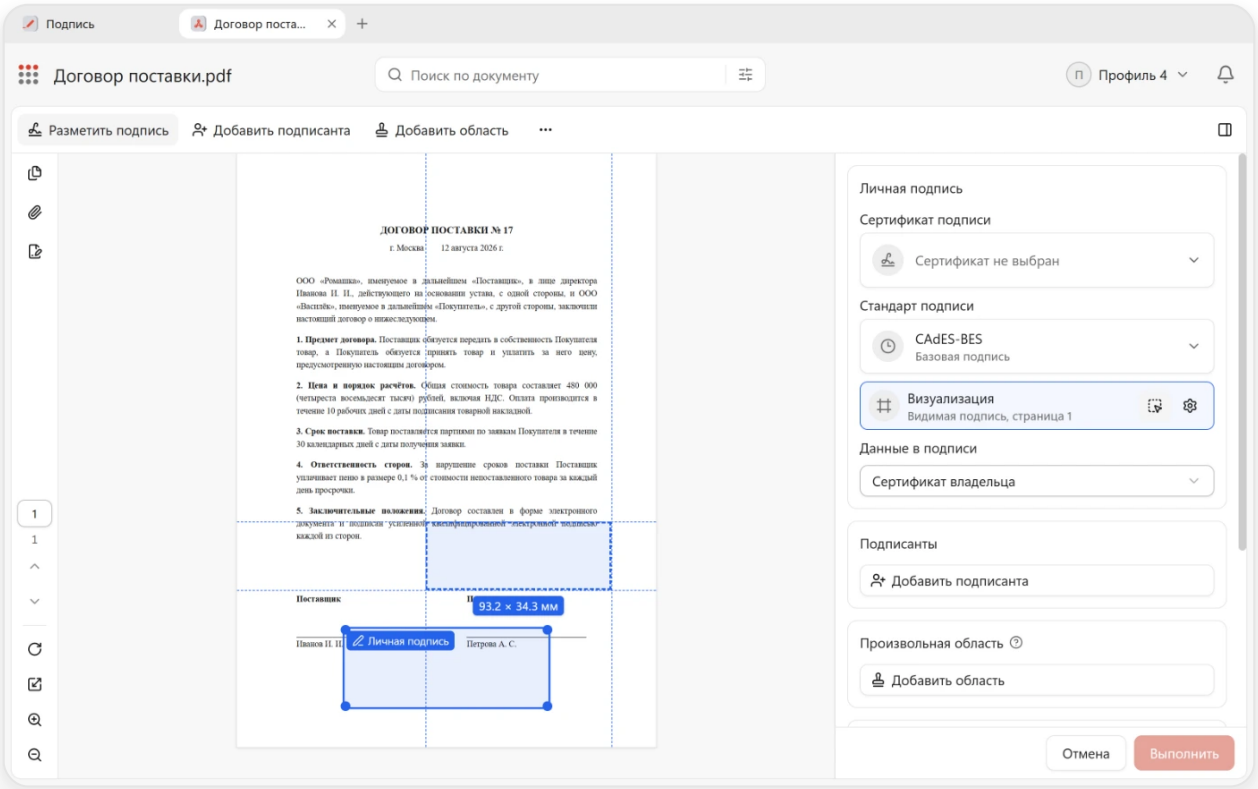
Строка **Визуализация** в блоке **Личная подпись** показывает, где окажется ваша подпись:

Состояние	Значение
Не размечена	Место ещё не выбрано
Видимая подпись, страница N	Штамп встанет на указанную страницу
В подготовленное место «...»	Подпись встанет в заранее подготовленное поле документа
Невидимая подпись	Штамп не рисуется, подпись хранится в документе как данные

При открытии документа мастер уже размечает вашу подпись так, как её поставил бы активный профиль: на странице, в положении и размере из настроек штампа. Дальше это обычное место — его можно передвинуть, перенести на другую страницу или удалить.

Чтобы разметить область заново:

1. Нажмите **Разметить** в строке **Визуализация**.
2. Обведите мышью прямоугольник на нужной странице.



1. Нажмите кнопку свойств в той же строке, чтобы настроить размер, положение и оформление штампа: реквизиты, шрифт, цвета, рамку и логотип.

Если подпись была невидимой, разметка сама делает её видимой. И наоборот: невидимая подпись — это то же место, только без прямоугольника на странице, поэтому документ подписывается в любом случае.

Что означают цвета на странице

Цвет рамки говорит о состоянии места, а вид рамки — о том, будет ли в нём что-то нарисовано:

Вид рамки	Значение
Синяя	Место, которое добавит текущая операция
Янтарная	Подготовленное место документа
Зелёная	Подпись, которая в этом месте уже есть

Вид рамки	Значение
Красная	Наложение на другое место — сдвиньте одно из них
Сплошная рамка	В месте что-то нарисуется
Пунктирная рамка	Место останется пустым

Подписанты

Мастер позволяет заранее подготовить в документе места, куда поставят подпись другие люди. Как и личная подпись, подпись подписанта может быть видимой и невидимой.

Добавление подписантов

1. В блоке **Подписанты** нажмите **Добавить подписанта**.
2. Нажмите **Разметить** на панели с подписантом и обведите прямоугольник на странице.
3. В свойствах места укажите **Название** — например, фамилию будущего подписанта.

Такие места отображаются со статусом **«Ждёт подписи»**. Когда документ вернётся подписанным, они получат статус подписи.

Подписантов в одном документе может быть до десяти: когда предел достигнут, команда становится недоступной, а подсказка объясняет причину — **«Больше 10 подписантов добавить нельзя»**.

> ⚠️ **Примечание**: два места не могут носить одно имя — ни среди размеченных сейчас, ни среди уже имеющихся в документе полей подписи. Приложение попросит изменить название.

Удаление подписанта

Чтобы убрать подписанта из документа, нажмите **Убрать** на панели с его именем.

> ⚠️ **Примечание**: нельзя удалить подписанта, который уже поставил подпись.

Произвольная область

Произвольная область — это прямоугольник на странице, в который помещается текст или изображение. Криптографической подписи в нём нет: это визуальная пометка на документе — комментарий, статус или отметка о конфиденциальности.

Произвольная область в документе может быть только одна.

Разметка произвольной области

1. В блоке **Произвольная область** нажмите **Добавить область**.

2. Обведите прямоугольник на странице.
3. В свойствах области выберите **Содержимое**:

- **Текст** — введите текст, задайте размер, выравнивание и цвет;
- **Изображение** — выберите файл PNG или JPEG;
- **Оставить пустым**.

1. При необходимости настройте заливку и рамку.

В свойствах области можно задать, на каких страницах она появится: **Только эта**, **Все** или **Список** номеров (например, `1-3, 7`) с возможностью исключить отдельные страницы.

Удаление произвольной области

Чтобы убрать произвольную область из документа, нажмите **Убрать** на панели с областью.

Подтверждение операции

Перед выполнением операции запрашивается её подтверждение.

Чтобы подтвердить операцию:

1. Ознакомьтесь со сведениями в окне **«Подтверждение»**: в нём указано, что будет выполнено и для скольких файлов — например, **«Будет выполнено: подпись для 1 файла»**.
2. Если выбранный сертификат подписи недействителен, в окне появится предупреждение **«Выбранный сертификат недействителен. Использовать сертификат?»**.
3. Нажмите **Выполнить** — под сводкой окно поясняет: **«Нажимая „Выполнить“, я подтверждаю ознакомление с подписываемым документом»**.

Отказаться от операции можно кнопкой **Отмена**.

Возможные ошибки

Технические подробности отказа записываются в журнал событий.

Ошибки при открытии файла

Ошибка	Описание	Рекомендуемые действия
Можно открыть только файл PDF	Выбран файл другого формата	Мастер работает только с PDF; другие файлы подписывайте в разделе «Подпись и шифрование»
Не удалось открыть документ	Файл повреждён или защищён паролем на открытие	Запросите у отправителя исправный файл либо снимите пароль в программе, где он был поставлен

Ошибка	Описание	Рекомендуемые действия
Не удалось проверить подписи документа	Проверка подписей открытого документа не выполнилась	Откройте документ заново; если ошибка повторяется, проверьте подпись в разделе «Проверка и расшифрование»

Ошибки при подписи файла

Ошибка	Описание	Рекомендуемые действия
Выберите сертификат подписи	Не указано, каким сертификатом подписывать	Выберите сертификат в блоке **Личная подпись**
Разметьте личную подпись на странице	Не указано, где на странице встанет подпись	Нажмите **Разметить** в строке **Визуализация** и обведите место
Заполните произвольную область или выберите «Оставить пустым»	Область создана, но её содержимое не задано	Введите текст, выберите изображение или отметьте **Оставить пустым**
Разметьте произвольную область или удалите её	Область создана, но не размещена на странице	Обведите для неё прямоугольник или уберите область
Два места названы одинаково — измените одно из названий	У двух размечаемых мест совпали названия	Дайте местам разные названия
Такое название уже занято в документе — выберите другое	Название совпало с полем подписи, которое уже есть в документе	Придумайте другое название
Накладывается на другое место	Два прямоугольника перекрывают друг друга	Сдвиньте или уменьшите одно из мест — рамка перестанет быть красной
Сертификация документа запрещает изменения	Автор документа запретил вносить в него любые изменения	Такой документ можно только просмотреть и проверить
Произвольная область запрещена сертификацией документа — удалите её	Автор документа разрешил добавлять только подписи	Уберите произвольную область и повторите подписание
Изображение больше 8 МБ	Выбранный файл слишком велик	Уменьшите изображение или выберите другой файл
Поддерживаются только PNG и JPEG	Для области выбран файл другого формата	Сохраните изображение в PNG или JPEG

Ошибки самой операции подписи — отсутствие лицензии, недоступный модуль CAdES, отказ криптопровайдера — совпадают с ошибками мастера **«Подпись и шифрование»**: см. Возможные ошибки.

Смотрите также

- Подпись и шифрование — пакетная подпись, в том числе PDF.
- Настройки подписи и шифрования — параметры PDF в профиле.
- Проверка и расшифрование — проверка подписей вне мастера.
- Активация лицензии — лицензии КриптоАРМ и КриптоПро CSP.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Настройки подписи и шифрования

В этом разделе описаны настройки электронной подписи и шифрования в мастерах КриптоАРМ, которые можно сохранить в профиле подписи для повторного использования. Вы узнаете, как выбрать личный сертификат, задать параметры для подписи по стандартам CAdES и PAdES и настроить шифрование документов.

Содержание:

- Операции
- Личная подпись
- Настройки подписи CAdES
- Настройки подписи PAdES
- Настройки защиты PDF-документа
- Печатная форма
- Сертификаты шифрования
- Настройки шифрования
- Сохранение результатов
- Настройки OpenPGP
- Общие настройки
- Смотрите также

Операции

Блок **Операции** определяет, что именно будет сделано с файлами.

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Подписать	Вкл	Электронная подпись со стандартом CAdES или PAdES	Вкл / Выкл
Архивировать	Выкл	Упаковка результата в ZIP-архив	Вкл / Выкл
Зашифровать	Выкл	Шифрование файлов в адрес выбранных получателей	Вкл / Выкл

Операции выполняются последовательно: подпись → архивирование → шифрование.

> ⚠️ **Примечание**: эти параметры доступны только в мастере Подпись и шифрование.

Личная подпись

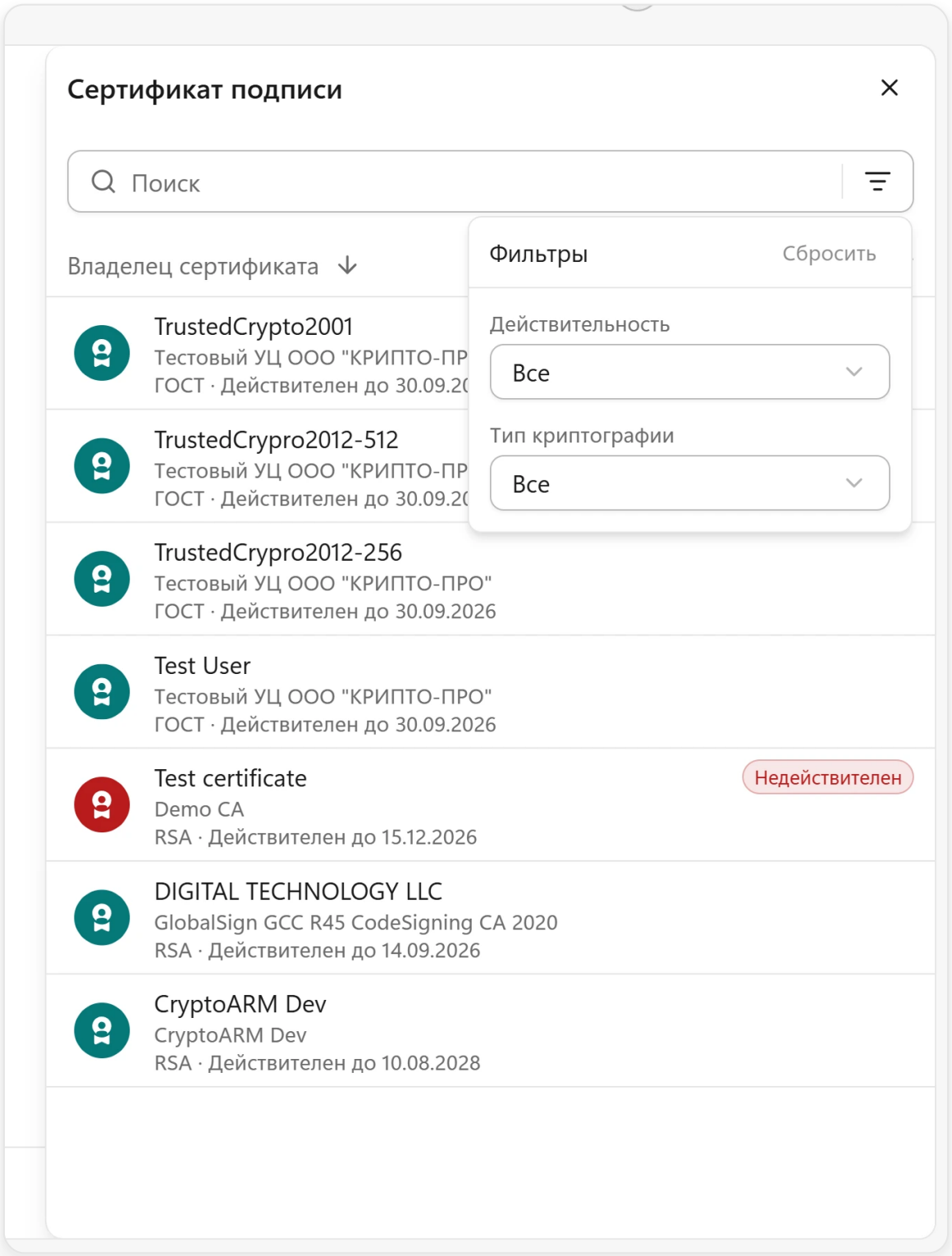
В блоке **Личная подпись** указывается сертификат, которым будет подписан документ, стандарт подписи и машиночитаемая доверенность.

Выбор сертификата подписи

Сертификат подписи — сертификат из хранилища **Личные**, у которого есть закрытый ключ. Только таким сертификатом можно создать электронную подпись.

Чтобы выбрать сертификат:

1. Нажмите на поле **Сертификат подписи** в блоке **Личная подпись** — откроется панель со списком сертификатов.



1. При необходимости воспользуйтесь фильтрацией списка:

- выберите **тип криптографии**:
  - **Российская Федерация** — сертификаты с алгоритмами ГОСТ;
  - **Открытая криптография** — сертификаты с алгоритмами RSA и ECDSA;
- выберите **действительность**: **Действительные** или **Недействительные**;
- воспользуйтесь **строкой поиска**, чтобы найти сертификат по владельцу или издателю;

- при необходимости включите **сортировку по владельцу**.

1. Нажмите на нужный сертификат.

Для каждого сертификата показаны владелец, издатель и срок действия. Недействительные помечены как **«Недействителен»**, с истёкшим ключом — **«Ключ истёк»**.

Сообщения при пустом списке:

Сообщение	Что это значит	Что сделать
(нет личного сертификата с закрытым ключом для подписи)	В хранилище нет сертификатов, которыми можно подписывать	Установите свой сертификат
(криптопровайдер для подписи недоступен)	Нужный криптопровайдер не установлен	Установите КриптоПро CSP и перезапустите приложение
(модуль CAdES недоступен)	Не установлен компонент КриптоПро ЭЦП Runtime	Установите его из дистрибутива КриптоПро

> 💡 **Примечание**: подписать недействительным сертификатом можно — приложение спросит подтверждение. При истёкшем закрытом ключе подпись невозможна: выберите другой сертификат.

Выбор стандарта подписи

Нажмите на поле **Стандарт подписи**, чтобы открыть панель выбора.

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Стандарт подписи	`CAdES-BES`	**CAdES-BES** — базовая подпись без меток времени. **CAdES-T** — подпись со штампом времени, подтверждающим момент её создания. **CAdES-X Long Type 1** — усовершенствованная подпись со сведениями, подтверждающими действительность сертификата на момент подписания. **CAdES-A** — архивная подпись для долговременного хранения.	`CAdES-BES`, `CAdES-T`, `CAdES-X Long Type 1`, `CAdES-A`

> 💡 **Примечание**: список относится к сертификатам КриптоПро. Если выбран сертификат встроенного провайдера OpenSSL, поле показывает **CMS** и недоступно для изменения: подписи CAdES такими сертификатами не создаются.

Служба штампов времени

Для стандартов CAdES-T, CAdES-X Long Type 1 и CAdES-A используется служба штампов времени (TSP). Её параметры находятся в той же панели, что и выбор стандарта.

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Адрес службы штампов времени (TSP)	`http://pki.tax.gov.ru/tsp/tsp.srf`	Служба, которая выдаёт штампы времени	Адрес вида `http(s)://сервер[:порт][/путь]`
Адрес OCSP	-	Служба проверки статуса сертификата. Нужна, если её требует стандарт подписи или УЦ	Адрес вида `http(s)://сервер[:порт][/путь]`
Использовать прокси для TSP	Выкл	Включает поля прокси-сервера — если TSP и OCSP доступны только через него	Вкл / Выкл

По умолчанию в поле TSP подставлен адрес службы штампов времени ФНС России. При необходимости замените его адресом службы, которую предоставил ваш удостоверяющий центр.

Если адрес не указан или записан неверно, приложение покажет метку **«Требуется TSP»** или **«Неверный TSP»**, сообщение **«Укажите корректный адрес TSP: http:// или https://»** и не даст запустить операцию.

Настройки прокси-сервера

Если доступ к службам TSP или OCSP выполняется через прокси, укажите параметры подключения:

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Адрес прокси	-	IP-адрес или доменное имя прокси-сервера	IPv4/IPv6-адрес или доменное имя
Порт прокси	-	Номер порта для подключения к прокси	Целое число от 1 до 65535
Логин прокси	-	Имя пользователя для доступа к прокси	Заполняется, только если прокси требует авторизации

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Пароль прокси	-	Пароль для доступа к прокси	Заполняется вместе с логином

Незаполненный адрес или порт приложение отмечает сообщениями **«Укажите адрес прокси»**, **«Укажите порт прокси»** и **«Укажите порт от 1 до 65535»**.

Выбор машиночитаемой доверенности

Машиночитаемая доверенность (МЧД) используется при подписании документов представителем организации.

В настройке указываются файл доверенности `.xml` и файлы подписи доверителя.

Порядок подключения и результаты проверки описаны в инструкции Подпись и шифрование.

Настройки подписи CAdES

Настройки CAdES определяют способ формирования электронной подписи, формат файла подписи и состав данных, включаемых в подпись.

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Вид подписи	`Присоединённая`	Способ хранения подписи относительно документа	`Присоединённая` (подпись и документ в одном файле), `Отсоединённая` (подпись хранится отдельно)
Формат файла подписи	`.sig`	Расширение файла, в который сохраняется подпись	`.sig`, `.p7s`, `.sgn`, `.sign`, `.bin`, `.pem`
Данные в подписи	`Сертификат владельца`	Какие сертификаты добавляются в атрибуты подписи	`Сертификат владельца`, `Цепочка без корневого сертификата`, `Все сертификаты цепочки`
Кодировка подписи	`DER`	Способ кодирования данных подписи	`DER` (двоичная), `BASE-64` (текстовая)
Убрать служебные заголовки	`Выкл`	Доступна для кодировки `BASE-64`. Убирает строки `-----BEGIN...` и `-----END...`	`Вкл` / `Выкл`

⚠️ **Примечание**: в мастере Подпись и защита PDF из этого блока доступна только настройка **Данные в подписи**: вид подписи, формат файла и кодировка относятся к отдельному файлу подписи, которого встроенная PAdES-подпись не создаёт.

Настройки подписи PAdES

Для PDF-файлов выбирается способ подписания.

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Способ подписания	`Обычная подпись CMS/ CAdES`	Как будет подписан PDF-документ	`Обычная подпись CMS/ CAdES`, `Встроенная подпись в PDF (PAdES)`, `Обычная подпись + печатная копия`
Видимый штамп подписи	`Выкл`	Добавляет в PDF видимую область подписи. Криптографическая подпись при этом не меняется — меняется её отображение	`Вкл` / `Выкл`

При включённом штампе становятся доступны кнопки **Оформление** и **Положение**.

Внешний вид штампа подписи

Настройки внешнего вида определяют, как подпись будет визуально отображаться в PDF-документе: макет штампа, реквизиты, фон, границу, цвет текста и логотип.

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Вид	`Штамп`	Макет штампа	`Штамп`, `Штамп с реквизитами слева`, `Штамп с реквизитами справа`, `Штамп с реквизитами слева и справа`
Реквизиты штампа	`По ГОСТу`	Набор реквизитов в центральной части штампа	`По ГОСТу` (по ГОСТ Р 7.0.97-2016: сертификат, срок действия,

Название настройки	Значение по умолчанию	Описание	Допустимые значения
			владелец), `Произвольно` (ручной набор реквизитов)
Реквизиты слева	`Издатель`	Реквизиты в левой колонке штампа	Любые реквизиты из списка
Реквизиты справа	`Отпечаток`	Реквизиты в правой колонке штампа	Любые реквизиты из списка
Фон	`Вкл`	Заливка штампа	`Вкл` / `Выкл`
Граница	`Вкл`	Рамка вокруг штампа	`Вкл` / `Выкл`
Цвет текста и границы, **Цвет фона**	`#111111`, `#ffffff`	Цвета элементов штампа	Значение в hex-формате или выбор из палитры
Логотип	-	Изображение с гербом или эмблемой в центре штампа	Файлы `.jpg`, `.jpeg`, `.png`. Максимальный размер — 10 МБ

Доступные реквизиты: ФИО, должность, организация, владелец, издатель, сертификат (серийный номер), отпечаток, срок действия, дата и время подписи, номер доверенности, описание, местоположение, примечание, алгоритм подписи.

Настройка внешнего вида штампа

1. Откройте окно настроек:

- кнопкой **Оформление** в мастере **Подпись и шифрование** или в профиле подписи;
- кнопкой свойств места в мастере **Подпись и защита PDF**.

1. В блоке **Настройки макета** выберите макет штампа в настройке **Вид**.
2. В блоке **Реквизиты** выберите набор реквизитов:

- **По ГОСТу** — вывод реквизитов по ГОСТ Р 7.0.97-2016: заголовок «Документ подписан электронной подписью», серийный номер сертификата, имя владельца и срок действия;
- **Произвольно** — ручная настройка: включение нужных реквизитов и изменение их значений.

> 💡 **Примечание**: по умолчанию в реквизите **Владелец** отображается общее имя (CN) из сертификата. Если в сертификате указано название организации, а требуется вывести ФИО подписанта, выберите набор **Произвольно** и включите реквизит **ФИО**.

1. Так же настройте реквизиты для колонок слева и справа, если выбранный макет их показывает.
2. В блоке **Оформление** настройте фон, границу и цвета — через палитру или hex-код.

3. В блоке **Логотип** загрузите изображение кнопкой **Загрузить**. Логотип можно временно скрыть переключателем **Не показывать** или удалить.
4. Проверьте результат кнопкой **Предпросмотр**.

Кнопка **Сбросить оформление** возвращает значения по умолчанию.

Положение штампа подписи

Настройки положения определяют размер штампа, его размещение на странице и страницу документа.

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Видимость	`Невидимая подпись`	То же, что переключатель **Видимый штамп подписи**	`Видимая подпись`, `Невидимая подпись`
Ширина, **Высота**	`102,3 мм`, `39,16 мм`	Размер штампа	Размер в миллиметрах
Ориентация	`0°`	Поворот штампа на странице	`0°`, `90°`, `180°`, `270°`
Страница	`Последняя`	Страница, на которую встанет штамп	`Первая`, `Последняя`, `Указать страницу`
По горизонтали	`По центру`	Выравнивание по ширине страницы	`Слева`, `По центру`, `Справа`
По вертикали	`Снизу`	Выравнивание по высоте страницы	`Сверху`, `По центру`, `Снизу`
Отступ по X, мм, **Отступ по Y, мм**	`0 мм`, `20 мм`	Смещение от выбранного положения	Отступ в миллиметрах
Добавить копию изображения штампа на все страницы	`Выкл`	Повторяет изображение штампа на каждой странице	`Вкл` / `Выкл`

Настройка размера и положения штампа подписи

1. Откройте окно настроек:

- кнопкой **Положение** в мастере **Подпись и шифрование** или в профиле подписи;
- кнопкой свойств места в мастере **Подпись и защита PDF**.

1. В блоке **Визуализация** выберите видимость подписи:

- **Видимая подпись** — подпись отображается в документе в виде штампа;
- **Невидимая подпись** — подпись существует, но на страницах не видна.

1. В блоке **Размер** укажите ширину и высоту штампа в миллиметрах.

2. В блоке **Положение** задайте ориентацию, страницу, выравнивание и отступы, а при необходимости включите **Добавить копию изображения штампа на все страницы**.

Кнопка **Сбросить положение** возвращает значения по умолчанию.

Внешний вид произвольной области

Произвольная область — прямоугольник на странице с текстом или изображением; электронной подписи в нём нет.

> ⚠️ **Примечание**: произвольная область создаётся и настраивается только в мастере Подпись и защита PDF — в профиле подписи её параметры не хранятся.

Настройки защиты PDF-документа

Настройки позволяют включить сертификацию документа с ограничением на внесение изменений и преобразовать PDF в формат PDF/A.

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Сертифицировать документ	Выкл	PAdES-подпись становится сертификационной: после неё разрешены заполнение форм и добавление подписей. Такая подпись должна быть первой в документе	Вкл / Выкл
Конвертировать в формат PDF/A	Выкл	Приводит документ к архивному профилю PDF/A перед встраиванием подписи	Вкл / Выкл

Настройки конвертации в PDF/A

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Формат PDF/A	`PDF/A-2b`	Архивный профиль, к которому приводится документ	`PDF/A-2b`, `PDF/A-3b`
Если при конвертации возникнут ошибки	`Преобразовать страницы с ошибками в изображения`	Поведение при ошибках конвертации	

Название настройки	Значение по умолчанию	Описание	Допустимые значения
			`Преобразовать страницы с ошибками в изображения`, `Преобразовать все страницы в изображения`
Разрешение изображений (DPI)	`150`	Разрешение для страниц, которые будут преобразованы в изображения	`70`, `100`, `150`, `200`, `300`
Безопасный режим	`Выкл`	Ограничивает параллельную обработку страниц и снижает расход памяти на больших документах	`Вкл` / `Выкл`

> 🔐 **Важно**: если вы конвертируете документ формата **PDF/A-3b** в **PDF/A-2b**, все вложенные файлы внутри документа будут удалены, потому что формат **PDF/A-2b** не поддерживает встроенные объекты.

Печатная форма

В мастере **Подпись и шифрование** при выполнении подписи можно создать отдельную копию PDF-документа с изображением штампа. Такая копия не содержит электронную подпись и предназначена только для визуального представления документа.

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Обычная подпись + печатная копия	`Выкл`	Кроме файла подписи создаётся неподписанный PDF со штампом — для просмотра или печати	`Вкл` / `Выкл`

Оформление и расположение штампа настраиваются так же, как при создании подписи PAdES:

- Внешний вид штампа подписи,
- Положение штампа подписи.

> ⚠️ **Примечание**: печатную форму можно создать и в разделе **Проверка и расшифрование** — см. Создание печатной формы.

Сертификаты шифрования

Сертификаты шифрования — сертификаты получателей, в адрес которых шифруется документ.

> 💡 **Совет**: всегда добавляйте **свой личный сертификат** к списку получателей, если планируете в дальнейшем расшифровывать файл.

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Сертификаты шифрования	-	Сертификаты, которые будут использованы при шифровании	Сертификаты из хранилищ **Личные** и **Других пользователей**, группы сертификатов

Выбор сертификатов шифрования

Чтобы выбрать сертификаты шифрования:

1. В блоке **Сертификаты шифрования** нажмите **Добавить сертификаты**.
2. Откроется панель с двумя вкладками:

- **Сертификаты** — сертификаты получателей;
- **Группы** — готовые списки получателей.

1. При необходимости воспользуйтесь поиском и фильтрами — так же, как при выборе сертификата подписи.
2. Отметьте нужные сертификаты или группы.

Выбранные получатели показываются списком; убрать получателя можно кнопкой **Убрать из списка**.

Если тип криптографии сертификата не совпадает с выбранным алгоритмом шифрования, он помечается как **«Несовместим»** или **«Не используется»**. Приложение предупредит об этом в окне подтверждения.

Настройки шифрования

Настройки определяют алгоритм и формат зашифрованных файлов, способ их кодирования и возможность удаления исходных документов после шифрования.

🔐 ГОСТ-алгоритмы шифрования доступны при установленном криптопровайдере КриптоПро CSP.

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Алгоритм шифрования	`ГОСТ Р 34.12-2015 Кузнечик`	Алгоритм, которым шифруются данные	`ГОСТ 28147-89`, `ГОСТ Р 34.12-2015 Магма`, `ГОСТ Р 34.12-2015 Кузнечик`, `AES-256-CBC`, `DES3-CBC`
Формат файла	`.enc`	Расширение зашифрованных файлов	`.enc`, `.p7m`, `.p7e`, `.pem`
Кодировка файлов	`DER`	Способ представления зашифрованных данных	`DER`, `BASE-64`
Удалить исходные файлы после шифрования	`Выкл`	Удаляет исходные файлы после успешного шифрования	`Вкл` / `Выкл`

💡 **Примечание**: для алгоритма «ГОСТ Р 34.12-2015 Магма» размер файла не должен превышать 16 ГБ — приложение показывает подсказку рядом с выбором алгоритма.

Сохранение результатов

Блок **Сохранение результатов** определяет, куда попадут файлы после выполнения операций и как они будут названы.

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Сохранение результатов	`Папка с исходным документом`	Место сохранения результатов операции	`Папка с исходным документом`, `Сохранить в папку...` (выбор папки вручную)
Добавлять пользовательский суффикс	`Выкл`	Добавляет заданный текст в конец имени файла	`Вкл` / `Выкл`
Суффикс имени файла	`signed`	Текст суффикса	Любая строка

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Добавлять ФИО подписанта	Выкл	Добавляет имя подписанта (CN) из сертификата к имени файла после пользовательского суффикса	Вкл / Выкл
ФИО подписанта	-	Своё значение вместо имени из сертификата	Любая строка
Копировать исходный файл рядом с отсоединённой подписью	Выкл	При сохранении отсоединённой подписи в отдельную папку копирует туда же исходный файл	Вкл / Выкл
Отдельный архив на каждый файл	Выкл	Каждый файл упаковывается в отдельный архив; иначе все файлы попадут в один архив	Вкл / Выкл

Если указанной папки не существует, появится сообщение **«Укажите существующую папку»**.

> 💡 **Примечание**: заменить исходный PDF подписанным можно только из командной строки — в настройках операции такого параметра нет.

Настройки OpenPGP

При стандарте операций **OpenPGP** набор параметров другой:

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Сертификат подписи	-	Сертификат OpenPGP с закрытым ключом	Сертификаты из раздела **Сертификаты** при стандарте OpenPGP
Подключ для подписи	Первый подходящий подключ	Выбирается, если у сертификата несколько подключей с правом подписи	Подключи выбранного сертификата
Вид подписи	`Присоединённая`	Способ хранения подписи относительно документа	`Присоединённая`, `Отсоединённая`

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Хэш-алгоритм	`Авто (по алгоритму ключа)`	Алгоритм хэширования подписи	`Авто`, `SHA-256`, `SHA-384`, `SHA-512`, `SHA3-256`, `SHA3-384`, `SHA3-512`
Получатели	-	Сертификаты, в адрес которых шифруются файлы	Сертификаты и группы OpenPGP
ASCII armor (.asc)	`Выкл`	Текстовое представление результата	`Вкл` / `Выкл`

Общие настройки

Блок виден при редактировании профиля подписи.

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Название профиля	-	Имя, под которым профиль показывается в списке и в меню Проводника	Любая строка
Показывать эти настройки перед выполнением	`Вкл`	Если выключить, операции запускаются сразу по сохранённым параметрам — в том числе из контекстного меню Проводника	`Вкл` / `Выкл`
Показывать в меню Проводника	`Выкл`	Выводит профиль в контекстное меню Проводника (только Windows, не более 10 профилей)	`Вкл` / `Выкл`

Смотрите также

- Профили подписи — как сохранить набор настроек для повторного применения.
- Подпись и шифрование — как выполняется операция.
- Подпись и защита PDF — разметка подписи в документе.
- Активация лицензии — лицензии КриптоАРМ и КриптоПро CSP.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Контекстное меню Проводника, быстрые действия Finder и открытие файлов

Операции можно запускать, не открывая приложение: из контекстного меню Проводника Windows, из быстрых действий Finder на macOS или двойным щелчком по файлу подписи.

Содержание:

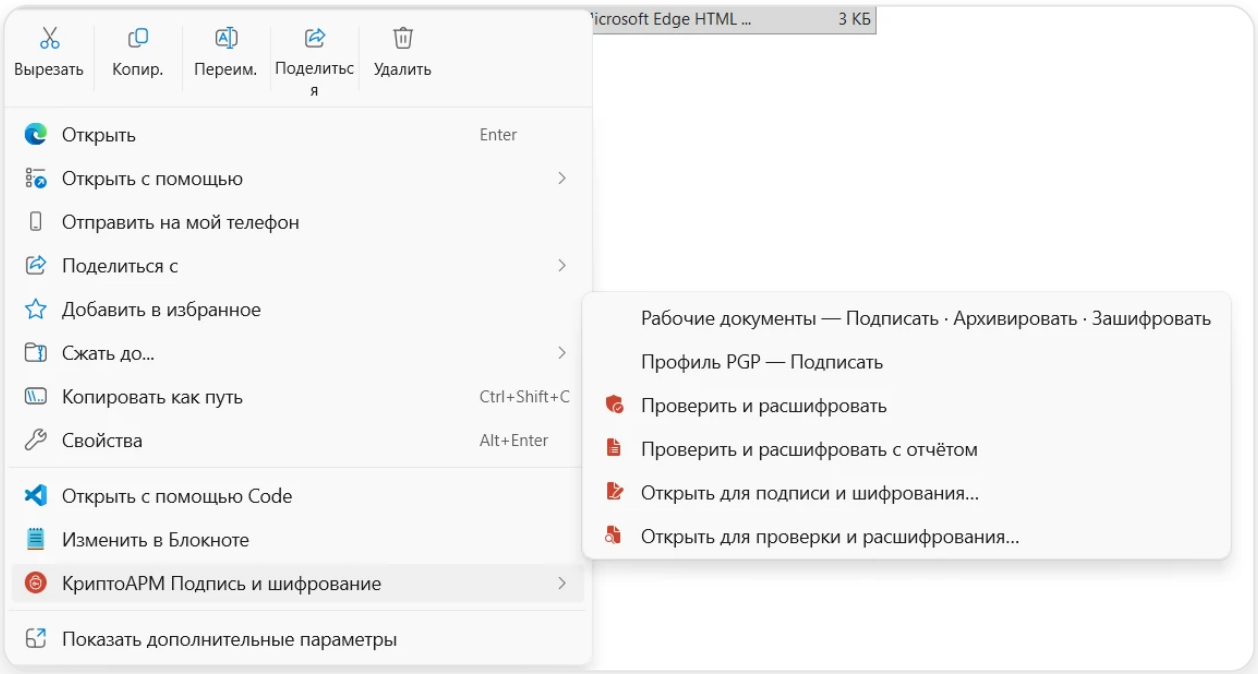
- Команды контекстного меню
- Быстрые действия Finder на macOS
- Подпись профилем
- Проверить и расшифровать
- Проверить и расшифровать с отчётом
- Команды «Открыть для...»
- Как приложение выбирает интерфейс
- Уведомления о результате
- Открытие файлов двойным щелчком
- Возможные ошибки
- Смотрите также

Команды контекстного меню

> 💡 **Примечание**: на Windows меню регистрируется при установке приложения, отдельных действий не требует. На macOS те же команды появляются в подменю быстрых действий Finder — см. ниже. На Linux меню нет.

Выделите файлы в Проводнике и вызовите контекстное меню. Пункт **КриптоАРМ Подпись и шифрование** раскрывается в список команд:

```
КриптоАРМ Подпись и шифрование
├── КЭП CAdES-T — Подписать · Архивировать · Зашифровать
├── Партнёры — Подписать
├── Документы бухгалтерии — Подписать · Зашифровать
├── Проверить и расшифровать
├── Проверить и расшифровать с отчётом
├── Открыть для подписи и шифрования…
└── Открыть для проверки и расшифрования…
```



Первыми идут профили подписи, выведенные в меню, — в том порядке, в каком они расположены в списке профилей. Рядом с названием профиля показан состав его операции.

Быстрые действия Finder на macOS

На macOS сторонние приложения не могут добавить свой пункт в корень контекстного меню Finder. Вместо этого КриптоАРМ добавляет команды в подменю **Быстрые действия** — там же, где живут действия других приложений. Команды те же, что в Проводнике, узнать их можно по значкам:

```
Быстрые действия
├── КЭП CAdES-T — Подписать
├── Открыть для подписи и шифрования…
├── Открыть для проверки и расшифрования…
├── Партнёры — Подписать · Зашифровать
├── Проверить и расшифровать
└── Проверить и расшифровать с отчётом
```

Выделите файлы в Finder, вызовите контекстное меню и раскройте **Быстрые действия**. Дальше всё работает так же, как из Проводника: профиль выполняет свою операцию, команды проверки идут по стандарту операций по умолчанию, команды «Открыть для...» передают файлы в приложение.

Чем macOS отличается от Windows:

- Список создаёт само приложение при первом запуске и обновляет его при каждом изменении профилей. Если пункты не появились, запустите приложение один раз.

- Порядок пунктов в подменю задаёт Finder, поэтому порядок профилей из списка в приложении в меню не сохраняется. Переставить пункты можно перетаскиванием в **Системные настройки → Основные → Расширения → Finder**.
- Любой пункт можно скрыть или вернуть в **Системные настройки → Основные → Расширения → Finder** или через пункт **Настроить...** внизу подменю. Скрытый там пункт остаётся скрытым и после изменения профилей; новые и переименованные профили приложение включает само.
- Значки у новых пунктов Finder может показать не сразу: до перезапуска Finder или повторного входа в систему у них значок документа Automator. Перезапустить Finder можно, удерживая ⌥ при правом щелчке по его значку в Dock.
- О результате сообщает уведомление macOS: разрешите уведомления приложению при первом запросе системы.

Подпись профилем

Выбор профиля выполняет операцию именно так, как она описана в профиле: те же действия, тот же сертификат, те же форматы и то же место сохранения результата. Отдельных команд «Подписать» или «Зашифровать» в меню нет — состав операции задаёт профиль.

Чтобы вывести профиль в меню, включите в его строке настройку **Показывать в меню Проводника** — см. Профили в контекстном меню Проводника.

Настройка профиля **«Показывать эти настройки перед выполнением»** определяет, появится ли окно подтверждения: в Проводнике настройки не показываются, поэтому она управляет самим подтверждением.

Проверить и расшифровать

Команда проверяет подписи и расшифровывает выбранные файлы. Профили здесь не используются: операция выполняется по настройке «Стандарт операций по умолчанию».

Проверить и расшифровать с отчётом

Та же операция плюс один документ — отчёт о проверке в формате PDF.

Отчёт всегда один, сколько бы файлов ни было выделено:

Что выделено	Имя отчёта
Один файл	`договор.sig_report.pdf`
Несколько файлов	`merged_report_<дата и время>.pdf`

Существующие файлы не перезаписываются, поэтому два запуска по одной папке сохранят оба отчёта.

Если отчёт сохранить не удалось, проверка всё равно считается выполненной — о неудаче сообщит отдельное уведомление.

Команды «Открыть для...»

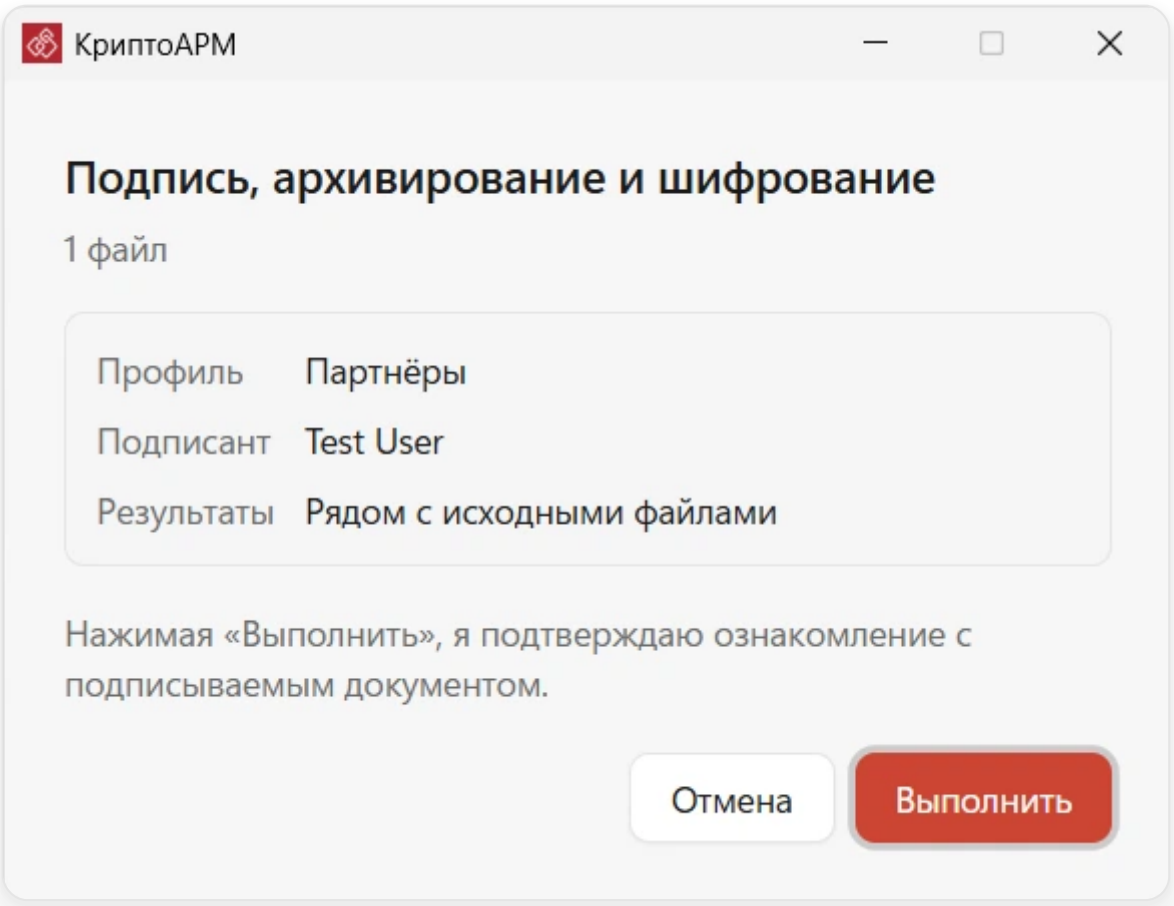
Две команды передают выбранные файлы в приложение, не запуская операцию:

- **Открыть для подписи и шифрования...** — открывает раздел «Подпись и шифрование» с этими файлами;
- **Открыть для проверки и расшифрования...** — открывает раздел «Проверка и расшифрование».

Как приложение выбирает интерфейс

В зависимости от того, чего не хватает для выполнения операции, приложение показывает минимально необходимый интерфейс:

Что происходит	Когда
Без окна	Операция полностью определена, подтверждение не требуется, а секрет либо не нужен, либо его запрашивает сам криптопровайдер
Компактное окно	Профиль требует подтверждения, нужен пароль или ПИН-код, который запрашивает приложение, либо есть предупреждение — недействительный сертификат подписи или удаление исходных файлов после шифрования
Рабочий экран	Профиль недоступен или неполон — например, в нём не выбран сертификат, — либо файл с именем результата уже существует



Компактное окно показывает профиль, подписанта, количество файлов и место сохранения результата, а также поле для пароля или ПИН-кода. Под ними — строка **«Нажимая „Выполнить“, я подтверждаю ознакомление с подписываемым документом»**. Кнопка **Выполнить** запускает операцию.

Закрытие окна до начала работы криптопровайдера отменяет операцию.

Уведомления о результате

Об окончании операции, запущенной из Проводника или Finder, сообщает системное уведомление.

Заголовок уведомления называет результат:

Заголовок	Когда появляется
Готово	Все файлы обработаны успешно
Выполнено с ошибками	Часть файлов обработать не удалось
Не удалось выполнить	Ни один файл не обработан

Заголовок	Когда появляется
Проверка завершена	Проверка и расшифрование прошли без замечаний
Найдены недействительные подписи	Среди проверенных подписей есть недействительные
Не все подписи проверены	Часть подписей проверить не удалось — например, не импортирован открытый ключ подписанта
Отчёт о проверке готов	Выполнена команда с отчётом, файл отчёта сохранён
Запрос не выполнен	Выборка не принята — см. Возможные ошибки

В теле уведомления перечислены название профиля и счётчики: действительных, недействительных и непроверенных подписей, расшифрованных файлов, ошибок.

Щелчок по уведомлению открывает приложение. Для команд проверки те же файлы открываются в разделе **«Проверка и расшифрование»** и проверяются заново — статус сертификата и списки отзыва к этому моменту могли измениться.

Все события попадают и в журнал приложения.

Открытие файлов двойным щелчком

При установке приложение регистрирует типы файлов:

Группа	Расширения
Подписи	`.sig`, `.sign`, `.sgn`, `.p7s`
Зашифрованные файлы	`.enc`, `.p7m`, `.p7e`
Файлы OpenPGP	`.gpg`, `.pgp`, `.asc`

Двойной щелчок по такому файлу открывает приложение на вкладке **«Проверка и расшифрование»** и добавляет файл в список: подпись сразу проверяется, зашифрованный файл расшифровывается. На диске при этом ничего не меняется — результат нужно сохранить самому.

Это работает на всех трёх платформах: Windows, Linux и macOS.

> 💡 **Примечание**: расширение `.asc` в OpenPGP используется и для подписи, и для шифртекста, и для экспортированного ключа. Экспортированный ключ, открытый двойным щелчком, попадёт в проверку и покажет ошибку — импортируйте его через раздел «Сертификаты».

Возможные ошибки

Сообщение	Что это значит	Что сделать
Не удалось подготовить операцию	В профиле не хватает настроек для запуска	Откройте профиль в приложении и проверьте его настройки
Сертификат подписи недействителен или требует внимания	Сертификат просрочен или его цепочка не построена	Подтвердите использование сертификата или выберите другой
Не удалось выполнить операцию	Операция прервалась	Причина записана в журнале
Выбрано слишком много файлов. Откройте приложение и добавьте их вручную	В выборке больше файлов, чем принимает команда меню	Откройте приложение и добавьте файлы частями
В выборке есть папки, а обрабатываются только файлы	Команды меню работают только с файлами	Выделите файлы или перетащите папку в окно приложения
Не удалось прочитать выбранные файлы	Файлы недоступны или удалены	Проверьте, на месте ли файлы и есть ли к ним доступ
Слишком много запросов подряд	Предыдущие операции ещё выполняются	Дождитесь их завершения и повторите
Пункт **КриптоАРМ Подпись и шифрование** отсутствует в меню	Команды меню не зарегистрированы в системе	Переустановите приложение — меню регистрирует установщик
В **Быстрых действиях** Finder нет пунктов **КриптоАРМ —**	Приложение ещё не запускалось или пункты отключены	Запустите приложение; проверьте раздел Finder в настройках расширений
Уведомление «Приложение не найдено. Его пункты убраны из быстрых действий»	Приложение удалено или перемещено	Если приложение перемещено, запустите его — список появится снова

Смотрите также

- Профили подписи — как вывести профиль в меню.
- Подпись и шифрование — те же операции в приложении.
- Выполнение операций в командной строке — автоматизация без интерфейса.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Выполнение операций в командной строке

Научитесь работать с командной строкой (CLI) КриптоАРМ: подписывать, шифровать, расшифровывать и проверять файлы. В этом руководстве собраны команды, параметры и практические примеры для Windows, Linux и macOS.

> 💡 **Примечание**: инструкция рассчитана на технических специалистов — тех, кто настраивает автоматическую обработку документов. Для повседневной работы командная строка не нужна: те же операции выполняются в окне приложения и из контекстного меню Проводника.

Содержание:

- Общая информация
- Список команд
- Подпись
- Шифрование
- Подпись и шифрование
- Архивирование
- Кодирование и декодирование файлов
- Расшифрование
- Проверка подписи
- Снятие подписи
- Сертификаты
- Работа с OpenPGP
- Результат и ошибки
- Смотрите также

Общая информация

CLI (Command Line Interface, интерфейс командной строки) — это способ управления приложением с помощью текстовых команд, вводимых через терминал или консоль.

Команды определяют, какие операции выполнить, с какими параметрами и над какими файлами.

CLI также подходит для автоматизации — выполнения операций без участия пользователя в составе систем обмена и скриптов `.bat` и `.sh`.

Важные замечания

- Перед использованием CLI убедитесь, что приложение готово к работе с электронной подписью: сертификат установлен, лицензия активирована.

> 🔍 Подробную информацию о подготовке можно найти в инструкции Начало работы.

- Для подписи, расшифрования и PAdES сертификатами КриптоПро требуется лицензия КриптоАРМ. Проверка подписи, просмотр сертификатов, перекодирование, снятие подписи и объединение подписей лицензии не требуют.
- Перед вводом команды указывается путь до исполняемого файла, затем через пробел — команда и её параметры.
- Недействительный сертификат останавливает операцию: подтверждения в командной строке не запрашиваются, согласие передаётся флагом `--force`.
- Если `--pin` не указан, КриптоПро может показать собственное системное окно ввода ПИН-кода.

Синтаксис команд

Общий формат вызова:

```
cryptoarm-sign <команда> [параметры]
```

- `команда` пишется первой, после пути до исполняемого файла;
- `<текст>` — значение параметра: путь к файлу, серийный номер сертификата, адрес службы и т. п.;
- `[текст]` — необязательный параметр: если его не задать, используется значение по умолчанию;
- все команды и параметры пишутся через пробел.

Пути к исполняемым файлам

Если каталог приложения не добавлен в `PATH`, укажите полный путь к исполняемому файлу:

Система	Путь при установке по умолчанию
Windows	`C:\Program Files\cryptoarm-sign\cryptoarm-sign.exe`
Linux	`"/opt/CryptoARM Sign and Encrypt/cryptoarm-sign"`
macOS	`"/Applications/CryptoARM Sign and Encrypt.app/Contents/MacOS/CryptoARM Sign and Encrypt"`

Ввод и вывод

Источник данных указывается одним из двух параметров:

Параметр	Описание	По умолчанию
`--source-file <путь>`	Один файл	—
`--source-folder <путь>`	Все файлы верхнего уровня папки	—

Правила путей:

- `--source-file` и `--source-folder` нельзя указывать одновременно;
- обход папки не рекурсивный;
- путь может быть обычным путём или URL вида `file://`;
- папку результата и конкретный файл результата нельзя указывать вместе;
- конкретный файл результата возможен только с `--source-file`;
- недостающие папки результата создаются автоматически.

Общие параметры

Параметр	Описание	По умолчанию
`--provider`	Криптопровайдер: `x509` или `pgp`	`x509`
`--pin <pin>`	ПИН-код закрытого ключа для подписи и расшифрования	—
`-f, --force`	Использовать недействительный сертификат без подтверждения	Отключено
`--logcrypto`	Включить журнал криптографической библиотеки	Отключено
`-h, --help`	Вывод справки по команде	—

> 💡 **Примечание**: подробный лог для обращения в поддержку включается переменной окружения `CRYPTOARM_TRACE=1` — отдельной настройки у CLI для этого нет.

Список команд

Команда	X.509	OpenPGP
`sign` / `sig`	✓	✓
`encrypt` / `enc`	✓	✓

Команда	X.509	OpenPGP
`sign-encrypt` / `se`	✓	✓
`archive` / `arc`	✓	—
`decrypt` / `dec`	✓	✓
`verify` / `ver`	✓	✓
`verify_ts` / `vts`	✓	—
`unsign`	✓	—
`certificates` / `cer`	✓	✓

Подпись

Команда: `sign` или `sig`

Команда позволяет выполнить операцию подписи одного или нескольких файлов.

Если в качестве исходного файла указать уже подписанный документ — файл с расширением `.sig`, `.p7s`, `.sgn`, `.sign`, `.bin` или `.pem`, — к нему будет добавлена соподпись. Для отсоединённой подписи исходный документ должен лежать рядом с контейнером и определяться по его имени.

Синтаксис

```
cryptoarm-sign sign --cert <идентификатор> [--detached] [--pin <PIN>] [--standard <стандарт>
--tsp <адрес>] [--enc DER|PEM|BASE-64] [--ext <расширение>] --source-file <файл>|--source-
folder <папка> [--signed-file-path <файл>|--folder-save-signed <папка>]
```

Описание команды

Общие параметры подписи

Параметр	Описание	По умолчанию
`--cert <id|отпечаток|серийный>`	Сертификат подписи: идентификатор из вывода `certificates`, отпечаток SHA-1 или серийный номер	—
`--standard <стандарт>`	Стандарт подписи: `cms`, `cades-bes`, `cades-t`, `cades-xlt1`, `cades-a`	`cades-bes` для сертификатов КриптоПро, `cms` для системного провайдера
`--attached`	Присоединённая подпись	Используется по умолчанию

Параметр	Описание	По умолчанию
`--detached`	Отсоединённая подпись	Отключено
`--enc <DER|PEM|BASE-64>`	Кодировка подписи	`DER`
`--ext <sig|p7s|sgn|sign|bin|pem>`	Расширение файла подписи	`sig`
`--include-certs <signer|without-root|full>`	Какие сертификаты вложить в подпись	`signer`
`--custom-suffix <суффикс>`	Суффикс имени результата	—

Если одновременно указаны `--attached` и `--detached`, используется `--attached`.

Архивирование результата

Параметр	Описание	По умолчанию
`--archive`	Упаковать результат подписи в ZIP	Отключено
`--separate-archives`	Отдельный ZIP на каждый исходный файл	Отключено

`--separate-archives` используется только вместе с `--archive`.

Объединение подписей

Подробнее про функцию **Объединение подписей** читайте в инструкции Подпись и шифрование.

Параметр	Описание	По умолчанию
`--join-signs <файлы...>`	Список путей к файлам отсоединённых подписей (минимум два файла)	—
`--join-signs-folder <папка>`	Папка с файлами подписей для объединения	—

Параметры подписи PDF (PAdES)

`--pades` включает встроенную подпись для PDF-файлов и по умолчанию создаёт видимый штамп из данных сертификата. Остальные файлы в том же вызове подписываются обычной подписью CMS/CAdES.

Параметр	Описание	По умолчанию
`--pades`	Подписать PDF по стандарту PAdES	Отключено

Параметр	Описание	По умолчанию
`--visual-copy`	Без `--pades`: сохранить рядом копию PDF со штампом без подписи	Отключено
`--pades-certify`	Сертифицирующая подпись	Отключено
`--signer-name <текст>`	Кем подписан (Name) в свойствах подписи	Имя из сертификата
`--reason <текст>`	Обоснование подписания (Reason)	—
`--location <текст>`	Местоположение (Location)	—
`--contact-info <текст>`	Контактная информация (ContactInfo)	—
`--pades-pdfa <pdfa-2b|pdfa-3b>`	Преобразовать PDF в PDF/A перед подписью	Отключено
`--pades-pdfa-mode <copy|image>`	Режим преобразования страниц	`copy`
`--pades-pdfa-dpi <70-300>`	Разрешение для страниц, преобразуемых в изображения	`150`
`--pades-page <номер|last>`	Страница размещения штампа	`last`
`--pades-all-pages`	Повторить изображение штампа на всех страницах	Отключено
`--pades-placement <x:y>`	Выравнивание: `left|center|right` : `top|center|bottom`	—
`--pades-width-mm <мм>`	Ширина штампа	`102.3`
`--pades-height-mm <мм>`	Высота штампа	`39.16`
`--pades-x-mm <мм>`	Горизонтальный отступ	`0`
`--pades-y-mm <мм>`	Вертикальный отступ	`20`
`--pades-rotation <0|90|180|270>`	Поворот изображения штампа	`0`
`--pades-visible-image <png>`	Готовое изображение вместо генерируемого штампа	—
`--pades-add-signer-name`	Добавить имя подписанта в имя PDF-файла	Отключено
`--pades-signer-name <имя>`	Имя подписанта для имени PDF-файла	—

Параметр	Описание	По умолчанию
`--overwrite-original-pdf`	Заменить исходный PDF подписанным	Отключено

> ⚠️ Ключ `--overwrite-original-pdf` изменяет исходный файл. Он работает только с `--pades` и `--source-file`, не сочетается с архивированием и указанием пути результата, а исходник заменяется лишь после успешного подписания.

Подписанный PDF сохраняет расширение исходного, поэтому имя результата задаёт `--custom-suffix` (`документ_signed.pdf`). Без суффикса результат рядом с исходником получает индекс — `документ(1).pdf`.

Содержимое генерируемого штампа:

Параметр	Описание	По умолчанию
`--stamp-individual`	Добавить ФИО владельца сертификата	—
`--stamp-job-position [значение]`	Добавить должность	—
`--stamp-organization-name [значение]`	Добавить организацию	—
`--stamp-issuer-friendly-name [значение]`	Добавить издателя сертификата	—
`--stamp-mark [значение]`	Добавить примечание	—
`--stamp-description [значение]`	Добавить описание	—
`--stamp-location [значение]`	Добавить местоположение	—
`--stamp-sign-time`	Добавить дату и время формирования штампа	—
`--stamp-mchd <номер>`	Добавить номер машиночитаемой доверенности	—

Положение и оформление генерируемого штампа:

Параметр	Описание	По умолчанию
`--stamp-width <мм>`	Ширина штампа	—
`--stamp-height <мм>`	Высота штампа	—
`--stamp-padding-left <мм>`	Отступ слева и размещение по левому краю	—

Параметр	Описание	По умолчанию
`--stamp-padding-bottom <мм>`	Отступ снизу	—
`--stamp-color <#RRGGBB>`	Цвет текста и границы	`#000000`
`--stamp-background-color <#RRGGBB>`	Цвет фона	`#ffffff`
`--stamp-title <текст>`	Заголовок вместо стандартного	—
`--stamp-no-background`	Прозрачный фон под штампом	Отключено
`--stamp-page <номер>`	Страница размещения	Последняя
`--stamp-on-all-pages`	Повторить штамп на всех страницах	Отключено
`--stamp-pixel-ratio <0.5-4>`	Масштаб отрисовки штампа	`1`

Без дополнительных `--stamp-*` параметров в штамп попадают реквизиты сертификата: имя владельца, серийный номер и срок действия. Реквизиты, которые не помещаются в заданную область, не обрезаются — штамп рисуется целиком и вписывается в неё, становясь мельче. Параметры содержания штампа нельзя сочетать с `--pades-visible-image`.

Машиночитаемая доверенность

Параметр	Описание	По умолчанию
`--mchd-xml <путь>`	XML-файл машиночитаемой доверенности	—
`--mchd-signatures <пути...>`	Файлы подписи доверителя	—
`--mchd-signatures-folder <папка>`	Папка с файлами подписи доверителя	—

Без `--archive` файлы МЧД копируются рядом с результатом подписи, с общим архивом — помещаются внутрь него.

Сетевые параметры

Параметр	Описание	По умолчанию
`--tsp <url>`	Адрес службы штампов времени	—
`--ocsp <url>`	Адрес службы OCSP	—
`--proxy <адрес>`	Адрес прокси-сервера	—
`--proxy-port <порт>`	Порт прокси	—
`--proxy-login <логин>`	Логин для прокси	—

Параметр	Описание	По умолчанию
`--proxy-password <пароль>`	Пароль для прокси	—

Для стандартов `cades-t`, `cades-xlt1` и `cades-a` параметр `--tsp` обязателен.

Ввод и вывод

Параметр	Описание	По умолчанию
`--source-file <файл>`	Путь к подписываемому файлу	—
`--source-folder <папка>`	Подписать все файлы из папки	—
`--signed-file-path <файл>`	Путь для результата подписи	—
`--folder-save-signed <папка>`	Папка для подписанных файлов	—

Практические примеры

Пример 1: Подпись со штампом на последней странице

В этом примере подписывается PDF-файл со штампом размером 100 × 30 мм, расположенным в 20 мм от левого и нижнего края последней страницы.

```
"C:\Program Files\cryptoarm-sign\cryptoarm-sign.exe" sign ^
  --source-file "C:\Doc\Пример.pdf" ^
  --cert "5883d78e000300093ab6" ^
  --pin "12345678" ^
  --pades ^
  --stamp-width 100 ^
  --stamp-height 30 ^
  --stamp-padding-left 20 ^
  --stamp-padding-bottom 20
```

Пример 2: Подпись со штампом красного цвета на всех страницах

```
"C:\Program Files\cryptoarm-sign\cryptoarm-sign.exe" sign ^
  --source-file "C:\Doc\Пример.pdf" ^
  --cert "5883d78e000300093ab6" ^
  --pin "12345678" ^
  --pades ^
  --stamp-width 80 ^
  --stamp-height 30 ^
  --stamp-padding-left 110 ^
  --stamp-padding-bottom 10 ^
  --stamp-color "#FF0000" ^
  --stamp-on-all-pages
```

Пример 3: Подпись документа с меткой времени

В этом примере файл подписывается по стандарту CAdES-T, который включает штамп времени. Результат сохраняется с расширением `.p7s` в кодировке `BASE-64`.

```
"C:\Program Files\cryptoarm-sign\cryptoarm-sign.exe" sign ^
  --source-file "C:\Documents\Example.pdf" ^
  --cert "5883d78e000300093ab6" ^
  --pin "12345678" ^
  --standard "cades-t" ^
  --tsp "https://example.com/tsp/tsp.srf" ^
  --enc "BASE-64" ^
  --ext "p7s"
```

Шифрование

Команды: `encrypt` или `enc`

Команда позволяет выполнить шифрование одного или нескольких файлов в адрес одного или нескольких сертификатов.

Синтаксис

```
cryptoarm-sign encrypt --cert <получатель...> [--alg <алгоритм>] [--enc DER|PEM|BASE-64] [--
ext <расширение>] [--delete-source] --source-file <файл>|--source-folder <папка> [--encrypted-
file-path <файл>|--folder-save-encrypted <папка>]
```

Описание команды

Параметр	Описание	По умолчанию
`--cert <получатели...>`	Сертификаты получателей; можно указать несколько	—
`--alg <алгоритм|OID>`	Алгоритм шифрования	`gost-28147`
`--enc <DER|PEM|BASE-64>`	Кодировка результата	`DER`
`--ext <enc|p7m|p7e|pem>`	Расширение зашифрованного файла	`enc`
`--delete-source`	Удалить исходный файл после успешного шифрования	Отключено
`--encrypted-file-path <файл>`	Путь для результата шифрования	—
`--folder-save-encrypted <папка>`	Папка для зашифрованных файлов	—

Поддерживаемые имена алгоритмов: `gost-28147`, `gost-2015-magma`, `gost-2015-kuznyechik`, `aes-256-cbc`, `des3-cbc`. Также принимаются OID — например, `1.2.643.2.2.21` для ГОСТ 28147.

Перед шифрованием файлы можно упаковать в архив параметрами `--archive`, `--separate-archives` и `--custom-suffix`.

Практический пример

В этом примере шифруется файл `Example.txt` в адрес сертификата с серийным номером `5883d78e000300093ab6`. Результат сохраняется в файл `Encrypted_Example.enc`, исходный файл удаляется.

```
"C:\Program Files\cryptoarm-sign\cryptoarm-sign.exe" encrypt ^
  --cert "5883d78e000300093ab6" ^
  --alg "gost-2015-kuznyechik" ^
  --enc "DER" ^
  --ext "enc" ^
  --delete-source ^
  --source-file "C:\Documents\Example.txt" ^
  --encrypted-file-path "C:\Documents\Encrypted_Example.enc"
```

Подпись и шифрование

Команды: `sign-encrypt` или `se`

Команда подписывает, а затем шифрует файл или папку за один вызов.

Синтаксис

```
cryptoarm-sign sign-encrypt --sign-cert <подписант> --recipient-cert <получатель...> --source-file <файл>|--source-folder <папка> [--folder-save-encrypted <папка>]
```

Описание команды

Параметр	Описание	По умолчанию
`--sign-cert <идентификатор>`	Сертификат подписи	—
`--recipient-cert <получатели...>`	Сертификаты получателей	—

Остальные параметры — подписи, шифрования, PAdES, МЧД, TSP, прокси и архивирования — те же, что у отдельных команд, и с теми же значениями по умолчанию.

Архивирование

Команды: `archive` или `arc`

Команда создаёт ZIP-архив без подписи и шифрования.

```
cryptoarm-sign archive \
  --source-folder ./docs \
  --folder-save-archive ./out
```

Параметр	Описание	По умолчанию
`--archive-file-path <файл>`	Путь одного ZIP-результата	—
`--folder-save-archive <папка>`	Папка результатов	—
`--separate-archives`	Отдельный ZIP на каждый исходный файл	Отключено
`--custom-suffix <суффикс>`	Суффикс имени ZIP	—

Кодирование и декодирование файлов

Для команд `sign` (файлы подписи), `certificates` (сертификаты и запросы на сертификат) и `encrypt` (сертификаты и запросы) доступны параметры кодирования и декодирования. Они преобразуют двоичные данные в текстовый формат `BASE-64` и обратно.

Кодирование удобно использовать, если файл нужно передать в текстовом виде — например, через системы, которые не поддерживают двоичные данные.

Параметр	Описание
`--decode <файл> [результат]`	Декодирование из формата `DER` в `PEM` (`BASE-64`)
`--encode <файл> [результат]`	Кодирование из формата `PEM` (`BASE-64`) в `DER`

```
cryptoarm-sign sign --decode ./document.sig
cryptoarm-sign certificates --encode ./request.pem
```

Расшифрование

Команды: `decrypt` или `dec`

Команда позволяет расшифровать один или несколько зашифрованных файлов.

Синтаксис

```
cryptoarm-sign decrypt [--pin <PIN>] [--enc DER|PEM|BASE-64] --source-file <файл>|--source-
folder <папка> [--decrypted-file-path <файл>|--folder-save-decrypted <папка>]
```

Описание команды

Параметр	Описание	По умолчанию
`--pin <pin>`	ПИН-код закрытого ключа расшифрования	—
`--enc <DER|PEM|BASE-64>`	Кодировка входного файла	`DER`
`--decrypted-file-path <файл>`	Путь для расшифрованного файла	—
`--folder-save-decrypted <папка>`	Папка для результатов расшифрования	—

Практический пример

```
"C:\Program Files\cryptoarm-sign\cryptoarm-sign.exe" decrypt ^
  --pin "12345678" ^
  --source-file "C:\Documents\Encrypted_Example.enc" ^
  --decrypted-file-path "C:\Documents\Decrypted_Example.txt"
```

Проверка подписи

Команды:

- `verify` или `ver`;
- `verify_ts` или `vts` — проверка штампов времени из подписи.

Команда позволяет проверить одну или несколько подписей либо штампы времени в файле подписи. Отчёт о проверке можно сохранить в формате PDF или JSON.

Синтаксис

```
cryptoarm-sign verify --source-file <файл>|--source-folder <папка> [--document <исходный
файл>] [-r-pdf [папка]] [-r-pdf-m [папка]] [-r-json [путь]]
```

```
cryptoarm-sign verify_ts --source-file <файл> [--document <исходный файл>] [-r [путь]]
```

Описание команды

Параметр	Описание	По умолчанию
`--source-file <файл>`	Файл подписи для проверки	—
`--source-folder <папка>`	Папка для пакетной проверки подписей	—

Параметр	Описание	По умолчанию
`--document <файл>`	Исходный файл для отсоединённой подписи	—
`--enc <DER|PEM|BASE-64>`	Кодировка подписи	`DER`
`-u, --unsign [папка]`	Извлечь исходный документ из присоединённой подписи	—
`-r-pdf, --save-report-pdf [папка]`	Отчёт PDF на каждый проверенный файл	—
`-r-pdf-m, --save-report-pdf-merged [папка]`	Общий отчёт PDF по всем файлам	—
`-r-json, --save-report-json [путь]`	Отчёт в формате JSON	—
`--visual-copy`	Печатная форма: копия PDF со штампами подписантов	Отключено

Для присоединённой подписи достаточно указать файл подписи; для отсоединённой дополнительно указывается документ.

При `--source-folder` проверяются только файлы `.sig`, `.p7s`, `.sgn`, `.sign`, `.bin`, `.pem` и `.pdf`.

Без указания пути отчёты сохраняются рядом с проверяемыми файлами: отдельные PDF — как `<файл>_report.pdf`, общий — как `merged_report_<дата и время>.pdf`, JSON — как `<файл>.verify-report.json`. Существующие файлы не перезаписываются, а пути созданных отчётов возвращаются в итоговом JSON.

С `--unsign` подпись сначала проверяется, и только после успешной проверки извлекается исходный документ.

С `--visual-copy` для каждого проверенного PDF рядом с ним сохраняется печатная форма `<файл>_штамп.pdf`: документ без электронной подписи со штампом каждого подписанта. Подходит для PDF с PAdES-подписью, присоединённой подписи PDF и отсоединённой подписи, если в `--document` передан PDF. Вид штампа задают те же параметры `--stamp-*`, что и при подписи.

Недействительная подпись возвращает статус `Error` и ненулевой код завершения; отчёт при этом всё равно сохраняется.

Практический пример

В этом примере проверяются подписи файлов в папке `C:\Foldername`, а отчёты сохраняются в папку `C:\Reports`.

```
"C:\Program Files\cryptoarm-sign\cryptoarm-sign.exe" verify ^
  --source-folder "C:\Foldername" ^
```

```
  --save-report-pdf "C:\Reports" ^
  --save-report-pdf-merged "C:\Reports"
```

Снятие подписи

Команда: `unsign`

Команда извлекает исходный документ из присоединённой подписи.

```
cryptoarm-sign unsign \
  --source-file ./document.txt.sig \
  --unsigned-file-path ./out/document.txt
```

Параметр	Описание	По умолчанию
`--enc <DER|PEM|BASE-64>`	Кодировка подписи	`DER`
`--unsigned-file-path <файл>`	Путь для извлечённого документа	—
`--folder-save-unsigned <папка>`	Папка результатов	—

Снять можно только присоединённую подпись. Для отсоединённой исходный документ и так лежит отдельным файлом — проверить его можно командой `verify --document`.

Сертификаты

Команды: `certificates` или `cer`

Команда выводит список сертификатов в формате JSON — из него берутся идентификаторы для параметров `--cert`, `--sign-cert` и `--recipient-cert`.

```
cryptoarm-sign certificates
cryptoarm-sign certificates --provider pgp
```

Та же команда перекодирует сертификаты и запросы на сертификат — см. Кодирование и декодирование файлов.

Работа с OpenPGP

Для OpenPGP в каждой команде указывается `--provider pgp`, а сертификаты задаются отпечатками:

```
cryptoarm-sign sign \
  --provider pgp \
  --cert <отпечаток> \
  --source-file ./document.txt \
  --folder-save-signed ./out
```

Параметр	Описание	По умолчанию
`--subkey <отпечаток>`	Подключ для подписи	—
`--armor`	Сохранить результат в текстовом виде (ASCII armor)	Отключено
`--archive`	Упаковать файлы в TAR внутри операции	Отключено
`--archive-name <имя>`	Имя TAR-архива	—

Пароль закрытого ключа нужен для `sign`, `sign-encrypt` и `decrypt`. Способы передачи:

```
--passphrase "secret"
--passphrase-file ./passphrase.txt
CRYPTOARM_PGP_PASSPHRASE="secret" cryptoarm-sign sign --provider pgp ...
```

Если пароль не передан, а команда запущена в интерактивном терминале, приложение запросит его. Для `encrypt` и `verify` пароль не нужен и не запрашивается.

Отдельной команды `archive` для OpenPGP нет.

Результат и ошибки

Результат выводится в stdout в формате JSON. Диагностика, запрос пароля и журналы идут в stderr.

Успешное выполнение:

```
{
  "method": "signAndEncrypt.outDirectResults",
  "status": "Completed",
  "results": [{ "id": "document.txt", "path": "/path/to/result.sig" }]
}
```

Ошибка:

```
{
  "method": "cli.error",
  "status": "Error",
  "error": {
    "code": "AMBIGUOUS_SOURCE",
```

```
    "message": "Specify only one of --source-file or --source-folder"
  }
}
```

При ошибке процесс возвращает ненулевой код завершения — его удобно проверять в скриптах.

Коды ошибок:

Код	Что означает
`MISSING_SOURCE`	Не указан `--source-file` или `--source-folder`
`AMBIGUOUS_SOURCE`	Указаны оба источника сразу
`AMBIGUOUS_OUTPUT`	Указаны и папка результата, и конкретный файл результата
`INVALID_OUTPUT`	Файл результата указан в неподдерживаемом сценарии
`INVALID_OPTION`	Параметр неприменим к выбранной операции
`INVALID_PATH`	Входной путь отсутствует, имеет неверный тип или недоступен
`UNSUPPORTED_PROVIDER`	Криптопровайдер не поддержан или недоступен
`COMMAND_ERROR`	Ошибка разбора команды или параметров
`OPERATION_ERROR`	Ошибка выполнения операции

Смотрите также

- Подпись и шифрование — те же операции в интерфейсе.
- Проверка и расшифрование — проверка подписей и расшифрование в приложении.
- Контекстное меню Проводника — запуск операций из Проводника.
- Активация лицензии — лицензии КриптоАРМ и КриптоПро CSP.
- API КриптоАРМ — вызов операций из внешних систем.

Открыть статью на сайте

Управление сертификатами

В этом разделе вы узнаете о возможностях раздела **Сертификаты**, научитесь находить нужные сертификаты и перейдёте к подробным инструкциям по установке, экспорту и управлению ключевыми контейнерами.

Содержание:

- Обзор раздела «Сертификаты»
- Профили доверия
- Проверка статуса сертификата
- Поиск сертификатов
- Смотрите также

Обзор раздела «Сертификаты»

Раздел **Сертификаты** предназначен для просмотра и управления сертификатами, ключевыми контейнерами, списками отзыва и запросами на сертификаты.

В разделе можно:

- искать сертификаты;
- переключать профили доверия;
- просматривать статус и сведения о сертификатах;
- устанавливать сертификаты;
- экспортировать и удалять сертификаты;
- создавать запросы на сертификаты;
- создавать самоподписанные сертификаты;
- управлять ключевыми контейнерами;
- объединять сертификаты в группы.

Хранилища сертификатов

Хранилища сгруппированы по назначению и отображаются в левой части окна. Выберите нужное хранилище, чтобы просмотреть его содержимое.

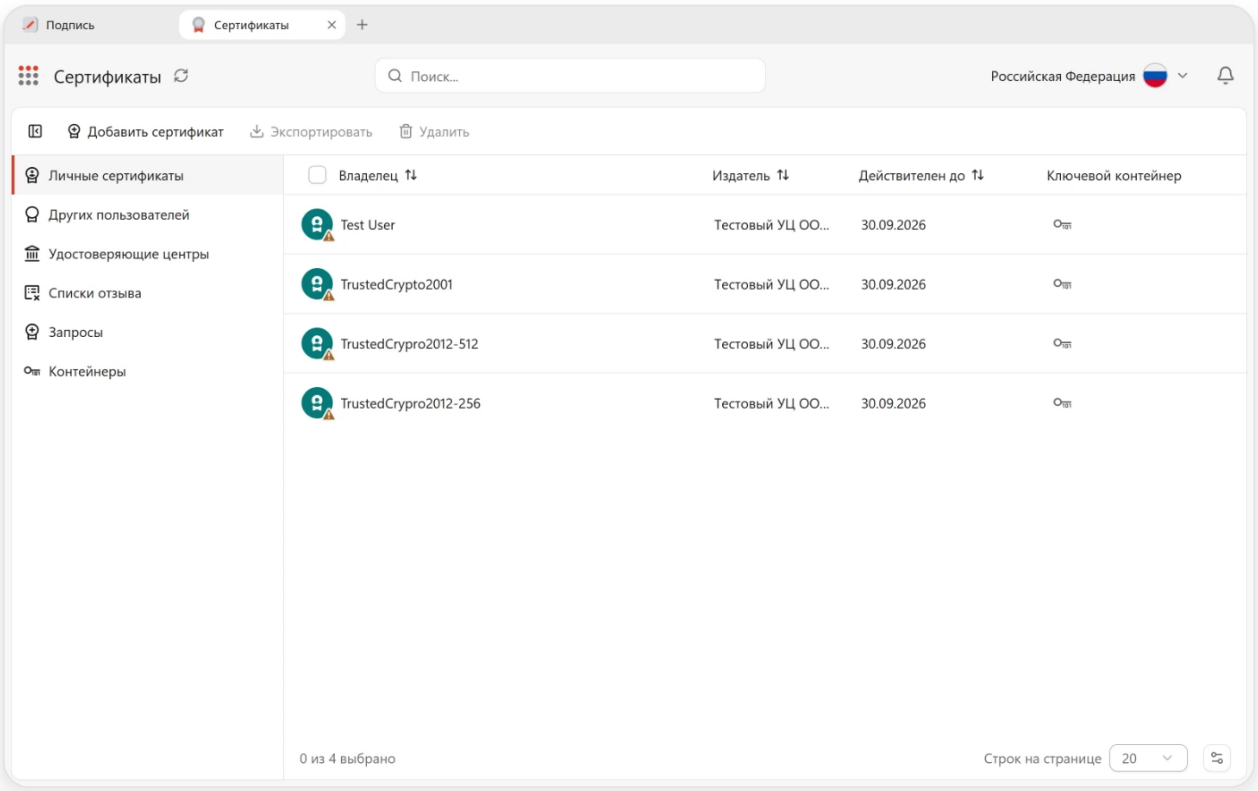
Хранилище	Назначение
Личные сертификаты	Ваши сертификаты с соответствующими закрытыми ключами. Используются для создания электронной подписи и расшифрования данных
Других пользователей	

Хранилище	Назначение
	Сертификаты других пользователей и организаций. Используются для проверки подписей и шифрования данных в адрес получателей
Удостоверяющие центры	Корневые и промежуточные сертификаты удостоверяющих центров, на которых строится цепочка доверия
Списки отзыва	Списки отозванных сертификатов (CRL). Используются для проверки того, не был ли сертификат отозван удостоверяющим центром
Запросы	Запросы на получение сертификатов. Используются для просмотра, экспорта и передачи запроса в удостоверяющий центр
Контейнеры	Ключевые контейнеры с закрытыми ключами

Под хранилищем **«Других пользователей»** располагаются группы сертификатов. Кнопка сворачивания списка освобождает место для таблицы.

> 💡 **Совет**: для создания электронной подписи личный сертификат должен находиться в хранилище **Личные сертификаты** и быть связан с закрытым ключом.

Таблица сертификатов



Столбцы таблицы:

- **Владелец**,
- **Издатель**,
- **Действителен до**,
- **Контейнер**,
- **Алгоритм ключа**.

Набор и порядок столбцов можно поменять — см. Настройка столбцов.

Строки можно выделять по одной или группой — панель действий работает и с несколькими сертификатами сразу.

Профили доверия

Если в системе смешаны сертификаты разных криптоалгоритмов (ГОСТ, RSA и ECDSA), их легко перепутать. Профили доверия решают эту проблему: они фильтруют сертификаты по типу алгоритма, чтобы вы видели только те, которые нужны для текущей задачи.

Доступны два профиля доверия:

Профиль	Отображаемые сертификаты
Российская Федерация	Сертификаты на алгоритмах ГОСТ — соответствие 63-ФЗ «Об электронной подписи»
Открытая криптография	Сертификаты на алгоритмах RSA и ECDSA

Профили доверия используются:

- в разделе **Сертификаты**;
- в панелях выбора сертификатов при подписи и шифровании.

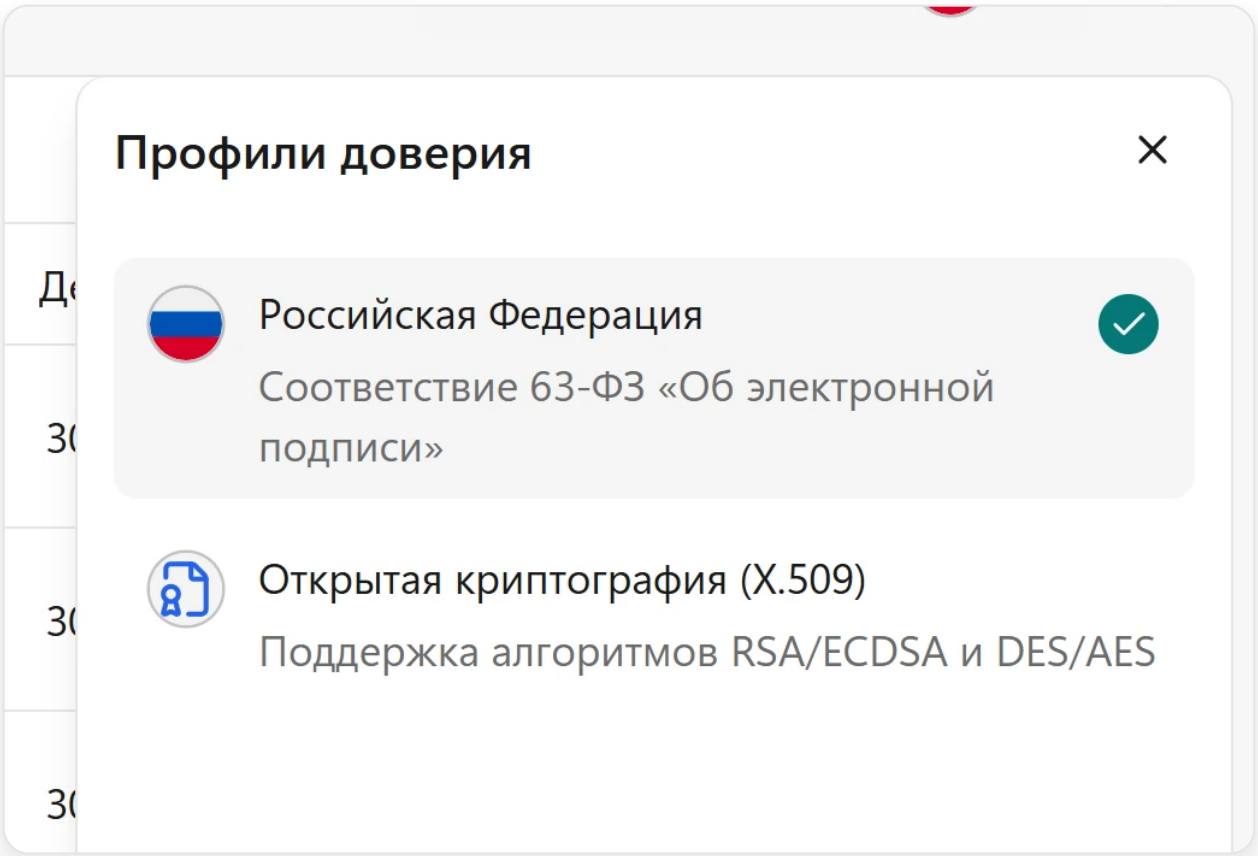
Профиль доверия влияет и на состав хранилищ: **Контейнеры** доступны только в профиле «Российская Федерация», потому что ключевые контейнеры предоставляет КриптоПро CSP. Группы сертификатов тоже принадлежат профилю: в каждом видны только его группы.

> 💡 Профиль доверия влияет только на отображение сертификатов. Он не изменяет сертификаты и не влияет на выполнение криптографических операций.

Переключение между профилями доверия

Чтобы переключить профиль доверия:

1. Перейдите в раздел **Сертификаты**.
2. Нажмите на название активного профиля в верхней части окна.
3. В открывшемся окне выберите профиль, который хотите сделать активным.



После переключения профиля список сертификатов обновится автоматически.

> 💡 **Примечание**: если в настройках выбран стандарт операций **OpenPGP**, раздел показывает сертификаты OpenPGP — см. О разделе OpenPGP.

Проверка статуса сертификата

Проверка позволяет убедиться, что сертификат:

- является действительным;
- не истёк и не отозван;
- имеет корректную цепочку доверия;
- связан с закрытым ключом (для личных сертификатов).

Статус отображается в списке цветом значка сертификата:

Индикатор	Статус	Описание
🟢 Зелёный	Действительный	Сертификат прошёл проверку и может использоваться

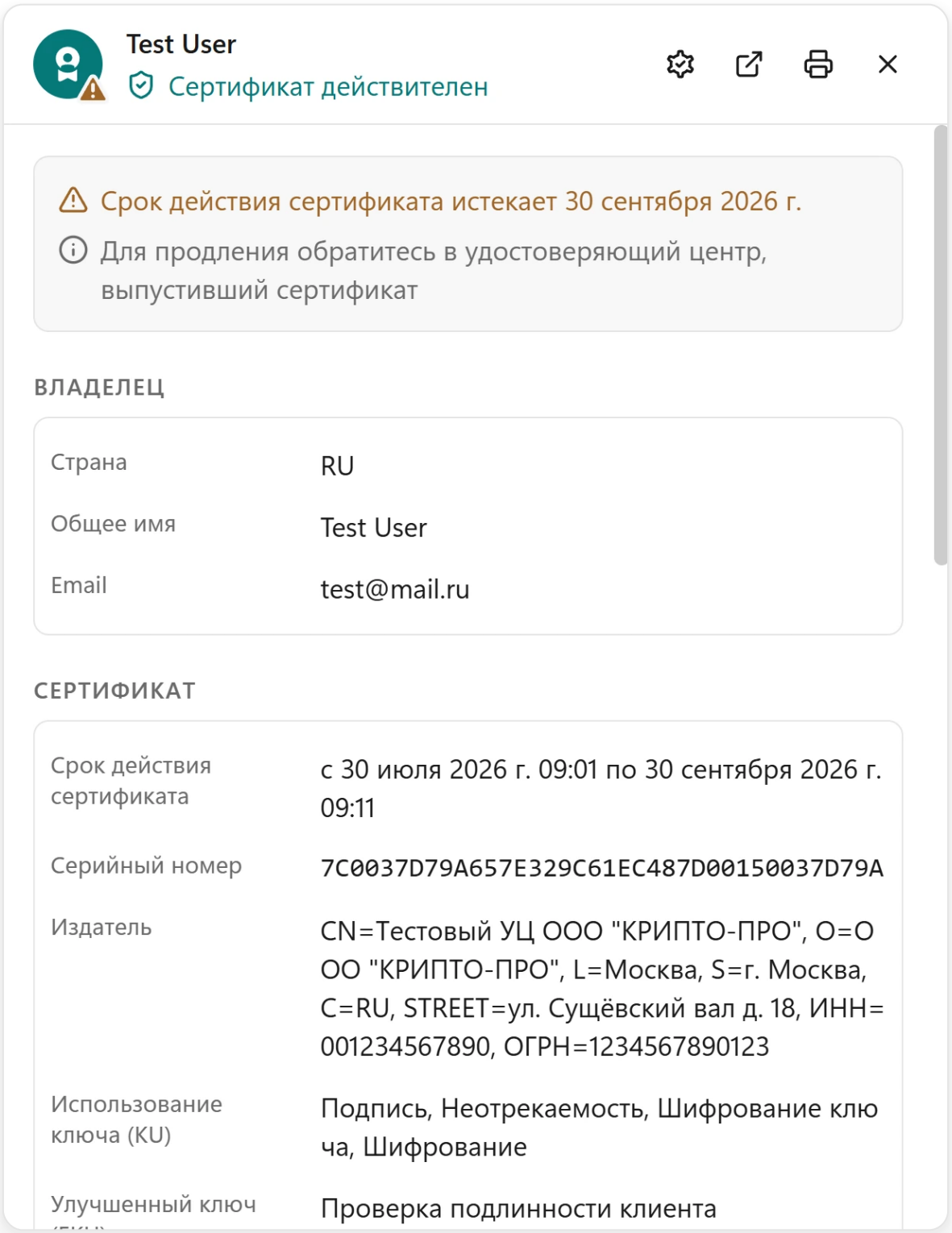
Индикатор	Статус	Описание
🔴 Красный	Недействительный	Сертификат использовать нельзя — например, истёк срок его действия
⚪ Серый	Не проверен	Проверка цепочки ещё не выполнялась

На значке сертификата, срок действия которого скоро закончится, дополнительно появляется предупреждающий знак.

Сведения о сертификате

Чтобы получить подробную информацию о сертификате:

1. Перейдите в раздел **Сертификаты**.
2. Выберите нужный сертификат — в правой части окна откроется панель сведений.



Блок	Содержание
Общие сведения	Владелец, издатель, серийный номер, срок действия, версия, отпечаток
Ключевая информация	Алгоритм открытого ключа, алгоритм подписи, хэш-алгоритм, наличие закрытого ключа, ключевой контейнер, срок действия закрытого ключа

Блок	Содержание
Использование ключа	Использование ключа (KU) и улучшенный ключ (EKU)
Расширения	Идентификаторы ключей субъекта и издателя
Точки распространения	Ссылки на списки отзыва, службу OCSP и сертификат издателя
Цепочка сертификации	Кем и через кого выдан сертификат — вплоть до корневого

Цепочка сертификации показывает путь доверия от сертификата пользователя до корневого удостоверяющего центра. Нажмите название сертификата в цепочке, чтобы посмотреть его сведения.

На Windows доступна команда **Открыть средствами Windows** — просмотр сертификата системным окном.

Статус сертификата и цепочка

В верхней части панели показан результат проверки: **Сертификат действителен**, **Сертификат недействителен** или **Не проверен**. Ниже — состояние цепочки: **действительна** или **недействительна**.

Если построить цепочку не удалось, появится сообщение **«Не удалось построить цепочку»**: как правило, не хватает сертификатов удостоверяющих центров — установите их в хранилище **Удостоверяющие центры**.

Пояснения к проблемам сертификата:

Сообщение	Значение
Срок действия сертификата истёк ...	Сертификат просрочен
Срок действия сертификата истекает ...	Сертификат скоро истечёт
Сертификат вступит в силу ...	Срок действия ещё не начался
Срок действия закрытого ключа истёк ...	Подписывать этим сертификатом нельзя
Срок действия закрытого ключа истекает ...	Ключ скоро перестанет действовать
Не удалось проверить цепочку доверия сертификата	Цепочка не построена или не подтверждена
Для работы с сертификатом требуется КриптоПро CSP	Не установлен нужный криптопровайдер
Сертификат использует неподдерживаемый алгоритм или криптопровайдер	Алгоритм недоступен на этом рабочем месте

Сообщение	Значение
Проверка цепочки доверия ещё не выполнена	Проверка не запускалась

Для продления сертификата обратитесь в выпустивший его удостоверяющий центр.

Проверка контейнера закрытого ключа

Для личного сертификата доступна команда **Протестировать контейнер**. Она проверяет, доступен ли закрытый ключ, и может запросить ПИН-код носителя.

Результаты:

- **Контейнер закрытого ключа доступен**;
- **Контейнер закрытого ключа недоступен. Проверьте, что ключевой носитель подключён.**

Печать карточки сертификата

Команда **Печать** формирует карточку сертификата — документ со сведениями о владельце, издателе, сроке действия и отпечатке, пригодный для печати.

Поиск сертификатов

Чтобы быстро найти нужный сертификат, начните вводить текст в строке поиска в заголовке окна. По мере ввода список обновляется автоматически.

Поиск выполняется по основным свойствам сертификата:

- владелец — краткое и полное имя;
- издатель — краткое и полное имя;
- серийный номер;
- отпечаток;
- ключевой контейнер;
- алгоритм ключа;
- дата окончания срока действия — в том виде, в каком она показана в таблице.

Списки отзыва, запросы и контейнеры ищутся по своим полям, поэтому при переключении хранилища строка поиска очищается.

Смотрите также

- Установка сертификатов — импорт из файла и установка из контейнера.
- Создание запроса и самоподписанного сертификата.
- Экспорт и удаление сертификатов.
- Контейнеры и списки отзыва — работа с ключевыми контейнерами и CRL.

- Группы сертификатов — списки получателей шифрования.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Установка сертификатов в КриптоАРМ

В этом руководстве вы узнаете, как установить в КриптоАРМ сертификаты: личные, других пользователей, корневые и промежуточные. Сертификат добавляется двумя способами — импортом файла или установкой из ключевого контейнера.

Содержание:

- Какое хранилище выбрать
- Импорт сертификата из файла
- Импорт сертификата с закрытым ключом (PKCS#12)
- Установка сертификата из контейнера
- Импорт сертификата другого пользователя
- Импорт сертификатов удостоверяющих центров
- Возможные ошибки
- Смотрите также

> 🚨 Чтобы сертификаты корректно проверялись, в приложении должны быть установлены корневые и промежуточные сертификаты цепочки, а также загружен актуальный список отзыва (CRL). Подробнее — импорт сертификатов удостоверяющих центров и импорт списка отзыва.

Какое хранилище выбрать

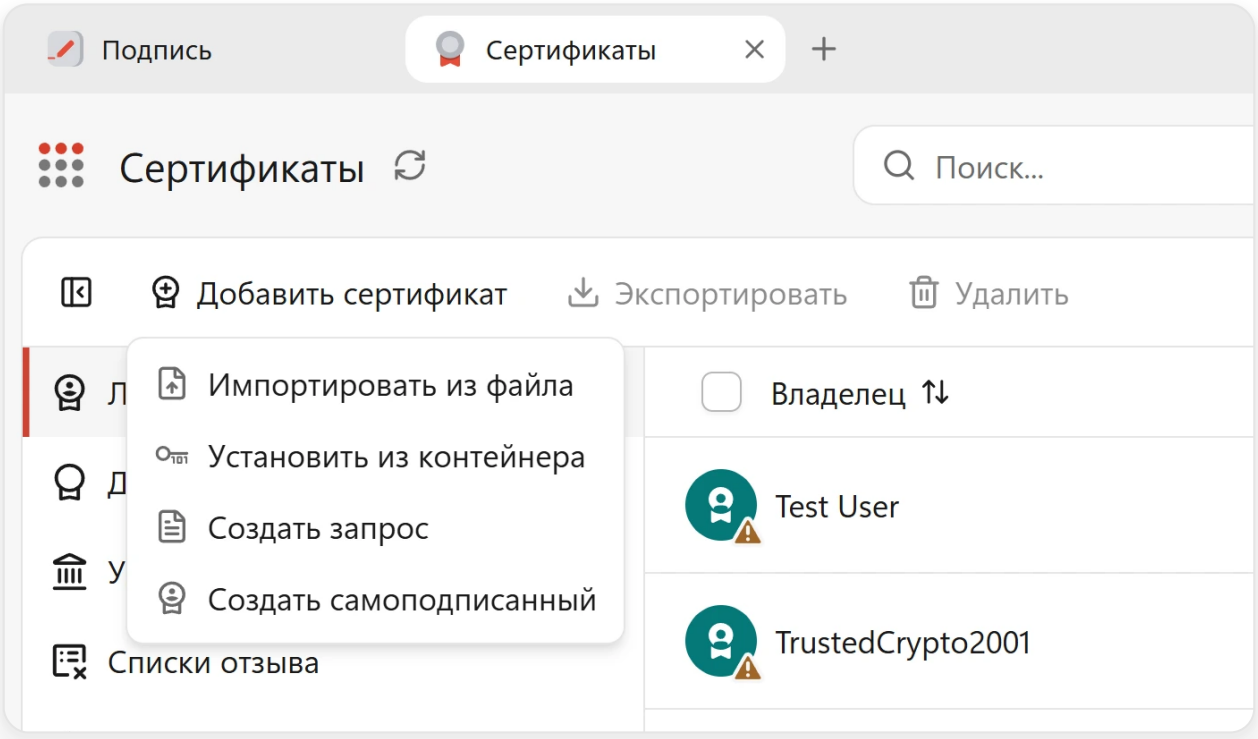
Хранилище	Что в нём хранить
Личные сертификаты	Ваши сертификаты, к которым есть закрытый ключ
Других пользователей	Сертификаты корреспондентов — для шифрования и проверки подписей
Удостоверяющие центры	Корневые и промежуточные сертификаты

Приложение само определяет подходящее хранилище по содержимому файла и при расхождении предлагает выбрать — в окне **«Выберите хранилище для сертификата»** показаны текущее и рекомендуемое хранилища.

Если для импортируемого сертификата в системе уже есть контейнер с его закрытым ключом, приложение связывает их само и помещает сертификат в хранилище **Личные сертификаты**. Так устанавливают сертификат, выпущенный по созданному ранее запросу: контейнер появился при создании запроса, а сертификат приходит из удостоверяющего центра отдельным файлом.

Импорт сертификата из файла

1. Откройте раздел **Сертификаты**.
2. Выберите раздел, в который импортируете сертификат.
3. Нажмите **Добавить сертификат → Импортировать из файла**.



1. Выберите файл сертификата.
2. Если приложение предложит другое хранилище, выберите нужное и нажмите **Импортировать**.

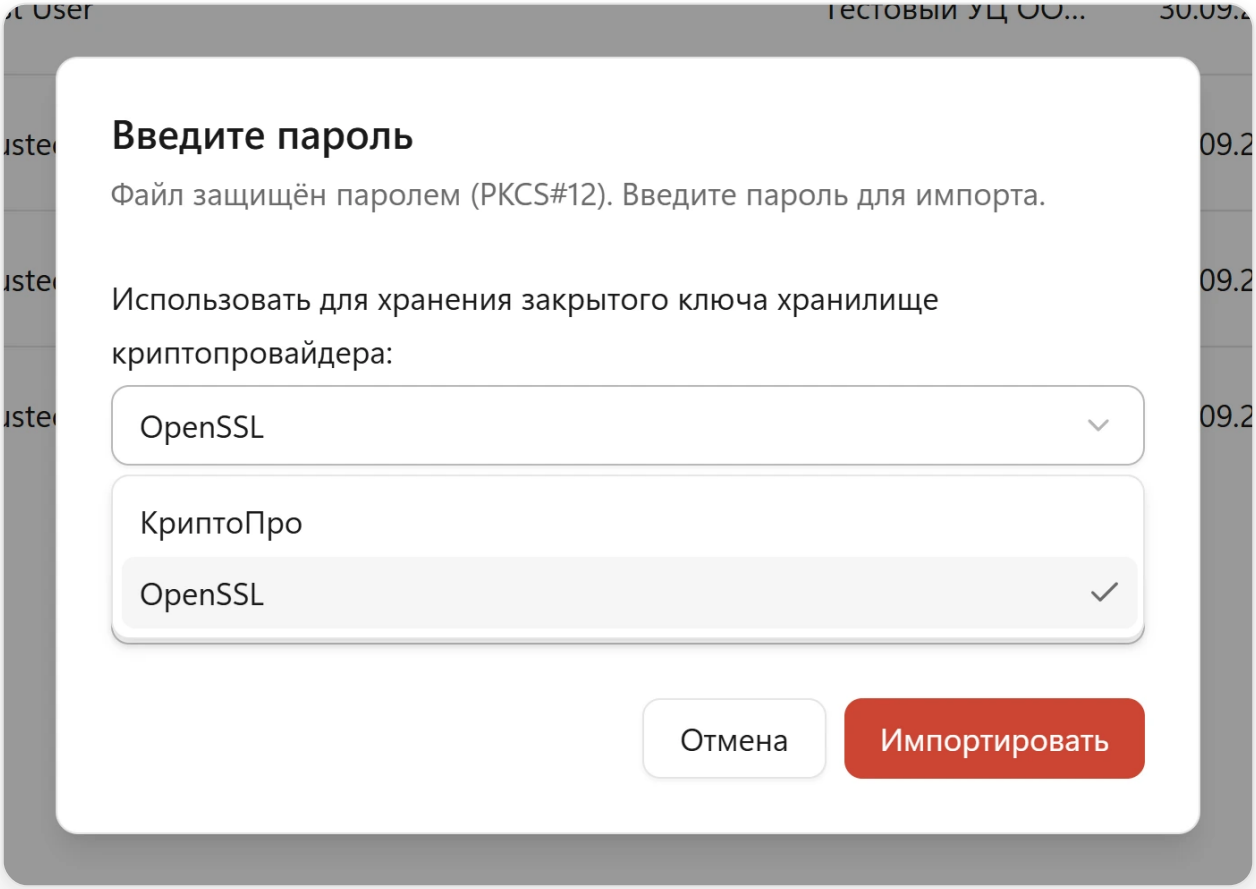
Появится сообщение **«Сертификат "..." импортирован»**.

Импорт сертификата с закрытым ключом (PKCS#12)

Файлы `.pfx` и `.p12` содержат сертификат вместе с закрытым ключом и защищены паролем.

1. Нажмите **Добавить сертификат → Импортировать из файла** и выберите файл.
2. В окне **«Введите пароль»** укажите, где хранить закрытый ключ:

- **КриптоПро** — ключ помещается в хранилище КриптоПро CSP;
- **OpenSSL** — ключ помещается во встроенное хранилище приложения.



1. Введите пароль от файла.
2. Нажмите **Импортировать**.

> 💡 **Примечание**: для ГОСТ-сертификатов выбирайте КриптоПро — иначе закрытый ключ не будет доступен для подписи алгоритмами ГОСТ.

Установка сертификата из контейнера

Если закрытый ключ уже находится в ключевом контейнере — на токене, флеш-накопителе или в реестре, — сертификат устанавливается прямо из него.

1. Откройте раздел **Сертификаты → Личные сертификаты**.
2. Нажмите **Добавить сертификат → Установить из контейнера**.
3. Выберите контейнер в списке и нажмите **Установить**.

Появится сообщение **«Сертификат "..." установлен из контейнера»**.

Подробнее о работе с контейнерами — в инструкции Контейнеры и списки отзыва.

> 💡 **Примечание**: команда доступна только при установленном КриптоПро CSP и в профиле доверия «Российская Федерация».

Импорт сертификата другого пользователя

Чтобы зашифровать файл в чей-то адрес, нужен сертификат корреспондента.

1. Откройте раздел **Сертификаты → Других пользователей**.
2. Нажмите **Добавить сертификат → Импортировать из файла**.
3. Выберите файл сертификата, полученный от корреспондента.

После импорта сертификат появится в списке получателей при шифровании. Часто используемых получателей удобно объединить в группу.

Импорт сертификатов удостоверяющих центров

Чтобы приложение строило цепочку доверия, в хранилище **Удостоверяющие центры** должны быть корневой и промежуточные сертификаты.

Проверка сертификата идёт снизу вверх: **пользовательский → промежуточный → корневой**. Пользовательские сертификаты выпускает удостоверяющий центр по своему промежуточному сертификату, а промежуточный подписан корневым — в России головным корневым сертификатом Минцифры. Пока в хранилище нет хотя бы одного звена, цепочка не строится, и подписи такого сертификата проверяются как недействительные.

Где взять сертификаты цепочки:

- на официальном сайте удостоверяющего центра — обычно в разделах «Поддержка», «Загрузки» или «Документы»;
- по адресам из блока **Ссылки на сертификат издателя** в сведениях о вашем сертификате — см. Сведения о сертификате.

> ⚠️ **Важно**: скачивайте сертификаты удостоверяющих центров только с их официальных сайтов. Файл, полученный из письма или стороннего архива, может оказаться поддельным.

1. Откройте раздел **Сертификаты → Удостоверяющие центры**.
2. Нажмите **Добавить сертификат → Импортировать из файла**.
3. Выберите файл сертификата удостоверяющего центра.

Проверить результат можно в блоке **Цепочка сертификации** сведений о личном сертификате: цепочка должна быть отмечена как действительная.

> 💡 **Примечание**: в это хранилище можно импортировать только сертификаты удостоверяющих центров. При попытке импортировать пользовательский сертификат появится сообщение **«В хранилище удостоверяющих центров можно импортировать только сертификат УЦ»**.

Возможные ошибки

Сообщение	Что это значит	Что сделать
Не удалось импортировать сертификат	Файл повреждён или имеет неподдерживаемый формат	Запросите сертификат у отправителя заново
Неверный пароль	Пароль от файла `.pfx` или `.p12` введён с ошибкой	Уточните пароль у того, кто выдал файл
В хранилище удостоверяющих центров можно импортировать только сертификат УЦ	Пользовательский сертификат попал не в тот раздел	Импортируйте его в хранилище **Личные сертификаты** или **Других пользователей**
Используйте раздел списков отзыва для импорта CRL	Выбран файл списка отзыва, а не сертификат	Импортируйте его в разделе «Списки отзыва»
Сертификат в контейнере отсутствует или недоступен	В контейнере есть ключ, но нет самого сертификата	Запросите сертификат в удостоверяющем центре и импортируйте его из файла
Сертификат из контейнера уже установлен в хранилище	Такой сертификат уже есть в приложении	Ничего делать не нужно — он в хранилище **Личные сертификаты**
КриптоПро CSP недоступен	Провайдер, который работает с ГОСТ-ключами, не установлен или не отвечает	Установите КриптоПро CSP и перезапустите приложение

Смотрите также

- Раздел «Сертификаты» — устройство раздела.
- Создание запроса и самоподписанного сертификата — если сертификата ещё нет.
- Экспорт и удаление сертификатов.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Создание запроса и самоподписанного сертификата

Запрос на сертификат — это файл, который приложение создаёт вместе с закрытым ключом и который вы передаёте в удостоверяющий центр, чтобы тот выпустил сертификат. Закрытый ключ остаётся у вас: в запрос попадают только открытый ключ и сведения о владельце.

Самоподписанный сертификат приложение выпускает само, без удостоверяющего центра. Он подходит для проверки работы и внутренних задач.

> 💡 **Примечание**: если сертификат вам выдал удостоверяющий центр — на токене, в файле или по ссылке, — эта инструкция не нужна. Переходите к установке сертификата.

Содержание:

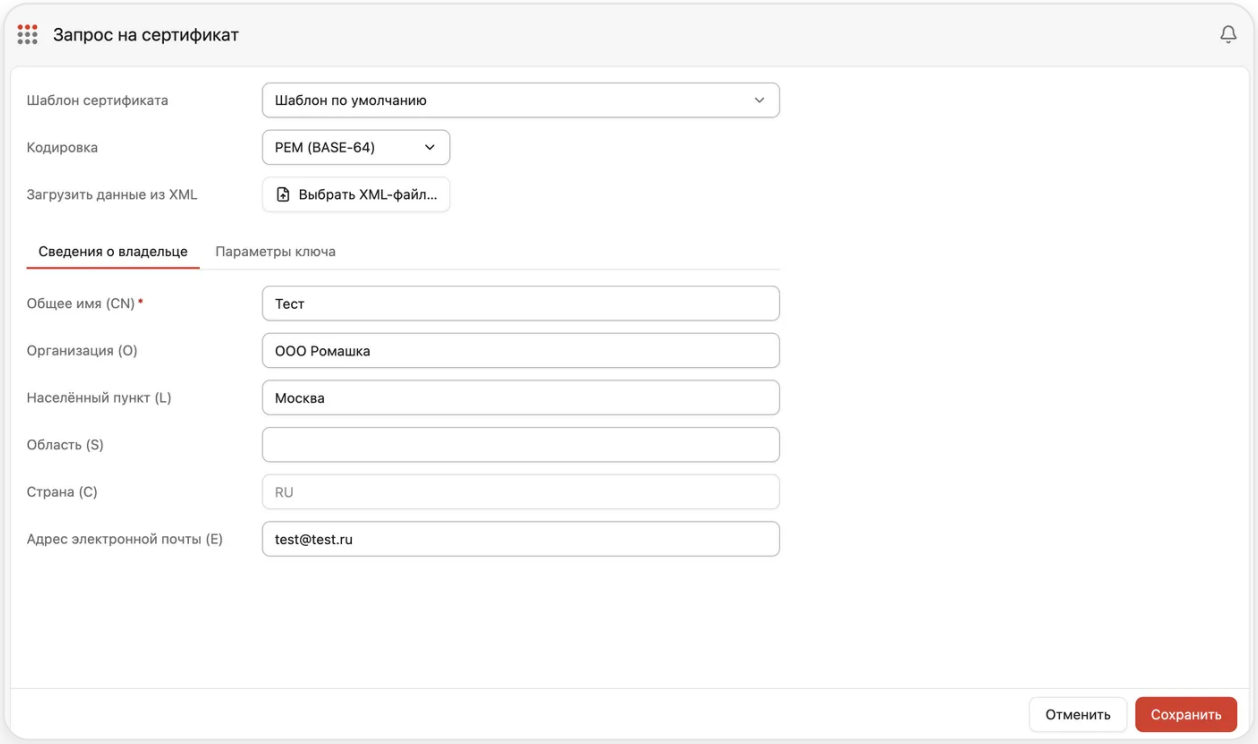
- Что потребуется
- Создание запроса на сертификат
- Шаблоны
- Загрузка данных из XML
- Сведения о владельце
- Параметры ключа
- Дополнительные параметры сертификата
- Сохранение запроса
- Создание самоподписанного сертификата
- Просмотр созданных запросов
- Возможные ошибки
- Смотрите также

Что потребуется

- **Криптопровайдер под нужный алгоритм**: КриптоПро CSP для ключей ГОСТ, встроенный OpenSSL для RSA и EC.
- **Сведения о владельце в том виде, в каком их требует удостоверяющий центр** — состав полей задаёт шаблон, а готовые данные можно загрузить из XML.
- **Место для контейнера закрытого ключа**: подключённый токен или флеш-накопитель, если ключ должен храниться на носителе.

Создание запроса на сертификат

1. Откройте раздел **Сертификаты → Личные сертификаты**.
2. Нажмите **Добавить сертификат → Создать запрос**.
3. Откроется вкладка **«Запрос на сертификат»**.



1. Выберите **Шаблон сертификата** — он заполнит нужный набор полей. Сразу после открытия выбран **Шаблон по умолчанию**.
2. Заполните **Сведения о владельце**.
3. Задайте **Параметры ключа**.
4. При необходимости уточните использование ключа и дополнительные расширения.
5. Нажмите **Сохранить**.
6. Если приложение запросит ПИН-код для защиты закрытого ключа, укажите его.

Появится сообщение **«Запрос сохранён в ...»**. Передайте полученный файл в удостоверяющий центр.

> ⚠️ **Важно**: закрытый ключ создаётся на вашем рабочем месте и остаётся на нём. Не удаляйте контейнер ключа до получения сертификата — иначе выпущенный сертификат будет непригоден.

Шаблоны

Шаблон задаёт набор полей и расширений под конкретный вид сертификата:

- **Шаблон по умолчанию**;
- **Шаблон с расширенным списком полей**;
- **Сертификат КЭП физического лица**, **юридического лица**, **индивидуального предпринимателя**;
- **DV-сертификат от Минцифры** (ГОСТ, RSA);
- **OV-сертификат от Минцифры** — ФЛ, ЮЛ, ИП (ГОСТ, RSA);
- **УЦ ЦБ. Личный сертификат. ЮЛ, ГОСТ**;
- **УЦ ЦБ. Сертификат для автоматизированной системы. ЮЛ, ГОСТ**.

Выбор шаблона не запрещает менять поля вручную — кроме закреплённых шаблоном: такие поля и флажки недоступны для изменения. Другой шаблон заполняет форму заново: введённые значения при этом сбрасываются.

Свои шаблоны

Если удостоверяющий центр или техническая поддержка прислали шаблон в формате JSON, откройте список шаблонов и нажмите **Загрузить шаблон**. Подходят файлы шаблонов КриптоАРМ «Защищенная почта»: и один шаблон, и файл `templates.json` со всеми шаблонами сразу. Загруженные шаблоны появляются в конце списка.

Свой шаблон удаляется кнопкой с корзиной в списке. Встроенные шаблоны удалить нельзя.

Загрузка данных из XML

Если данные владельца уже подготовлены в XML, нажмите **Выбрать XML-файл** в строке **Загрузить данные из XML**. Поля формы заполнятся автоматически, а рядом с кнопкой появится имя файла.

Подходит и XML, который приложение сохраняет рядом с каждым запросом: окно выбора файла открывается в папке запросов. Так удобно создать запрос заново, если удостоверяющий центр отклонил прежний. Формат файла тот же, что у КриптоАРМ «Защищенная почта»: данные, сохранённые одним приложением, загружаются в другое.

Ошибки загрузки:

Сообщение	Что это значит	Что сделать
Не удалось разобрать XML-файл	Файл повреждён или это не XML	Запросите файл заново в удостоверяющем центре
В XML-файле не найден раздел person	В файле нет данных владельца	Проверьте, тот ли файл выбран

Сообщение	Что это значит	Что сделать
В XML-файле нет поддерживаемых полей владельца	Формат файла не подходит	Заполните поля вручную

Сведения о владельце

Какие поля показаны, в каком порядке и какие из них обязательны, задаёт шаблон; обязательные отмечены звёздочкой. **Общее имя (CN)** обязательно всегда. Во встроенных шаблонах страна — RU, и изменить её нельзя.

Параметры ключа

Здесь задаётся ключ будущего сертификата. Если удостоверяющий центр прислал требования к запросу, заполняйте поля по ним; в остальных случаях достаточно выбрать криптопровайдер и алгоритм, а прочие поля не менять.

Параметр	Описание
Криптопровайдер	«КриптоПро CSP 5.0» для ГОСТ, если он установлен, или «OpenSSL» для RSA и EC
Алгоритм	ГОСТ Р 34.10-2012, RSA или EC
Размер ключа	256, 384, 512 или 2048 бит — в зависимости от алгоритма
Способ идентификации	Как удостоверяющий центр идентифицирует владельца: лично, по квалифицированной ЭП, по электронному документу или через ЕСИА и ЕБС
Назначение ключа	«Подпись», «Шифрование» или «Подпись и шифрование»; «Пользовательский» — если флажки использования ключа изменены вручную
Контейнер (будет создан новый)	Имя нового контейнера для ключа; приложение предлагает случайное
Разрешить экспорт закрытого ключа	Позволяет впоследствии выгрузить закрытый ключ

Способ идентификации, контейнер и экспорт ключа есть только у КриптоПро CSP.

> ⚠️ **Важно**: если ПИН-код не задан, закрытый ключ не будет защищён — приложение отдельно спросит подтверждение.

Дополнительные параметры сертификата

> 💡 **Примечание**: эти блоки заполняются только по требованиям удостоверяющего центра. Если таких требований вам не давали, оставьте значения по умолчанию: неверно заполненные поля помешают выпустить сертификат.

Использование ключа (KeyUsage) и **Расширенное использование ключа (ExtendedKeyUsage)** ограничивают, для чего можно применять сертификат: подпись документов, шифрование, проверка подлинности сервера, подпись кода и так далее. Удостоверяющий центр обычно выдаёт готовый перечень значений.

В разделе **Дополнительные расширения** собраны остальные сведения для сертификата. У КриптоПро CSP в нём всегда есть **Средство ЭП владельца** и **Класс средства ЭП**: их требует российское регулирование. Класс, если его не задаёт шаблон, совпадает с классом установленного КриптоПро CSP. Остальные поля появляются, если их задаёт шаблон:

- **Альтернативное имя субъекта (SAN)** — дополнительные имена владельца, в том числе доменные;
- **Дополнительные OID EKU** — назначения, которых нет в списке выше, через точку с запятой;
- у КриптоПро CSP — средство ЭП и УЦ издателя, период использования закрытого ключа, дополнительные политики сертификата и **OID шаблона сертификата**, по которому удостоверяющий центр выбирает вид выпускаемого сертификата.

Все значения берутся из документов удостоверяющего центра.

Сохранение запроса

Кодировку файла — DER или PEM (BASE-64) — предлагает шаблон, а сменить её можно в поле **Кодировка** под шаблоном. Расширение файла задаёт шаблон, обычно это `.req`.

Рядом с запросом сохраняется XML-файл с тем же именем и введёнными сведениями о владельце. Из него можно заполнить форму следующего запроса.

Создание самоподписанного сертификата

1. Откройте раздел **Сертификаты → Личные сертификаты**.
2. Нажмите **Добавить сертификат → Создать самоподписанный**.
3. Заполните форму так же, как для запроса.
4. На вкладке **Параметры ключа** дополнительно укажите срок действия сертификата в полях **Действителен с** и **Действителен до**.

5. Нажмите **Сохранить**.

Появится сообщение **«Самоподписанный сертификат создан»**, и сертификат появится в разделе **Личные сертификаты**.

> ⚠️ **Важно**: самоподписанный сертификат не выпущен удостоверяющим центром. Для юридически значимого документооборота он не подходит: у получателя не будет оснований доверять такой подписи.

Просмотр созданных запросов

Файлы запросов сохраняются в отдельной папке приложения. Их список показывает раздел **Сертификаты → Запросы** со столбцами **Файл**, **Тип**, **Изменён** и **Размер**. Набор и порядок столбцов можно поменять — см. Настройка столбцов.

Доступные действия:

- **Открыть папку** — открыть каталог с файлами запросов;
- **Экспортировать** — сохранить файл запроса в другое место;
- просмотр сведений о файле: имя, тип, размер, даты, путь;
- **Удалить** — удалить файл запроса вместе с XML-файлом сведений о владельце. Чтобы удалить несколько запросов, отметьте их флажками. Закрытый ключ при этом не удаляется.

Возможные ошибки

Сообщение	Что это значит	Что сделать
Криптопровайдер с поддержкой ГОСТ недоступен	Для ключей ГОСТ нужен КриптоПро CSP, а он не установлен	Установите КриптоПро CSP и перезапустите приложение
Системный криптопровайдер недоступен	Приложение не смогло обратиться к встроенному провайдеру	Перезапустите приложение; если повторяется — обратитесь в поддержку
Не удалось инициализировать криптопровайдер	Провайдер не отвечает	Перезапустите приложение
Не удалось создать сертификат	Операция прервалась	Причина записана в журнале

Смотрите также

- Установка сертификатов — установка выпущенного сертификата.
- Контейнеры и списки отзыва — работа с ключевыми контейнерами.
- Экспорт и удаление сертификатов.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Экспорт и удаление сертификатов

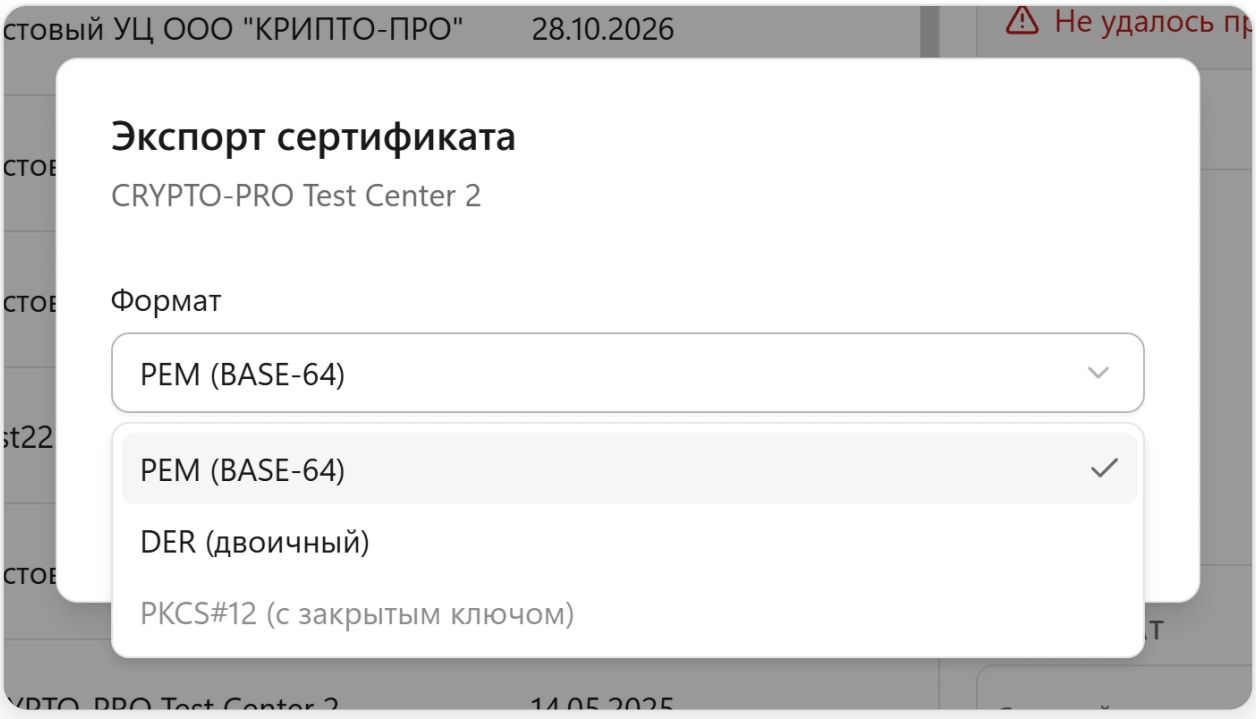
Экспорт нужен, чтобы передать сертификат корреспонденту или перенести его на другое рабочее место. Удаление убирает сертификат из хранилища.

Содержание:

- Экспорт сертификата
- Выбор формата экспорта
- Экспорт с закрытым ключом
- Удаление сертификата
- Удаление связанного контейнера
- Возможные ошибки
- Смотрите также

Экспорт сертификата

1. Откройте раздел **Сертификаты**.
2. Выделите сертификат в списке.
3. Нажмите **Экспортировать** на панели действий.



1. Выберите **Формат**.
2. Нажмите **Экспортировать** и укажите, куда сохранить файл.

Появится сообщение **«Сертификат успешно экспортирован»**.

Выбор формата экспорта

Сертификат экспортируется двумя способами — с закрытым ключом и без него. От этого зависит, что можно сделать с полученным файлом:

Способ	Что получается	Когда применять
Без закрытого ключа	Файл с сертификатом: DER или PEM	Передать корреспонденту, чтобы он шифровал файлы в ваш адрес и проверял ваши подписи
С закрытым ключом	Файл PKCS#12, защищённый паролем	Перенести личный сертификат на другое рабочее место, где им нужно подписывать и расшифровывать

Формат	Что содержит	Когда использовать
DER (двоичный)	Только сертификат	Передача корреспонденту, импорт в другие системы
PEM (BASE-64)	Только сертификат, текстовый вид	Когда нужен текстовый файл — например, для вставки в конфигурацию
PKCS#12 (с закрытым ключом)	Сертификат и закрытый ключ	Перенос личного сертификата на другое рабочее место

> 💡 **Примечание**: формат PKCS#12 доступен только для сертификатов, у которых есть закрытый ключ и он помечен как экспортируемый.

Экспорт с закрытым ключом

При выборе формата **PKCS#12** нужно задать пароль:

1. Введите пароль в поле **Пароль**.
2. Повторите его в поле **Подтверждение пароля**.
3. Нажмите **Экспортировать**.

Если пароли не совпадают, появится сообщение **«Пароли не совпадают»**.

⚠️ **Важно**: файл PKCS#12 содержит закрытый ключ. Передавайте его только по защищённому каналу и не храните пароль вместе с файлом. Тот, у кого есть файл и пароль, сможет подписывать документы от вашего имени.

Удаление сертификата

1. Выделите сертификат в списке или отметьте флажками несколько.
2. Нажмите **Удалить**.
3. Подтвердите действие. Для одного сертификата окно называется **«Удаление сертификата»**, для нескольких в заголовке указано их число, например **«Удаление 3 сертификатов»**. Если открыта группа, окно предупредит, что сертификаты удаляются из хранилища, а не только из группы: чтобы убрать их только из группы, выберите Убрать из группы.

Появится сообщение **«Сертификат удалён»** или с числом удалённых. Если часть сертификатов удалить не удалось, сообщение покажет, сколько удалено из выбранных, а причина отказа будет в журнале.

⚠️ **Важно**: удаление нельзя отменить. Прежде чем удалять личный сертификат, убедитесь, что он больше не нужен: без него не получится ни подписать документ, ни расшифровать ранее зашифрованные файлы.

Удаление связанного контейнера

Для личного сертификата с контейнером КриптоПро в окне подтверждения доступна дополнительная настройка **«Удалить связанный контейнер закрытого ключа»**. Если её включить, вместе с сертификатом будет удалён и закрытый ключ.

Если выбрано несколько сертификатов, настройка называется **«Удалить связанные контейнеры закрытых ключей»** и появляется, когда контейнер есть хотя бы у одного из них. Контейнер есть не у всех — окно покажет, у скольких: например, «Контейнер есть у 2 из 5 выбранных». Остальные сертификаты удаляются как обычно.

⚠️ **Важно**: удалять контейнер не рекомендуется, если он используется другими сертификатами. Восстановить закрытый ключ после удаления невозможно.

Возможные ошибки

Сообщение	Что это значит	Что сделать
Не удалось экспортировать сертификат	Закрытый ключ запрещено выгружать или носитель недоступен	Проверьте, подключён ли токен; ключ без разрешения на экспорт выгрузить нельзя
Пароли не совпадают	Пароль и подтверждение введены по-разному	Введите пароль в оба поля заново
Не удалось удалить сертификат	Сертификат занят другой операцией или нет прав на хранилище	Закройте выполняемые операции и повторите; для системного хранилища нужны права администратора

Подробности отказа записываются в журнал.

Смотрите также

- Установка сертификатов — обратная операция.
- Раздел «Сертификаты» — где находятся действия.
- Контейнеры и списки отзыва — удаление контейнеров отдельно от сертификатов.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Ключевые контейнеры и списки отзыва (CRL)

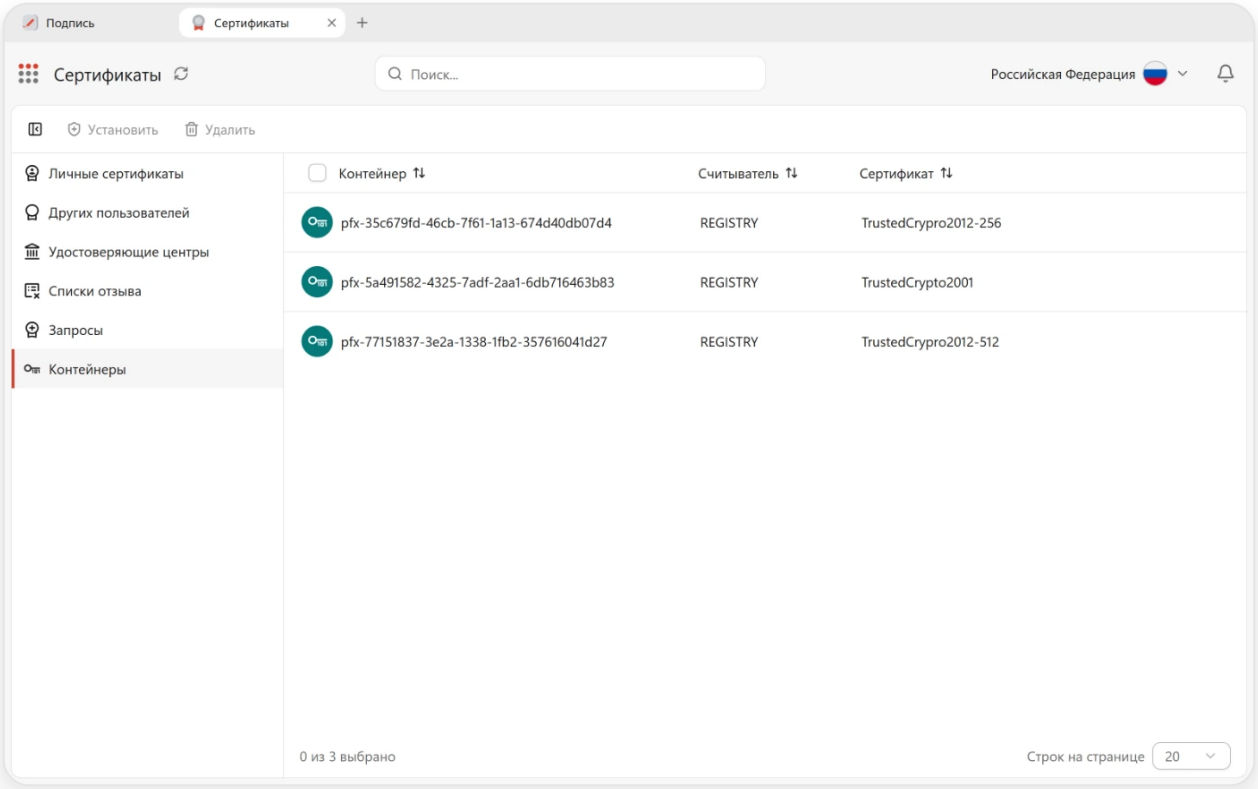
Ключевой контейнер — защищённое хранилище закрытого ключа: на токене, флеш-накопителе или в реестре компьютера. **Список отзыва (CRL)** — публикуемый удостоверяющим центром перечень сертификатов, действие которых прекращено досрочно; по нему приложение проверяет, не отозван ли сертификат.

Содержание:

- Раздел «Контейнеры»
- Сведения о контейнере
- Установка сертификата из контейнера
- Удаление контейнера
- Списки отзыва (CRL)
- Импорт списка отзыва
- Сведения о списке отзыва
- Экспорт списка отзыва
- Удаление списков отзыва
- Возможные ошибки
- Смотрите также

Раздел «Контейнеры»

Раздел **Сертификаты → Контейнеры** показывает ключевые контейнеры, доступные КриптоПро CSP: в реестре, на флеш-накопителях, смарт-картах и токенах.



Столбцы:

- **Контейнер** — имя контейнера;
- **Считыватель** — где расположен контейнер;
- **Сертификат** — сертификат, находящийся в контейнере.

Набор и порядок столбцов можно поменять — см. Настройка столбцов.

> 💡 **Примечание**: раздел доступен только при установленном КриптоПро CSP и в профиле доверия «Российская Федерация». Если провайдер не найден, появится сообщение **«КриптоПро CSP недоступен»**.

Сведения о контейнере

Выделите контейнер, чтобы увидеть:

- **Имя** и **Уникальное имя** контейнера;
- **Считыватель**;
- состояние сертификата: **Установлен** или **Не установлен** в хранилище.

Действия с сертификатом из контейнера выполняются в разделе **Личные сертификаты** после его установки:

- проверить, доступен ли закрытый ключ — команда **Протестировать контейнер**;
- распечатать карточку сертификата со сведениями о владельце, издателе и отпечатке.

Установка сертификата из контейнера

Если в контейнере есть сертификат, его можно установить в хранилище **Личные сертификаты** — после этого им можно подписывать и расшифровывать.

1. Откройте раздел **Сертификаты → Контейнеры**.
2. Выделите контейнер.
3. Нажмите **Установить**.

Появится сообщение **«Сертификат "..." установлен из контейнера»**.

Если сертификат уже установлен, появится сообщение **«Сертификат из контейнера уже установлен в хранилище»**.

Удаление контейнера

1. Выделите контейнер или отметьте его флажком.
2. Нажмите **Удалить**.
3. При необходимости включите **«Удалить связанный с контейнером сертификат»**.
4. Подтвердите действие в окне **«Удаление контейнера»**.

Контейнеры удаляются по одному: если отмечено несколько, кнопка **Удалить** недоступна.

> ⚠️ **Важно**: удаление контейнера уничтожает закрытый ключ. Восстановить его невозможно: подписать документы и расшифровать ранее зашифрованные файлы будет нельзя.

Списки отзыва (CRL)

Список отзыва (CRL) — документ удостоверяющего центра со сведениями о сертификатах, которые перестали действовать до окончания своего срока: закрытый ключ скомпрометирован, изменились данные владельца, сертификат выпущен с ошибкой, владелец прекратил работу с ним. Без актуального списка приложение не может подтвердить, что сертификат подписанта не отозван, — в сведениях о подписи появится **«Статус отзыва не проверен»**.

Где взять список отзыва:

- по адресу из блока **Точки распространения списков отзыва** в сведениях о сертификате — см. Сведения о сертификате;
- на официальном сайте удостоверяющего центра, рядом с корневым и промежуточными сертификатами.

Список отзыва действует ограниченное время: у него есть дата следующего обновления, после которой сведения считаются устаревшими и список нужно скачать заново.

Раздел **Сертификаты → Списки отзыва** показывает установленные списки отзыва.

Столбцы:

- **Издатель**,
- **Выпущен**,
- **Действует до**,
- **Номер CRL**.

Набор и порядок столбцов можно поменять — см. Настройка столбцов.

Статус списка:

Статус	Значение
Действителен	Список актуален
Просрочен	Наступил срок следующего обновления — сведения об отзыве могли устареть
Недействителен	Список не прошёл проверку
Ожидает	Срок действия ещё не наступил

Импорт списка отзыва

1. Откройте раздел **Сертификаты → Списки отзыва**.
2. Нажмите **Импортировать**.
3. Выберите файл списка отзыва.

Появится сообщение **«Список отзыва "..." импортирован»**.

Адрес, по которому удостоверяющий центр публикует список отзыва, указан в сведениях о сертификате — блок **Точки распространения списков отзыва**.

Сведения о списке отзыва

Выделите список, чтобы увидеть:

- **Издатель**,
- **Номер списка отзыва**,
- **Выпущен** и **Следующее обновление**,
- **Алгоритм подписи** и **хэш-алгоритм подписи**,
- **Отпечаток**,
- **Идентификатор ключа издателя**.

Экспорт списка отзыва

1. Выделите список отзыва.
2. Нажмите **Экспортировать**.
3. Укажите, куда сохранить файл.

Появится сообщение **«Список отзыва успешно экспортирован»**.

Удаление списков отзыва

1. Выделите список отзыва или отметьте флажками несколько.
2. Нажмите **Удалить**.
3. Подтвердите удаление.

Удалённый список отзыва можно снова импортировать из файла, скачанного у удостоверяющего центра.

Возможные ошибки

Сообщение	Что это значит	Что сделать
КриптоПро CSP недоступен	Провайдер, который работает с контейнерами, не установлен или не отвечает	Установите КриптоПро CSP и перезапустите приложение
Ключевые контейнеры не найдены	Носитель не подключён или на нём нет контейнеров	Подключите носитель и откройте раздел заново
Сертификат в контейнере отсутствует или недоступен	В контейнере нет сертификата либо носитель требует ПИН-код	Введите ПИН-код; если сертификата нет, запросите его в удостоверяющем центре

Сообщение	Что это значит	Что сделать
Не удалось установить сертификат из контейнера	Операция прервалась	Причина записана в журнале
Файл не является списком отзыва	Выбран файл другого формата	Скачайте список отзыва с сайта удостоверяющего центра
Не удалось импортировать список отзыва	Файл повреждён или подписан неизвестным издателем	Скачайте список заново и убедитесь, что сертификат его издателя установлен

Смотрите также

- Установка сертификатов — установка личного сертификата из контейнера.
- Раздел «Сертификаты» — проверка контейнера закрытого ключа.
- Проверка и расшифрование — как используется список отзыва.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Группы сертификатов

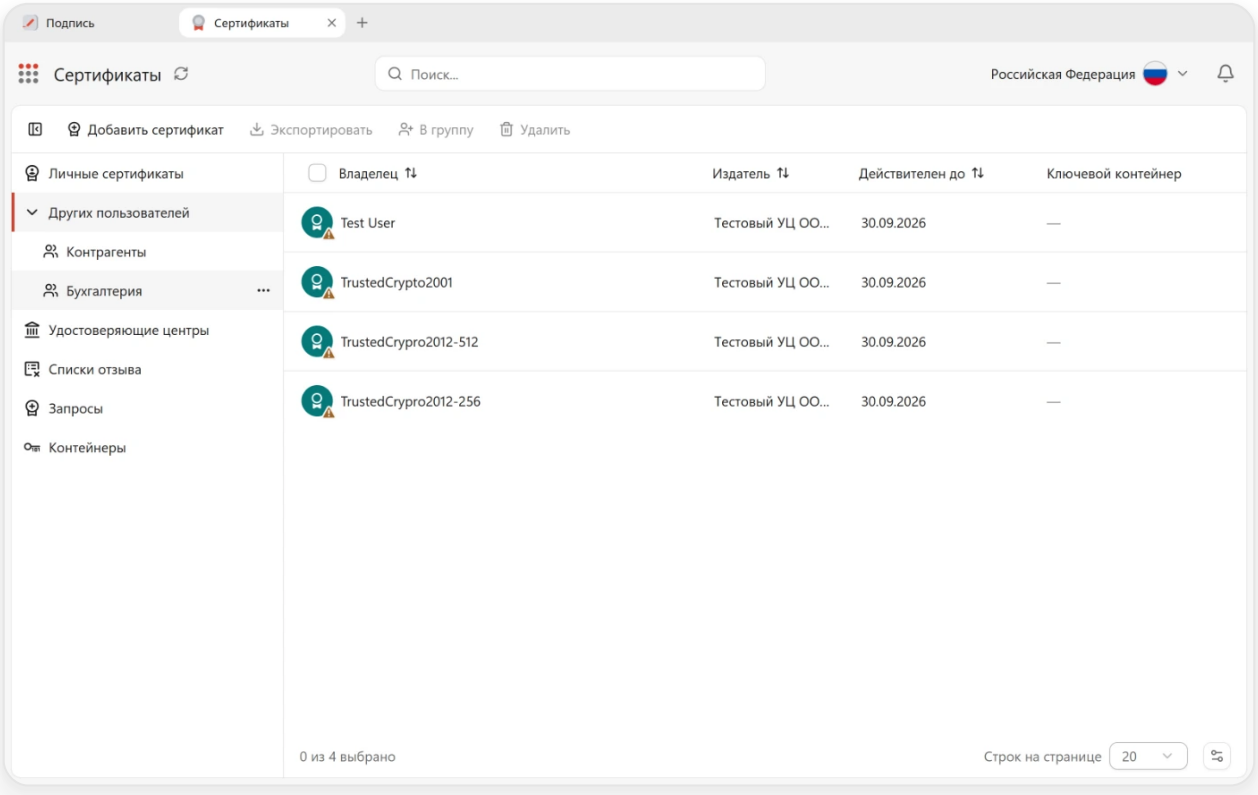
Группа — именованный список сертификатов. Она избавляет от выбора одних и тех же получателей по одному: при шифровании достаточно указать группу.

Содержание:

- Где находятся группы
- Создание группы
- Добавление сертификатов в группу
- Просмотр состава группы
- Редактирование группы
- Удаление сертификата из группы
- Удаление группы
- Шифрование для группы
- Возможные ошибки
- Смотрите также

Где находятся группы

Группы располагаются в разделе **Сертификаты**, под хранилищем **«Других пользователей»**.



Сколько сертификатов входит в группу, видно в панели выбора получателей — см. Шифрование для группы.

> 💡 **Примечание**: группы принадлежат профилю доверия и стандарту операций. В профиле «Российская Федерация» видны группы ГОСТ-сертификатов, в «Открытой криптографии» — свои, а при стандарте операций OpenPGP — группы сертификатов OpenPGP.

Создание группы

1. Откройте раздел **Сертификаты**.
2. Нажмите **Создать группу** рядом с хранилищем **«Других пользователей»**.
3. Введите название группы.
4. Отметьте сертификаты, которые войдут в группу.
5. Нажмите **Создать**.

Появится сообщение **«Группа создана»**, и группа появится в списке.

Добавление сертификатов в группу

1. Выделите один или несколько сертификатов в списке.
2. Нажмите **Добавить в группу** на панели действий.
3. Отметьте нужные группы — сертификаты, которые уже состоят в группе, помечены как **«Уже в группе»**.
4. Нажмите **Добавить**.

Просмотр состава группы

Щелчок по названию группы показывает только входящие в неё сертификаты. Все обычные действия — просмотр сведений, экспорт, удаление — доступны и здесь.

Редактирование группы

1. Нажмите кнопку меню в строке группы и выберите **Редактировать**.
2. Измените название или состав.
3. Нажмите **Сохранить**.

Удаление сертификата из группы

1. Откройте группу.
2. Выделите сертификат.
3. Выберите действие **Убрать из группы**.

Сертификат останется в хранилище — он исчезнет только из этой группы.

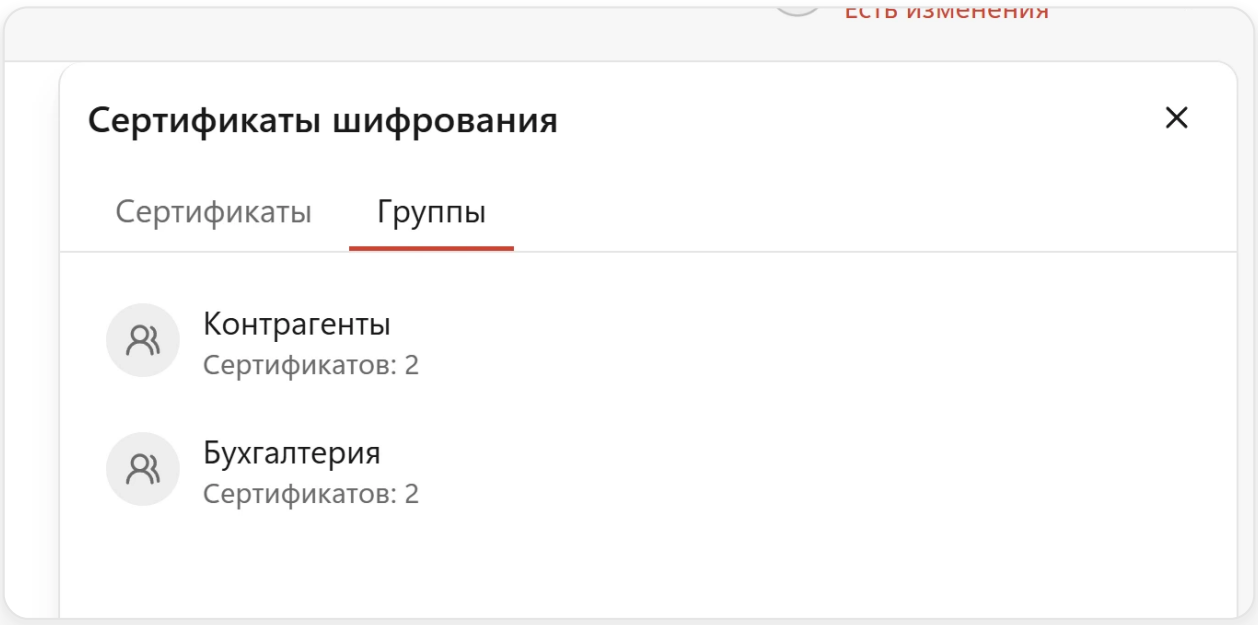
Удаление группы

1. Нажмите кнопку меню в строке группы и выберите **Удалить**.
2. Подтвердите действие.

> 💡 **Примечание**: удаление группы не удаляет сертификаты — исчезает только список.

Шифрование для группы

1. Откройте раздел **«Подпись и шифрование»** и добавьте файлы.
2. В настройках операции включите **Зашифровать**.
3. Нажмите **Добавить сертификаты** и перейдите на вкладку **Группы**.
4. Отметьте нужные группы.



Файл будет зашифрован для всех сертификатов группы. Если в группе окажутся сертификаты, несовместимые с выбранным алгоритмом шифрования, приложение отметит их как **«Не используется»** и предупредит об этом в окне подтверждения.

Группу можно сохранить в профиле подписи — тогда получатели будут подставляться автоматически.

Возможные ошибки

Сообщение	Что это значит	Что сделать
Введите название группы	Название не заполнено	Укажите название и повторите сохранение
Не удалось сохранить группу	Группу не удалось записать в базу данных	Причина записана в журнале

Смотрите также

- Раздел «Сертификаты» — устройство раздела.
- Установка сертификатов — как добавить сертификаты получателей.
- Подпись и шифрование — выполнение операции.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

OpenPGP в КриптоАРМ

OpenPGP — второй стандарт подписи и шифрования, который поддерживает приложение. Он полностью независим от X.509: свои сертификаты, своё хранилище и свой способ понять, можно ли доверять чужому ключу.

В России для юридически значимого документооборота применяется X.509 с алгоритмами ГОСТ. OpenPGP выбирают, когда так принято у корреспондентов — например, при обмене файлами с зарубежными коллегами или внутри технических команд.

Содержание:

- Когда использовать OpenPGP
- Переключение на OpenPGP
- Раздел «Сертификаты»
- Сведения о сертификате
- Достоверность и доверие
- Подключи
- Постквантовые схемы
- Где хранятся ключи
- Смотрите также

Когда использовать OpenPGP

Задача	Что выбрать
Юридически значимый документооборот, обмен с госорганами	X.509 (ГОСТ)
Обмен файлами внутри команды или сообщества, где приняты ключи OpenPGP	OpenPGP
Долговременное шифрование с постквантовыми алгоритмами	OpenPGP

Операции OpenPGP не требуют ни КриптоПро CSP, ни лицензии КриптоАРМ: провайдер встроен в приложение.

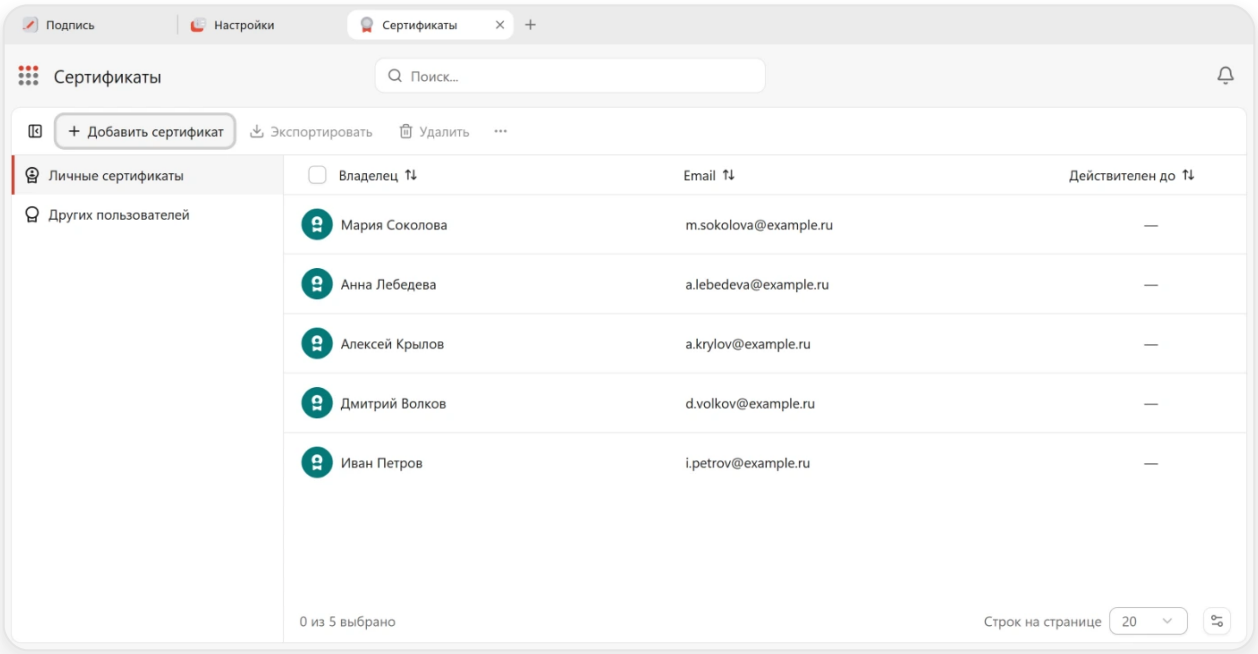
Переключение на OpenPGP

1. Откройте **Настройки → Криптопровайдеры**.
2. В настройке **«Стандарт операций по умолчанию»** выберите **OpenPGP**.

После этого разделы **«Сертификаты»**, **«Подпись и шифрование»** и **«Проверка и расшифрование»** переключатся на OpenPGP.

> 💡 **Примечание**: мастер **«Подпись и защита PDF»** работает только по стандарту X.509 — встроенной подписи PDF в OpenPGP не существует.

Раздел «Сертификаты»



Слева расположены два хранилища и группы:

Хранилище	Содержание
Личные сертификаты	Сертификаты, к которым есть закрытый ключ
Других пользователей	Открытые ключи корреспондентов

По умолчанию в таблице показаны столбцы **Владелец**, **Email**, **Создан**, **Действителен до** и **Идентификатор ключа**. Ещё три — **Достоверность**, **Алгоритм** и **Отпечаток** — скрыты. Включить их можно в списке **Столбцы** — см. Настройка столбцов.

Состояние сертификата показывает цвет значка в столбце **Владелец**: зелёный — действителен, красный — нет. Само состояние — **Действителен**, **Истёк**, **Отозван**, **Скомпрометирован** или **Отключён** — указано в панели сведений.

Сведения о сертификате

Выделите сертификат — панель сведений содержит три вкладки:

Вкладка	Содержание
О сертификате	Блок **Владелец**: имя, email и доверие владельцу. Блок **Сертификат**: даты создания и окончания, статус, достоверность, алгоритм, идентификатор ключа, отпечаток, наличие закрытого ключа, происхождение. Если идентификаторов пользователя несколько — их список с достоверностью каждого
Подключи	Список подключей с их назначением и сроком
Заверения	Кто и как заверил этот сертификат

Происхождение сертификата: **Создан локально**, **Импортирован**, **Внешний источник** или **Мигрирован**.

Отметки **PQ подпись** и **PQ шифрование** означают, что сертификат использует постквантовые схемы.

Достоверность и доверие

В OpenPGP нет удостоверяющих центров — их роль выполняет сеть доверия.

Достоверность отвечает на вопрос «подтверждена ли принадлежность сертификата его владельцу»: **Абсолютная**, **Полная**, **Частичная**, **Недостоверна**, **Не определена**, **Неизвестна**. Её вычисляет приложение — из заверений сертификата и доверия к тем, кто заверил. Она же показывается в результатах проверки подписи.

Доверие владельцу отвечает на вопрос «насколько мы полагаемся на заверения этого владельца»: **Абсолютное**, **Полное**, **Частичное**, **Нет доверия**, **Неизвестно**. Его задаёте вы — см. Доверие владельцу.

Достоверность повышается заверением — см. Заверение сертификата.

> ⚠️ **Важно**: перед заверением обязательно сверьте отпечаток сертификата с владельцем по независимому каналу — например, по телефону. Заверение подтверждает принадлежность ключа человеку, и ошибка здесь обесценивает всю сеть доверия.

Подключи

Сертификат OpenPGP состоит из основного ключа и подключей. Основной ключ отвечает за сертификацию, подключи — за конкретные задачи:

- **Подпись**,
- **Шифрование**,
- **Аутентификация**.

Подключ можно добавить или отозвать, не трогая основной ключ. Если у сертификата несколько подключей подписи, при подписании можно выбрать нужный.

Постквантовые схемы

Обычные алгоритмы шифрования рассчитаны на возможности сегодняшних компьютеров. Постквантовые схемы устроены так, чтобы выдержать и появление квантового компьютера, — их выбирают, когда защищённые данные должны остаться закрытыми через много лет.

В приложении такие схемы гибридные: они соединяют привычный алгоритм с постквантовым, и защита не слабеет, даже если один из двух окажется уязвим. Есть варианты и для подписи (ML-DSA, SLH-DSA), и для шифрования (ML-KEM). Полный перечень показан в разделе **Настройки → Криптопровайдеры → OpenPGP**, выбор схемы — при создании сертификата.

> 💡 **Примечание**: гибридный сертификат шифрует и в адрес обычных ключей — RSA, X25519, X448 и ECDH.

Где хранятся ключи

Сертификаты и закрытые ключи OpenPGP хранит само приложение, а не КриптоПро CSP и не операционная система. Закрытый ключ защищён паролем, который вы задаёте при создании или импорте сертификата.

Поэтому ключи не переносятся вместе с системным хранилищем сертификатов и не восстанавливаются при переустановке. Единственный способ их сохранить — резервная копия.

> ⚠️ **Важно**: восстановить закрытый ключ OpenPGP невозможно: удостоверяющего центра, который выпустит его заново, здесь нет. Сразу после создания ключа сделайте резервную копию.

Смотрите также

- Создание и импорт сертификатов.
- Действия с сертификатами — подключи, заверение, отзыв, смена пароля.
- Экспорт и резервное копирование.
- Подпись и шифрование — операции с файлами.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Создание и импорт сертификатов OpenPGP

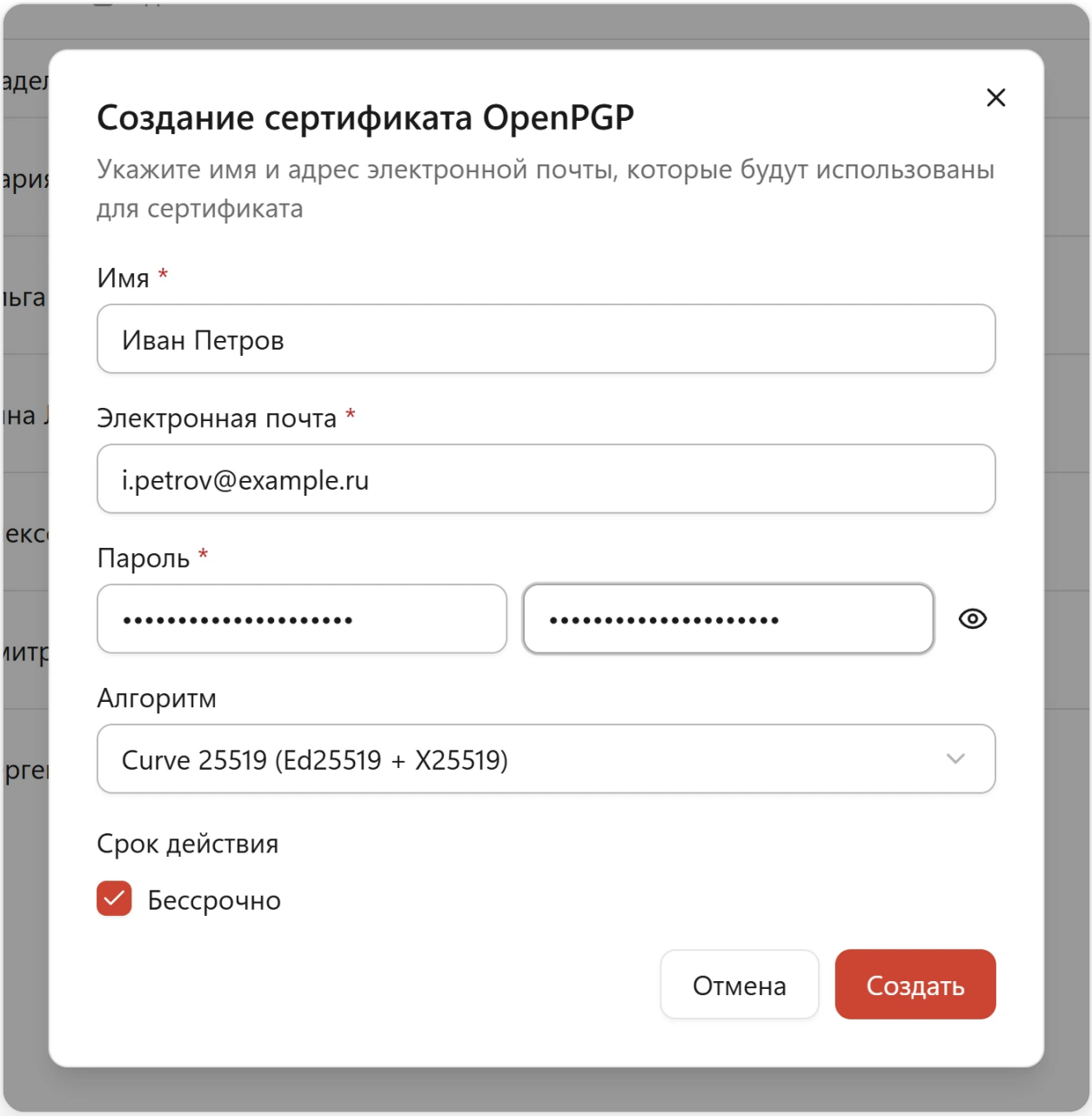
Содержание:

- Создание сертификата
- Выбор алгоритма
- Срок действия и пароль
- Импорт сертификата
- Импорт закрытого ключа
- Восстановление из бумажной копии
- Удаление сертификата
- Возможные ошибки
- Смотрите также

Создание сертификата

1. Убедитесь, что в настройках выбран стандарт операций **OpenPGP**.
2. Откройте раздел **Сертификаты**.
3. Нажмите **Добавить сертификат → Создать новый**.
4. В окне **«Создание сертификата OpenPGP»** заполните:

- **Имя** — например, «Иван Петров»;
- **Электронная почта** — адрес, по которому вас узнают корреспонденты;
- **Алгоритм** — схема ключа;
- **Срок действия** — дата или **Бессрочно**;
- **Пароль** и его подтверждение.



1. Нажмите **Создать**.

Появится сообщение **«Сертификат успешно создан»**, и сертификат появится в разделе **Личные сертификаты**.

> ⚠️ **Важно**: сразу после создания сделайте резервную копию закрытого ключа. Восстановить его иначе невозможно.

Выбор алгоритма

Если вы не знаете, что выбрать, выбирайте **Curve 25519**: современная схема, которую понимают современные программы OpenPGP. **RSA 4096** выбирают ради совместимости со старыми программами. Постквантовые схемы (PQ-гибриды) выбирают по договорённости с корреспондентом: постквантовое шифрование (ML-KEM) GnuPG понимает начиная с версии 2.5, а постквантовой подписи (ML-DSA) в нём пока нет вовсе — ключ с такой подписью он не импортирует.

Алгоритм основного ключа задаётся один раз при создании и потом не меняется. Если позже понадобится другой алгоритм, к сертификату добавляют подключ.

Полный список схем

Схема	Описание
Curve 25519 (Ed25519 + X25519)	Современная схема на эллиптических кривых, компактные ключи и быстрые операции
Curve 448 (Ed448 + X448)	То же с повышенным запасом стойкости
NIST P-256 (ECDSA + ECDH), **NIST P-384 (ECDSA + ECDH)**	Кривые NIST — для систем, где они требуются
Brainpool P-384 (ECDSA + ECDH)	Кривая Brainpool
RSA 4096	Классическая схема, наибольшая совместимость со старыми программами
Curve 25519 + ML-KEM-768 (PQ-гибрид), **Curve 448 + ML-KEM-1024 (PQ-гибрид)**	Обычная подпись, постквантовое шифрование
Brainpool P-256 + ML-KEM-768 (PQ-гибрид), **Brainpool P-384 + ML-KEM-1024 (PQ-гибрид)**	То же на кривых Brainpool
ML-DSA-65/Ed25519 + ML-KEM-768/X25519, **ML-DSA-87/Ed448 + ML-KEM-1024/X448**	Постквантовые и подпись, и шифрование

Кривая Brainpool P-256 доступна только в гибридной схеме с ML-KEM-768: отдельной классической схемы на ней в списке нет.

Срок действия и пароль

Срок действия ограничивает время использования сертификата. Значение **«Бессрочно»** снимает ограничение.

Пароль защищает закрытый ключ. Он запрашивается при подписании, расшифровании, заверении, отзыве и экспорте закрытого ключа.

> ⚠️ **Важно**: пароль восстановить нельзя. Если он утерян, закрытый ключ становится непригоден.

Импорт сертификата

Чтобы проверять подписи корреспондентов и шифровать в их адрес, импортируйте их открытые ключи.

1. Откройте раздел **Сертификаты**.
2. Нажмите **Добавить сертификат → Импортировать из файла**.
3. Выберите файл ключа — обычно `.asc`, `.gpg` или `.pgp`.

Появится сообщение об импорте. Если в файле несколько сертификатов, будет указано их количество.

Пока сертификат не заверен, его достоверность — **Неизвестна**. Сверьте отпечаток ключа с владельцем и заверьте сертификат.

Если импортирован один чужой сертификат, а у вас есть личный сертификат для заверения, приложение сразу спросит **«Заверить импортированный сертификат?»** и покажет отпечаток. **Заверить** открывает окно заверения, **Не сейчас** — закрывает вопрос: заверить сертификат можно и позже. Чтобы вопрос больше не появлялся, отметьте **«Больше не спрашивать»**. При импорте нескольких файлов сразу приложение не спрашивает.

Импорт закрытого ключа

Импортировать можно закрытый ключ, выгруженный из КриптоАРМ, бумажную резервную копию и закрытый ключ в стандартном формате OpenPGP — например, выгруженный из GnuPG.

Если в файле находится закрытый ключ, приложение попросит **пароль закрытого ключа**. Окно называет файл, о котором спрашивает. Если выбрано несколько файлов с закрытыми ключами, пароль запрашивается для каждого по очереди — **«Файл 1 из 2»**, — потому что защищены они могут быть по-разному.

1. Введите пароль, которым защищён ключ в файле, и подтверждение. Если ключ в файле паролем не защищён, задайте новый.
2. Оставьте флажок **«Это мой ключ, им пользуюсь только я»**, если ключ ваш. Снимите его, если ключом пользуется кто-то ещё, — например, это общий ключ отдела.
3. Нажмите **Импортировать**.

Этот же пароль будет защищать ключ в приложении и запрашиваться при операциях с ним. Сменить его можно в действиях сертификата.

Если закрыть окно на втором или следующем файле, уже импортированные ключи останутся в приложении, остальные файлы импортированы не будут.

С флажком сертификат получает **Абсолютное** доверие владельцу и **Абсолютную** достоверность — как сертификат, созданный в приложении. Без флажка доверие остаётся **Неизвестно**, а достоверность — **Неизвестна**, как у чужого сертификата: подписывать и расшифровывать ключом можно, но при проверке его подписей приложение предупредит о недостоверном сертификате. Чтобы сделать такой сертификат достоверным, заверьте его другим своим сертификатом — если он у вас есть, приложение предложит это сразу после импорта.

Восстановление из бумажной копии

Закрытый ключ, распечатанный на бумаге, можно вернуть в приложение: наберите содержимое распечатки в текстовый файл и импортируйте его как обычный файл ключа.

Каждая строка распечатки снабжена контрольной суммой, поэтому опечатка будет обнаружена:

Сообщение	Что это значит	Что сделать
Резервная копия повреждена: ошибка проверки контрольной суммы строки	Ошибка в одной из набранных строк	Сверьте эту строку с распечаткой посимвольно
Резервная копия повреждена: контрольная сумма не сошлась	Ошибка в содержимом копии целиком	Проверьте, все ли строки распечатки набраны и в том же порядке

Удаление сертификата

1. Выделите сертификат в списке или отметьте флажками несколько.
2. Нажмите **Удалить**.
3. Подтвердите действие. Для одного сертификата окно называется **«Удаление сертификата»**, для нескольких в заголовке указано их число. Если открыта группа, окно предупредит, что сертификаты удаляются из хранилища, а не только из группы.

Появится сообщение **«Сертификат удалён»** или с числом удалённых. Если часть сертификатов удалить не удалось, сообщение покажет, сколько удалено из выбранных, а причина отказа будет в журнале.

> ⚠️ **Важно**: вместе с личным сертификатом безвозвратно удаляется закрытый ключ — окно подтверждения предупреждает об этом. Восстановить ключ можно только из резервной копии; без неё расшифровать ранее зашифрованные файлы будет невозможно.

Возможные ошибки

Сообщение	Что это значит	Что сделать
Пароли не совпадают	Пароль и подтверждение введены по-разному	Введите пароль в оба поля заново
В файле нет сертификата или ключа OpenPGP	Выбран файл другого типа или пустой файл	Проверьте, тот ли файл выбран
Не удалось импортировать сертификат	Файл повреждён или закрытый ключ записан в формате, который приложение не читает	Попросите корреспондента прислать ключ заново. Если это ваш закрытый ключ из GnuPG, перевыгрузите его без пароля и задайте пароль при импорте
Алгоритм ключа не поддерживается	Приложение не работает с алгоритмом этого ключа	Попросите владельца создать ключ на одном из алгоритмов, которые предлагает приложение
Формат защиты закрытого ключа не поддерживается. Выгрузите ключ без пароля и импортируйте снова	Ключ в файле защищён схемой, которую приложение не читает	Выгрузите ключ из GnuPG без пароля, а пароль задайте при импорте
Неверный пароль	Пароль не подошёл к ключу в файле	Введите пароль, которым ключ защищён в GnuPG
Не удалось создать сертификат	Операция прервалась	Причина записана в журнале

Смотрите также

- О разделе OpenPGP — устройство раздела.
- Действия с сертификатами — подключи, заверение, отзыв.
- Экспорт и резервное копирование.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Действия с сертификатами OpenPGP

Содержание:

- Добавление подключа
- Заверение сертификата
- Просмотр заверений
- Доверие владельцу
- Отзыв сертификата
- Отзыв подключа
- Смена пароля закрытого ключа
- Группы сертификатов
- Возможные ошибки
- Смотрите также

Добавление подключа

Подключ выделяет отдельную ключевую пару под конкретную задачу. Его можно отозвать, не отзывая сертификат целиком.

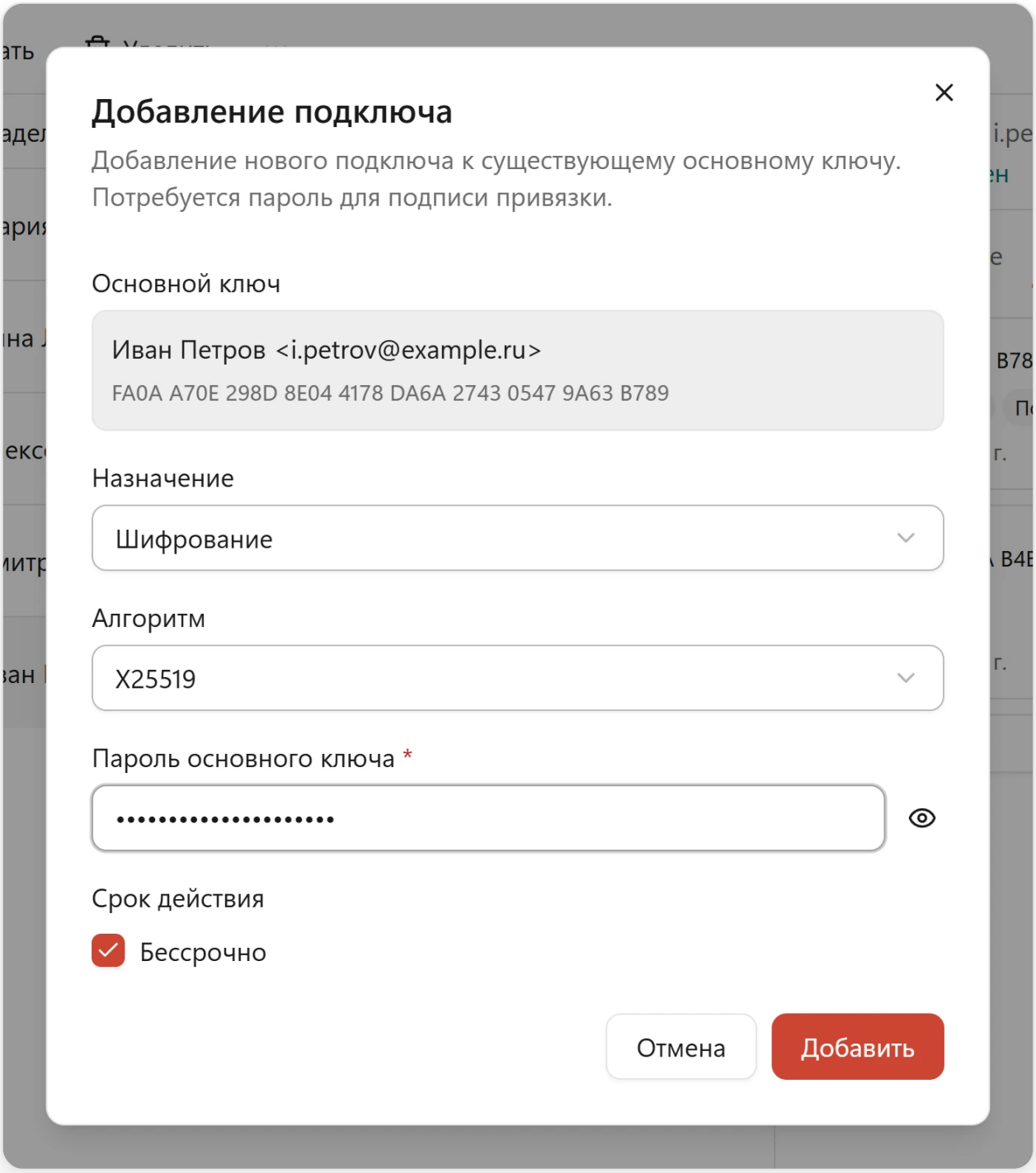
1. Выделите личный сертификат.
2. В панели сведений перейдите на вкладку **Подключи** и нажмите **Добавить подключ**.
3. В окне **«Добавление подключа»** укажите:

- **Назначение** — «Шифрование», «Подпись» или «Аутентификация»;
- **Алгоритм** — набор зависит от назначения:

Назначение	Доступные алгоритмы
Шифрование	RSA 4096, X25519, X448, ECDH secp256r1, ECDH secp384r1, ECDH brainpoolP384, а также гибриды ML-KEM-768 + X25519, ML-KEM-1024 + X448, ML-KEM-768 + brainpoolP256, ML-KEM-1024 + brainpoolP384
Подпись	Ed25519, Ed448, RSA 4096, ECDSA brainpoolP256, ECDSA brainpoolP384, ECDSA secp256r1, ECDSA secp384r1, ML-DSA-65 + Ed25519, ML-DSA-87 + Ed448, SLH-DSA-SHAKE-128s, SLH-DSA-SHAKE-128f, SLH-DSA-SHAKE-256s
Аутентификация	Ed25519, Ed448, RSA 4096, ML-DSA-65 + Ed25519, ML-DSA-87 + Ed448

- **Срок действия** — дата или **Бессрочно**;

- **Пароль основного ключа**.



1. Нажмите **Добавить**.

Появится сообщение **«Подключ добавлен»**.

> 💡 **Примечание**: если у сертификата несколько активных подключей подписи, при подписании файлов можно выбрать нужный — поле **«Подключ для подписи»** в настройках операции.

Заверение сертификата

Заверение — подпись, которой вы подтверждаете, что сертификат действительно принадлежит своему владельцу. Из заверений складывается сеть доверия.

1. Выделите сертификат другого пользователя.
2. Нажмите **Заверить сертификат** — в меню ··· или на вкладке **Заверения**. Сразу после импорта одного сертификата это окно можно открыть и из вопроса **«Заверить импортированный сертификат?»**.
3. В открывшемся окне:

- сверьте **Отпечаток** с владельцем сертификата по независимому каналу;
- отметьте **идентификаторы пользователя**, которые заверяете, — отозванные идентификаторы в списке не показываются;
- выберите сертификат в поле **Заверить сертификатом** — если личный сертификат один, он уже выбран;
- введите **пароль** закрытого ключа.

1. Нажмите **Заверить**.

Появится сообщение **«Сертификат успешно заверен»**. Если у сертификата, которым вы заверяли, **Абсолютное** доверие владельцу, заверенный сертификат становится достоверным (**Полная**). Доверие владельцу заверенного сертификата при этом не меняется и остаётся **Неизвестно**: заверение подтверждает, чей это ключ, но не говорит, насколько вы полагаетесь на заверения его владельца.

Заверение попадает в экспортируемый открытый ключ и видно тем, кому вы его передадите.

> ⚠️ **Важно**: заверение — публичное утверждение о принадлежности ключа. Не заверяйте сертификат, пока не сверили отпечаток с его владельцем.

Просмотр заверений

Вкладка **Заверения** в панели сведений показывает, кто заверил сертификат. Локальные заверения помечены как **«Локальное»**, неизвестные заверители — как **«Неизвестный заверитель»**.

Если заверений нет, вкладка показывает **«Нет заверений»**.

Доверие владельцу

Заверение отвечает на вопрос «принадлежит ли сертификат владельцу». Доверие владельцу — на другой: насколько вы полагаетесь на заверения, которые этот человек делает для чужих сертификатов. Из обоих складывается достоверность сертификатов.

1. Выделите сертификат.
2. Откройте меню ··· и выберите **Доверие владельцу** — или нажмите значок карандаша рядом с полем **Доверие владельцу** на вкладке **О сертификате**.
3. Выберите уровень и нажмите **Сохранить**.

Уровень	Что значит
Неизвестно	Решение не принято — заверения владельца не учитываются
Нет доверия	Заверения владельца не учитываются
Частичное	Одного заверения владельца мало: нужно несколько заверений с частичным доверием
Полное	Одного заверения владельца достаточно, чтобы сертификат стал достоверным
Абсолютное	Только для ваших ключей: заверения владельца равны вашим собственным

После сохранения приложение пересчитывает достоверность всех сертификатов: изменение доверия к одному владельцу меняет достоверность сертификатов, которые он заверил. Доверие хранится только в приложении на этом компьютере и в экспортируемые ключи не попадает — корреспонденты его не видят.

Прежде чем доверять заверениям владельца, заверьте его сертификат: полагаться на заверения имеет смысл, только если вы уверены, что ключ принадлежит этому человеку. Если сертификат ещё не достоверен, окно предупредит об этом.

Доверие к собственным ключам

Абсолютное доверие приложение задаёт само — сертификатам, созданным в приложении, и импортированным с закрытым ключом, если при импорте оставлен флажок **«Это мой ключ, им пользуюсь только я»**. Чужим сертификатам его не выставляйте: всё, что заверит их владелец, станет для вас достоверным. Если у сертификата нет закрытого ключа, окно предупредит об этом.

Доверие к собственному ключу можно понизить — например, если это общий ключ отдела или старый ключ, который вы больше не используете. Учтите последствия: заверения этого ключа перестанут учитываться, поэтому и сертификаты, которые вы им заверили, и сам этот сертификат потеряют достоверность. Окно предупредит об этом перед сохранением.

Достоверность идентификаторов пользователя

Достоверность считается для каждого идентификатора пользователя отдельно. Если их у сертификата несколько, на вкладке **О сертификате** у каждого показана своя достоверность — например, один адрес может быть заверен, а другой нет.

Отзыв сертификата

Отзыв помечает сертификат как недействительный. Запись об отзыве попадает в экспортируемый открытый ключ, поэтому корреспонденты узнают, что ключ больше использовать не следует.

1. Выделите личный сертификат.
2. Нажмите **Отозвать сертификат**.
3. Укажите:

- **Причину отзыва** — «Скомпрометирован», «Больше не используется», «Заменён новым», «Идентификатор пользователя недействителен» или «Причина не указана»;
- **Описание** — при необходимости пояснение в свободной форме;
- **пароль** закрытого ключа.

1. Нажмите **Отозвать сертификат**.

> ⚠️ **Важно**: отзыв необратим. После отзыва экспортируйте открытый ключ и передайте его корреспондентам — иначе они не узнают об отзыве.

Отзыв подключа

Если скомпрометирован только подключ, отзовите его отдельно:

1. Откройте вкладку **Подключи** в панели сведений.
2. Выберите подключ и нажмите **Отозвать подключ**.
3. Введите пароль закрытого ключа и подтвердите операцию.

Появится сообщение **«Подключ отозван»**. Остальные подключи и основной ключ продолжат работать, а запись об отзыве попадёт в экспортируемый открытый ключ.

Смена пароля закрытого ключа

1. Выделите личный сертификат.
2. Нажмите **Сменить пароль**.

3. Введите текущий пароль, новый пароль и его подтверждение.
4. Нажмите **Изменить**.

Появится сообщение **«Пароль успешно изменён»**.

> 💡 **Примечание**: смена пароля не изменяет сам ключ — корреспондентам ничего пересылать не нужно. Уже сделанные резервные копии она не затрагивает: паролем они не защищены, и сохранённым в них ключом можно пользоваться и после смены пароля.

Группы сертификатов

Сертификаты OpenPGP объединяются в группы так же, как X.509 — см. Группы сертификатов. Группы OpenPGP видны только при стандарте операций OpenPGP.

Возможные ошибки

Сообщение	Что это значит	Что сделать
Нет личных сертификатов для заверения	Заверять чужой ключ нужно своим, а его нет	Создайте свой сертификат OpenPGP
Не удалось добавить подключ	Неверный пароль основного ключа или сбой операции	Проверьте пароль и повторите
Не удалось отозвать сертификат	Неверный пароль или сбой операции	Проверьте пароль и повторите
Пароли не совпадают	Новый пароль и подтверждение введены по-разному	Введите пароль в оба поля заново
Не удалось изменить доверие владельцу	Сбой записи в хранилище	Повторите; причина записана в журнале

Подробности — в журнале.

Смотрите также

- О разделе OpenPGP — достоверность и доверие.
- Экспорт и резервное копирование — передача открытого ключа корреспондентам.
- Подпись и шифрование.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Экспорт и резервное копирование ключей OpenPGP

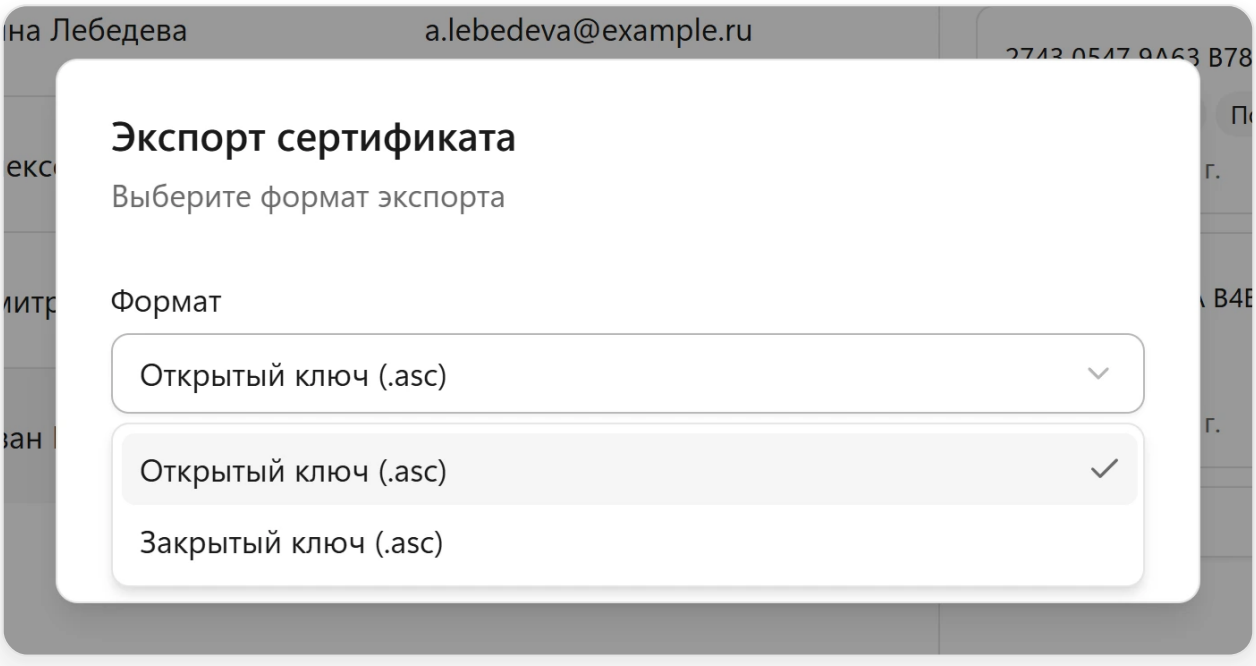
Открытый ключ передают корреспондентам, закрытый — хранят в резервной копии. Восстановить закрытый ключ OpenPGP невозможно, поэтому копия обязательна.

Содержание:

- Экспорт открытого ключа
- Экспорт закрытого ключа
- Групповой экспорт
- Печать закрытого ключа
- Как хранить резервную копию
- Возможные ошибки
- Смотрите также

Экспорт открытого ключа

1. Выделите сертификат в списке.
2. Нажмите **Экспортировать**.
3. В поле **Формат** выберите **Открытый ключ (.asc)**.
4. Нажмите **Экспортировать** и укажите, куда сохранить файл.



Полученный файл можно передавать свободно: он не содержит закрытого ключа. Корреспондент импортирует его и сможет проверять ваши подписи и шифровать файлы в ваш адрес.

> 💡 **Примечание**: после отзыва сертификата экспортируйте открытый ключ заново и разошлите его — запись об отзыве передаётся именно так.

Экспорт закрытого ключа

1. Выделите личный сертификат.
2. Нажмите **Экспортировать**.
3. В поле **Формат** выберите **Закрытый ключ (.asc)**.
4. Введите **пароль** закрытого ключа.
5. Нажмите **Экспортировать** и укажите, куда сохранить файл.

Файл сохраняется в собственном формате приложения — он подходит для резервной копии и переноса ключа в другую установку КриптоАРМ, но сторонние программы OpenPGP его не прочитают. Открытый ключ, наоборот, выгружается в обычном формате OpenPGP и понятен любой программе.

> ⚠️ **Важно**: закрытый ключ записывается в файл без защиты паролем — пароль нужен только чтобы извлечь ключ из приложения. Любой, у кого окажется файл, сможет подписывать документы от вашего имени и читать зашифрованную для вас переписку. Храните такой файл на защищённом носителе и не передавайте по открытым каналам.

Групповой экспорт

1. Выделите несколько сертификатов.
2. Нажмите **Экспортировать**.
3. Подтвердите операцию — приложение сообщит, сколько сертификатов будет экспортировано.
4. Выберите папку для сохранения.

По завершении появится сообщение с числом экспортированных сертификатов. Если часть экспортировать не удалось, будет показано количество ошибок.

Печать закрытого ключа

Бумажная копия — способ сохранить закрытый ключ вне компьютера: её не затронут ни сбой диска, ни вредоносная программа.

1. Выделите личный сертификат.
2. Нажмите **Печать закрытого ключа**.
3. Введите **пароль** закрытого ключа.
4. Отправьте документ **«Резервная копия закрытого ключа»** на печать.

Каждая строка распечатки снабжена контрольной суммой, поэтому при вводе копии обратно ошибка будет обнаружена — см. Восстановление из бумажной копии.

> ⚠️ **Важно**: закрытый ключ печатается без защиты паролем — воспользоваться им сможет любой, кто получит распечатку. Храните её так же, как хранили бы печать организации или доступ к сейфу.

Как хранить резервную копию

- храните копию отдельно от рабочего компьютера;
- копия паролем не защищена, поэтому доступ к ней должен быть только у вас: смена пароля в приложении уже сделанные копии не затрагивает;
- проверьте копию сразу после создания: импортируйте её на другом рабочем месте или сверьте отпечаток.

Возможные ошибки

Сообщение	Что это значит	Что сделать
Неверный пароль в окне экспорта	Пароль закрытого ключа не подошёл	Введите пароль заново — окно остаётся открытым
Не удалось экспортировать сертификат	Сбой доступа к хранилищу или записи файла	Повторите; причина записана в журнале
Не удалось экспортировать сертификаты	Групповой экспорт не выполнен целиком	Повторите экспорт; при повторении выгружайте сертификаты по одному
Экспортировано N из M, ошибок: K	Часть сертификатов выгрузить не удалось	Выгрузите оставшиеся по одному — так видно, на каком возникает ошибка
		Проверьте пароль и повторите

Сообщение	Что это значит	Что сделать
Не удалось подготовить резервную копию закрытого ключа к печати	Неверный пароль или сбой операции	

Смотрите также

- Создание и импорт сертификатов — восстановление ключа из копии.
- Действия с сертификатами — отзыв и смена пароля.
- О разделе OpenPGP — где хранятся ключи.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Описание и возможности API КриптоАРМ

API КриптоАРМ позволяет встроить подпись, шифрование и работу с сертификатами в веб-сервис или в локальное приложение. Приложение получает параметры вызова, открывает обычный экран операции, выполняет её после действия пользователя и возвращает результат вызывающей стороне.

Это руководство описывает протокол `cryptoarm://`, доступные команды, форматы запросов и ответов и сценарии интеграции.

Содержание:

- Общая информация
- Доступные команды
- Сценарий вызова из веб-приложения
- Сценарий вызова из локального приложения
- Формат ссылки для сетевого вызова
- Формат ссылки для локального вызова
- Кодирование ссылки
- Аутентификация
- Описание запросов и ответов
- Смотрите также

Общая информация

Для взаимодействия используется зарегистрированный протокол `cryptoarm://`. Ссылку можно разместить на веб-странице, открыть из адресной строки браузера или передать из терминала.

Возможны две точки вызова:

- **сетевой вызов** — параметры операции приложение запрашивает у сервиса по HTTPS, результат отправляет ему же;
- **локальный вызов** — параметры приходят прямо в ссылке или в файле на этом же компьютере, результат сохраняется в указанный каталог.

API работает с сертификатами X.509. Операции OpenPGP через него недоступны — для их автоматизации используйте командную строку.

> 📌 **Примечание**: криптографические операции требуют действующей лицензии на КриптоАРМ. Временную лицензию на одну операцию можно передать в параметре `props.license`.

Доступные команды

Команда	Описание
`signAndEncrypt`	Подпись, архивирование, шифрование, проверка подписи, расшифрование, снятие подписи
`certificates`	Импорт и экспорт сертификатов, просмотр сведений о сертификате
`certrequests`	Создание запроса на сертификат (PKCS#10)
`diagnostics`	Сведения о рабочем месте: система, провайдеры, лицензии, личные сертификаты
`startView`	Открытие раздела приложения

Имя команды в ссылке нечувствительно к регистру.

Сценарий вызова из веб-приложения

1. **Инициация операции.** Пользователь выбирает на портале документы и действие — например, подпись.
2. **Формирование ссылки.** Портал отображает ссылку `cryptoarm://` с идентификатором транзакции или перенаправляет на неё браузер.
3. **Запуск приложения.** Система запускает КриптоАРМ, если он ещё не запущен, и передаёт ему ссылку.
4. **Проверка сервиса.** При первом обращении с этого адреса приложение показывает сертификат сервиса и запрашивает разрешение — см. Запрос от сетевого сервиса.
5. **Запрос параметров.** Приложение сообщает сервису о получении вызова уведомлением `<команда>.callback` и отправляет на указанный адрес JSON-RPC запрос `<команда>.parameters`, чтобы получить параметры операции.
6. **Подготовка операции.** Приложение загружает нужные файлы и открывает экран операции с переданными настройками.
7. **Подтверждение пользователем.** Пользователь проверяет, что именно запрошено, и запускает операцию.
8. **Отправка результата.** Результат уходит на адрес из `props.uploader` — в JSON или в `multipart/form-data`. Без этого адреса результат остаётся у пользователя.

Сценарий вызова из локального приложения

1. **Инициация операции.** Пользователь выбирает файлы и действие в стороннем приложении.
2. **Формирование запроса.** Приложение готовит JSON-RPC объект с параметрами и открывает ссылку `cryptoarm://` со встроенным JSON либо со ссылкой на файл параметров.
3. **Запуск приложения.** Система запускает КриптоАРМ, если он ещё не запущен.
4. **Разрешение вызова.** Приложение показывает окно «Разрешить локальный API-вызов?».
5. **Подтверждение пользователем.** Пользователь проверяет параметры операции и запускает её.
6. **Сохранение результата.** Результат сохраняется в каталог, указанный в параметрах операции.

Формат ссылки для сетевого вызова

```
cryptoarm://<command>/<URL>?id=<id>
```

- `cryptoarm://` — зарегистрированный протокол;
- `<command>` — выполняемая команда;
- `<URL>` — адрес, по которому приложение запросит параметры операции и на который отправит результат;
- `id=<id>` — обязательный параметр. Идентификатор транзакции.

Пример сетевого вызова:

```
cryptoarm://signAndEncrypt/https://api.example.ru/cryptoarm/json?id=tx-42
```

Требования к адресу:

- только HTTPS: незащищённые соединения приложение отклоняет;
- ровно один непустой параметр `id`;
- имя пользователя и пароль в адресе не допускаются.

Формат ссылки для локального вызова

Вариант 1 — JSON в ссылке:

```
cryptoarm://<command>/<JSON>
```

Конверт приложение отличает от адреса по первому символу: значение, начинающееся с `{`, читается как JSON. Порядок ключей внутри конверта не важен. Объём встроенного JSON ограничен 64 МиБ. Состав `result` зависит от команды и описан на её странице.

```
cryptoarm://startView/{"jsonrpc":"2.0","id":"tx-42","result":{"uiView":"SIGN_AND_ENCRYPT"}}
```

Вариант 2 — файл параметров:

```
cryptoarm://<command>/file:///C:/work/request.json
```

Путь к файлу указывается в форме `file://`; сетевые узлы в таком адресе не поддерживаются. Входные файлы локального вызова задаются через `file://` или обычным абсолютным путём.

Дополнительные поля конверта в ссылке:

Ключ	Тип	Описание
`appName`	string	Необязательное поле. Название приложения, которое будет показано в окне разрешения.
`apiKey`	string	Необязательное поле. Проверочный код, который будет показан в окне разрешения.

Приложение показывает эти значения пользователю, но не проверяет их: решение принимает пользователь. Оба поля читаются только из конверта в ссылке: для варианта 2 разрешение запрашивается до чтения файла параметров, поэтому в окне показывается путь к файлу.

> ⚠️ **Важно**: сетевой вызов не может записать результат в локальный путь. Каталог результата задаётся только для локального вызова.

Кодирование ссылки

Хвост ссылки — адрес или JSON — передаётся либо как есть, либо целиком в процентной кодировке (`encodeURIComponent`). Приложение принимает оба вида:

```
cryptoarm://signAndEncrypt/https://api.example.ru/cryptoarm/json?id=tx-42
cryptoarm://signAndEncrypt/https%3A%2F%2Fapi.example.ru%2Fcryptoarm%2Fjson%3Fid%3Dtx-42
```

Откуда вызов	Как передавать
Ссылка на веб-странице	В процентной кодировке: браузер не примет кавычки и фигурные скобки
Командная строка, своё приложение	Как есть, взяв ссылку целиком в кавычки

В командной строке кавычки обязательны: без них пробелы и & разорвут ссылку на несколько аргументов, и приложение получит только её начало.

Аутентификация

Подлинность сервиса подтверждается сертификатом ресурса, который пользователь видит и принимает при первом обращении, и проверкой этого сертификата при каждом запросе. Подробности — в разделе Транспорт и доверие. Аутентификация пользователя — отдельный механизм, и включает её сам сервис.

`authType=oidc`

Сервису, которому нужен вошедший пользователь, достаточно добавить в ссылку `authType=oidc`:

```
cryptoarm://signAndEncrypt/https://api.example.ru/cryptoarm/json?id=tx-42&authType=oidc
```

Дальше приложение:

1. запрашивает у сервиса параметры входа — `{"jsonrpc": "2.0", "method": "authorization.parameters", "id": "<id>"}`;
2. ожидает в ответе `params.authorizationParams` с полями `issuer` и `clientId` (необязательный массив `scopes` или строка `scope` через пробел, по умолчанию `openid offline_access`), `params.nextUrl` и необязательный `params.customAuth`;
3. выполняет вход в указанный провайдер: Authorization Code с PKCE, системный браузер, возврат на `cryptoarm://callback/`. Вход принадлежит сетевому профилю этого же ресурса: если профиля ещё нет, он создаётся по `authorizationParams`, а серверы лицензий и документов берутся из `/.well-known/service-resources` ресурса, когда тот их публикует; уже выполненный вход используется повторно и продлевается по refresh-токену без вопросов к пользователю;
4. повторяет исходную команду по адресу `nextUrl`, добавляя токен в заголовок. Токен — `id_token` провайдера, не `access_token`: сервис проверяет его подпись по JWKS провайдера.

Если сервис отвечает `401` на запрос с токеном, приложение считает токен отозванным: профиль переходит в состояние «требуется вход», пользователь входит заново, и команда повторяется один раз с новым токеном. Второй `401` — уже отказ вызова. `403` входом не лечится и повторов не вызывает.

`nextUrl` обязан оставаться на том же origin, что и исходный вызов: токен не уходит на другой хост. `customAuth` задаёт только имя заголовка и схему (`{"in": "header", "headerName": "Authorization", "scheme": "bearer"}` — значения по умолчанию; вместо `headerName` принимается и `key`). Передача токена в query или в теле запроса не поддерживается. Тот же заголовок добавляется к загрузке входных файлов и к отправке результата, если они идут на этот же origin.

Другие значения `authType` — включая `mtls` и `oidc:mtls` — отклоняются ещё при разборе ссылки, до подтверждения доверия к сервису: приложение не обращается к нему, сообщения об ошибке сервис не получает, а код `UNSUPPORTED_AUTH_TYPE` остаётся только в лог-файле. Локальный вызов (JSON или файл параметров) с `authType` отклоняется так же: аутентифицироваться там не к кому.

Токен доступа к файлам

Токен доступа к файлам передаётся в `extra.token` команды `signAndEncrypt` и добавляется только к загрузке с адреса исходного вызова.

Описание запросов и ответов

Все запросы между приложением и сервисом соответствуют спецификации **JSON-RPC 2.0**. Транспорт — HTTP поверх TLS.

POST-запрос

Приложение выполняет POST-запросы с заголовками:

- `Content-Type: application/json; charset=utf-8`;
- `Content-Length` — длина тела запроса;
- `Accept: application/json`.

GET-запрос

GET-запросы используются для загрузки файлов — например, документов для подписи. Своих заголовков приложение к ним не добавляет; токен доступа передаётся параметром `accessToken` в адресе файла.

Перенаправления выполняются в пределах серверов с тем же ключом — см. Адреса файлов и токен.

Запрос параметров

Ключ	Значение	Описание
`jsonrpc`	`2.0`	Версия протокола JSON-RPC. Всегда `2.0`.
`method`	`<команда>.parameters`	Имя метода — например, `signAndEncrypt.parameters`.
`id`	Идентификатор транзакции	Значение параметра `id` из ссылки.
`diagnostic`	Сведения о рабочем месте	

Ключ	Значение	Описание
		Поля `VERSIONS`, `PROVIDERS` и `LICENSES` — см. `diagnostics`.

Для самой команды `diagnostics` поле `diagnostic` — пустой объект: сведения о рабочем месте не передаются до того, как пользователь разрешит операцию.

Ответ с параметрами

В теле ответа сервис возвращает конверт JSON-RPC. Заголовки ответа приложение не проверяет и разбирает тело как JSON:

Ключ	Значение	Описание
`jsonrpc`	`2.0`	Версия протокола JSON-RPC. Всегда `2.0`.
`result`	Параметры операции	Состав зависит от команды.
`id`	Идентификатор транзакции	Совпадает с `id` из ссылки.

Правила разбора конверта:

- параметры берутся из `result`; `params` принимается для совместимости, если `result` нет;
- `jsonrpc` равен `"2.0"`; `id` совпадает с идентификатором из ссылки, `id` другой транзакции отклоняется;
- объект в `error` — ответ с ошибкой;
- поле со значением `null` на любой глубине считается отсутствующим;
- пакетные (batch) запросы и скалярные значения вместо объекта не принимаются;
- неизвестные значения перечислимых полей и недопустимые сочетания операций отклоняются, а не заменяются значениями по умолчанию.

Объект Error

Если параметры выдать нельзя, сервис отвечает объектом ошибки:

Ключ	Тип	Описание
`code`	number	Код ошибки
`message`	string	Короткое описание ошибки
`data`	string/Object	Необязательное поле с дополнительными сведениями

Ответ на результат

Результат операции приложение отправляет как уведомление JSON-RPC. Сервис может ответить любым кодом `2xx`, включая `204 No Content`; тело ответа не требуется.

HTTP-коды

Код	Ошибка	Описание
200	OK	Успешный ответ и ответ с объектом ошибки
204	No Content	Для уведомлений без тела ответа
405	Method Not Allowed	Метод недоступен
415	Unsupported Media Type	`Content-Type` не `application/json`

Смотрите также

- Приложение и пользователь — окна согласия на стороне пользователя.
- Транспорт и доверие — HTTPS, доверенные сервисы, локальный вызов.
- Лимиты, статусы и ошибки — ограничения и завершение операции.
- Выполнение операций в командной строке — другой способ автоматизации.

Открыть статью на сайте

Приложение и пользователь

Операция по ссылке `cryptoarm://` выполняется на рабочем месте пользователя и от его имени. Поэтому приложение открывает обычный экран операции, показывает, что именно запрошено, и выполняет операцию только после подтверждения.

Эта статья описывает интерфейс со стороны пользователя: что показано в окнах согласия и как отозвать доступ, который больше не нужен.

Содержание:

- Запрос от сетевого сервиса
- Запрос от локального приложения
- Подтверждение операции
- Разрешение на диагностику
- Доверенные сервисы
- Фоновые разрешения
- Отзыв доверия
- Смотрите также

Запрос от сетевого сервиса

При первом обращении сервиса открывается окно **«Доступ к приложению КриптоАРМ»**.

В нём показаны:

Сведения	Что означают
Сервис	Адрес обратившегося ресурса
Сертификат ресурса	Владелец, издатель, серийный номер, срок действия, отпечаток SHA-256
Состав цепочки сертификации	Цепочка сертификата сервиса

Сертификат сервиса приложение дополнительно проверяет по своему хранилищу сертификатов и показывает результат двумя строками: **«Соединение защищено»** и **«Сертификат ресурса действителен»** либо **«Соединение не защищено»** и **«Сертификат ресурса недействителен»**. Обе строки отражают одну и ту же проверку сертификата: данные в любом случае передаются по HTTPS.

> ⚠️ **Важно**: разрешайте доступ только тем сервисам, которым доверяете. Сверьте адрес и отпечаток сертификата с тем, что сообщает сама организация. Если приложение показывает **«Сертификат ресурса недействителен»**, не разрешайте доступ.

Если сертификат ранее известного сервиса изменился, появится предупреждение **«Сертификат этого сервиса изменился. Проверьте новый отпечаток перед подтверждением доверия.»**

Нажмите **Сохранить**, чтобы разрешить доступ. Настройки ресурса сохранятся в профиле внешнего сервиса — см. Доверенные сервисы.

Запрос от локального приложения

Локальный вызов открывает окно **«Разрешить локальный API-вызов?»**. В нём показаны **«Приложение»** и **«Проверочный код»**, если вызывающая сторона передала их в конверте ссылки, а для вызова с файлом параметров — путь к нему в поле **«Файл параметров»**. Приложение не проверяет эти значения и не определяет, какая программа открыла ссылку: они помогают опознать вызов, но не подтверждают его источник.

Доступные решения:

- **Разрешить один раз** — только для текущего вызова;
- **Разрешить локальные вызовы до выхода** — до завершения работы приложения и для всех локальных вызовов, а не только для этой программы.

Разрешение локальных вызовов не сохраняется между запусками.

> ⚠️ **Важно**: разрешение «до выхода» не привязано к вызывающей программе. Пока приложение не закрыто, любой следующий локальный вызов — от другой программы или по ссылке, открытой в браузере, — выполняется без запроса. Выбирайте его только для серии вызовов подряд; в остальных случаях надёжнее **Разрешить один раз**.

Подтверждение операции

Перед выполнением открывается окно **«Подтвердите операцию»**. В нём показаны:

- **Команда** и **Действия** — что именно будет сделано;
- **Файлы** и их источник, для отсоединённой подписи — исходный файл;
- **Личный сертификат** — которым выполняется операция; если сервис его не задал, сертификат выбирает пользователь;

- **Параметры операции** — стандарт подписи, тип подписи, кодировки, алгоритм шифрования, подпись PAdES и видимый штамп, формат передачи результата;
- **Сетевые службы операции** — адреса службы штампов времени и службы проверки статуса сертификата, к которым обратится приложение;
- **Назначение результата** — куда будет передан результат.

Нажмите **Выполнить операцию**, чтобы запустить её, или **Отмена**, чтобы отказаться.

Параметры, которые сервис задал явно, показаны без возможности изменения; остальные пользователь может изменить перед запуском.

> 💡 **Совет**: перед подписанием откройте файлы и убедитесь, что на подпись отправлены нужные документы.

Разрешение на диагностику

Запрос сведений о рабочем месте открывает окно **«Диагностика рабочего места»**. В блоке **«Запрашиваемые сведения»** перечислено, что именно запросил сервис: сведения о системе, версии КриптоАРМ, КриптоПро CSP и OpenSSL, доступность провайдеров, сведения о лицензиях, сведения о личных сертификатах.

Нажмите **Разрешить** или **Отклонить**. Для сетевого сервиса в этом окне можно включить **«Разрешить проведение диагностики приложения в фоновом режиме»** — тогда последующие запросы диагностики от этого сервиса будут выполняться без подтверждения.

Доверенные сервисы

Сервисы, которым вы разрешили доступ, сохраняются как профили внешних сервисов. Их список находится в разделе **«Подпись и шифрование»** в панели профилей — под списком профилей подписи, в группе **«Доверенные сервисы»**.

Щелчок по записи открывает вкладку **«Профиль внешнего сервиса»** с двумя вкладками:

Вкладка	Содержание
Настройки профиля	Параметры подписи и шифрования, с которыми выполняются операции этого сервиса
Параметры ресурса	Адрес ресурса, статус соединения, сертификат ресурса и его цепочка, фоновые разрешения

Для каждого сервиса создаётся отдельный профиль подписи. Операции этого сервиса выполняются по нему, а не по профилю, с которым работал пользователь в последний раз.

Фоновые разрешения

Два действия сервис может выполнять без подтверждения, если это разрешено явно:

Разрешение	Что позволяет
Фоновая диагностика	Получать сведения о рабочем месте: провайдеры, версии, лицензии
Фоновая проверка подписи	Проверять подписи без запроса подтверждения

Оба разрешения выключены по умолчанию. Включить их можно в окне согласия в блоке **«Дополнительно»** или позже — на вкладке **«Параметры ресурса»** профиля внешнего сервиса.

> ⚠️ **Важно**: фоновая диагностика действует, пока вы не выключите её на вкладке **«Параметры ресурса»** или не удалите профиль сервиса. Пока она включена, сервис без запроса получает при каждом обращении те сведения, которые запросит, — вплоть до состава рабочего места и данных обо всех личных сертификатах: владельца, организации, криптопровайдера, сроков действия и наличия закрытого ключа. Полный перечень — в разделе Сведения о личных сертификатах.

Подпись, шифрование, расшифрование, снятие подписи, импорт и экспорт сертификатов и создание запроса всегда требуют подтверждения.

Отзыв доверия

1. Откройте панель профилей в разделе **«Подпись и шифрование»**.
2. В группе **«Доверенные сервисы»** найдите нужный сервис.
3. Удалите запись и подтвердите действие в окне **«Удаление профиля внешнего сервиса»**.

Появится сообщение **«Профиль внешнего сервиса „...“ удалён»**. Вместе с профилем удаляются сохранённый сертификат сервиса и его настройки: при следующем обращении сервис снова должен будет получить разрешение.

Смотрите также

- Описание и возможности API — команды и форматы вызова.
- Транспорт и доверие — как проверяется сертификат сервиса.
- Профили подписи — где хранятся профили.
- Общие настройки — остальные настройки приложения.

Открыть статью на сайте

Транспорт и доверие

Приложение выступает HTTP-клиентом: оно само обращается к сервису за параметрами и само отправляет результат. Локального сервера, принимающего входящие соединения, у него нет.

Содержание:

- Сетевой вызов
- Доверенный сервис
- Профиль сервиса и настройки операции
- Адреса файлов и токен
- Локальный вызов
- Подтверждение пользователем
- Смотрите также

Сетевой вызов

Формат ссылки:

```
cryptoarm://<command>/<https-url>
```

Адрес должен содержать ровно один непустой параметр `id` — идентификатор всей транзакции. Он используется в запросе параметров, в ответе сервиса и в результате операции.

```
cryptoarm://diagnostics/https://api.example.ru/cryptoarm/json?id=tx-42
```

После подтверждения доверия приложение сообщает сервису, что вызов получен:

```
{
  "jsonrpc": "2.0",
  "method": "diagnostics.callback",
  "id": "tx-42",
  "params": {
    "status": "Received",
    "VERSIONS": { "cryptoarm": "7.0.0" }
  }
}
```

Имя команды в методе записывается в нижнем регистре — например, `signandencrypt.callback`. Ответ на уведомление не требуется, и его доставка на выполнение команды не влияет.

Одновременно приложение отправляет запрос параметров:

```
{
  "jsonrpc": "2.0",
  "method": "diagnostics.parameters",
  "id": "tx-42",
  "diagnostic": {}
}
```

Для остальных команд поле `diagnostic` содержит `VERSIONS`, `PROVIDERS` и `LICENSES`.

Сервис отвечает параметрами команды:

```
{
  "jsonrpc": "2.0",
  "id": "tx-42",
  "result": {
    "operation": ["VERSIONS", "LICENSES"]
  }
}
```

Требования к ответу перечислены в разделе Описание запросов и ответов. Оформление видимого штампа PAdES проверяется менее строго, чем остальные поля: неизвестные поля игнорируются, а непригодные декоративные значения — цвет, логотип, масштаб — заменяются оформлением по умолчанию.

Результат отправляется как уведомление JSON-RPC. Получатель может вернуть любой код `2xx`, включая `204 No Content`; тело ответа не требуется.

Доверенный сервис

Сетевой вызов работает только по HTTPS; имя пользователя и пароль в адресе запрещены. При первом обращении с нового адреса приложение показывает сертификат сервиса и предлагает отменить вызов или сохранить сервис как доверенный. Об отмене сервис узнаёт из сообщения со статусом `Canceled` — см. Ошибки и отмена.

Доверие определяется тремя значениями:

- точный адрес ресурса — схема, узел и порт;
- отпечаток SHA-256 открытого ключа сертификата (SPKI pin);
- отпечаток самого сертификата.

Обычная проверка цепочки TLS и имени узла сохраняется, а закреплённый ключ дополнительно проверяется при каждом запросе к сервису. Смена сертификата требует нового решения пользователя.

В окне согласия сертификат дополнительно проверяется по хранилищу сертификатов приложения: цепочка, срок действия, пригодность сертификата для TLS-сервера и соответствие имени узла. Результат этой проверки показывается пользователю вместе со сведениями о сертификате и цепочке.

Сохранённый сервис отображается в группе **«Доверенные сервисы»** панели профилей подписи — см. Доверенные сервисы. После удаления профиля доверие, закреплённый ключ и связанный профиль удаляются, и следующее обращение снова требует подтверждения.

Профиль сервиса и настройки операции

Вместе с доверием создаётся отдельный профиль подписи для этого сервиса. Итоговые настройки операции вычисляются в порядке:

1. Значения по умолчанию, заданные приложением.
2. Профиль сервиса.
3. Явные параметры вызова.
4. Изменения пользователя в незаблокированных полях.

Профиль, с которым пользователь работал в последний раз вручную, не используется. Из профиля сервиса не переносятся состав операций, локальная выходная папка, удаление исходных файлов, МЧД и назначение результата: они задаются транзакцией API.

Адреса файлов и токен

Адреса входных файлов и адрес получателя результата проверяются отдельно от адреса вызова. Новый адрес требует собственного подтверждения доверия.

Перенаправления (HTTP 3xx) выполняются только по HTTPS и только на серверы с тем же ключом, что у исходного адреса. Переход на сервер с другим ключом — например, в хранилище S3 — завершается ошибкой.

Значение `extra.token` добавляется как параметр `accessToken` к адресу получателя результата — на любом ресурсе, который прошёл проверку доверия. К адресу входного файла токен добавляется, только если файл на том же ресурсе, что и сам вызов. Для файлов на другом ресурсе используйте предподписанные ссылки либо передайте нужный параметр доступа прямо в адресе файла.

Службы штампов времени (TSP) и проверки статуса сертификата (OCSP) — исключение: к ним обращается не приложение, а криптографический провайдер. Принимается корректный адрес HTTP или HTTPS; `ocspURL` требует `tspURL`. Оба адреса показываются пользователю в окне подтверждения операции.

Локальный вызов

Вместо адреса HTTPS ссылка может содержать JSON-конверт или адрес `file://` файла с параметрами:

```
cryptoarm://startView/{"jsonrpc":"2.0","id":"tx-42","result":{"uiView":"SIGN_AND_ENCRYPT"}}
cryptoarm://signAndEncrypt/file:///C:/work/request.json
```

Конверт имеет вид `{ "jsonrpc": "2.0", "id": ..., "result": ... }`. Если `id` не задан, приложение присваивает вызову случайный идентификатор, и он же попадает в имя файла результата. Входные файлы задаются адресами `file://` или обычными абсолютными путями. Ссылку можно передать и в процентной кодировке — правило описано в разделе Кодирование ссылки.

Каталог результата задаётся обычным путём или адресом `file://`:

Команда	Где указывается
`signAndEncrypt`	`props.localResultParams.savePath`
`certificates`	`localResultParams` рядом с `operation` и `props`
`certrequests` и `diagnostics`	Рядом с `operation` и `props` либо внутри `props`

Для локального вызова `signAndEncrypt` и `certrequests` в `props.uploader` принимается адрес `file://`, обычный путь к каталогу или адрес HTTPS. Значение `saveResultsSeparately: true` создаёт отдельный файл результата для каждого идентификатора файла. Каталог может ещё не существовать — приложение создаст его после подтверждения вызова.

Если локальный вызов завершился ошибкой или пользователь отказал в разрешении, в тот же каталог записывается `direct-result-<id>.json` (для проверки подписи — `verify-result-<id>.json`) со статусом `Canceled` и причиной в `ErrorDescription`. Если каталог в параметрах не указан или параметры не читаются, файл не создаётся.

> ⚠️ **Важно**: сетевой вызов не может записать результат в локальный путь или в `file://`. Разрешение **«Разрешить локальные вызовы до выхода»** действует только до завершения работы приложения и не сохраняется.

Подтверждение пользователем

Доверие к сервису не даёт права выполнять криптографические операции без участия человека. Подпись, шифрование, расшифрование, снятие подписи, импорт и экспорт сертификатов и создание запроса открывают соответствующий экран или диалог приложения.

Фоновая диагностика и фоновая проверка подписи разрешаются отдельными настройками доверенного сервиса, выключенными по умолчанию. Фоновая проверка действует только для одиночной операции `VERIFYSIGN`.

ПИН-код и временная лицензия из `props.license` хранятся только в памяти одной операции: в журнал и в лог они не попадают.

Смотрите также

- Описание и возможности API — команды и форматы вызова.
- Приложение и пользователь — окна согласия и доверенные сервисы.
- Лимиты, статусы и ошибки — ограничения транспорта.

Открыть статью на сайте

Команда signAndEncrypt

Команда запускает подпись, архивирование и шифрование документов либо одну обратную операцию — проверку подписи, расшифрование или снятие подписи. Перед запуском пользователь видит обычный экран операции с файлами, сертификатами и настройками.

Содержание:

- Общая информация
- Формат ссылки
- Операции
- Получение параметров операции
- Файлы
- Параметры операции
- Параметры extra
- Сертификаты
- Подпись PDF и штамп
- Машиночитаемая доверенность
- Настройки и подтверждение
- Отправка результатов
- Справочник полей результата
- Смотрите также

Общая информация

Команда работает с сертификатами X.509. Операции OpenPGP через внешний API недоступны.

> 📌 **Примечание**: выполнение операции требует действующей лицензии на КриптоАРМ. Временную лицензию на одну операцию можно передать в `props.license`.

Формат ссылки

```
cryptoarm://signAndEncrypt/<URL>?id=<id>
```

Пример сетевого вызова:

```
cryptoarm://signAndEncrypt/https://api.example.ru/cryptoarm/json?id=tx-42
```

Формат локального вызова описан в разделе Формат ссылки для локального вызова.

Операции

Поле `operation` — непустой массив без повторов:

Прямые операции (можно комбинировать):

Значение	Описание
`SIGN`	Подпись
`ARCHIVE`	Архивирование
`ENCRYPT`	Шифрование

Обратные операции (выполняются по одной):

Значение	Описание
`UNSIGN`	Снятие подписи
`DECRYPT`	Расшифрование

Проверка подписи:

Значение	Описание
`VERIFYSIGN`	Проверка подписи

Ограничения:

- прямые и обратные операции не смешиваются;
- `VERIFYSIGN` и `UNSIGN` выполняются только по одной;
- отдельной операции `UNZIP` нет: ZIP-слой снимается вместе с проверкой или расшифрованием.

Получение параметров операции

Формат запроса

Получив команду, приложение отправляет на указанный адрес запрос параметров.

Ключ	Значение	Описание
`jsonrpc`	`2.0`	Версия протокола JSON-RPC. Всегда `2.0`.
`method`	`signAndEncrypt.parameters`	Имя метода. Всегда `signAndEncrypt.parameters`.
`id`	Идентификатор транзакции	Значение параметра `id` из ссылки.
`diagnostic`	Сведения о рабочем месте	Поля `VERSIONS`, `PROVIDERS` и `LICENSES`.

```
{
  "jsonrpc": "2.0",
  "method": "signAndEncrypt.parameters",
  "id": "tx-42",
  "diagnostic": {
    "VERSIONS": { "csp": "5.0.13000", "cryptoarm": "1.2.0", "openssl": "3.0.13" },
    "PROVIDERS": { "GOST2012_256": true, "GOST2012_512": true, "openssl": true },
    "LICENSES": {
      "csp": { "status": true, "type": "client", "expiration": "" },
      "cryptoarm": { "status": true, "type": "Permanent", "expiration": "" }
    }
  }
}
```

Формат ответа

Пример для прямых операций:

```
{
  "jsonrpc": "2.0",
  "id": "tx-42",
  "result": {
    "operation": ["SIGN", "ENCRYPT"],
    "props": {
      "headerText": "Подписание документов",
      "descriptionText": "Пакет документов на согласование",
      "files": [
        {
          "id": "document-1",
          "name": "document.pdf",
          "url": "https://api.example.ru/files/document.pdf"
        }
      ],
      "uploader": "https://api.example.ru/cryptoarm/result",
      "uploadMethod": "json",
      "extra": {
        "signType": 0,
        "signStandard": "cades-bes",
        "encryptAlgorithm": 0,
        "returnFiles": true
      }
    }
```

```
  }
}
```

Пример для проверки подписи:

```
{
  "jsonrpc": "2.0",
  "id": "tx-42",
  "result": {
    "operation": ["VERIFYSIGN"],
    "props": {
      "files": [
        {
          "id": "signature-1",
          "name": "document.pdf.sig",
          "url": "https://api.example.ru/files/document.pdf.sig",
          "urlDetached": "https://api.example.ru/files/document.pdf"
        }
      ],
      "uploader": "https://api.example.ru/cryptoarm/result",
      "extra": { "printReport": true }
    }
  }
}
```

Файлы

Файл описывается объектом:

Поле	Тип	Описание
`id`	string	Идентификатор файла. Возвращается в результате и используется в multipart.
`name`	string	Имя файла.
`url`	string	Адрес файла: HTTPS для сетевого вызова, `file://` — для локального.
`urlDetached`	string	Необязательное поле. Исходный документ для отсоединённой подписи.

Числовой `id` принимается и возвращается строкой.

Поля `props.files` и `props.archive` взаимоисключающие. В `archive` передаётся ZIP с входными файлами: он распаковывается до запуска операции. Результат прямой операции над `archive` упаковывается в ZIP, как при `ARCHIVE`. Идентификаторы файлов должны быть уникальны.

Если хотя бы один файл не удалось получить, вызов завершается до открытия экрана операции, и остальные файлы не обрабатываются. Сервис получает сообщение об отмене, где `ErrorDescription` называет файл: `Input file document-2 cannot be used: ….`

Для прямых операций (`SIGN`, `ARCHIVE`, `ENCRYPT`) оба поля можно не передавать: тогда экран операции открывается пустым, и файлы добавляет сам пользователь. Каждый добавленный файл получает новый идентификатор, и в результате приходит именно он: сопоставить результат с файлом сервиса в этом режиме нельзя. Для проверки подписи, расшифрования и снятия подписи файлы обязательны.

Параметры операции

Поле	Описание
`props.headerText`	Заголовок операции; длиннее 40 символов сокращается
`props.descriptionText`	Описание операции; длиннее 120 символов сокращается
`props.files`	Массив входных файлов; без него файлы выбирает пользователь
`props.archive`	ZIP с входными файлами вместо `props.files`
`props.license`	Временная лицензия на одну операцию
`props.uploader`	Адрес, на который отправляется результат; без него результат не отправляется
`props.uploadMethod`	`json` (по умолчанию) или `multipart/form-data`
`props.localResultParams.savePath`	Каталог результата; только для локального вызова
`props.localResultParams.saveResultsSeparately`	Отдельный файл результата для каждого входного файла
`props.extra`	Настройки операции — см. ниже

Параметры extra

Поле	Значения
`signType`	`0` — присоединённая подпись (по умолчанию), `1` — отсоединённая
`signStandard`	

Поле	Значения
	`0`, `cms` или `cades-bes` (по умолчанию), `1` или `cades-xlt1`, `2` или `cades-t`, `3` или `cades-a`
`signEncoding`	`0`, `PEM` или `BASE-64`; `1` или `DER`
`encryptEncoding`	`0`, `PEM` или `BASE-64`; `1` или `DER`
`encryptAlgorithm`	`0` — ГОСТ 28147-89, `1` — Магма, `2` — Кузнечик; по умолчанию выбирается по ключам получателей
`signatureExtension`	`sig` (по умолчанию), `p7s`, `sgn`, `sign`, `bin`, `pem`
`encryptionExtension`	`enc` (по умолчанию), `p7m`, `p7e`, `pem`
`signerChainIncludeKind`	`personal` — только сертификат подписанта (по умолчанию), `full` — вся цепочка
`timestampOnSign`	`true` вместе с CAdES-BES включает CAdES-T; при CAdES-T, XLT1 и A штамп ставится всегда
`tspURL`, `ocspURL`	Адреса служб штампа времени и проверки статуса сертификата; `ocspURL` требует `tspURL`
`isSignaturePades`	Подпись PDF в формате PAdES
`isPdfCertificationSign`	Сертифицирующая подпись PDF
`isAddStampToPdf`	Отдельная печатная копия PDF со штампом подписи
`printReport`	PDF-отчёт о проверке подписи
`returnFiles`	`true` (по умолчанию) — возвращать содержимое файлов результата
`showSettingsBeforeOperation`	`true` (по умолчанию) открывает настройки операции, `false` открывает подтверждение запуска без экрана настроек
`signCertificate`	Сертификат подписанта
`encryptCertificates`	Сертификаты получателей
`MCHD`	Машиночитаемая доверенность
`token`	Токен доступа к получателю результата и к входным файлам на ресурсе исходного вызова
`pin`	ПИН-код контейнера закрытого ключа. Хранится только в памяти операции

Числовые значения принимаются и строками: `"1"` равнозначно 1.

Неизвестное значение перечислимого поля — ошибка: приложение не заменяет его значением по умолчанию.

Сертификаты

Сертификат подписанта задаётся одним из трёх способов:

Селектор	Пример
Отпечаток SHA-1	`{ "hash": "b0a1…" }`
Сам сертификат	`{ "x509": "<DER Base64>" }`
Издатель и серийный номер	`{ "issuerName": "CN=Example CA", "serial": "01AB" }`

```
{
  "extra": {
    "signCertificate": { "hash": "b0a1c2d3e4f5a6b7c8d9e0f1a2b3c4d5e6f7a8b9" }
  }
}
```

Если сертификата подписанта нет в хранилище пользователя, у него нет закрытого ключа или это не сертификат ГОСТ, операция не отклоняется: пользователь выбирает сертификат подписи сам.

Получатели шифрования передаются в `encryptCertificates` — массивом сертификатов в формате DER, закодированном в Base64. Устанавливать их пользователю не нужно: они используются в том виде, в котором их передал сервис, и в хранилище не добавляются. Сертификат УЦ получателем быть не может. Строка, которая не является сертификатом, и повторяющиеся сертификаты отклоняются.

Получатель может быть сертификатом ГОСТ или сертификатом с ключом другого алгоритма, например RSA. Если `encryptAlgorithm` не задан, алгоритм выбирается по ключам получателей: для ГОСТ — ГОСТ 28147-89 или алгоритм из профиля доверенного сервиса, для остальных — AES-256. Алгоритмы `encryptAlgorithm` относятся к ГОСТ, поэтому зашифровать с ними для получателя с ключом RSA нельзя.

Если сертификат не задан, приложение предлагает выбрать его в обычной форме операции. Переданные сервисом получатели и найденный сертификат подписанта показываются без возможности изменения.

Подпись PDF и штамп

Оформление видимого штампа задаётся объектом `PAdESStampAppearance` — для подписи PAdES — и объектом `signStampAppearance` — для отдельной печатной копии со штампом.

Блок `mockupSettings` — вид штампа:

Поле	Значения
`elementsColor`	Цвет текста и рамки в формате `#rrggbb`
`backgroundColor`	Цвет фона
`addBackground`	Заливать фон. По умолчанию `true`
`addBorders`	Рисовать рамку. По умолчанию `true`
`pixelRatio`	Масштаб отрисовки от 0.5 до 4. По умолчанию 2
`logotype`	Логотип: `…` или `…`
`isHiddenLogo`	Скрыть логотип

Блок `requisitesSettings` — состав реквизитов:

Поле	Значения
`centralDisplayType`	`arbitrary` — произвольный состав центрального блока; иначе используется состав по ГОСТ
`stampTitle`	Заголовок вместо «Документ подписан электронной подписью»; перенос строки делит его на две
`central`	Реквизиты центрального блока
`left`, `right`	Реквизиты боковых блоков
`position`	`left`, `right` или `leftAndRight`

Элемент списка реквизитов: `{ "dataKey": "…", "isEnabled": true, "editedValue": "…", "title": "…" }`. Отключённые и повторяющиеся реквизиты отбрасываются. Доступные значения `dataKey`: `serialNumber`, `validityTimeSpan`, `subjectFriendlyName`, `individual`, `jobPosition`, `issuerFriendlyName`, `organizationName`, `mark`, `description`, `location`, `signingTime`, `MCHDNumber`, `hash`, `signatureAlgorithm`.

Размещение штампа для PAdES задаётся объектом `signStampPAdES`:

Поле	Значения
`pagesSelection`	`all`, `last` или `some`
`pageNumbers`	Массив номеров страниц; обязателен при `some`
`isDisplayedOnAllPages`	Показывать штамп на всех страницах
`pdfMarkedArea.stampSize`	`width` и `height` штампа в пунктах PDF
`pdfMarkedArea.dimensionsDocument`	`width`, `height`, `horizontalPadding`, `verticalPadding`

Поле	Значения
`pdfMarkedArea.placementOnPage`	`horizontal`: `left`, `center`, `right`; `vertical`: `top`, `center`, `bottom`
`pdfMarkedArea.orientationDegrees`	Поворот: `0`, `90`, `180` или `270`

Для печатной копии страницы задаются внутри `signStampAppearance`: `pageSelection` и строка `pageNumbers` вида `"1,3-5"`.

Устаревший способ размещения `signStampPosition` с полями `width`, `height`, `horizontalPadding` и `verticalPadding` также принимается; его значения задаются в миллиметрах, тогда как размеры в `signStampPAdES` — в пунктах PDF. По умолчанию штамп имеет размер 102,3 × 39,16 мм и отступы 66,6 мм по горизонтали и 20 мм по вертикали.

Недопустимые размеры, выбор страниц, поворот и размещение возвращают ошибку и не заменяются значениями по умолчанию. Значения по умолчанию подставляются только для декоративных полей — цвета, логотипа и масштаба.

Машиночитаемая доверенность

МЧД передаётся в `extra.MCHD` вместе с отсоединёнными подписями:

```
{
  "MCHD": {
    "xml": {
      "id": "mchd",
      "name": "power.xml",
      "url": "https://api.example.ru/files/power.xml"
    },
    "signatures": [
      {
        "id": "mchd-sign",
        "name": "power.xml.sig",
        "url": "https://api.example.ru/files/power.xml.sig"
      }
    ]
  }
}
```

Требуется файл XML и хотя бы одна подпись; идентификаторы всех файлов МЧД должны быть уникальны.

Настройки и подтверждение

Явно переданные через API тип и стандарт подписи, кодировки, расширения файлов, алгоритм шифрования, параметры PAdES и МЧД и сертификаты заблокированы для изменения. Если параметр не передан, начальное значение берётся из профиля сервиса, и пользователь может его изменить.

Состав операций, входные файлы и назначение результата задаются транзакцией API и не редактируются. Значение `showSettingsBeforeOperation: false` пропускает экран настроек, но не подтверждение запуска.

Отправка результатов

Прямые и обратные операции

Результат отправляется методом `signAndEncrypt.outDirectResults`.

Ключ	Значение	Описание
`jsonrpc`	`2.0`	Версия протокола JSON-RPC. Всегда `2.0`.
`method`	`signAndEncrypt.outDirectResults`	Имя метода
`params`	Объект результата	Идентификатор транзакции, статус и список файлов

```
{
  "jsonrpc": "2.0",
  "method": "signAndEncrypt.outDirectResults",
  "params": {
    "id": "tx-42",
    "status": "Completed",
    "directResults": [
      {
        "id": "document-1",
        "out": "<Base64>",
        "signValid": true,
        "signers": [
          {
            "isValid": true,
            "signingTime": 1594209848000,
            "isDetached": true,
            "signerCertificate": {
              "hash": "b0a1c2d3e4f5a6b7c8d9e0f1a2b3c4d5e6f7a8b9",
              "subjectName": "CN=Example User",
              "status": true
            }
          }
        ]
      }
```

```
    ]
  }
}
```

После подписи приложение проверяет получившуюся подпись и возвращает её сведения в полях `signValid` и `signers` — в том же виде, что и при проверке подписи. Результат `SIGN` вместе с `ENCRYPT` не проверяется: он зашифрован для получателя. Если проверка не выполнилась, результат отправляется без этих полей; недействительная по итогам проверки подпись результат не отменяет.

Необработанные файлы

Если подпись, шифрование, архивирование, расшифрование или снятие подписи не выполнены хотя бы для одного файла, результаты на `uploader` не отправляются. Так сервис не получит пустой файл вместо необработанного.

Вместо результатов сервис получает сообщение об отмене на адрес, с которого получены параметры:

```
{
  "jsonrpc": "2.0",
  "method": "signAndEncrypt.outDirectResults",
  "id": "tx-42",
  "params": {
    "status": "Canceled",
    "Error": true,
    "ErrorDescription": "Operation failed for files: document-2 (x509.sign.failed)"
  }
}
```

Для локального вызова сообщение сохраняется туда же, куда сохранился бы результат. Проверки подписи это не касается: её результат отправляется и тогда, когда часть файлов проверить не удалось.

Проверка подписи

Результат проверки отправляется методом `signAndEncrypt.verifySignResults` в поле `verifySignResults`. Содержимое файлов при проверке не возвращается: вместо него передаются сведения о подписи, а при `printReport: true` — PDF-отчёт в поле `outReport`.

```
{
  "jsonrpc": "2.0",
  "method": "signAndEncrypt.verifySignResults",
  "params": {
    "id": "tx-42",
    "status": "Completed",
    "verifySignResults": [
      {
        "id": "signature-1",
        "signValid": false,
        "isSignaturePades": false,
        "signers": [
```

```
          {
            "isValid": false,
            "isDetached": true,
            "isCades": true,
            "cadesType": 1,
            "signingTime": 1594209848000,
            "signatureAlgorithm": "1.2.643.7.1.1.3.2",
            "signatureDigestAlgorithm": "1.2.643.7.1.1.2.2",
            "signerCertificate": {
              "hash": "b0a1c2d3e4f5a6b7c8d9e0f1a2b3c4d5e6f7a8b9",
              "issuerFriendlyName": "Example CA",
              "issuerName": "CN=Example CA",
              "subjectFriendlyName": "Example User",
              "subjectName": "CN=Example User",
              "status": true,
              "serial": "01AB",
              "notBefore": 1593603200000,
              "notAfter": 1725139200000
            }
          }
        ]
      }
    ]
  }
}
```


> 💡 **Примечание**: недействительная подпись — это результат проверки, а не ошибка. Конверт имеет `status: "Completed"`, а `signValid` и `signers[].isValid` — значение `false`.

Передача файлов

При `uploadMethod: "json"` и `returnFiles: true` содержимое файлов передаётся в поле `out` в Base64. Base64 увеличивает объём передачи примерно на треть, поэтому для больших результатов используйте `multipart/form-data` или `returnFiles: false`.

При `uploadMethod: "multipart/form-data"` конверт JSON передаётся в поле `operation-response`, а файлы — отдельными частями, имя каждой части равно идентификатору исходного файла. Отчёт о проверке и печатная копия со штампом остаются полями конверта в Base64.

Значение `returnFiles: false` оставляет метаданные результата без содержимого файлов.

Сохранение результата локально

Для локального вызова файлы результата — подписанные, зашифрованные, расшифрованные — сохраняются на диск:

- в каталог из `props.uploader` (`file://` или обычный путь), если он задан;
- иначе — рядом с исходными файлами, для архива — рядом с архивом.

Файл JSON с результатом записывается в тот же каталог `props.uploader` либо в каталог `props.localResultParams.savePath`. Содержимого файлов в нём нет — поля `out`, `outSignStamp` и `outReport` не передаются, а файлы берутся с диска; `name` называет файл результата. Имена файлов JSON:

Операция	Имя файла
Прямая и обратная	`direct-result-<id>.json`
Проверка подписи	`verify-result-<id>.json`

При `saveResultsSeparately: true` для каждого входного файла создаётся отдельный файл `direct-result-<id>-<fileId>.json`. Существующие файлы не перезаписываются: к имени добавляется порядковый номер.

Без получателя результата

Если задан `props.uploader`, после успешной отправки результата вкладка операции закрывается; исключение — `VERIFYSIGN`, результат проверки остаётся на экране.

Если не заданы ни `props.uploader`, ни `props.localResultParams.savePath`, результат никуда не отправляется и остаётся у пользователя: экран операции открывается как обычно, а после завершения вкладка не закрывается. Сервис в этом режиме не получает ни результата, ни уведомления об успехе. Об ошибке сообщение уходит, как обычно, — см. Ошибки и отмена.

Справочник полей результата

Объект результата файла

Поле	Тип	Описание
`id`	string	Идентификатор входного файла
`name`	string	Имя файла результата
`out`	string	Содержимое результата в Base64
`outReport`	string	PDF-отчёт о проверке подписи в Base64
`outSignStamp`	string	Печатная копия PDF со штампом в Base64
`signValid`	boolean	Все подписи файла действительны
`timestampValid`	boolean	Штамп времени действителен

Поле	Тип	Описание
`isSignaturePades`	boolean	Подпись встроена в PDF
`signers`	Object[]	Сведения о подписантах
`error`	string	Код ошибки для этого файла

Статус подписанта

Поле	Тип	Описание
`isValid`	boolean	Подпись действительна
`signingTime`	number	Время подписания, Unix-время в миллисекундах
`verifyingTime`	number	Время проверки, Unix-время в миллисекундах
`isDetached`	boolean	Отсоединённая подпись
`isCades`	boolean	Подпись в формате CAdES
`cadesType`	number	Тип CAdES
`isSignaturePades`	boolean	Подпись встроена в PDF
`signatureAlgorithm`	string	Идентификатор алгоритма подписи
`signatureDigestAlgorithm`	string	Идентификатор алгоритма хеширования
`signerCertificate`	Object	Сертификат подписанта

Сертификат подписанта

Поле	Тип	Описание
`hash`	string	Отпечаток сертификата SHA-1
`issuerName`	string	Издатель
`issuerFriendlyName`	string	Издатель в удобочитаемом виде
`subjectName`	string	Владелец
`subjectFriendlyName`	string	Владелец в удобочитаемом виде
`serial`	string	Серийный номер
`status`	boolean	Результат проверки сертификата

Поле	Тип	Описание
`provider`	string	Криптопровайдер
`notBefore`	number	Начало срока действия, Unix-время в миллисекундах
`notAfter`	number	Окончание срока действия, Unix-время в миллисекундах
`rootCAMinComSvyaz`	boolean	Цепочка завершается корневым сертификатом Минцифры

Смотрите также

- Описание и возможности API — общий формат вызова.
- Транспорт и доверие — адреса файлов, токен, локальный вызов.
- Лимиты, статусы и ошибки — ограничения и завершение операции.
- Подпись и шифрование — те же операции в интерфейсе.

Открыть статью на сайте

Команда certificates

Команда импортирует сертификат X.509 в локальное хранилище, экспортирует выбранные сертификаты либо показывает сведения о переданном сертификате.

Содержание:

- Общая информация
- Формат ссылки
- Параметры
- Импорт сертификата
- Экспорт сертификатов
- Просмотр сведений о сертификате
- Справочник полей результата
- Смотрите также

Общая информация

Все три операции требуют действия пользователя: приложение открывает соответствующий экран, и без подтверждения хранилище не изменяется и сертификаты не выдаются.

Закрытые ключи через эту команду не передаются.

Формат ссылки

```
cryptoarm://certificates/<URL>?id=<id>
```

Формат локального вызова описан в разделе Формат ссылки для локального вызова.

Параметры

Параметры содержат поле `operation` и объект `props`:

Поле	Значение
`operation`	`import`, `export` или `information`
`props.headerText`	Необязательный заголовок; длиннее 40 символов сокращается

Поле	Значение
`props.descriptionText`	Необязательное описание; длиннее 120 символов сокращается
`props.store`	Массив хранилищ
`props.multy`	Разрешить выбор нескольких сертификатов при экспорте; по умолчанию `false`
`props.certificateBase64`	Сертификат в формате DER, закодированном в Base64 — для `import` и `information`
`localResultParams.savePath`	Каталог результата локального вызова; без него результат в файл не записывается

Хранилища:

Значение	Раздел приложения
`MY`	Личные сертификаты
`AddressBook`	Сертификаты других пользователей
`CA`	Промежуточные удостоверяющие центры
`ROOT`	Корневые удостоверяющие центры
`CA_OR_ROOT`	Удостоверяющие центры — без разделения на промежуточные и корневые

`MyAll` принимается как `MY`, `CaAndRoot` — как `CA_OR_ROOT`. Повторяющиеся значения `store` отбрасываются. Неизвестное хранилище — ошибка: список не расширяется до всех сертификатов.

Импорт сертификата

```
{
  "jsonrpc": "2.0",
  "id": "tx-import",
  "result": {
    "operation": "import",
    "props": {
      "store": ["MY"],
      "certificateBase64": "<DER Base64>"
    }
  }
}
```

Приложение показывает сертификат и хранилища, допустимые для него: пользовательский сертификат — **Личные** и **Другие пользователи**, самоподписанный сертификат УЦ — **Корневые удостоверяющие центры**, остальные сертификаты УЦ — **Промежуточные удостоверяющие центры**; для сертификата УЦ доступно также хранилище **Удостоверяющие центры**. Значение `props.store[0]` подставляется как предварительный выбор, но окончательное хранилище выбирает пользователь. Если `props.store[0]` недопустимо для сертификата, импорт отклоняется без окна.

Результат:

```
{
  "jsonrpc": "2.0",
  "method": "certificates.import",
  "params": {
    "id": "tx-import",
    "status": "Completed"
  }
}
```

Экспорт сертификатов

```
{
  "jsonrpc": "2.0",
  "id": "tx-export",
  "result": {
    "operation": "export",
    "props": {
      "store": ["MY", "AddressBook"],
      "multy": true
    }
  }
}
```

Если `props.store` не задан, предлагаются личные сертификаты. Пользователь выбирает один или несколько сертификатов, и приложение отправляет их в формате DER, закодированном в Base64, вместе со сведениями о владельце:

```
{
  "jsonrpc": "2.0",
  "method": "certificates.base64",
  "params": {
    "id": "tx-export",
    "certificates": [
      {
        "certificateBase64": "<DER Base64>",
        "hash": "b0a1c2d3e4f5a6b7c8d9e0f1a2b3c4d5e6f7a8b9",
        "issuerFriendlyName": "Example CA",
        "issuerName": "CN=Example CA",
        "notAfter": "2027-07-13T10:00:00.000Z",
        "notBefore": "2026-07-13T10:00:00.000Z",
        "rootCAMinComSvyaz": false,
```

```
        "subjectFriendlyName": "Example User",
        "subjectName": "CN=Example User",
        "status": true,
        "serial": "01AB",
        "x509": "<DER Base64>"
      }
    ]
  }
}
```

Просмотр сведений о сертификате

```
{
  "jsonrpc": "2.0",
  "id": "tx-information",
  "result": {
    "operation": "information",
    "props": {
      "certificateBase64": "<DER Base64>"
    }
  }
}
```

Приложение открывает карточку сертификата в отдельной вкладке и отправляет:

```
{
  "jsonrpc": "2.0",
  "method": "certificates.information",
  "params": {
    "id": "tx-information",
    "status": "Completed"
  }
}
```

Для сетевого вызова результат уходит на адрес исходного вызова; локальный вызов сохраняет тот же конверт в файл `certificates-<id>.json` в каталоге `localResultParams.savePath`.

Справочник полей результата

Поле	Тип	Описание
`certificateBase64`	string	Сертификат в формате DER, закодированном в Base64
`hash`	string	Отпечаток сертификата SHA-1
`issuerName`	string	Издатель
`issuerFriendlyName`	string	Издатель в удобочитаемом виде

Поле	Тип	Описание
`subjectName`	string	Владелец
`subjectFriendlyName`	string	Владелец в удобочитаемом виде
`serial`	string	Серийный номер
`notBefore`	string	Начало срока действия
`notAfter`	string	Окончание срока действия
`status`	boolean	Результат проверки цепочки сертификата
`rootCAMinComSvyaz`	boolean	Цепочка завершается корневым сертификатом Минцифры

Смотрите также

- Описание и возможности API — общий формат вызова.
- Команда certrequests — создание запроса на сертификат.
- Управление сертификатами — те же операции в интерфейсе.

Открыть статью на сайте

Команда certrequests

Команда создаёт запрос на сертификат в формате PKCS#10. Сервис передаёт шаблон запроса, а алгоритм, контейнер и доступные поля пользователь проверяет в обычной форме создания запроса.

Содержание:

- Общая информация
- Формат ссылки
- Параметры
- Шаблон JSONTemplate
- Параметры ключа и расширения
- Поля владельца
- Назначения ключа
- Шаблон по сертификату
- Результат
- Смотрите также

Общая информация

Поддерживается единственная операция — `GENERATE`. Создание самоподписанного сертификата через эту команду недоступно.

Формат ссылки

```
cryptoarm://certrequests/<URL>?id=<id>
```

Формат локального вызова описан в разделе Формат ссылки для локального вызова.

Параметры

Поле	Значение
`operation`	`GENERATE`
`props.headerText`	Необязательный заголовок; длиннее 40 символов сокращается

Поле	Значение
`props.descriptionText`	Необязательное описание; длиннее 120 символов сокращается
`props.templateType`	`JSONTemplate` или `CertificateTemplate` — шаблон по сертификату
`props.template`	Объект шаблона выбранного типа
`props.uploader`	Адрес получателя результата: HTTPS или `file://` для локального вызова
`props.returnFiles`	Передавать ли запрос получателю; по умолчанию `true`
`localResultParams.savePath`	Каталог результата локального вызова; без него и без `props.uploader` результат в файл не записывается

Шаблон по сертификату без `certificateBase64` открывает пустую форму запроса: пользователь заполняет её сам.

Шаблон JSONTemplate

```
{
  "jsonrpc": "2.0",
  "id": "tx-csr",
  "result": {
    "operation": "GENERATE",
    "props": {
      "templateType": "JSONTemplate",
      "template": {
        "Description": "Сертификат для электронной подписи",
        "RDN": [
          {
            "Oid": "2.5.4.3",
            "LocalizedName": "Имя владельца",
            "DefaultValue": "Example User",
            "Length": 64,
            "ProhibitEmpty": true,
            "ProhibitChange": false
          }
        ],
        "Extensions": {
          "KeyUsage": [{ "Name": "digitalSignature", "DefaultValue": true }],
          "ExtendedKeyUsage": [{ "Name": "1.3.6.1.5.5.7.3.2", "DefaultValue": true }]
        },
        "MarkExportable": false
      }
    }
  }
}
```

Поля шаблона:

Поле	Описание
`Description`	Описание над формой, если не задан `props.descriptionText`
`RDN[]`	Поля владельца
`Extensions.KeyUsage[]`	Назначения ключа
`Extensions.ExtendedKeyUsage[]`	Расширенные назначения ключа, OID
`MarkExportable`	Начальное значение экспортируемости контейнера
`CREncoding`	`DER` или `BASE-64`; по умолчанию `BASE-64`

Имена полей шаблона сравниваются без учёта регистра.

Параметры ключа и расширения

Значение настройки в `Extensions` задаётся строкой либо объектом с полями `DefaultValue` и `ProhibitChange`. При `ProhibitChange: true` текстовое поле показывается без возможности изменения.

Поле	Описание
`provider`, `algorithm`, `keyLength`	Начальные значения: `CRYPTOPRO` или `SYSTEM`, `gost2012`, `RSA` или `EC`, длина ключа
`IdentificationKind`	Способ идентификации владельца: `0`–`3`; `4` — не указан
`subjectSignTool`	Средство электронной подписи владельца; без него — установленный КриптоПро CSP
`issuerSignTool`	Средство ЭП и УЦ издателя: четыре значения через `\n`
`certificatePolicies`	OID класса средства ЭП; без него — класс установленного КриптоПро CSP; другой OID добавляется к дополнительным политикам
`additionalCertificatePolicies`	Дополнительные политики, OID через `;`
`subjectAltName`	Альтернативные имена владельца через `;`, например `dnsName=example.ru;dnsName=www.example.ru`
`customEKU`	Дополнительные расширенные назначения ключа, OID через `;`

Поле	Описание
`privateKeyUsagePeriod`	Срок использования закрытого ключа в секундах от момента создания запроса
`certificateTemplate`	OID шаблона сертификата, по которому УЦ выбирает профиль сертификата
`extensionsOID`	OID атрибута, в который упаковываются расширения

Если `provider` не задан, а КриптоПро CSP установлен, запрос создаётся на ключе ГОСТ Р 34.10-2012. Если шаблон требует `CRYPTOPRO`, а КриптоПро CSP не установлен, используется системный провайдер. Способ идентификации, средства ЭП, политики, срок ключа и OID шаблона сертификата записываются в запрос только для ключа КриптоПро.

Поля владельца

Поле `Oid` принимает как OID в точечной записи, так и распространённые сокращения: `CN`, `SN`, `GN` или `G`, `O`, `OU`, `T` или `TITLE`, `L`, `S` или `ST`, `STREET`, `C`, `E` или `EMAILADDRESS`, `OGRN`, `OGRNIP`, `SNILS`, `INN`, `INNLE`.

Для каждого поля поддерживаются:

Свойство	Описание
`DefaultValue`	Начальное значение
`LocalizedName`	Название поля в интерфейсе
`ProhibitEmpty`	Поле обязательно для заполнения
`ProhibitChange`	Значение нельзя изменить
`SettingsValues` и `ProhibitAnyValue`	Ограниченный список допустимых значений
`Length`	Максимальная длина значения

Назначения ключа

В `KeyUsage` поддерживаются: `digitalSignature`, `nonRepudiation` (синоним `contentCommitment`), `keyEncipherment`, `dataEncipherment`, `keyAgreement`, `keyCertSign`, `cRLSign`, `encipherOnly`, `decipherOnly`.

Элемент может быть строкой либо объектом с полями `Name`, `DefaultValue`, `ProhibitChange` и `LocalizedName`. В `ExtendedKeyUsage` поле `Name` содержит OID в точечной записи.

Шаблон по сертификату

Чтобы построить шаблон по существующему сертификату, передайте его в формате DER, закодированном в Base64:

```
{
  "jsonrpc": "2.0",
  "id": "tx-csr",
  "result": {
    "operation": "GENERATE",
    "props": {
      "templateType": "CertificateTemplate",
      "template": {
        "certificateBase64": "<DER Base64>"
      }
    }
  }
}
```

Поля владельца, назначения ключа и расширенные назначения исходного сертификата становятся заблокированными значениями шаблона.

Результат

После подтверждения параметров и создания ключа приложение отправляет:

```
{
  "jsonrpc": "2.0",
  "method": "certrequests.base64",
  "params": {
    "id": "tx-csr",
    "certificaterequestBase64": "<Base64 файла запроса>",
    "friendlyName": ""
  }
}
```

Если задан `props.uploader`, результат уходит только туда, методом `certrequests.outDirectResults`:

```
{
  "jsonrpc": "2.0",
  "method": "certrequests.outDirectResults",
  "params": {
    "id": "tx-csr",
    "status": "Completed",
    "directResults": [{ "out": "<Base64 файла запроса>", "friendlyName": "" }]
  }
}
```

При `returnFiles: false` поле `out` не передаётся. Адрес `uploader` на другом ресурсе требует собственного подтверждения доверия. Для локального вызова `uploader` вида `file://` задаёт каталог, в который записывается `direct-result-<id>.json` с тем же содержимым.

Если пользователь отменил создание запроса, сервис получает `certrequests.parameters` со статусом `Canceled` и `ErrorDescription: "Access denied"`.

`certificaterequestBase64` — файл запроса в Base64. По умолчанию запрос записывается в PEM, поэтому внутри Base64 находится текст `-----BEGIN CERTIFICATE REQUEST-----`; при `CREncoding: "DER"` — двоичный DER. Шаблон по сертификату всегда даёт PEM. Поле `friendlyName` для запроса пустое.

Для сетевого вызова результат уходит на адрес исходного вызова; локальный вызов сохраняет конверт в файл `certrequests-<id>.json` в каталоге `localResultParams.savePath`.

Смотрите также

- Описание и возможности API — общий формат вызова.
- Команда certificates — установка выпущенного сертификата.
- Создание запроса и самоподписанного сертификата — та же операция в интерфейсе.

Открыть статью на сайте

Команда diagnostics

Команда возвращает сведения о рабочем месте: систему, доступность криптопровайдеров, версии, состояние лицензий и сведения о личных сертификатах.

Содержание:

- Общая информация
- Формат ссылки
- Параметры
- Подтверждение пользователем
- Результат
- Сведения о личных сертификатах
- Смотрите также

Общая информация

Возвращаются только запрошенные сведения: приложение не собирает и не отправляет сведения, которые сервис не запрашивал. Повторяющиеся и неизвестные значения `operation` отбрасываются; если известных значений не осталось, команда отклоняется.

В запросе параметров самой команды `diagnostics` поле `diagnostic` — пустой объект: сведения о рабочем месте не передаются до того, как получены параметры и разрешение пользователя.

Формат ссылки

```
cryptoarm://diagnostics/<URL>?id=<id>
```

Формат локального вызова описан в разделе Формат ссылки для локального вызова.

Параметры

Поле `operation` — непустой массив значений:

Значение	Что возвращается
`SYSTEMINFORMATION`	Тип системы, архитектура, платформа и тип установочного пакета
`CSP_ENABLED`	Доступность КриптоПро CSP

Значение	Что возвращается
`CADES_ENABLED`	Доступность CAdES
`VERSIONS`	Версии КриптоПро CSP, КриптоАРМ и системного OpenSSL
`PROVIDERS`	Доступность ГОСТ 2012-256, ГОСТ 2012-512 и OpenSSL
`LICENSES`	Состояние лицензий КриптоПро CSP и КриптоАРМ
`PERSONALCERTIFICATES`	Сведения о сертификатах из хранилища личных сертификатов

Поля `props.headerText` и `props.descriptionText` задают текст в окне подтверждения. Текст длиннее 40 и 120 символов соответственно сокращается. Для локального вызова `localResultParams.savePath` принимается рядом с `operation` либо внутри `props`; без него сведения показываются пользователю, но в файл не записываются.

```
{
  "jsonrpc": "2.0",
  "id": "tx-diagnostics",
  "result": {
    "operation": ["SYSTEMINFORMATION", "VERSIONS", "PROVIDERS", "LICENSES"],
    "props": {
      "headerText": "Проверка рабочего места"
    }
  }
}
```

Подтверждение пользователем

Доверие к сервису само по себе не разрешает диагностику. Приложение показывает адрес сервиса и запрошенный набор сведений в окне **«Диагностика рабочего места»** и ждёт решения пользователя.

Для сетевого сервиса в этом окне можно разрешить последующие запуски диагностики в фоне. Разрешение сохраняется в профиле сервиса только вместе с подтверждением текущей операции; отказ профиль не изменяет. Изменить его позже можно на вкладке «Параметры ресурса». Пока разрешение действует, последующие запросы этого сервиса выполняются без окна подтверждения — включая `PERSONALCERTIFICATES`, который возвращает сведения обо всех личных сертификатах пользователя.

Результат

Результат отправляется методом `diagnostics.information` и содержит только запрошенные поля:

```
{
  "jsonrpc": "2.0",
  "method": "diagnostics.information",
  "params": {
    "id": "tx-diagnostics",
    "SYSTEMINFORMATION": {
      "type": "Darwin",
      "arch": "arm64",
      "platform": "darwin",
      "packageType": "pkg"
    },
    "VERSIONS": {
      "csp": "5.0.13000",
      "cryptoarm": "1.2.0",
      "openssl": "3.0.13"
    },
    "PROVIDERS": {
      "GOST2012_256": true,
      "GOST2012_512": true,
      "openssl": true
    },
    "LICENSES": {
      "csp": { "status": true, "type": "", "expiration": "" },
      "cryptoarm": { "status": true, "type": "GOST", "expiration": 0 }
    }
  }
}
```

Поле `packageType` принимает значения `msi`, `pkg` или `deb` — по платформе, на которой запущено приложение.

Сведения о лицензии:

Поле	КриптоАРМ	КриптоПро CSP
`status`	Лицензия действует	Лицензия действует
`type`	`TRIAL`, `GOST`, `GOST_PDF`, `GOST_PROTECTED_MAIL`, `GOST_SERVER` или пустая строка	Всегда пустая строка
`expiration`	Окончание срока в Unix-времени, в секундах; `0` — бессрочная лицензия; поля нет, если срок неизвестен	Всегда пустая строка

Без установленной лицензии сведения КриптоАРМ относятся к пробному периоду: `type` — `TRIAL`, а `status` — `false`, если пробный период закончился.

Сведения о личных сертификатах

Значение `PERSONALCERTIFICATES` возвращает массив объектов. Закрытые ключи и содержимое сертификатов в него не входят.

Поле	Тип	Описание
`hash`	string	Отпечаток сертификата SHA-1
`serial`	string	Серийный номер
`issuerName`	string	Издатель
`issuerFriendlyName`	string	Издатель в удобочитаемом виде
`subjectName`	string	Владелец
`subjectFriendlyName`	string	Владелец в удобочитаемом виде
`organizationName`	string	Организация
`notBefore`	number	Начало срока действия, Unix-время в миллисекундах
`notAfter`	number	Окончание срока действия, Unix-время в миллисекундах
`keyNotAfter`	number	Окончание срока действия закрытого ключа
`key`	boolean	К сертификату есть закрытый ключ
`isSelfSigned`	boolean	Самоподписанный сертификат
`pubKeyAlg`	string	Алгоритм открытого ключа
`signatureAlgorithm`	string	Алгоритм подписи
`signatureDigestAlgorithm`	string	Алгоритм хеширования подписи
`keyUsageString`	string	Назначения ключа, перечисленные через запятую
`provider`	string	Криптопровайдер

Смотрите также

- Описание и возможности API — общий формат вызова.
- Приложение и пользователь — окно разрешения на диагностику.
- Криптопровайдеры и стандарты — назначение криптопровайдеров и стандартов.

Открыть статью на сайте

Команда startView

Команда открывает существующий раздел приложения после обычной проверки доверия к вызову.

Содержание:

- Формат ссылки
- Параметры
- Завершение
- Смотрите также

Формат ссылки

```
cryptoarm://startView/<URL>?id=<id>
```

Формат локального вызова описан в разделе Формат ссылки для локального вызова.

Параметры

Параметры содержат единственное обязательное поле `uiView`:

```
{
  "jsonrpc": "2.0",
  "id": "tx-view",
  "result": {
    "uiView": "SIGN_AND_ENCRYPT"
  }
}
```

Поддерживаемые значения:

`uiView`	**Раздел приложения**
`SIGN_AND_ENCRYPT`	Подпись и шифрование
`VERIFY_AND_DECRYPT`	Проверка и расшифрование
`CERTIFICATES_MY`	Личные сертификаты
`CERTIFICATES_ADDRESS_BOOK`	Сертификаты других пользователей
`CERTIFICATES_CA`, `CERTIFICATES_ROOT`	

uiView	Раздел приложения
	Сертификаты удостоверяющих центров; оба значения открывают один раздел
KEYS	Ключевые контейнеры
ABOUT, DIAGNOSTICS	Настройки приложения; оба значения открывают один раздел

Пустое и неизвестное значение возвращает ошибку.

Значения CERTIFICATES_CA и CERTIFICATES_ROOT принимаются оба и открывают один и тот же раздел: отдельной вкладки для корневых сертификатов в приложении нет. Разделять промежуточные и корневые хранилища можно в команде certificates — там CA и ROOT задают разные хранилища.

Завершение

После открытия раздела отдельный результат не отправляется. Ошибка открытия, отказ в доверии или неподдерживаемое значение завершаются по общим правилам — см. Ошибки и отмена.

Смотрите также

- Описание и возможности API — общий формат вызова.
- Интерфейс приложения — из каких разделов состоит приложение.

Открыть статью на сайте

Лимиты, статусы и ошибки

Эта статья описывает ограничения внешнего API, статусы завершения операции и поведение приложения при ошибке и отмене.

Содержание:

- Лимиты
- Статусы операции
- Ошибки и отмена
- Завершение вкладки операции
- Смотрите также

Лимиты

Что ограничивается	Значение
Ожидающие вызовы API	8; выполняются последовательно
Один запрос: параметры, файл или результат	600 секунд
Сообщение сервису об ошибке или отмене	10 секунд
Установка соединения с сервером	30 секунд
Ожидание действия пользователя	5 минут
Ответ сервиса, встроенный JSON или локальный файл	64 МиБ
Один входной файл	512 МиБ
Все входные файлы одной операции	512 МиБ и не более 100 файлов
Транспортный ZIP-архив	Не более 100 записей и 512 МиБ распакованных данных
Данные, встроенные в один JSON-результат в Base64	64 МиБ суммарно

Повторный вызов отклоняется, пока предыдущий не завершён. Вызовы различаются по источнику, команде и идентификатору транзакции, а вызов со ссылкой на файл параметров — по пути к этому файлу.

Base64 увеличивает объём передачи примерно на треть. Для больших результатов используйте `multipart/form-data` или `returnFiles: false`.

Время ожидания запроса и время ожидания действия пользователя отсчитываются независимо. Общего времени ожидания у сессии нет: прервать запущенную криптографическую операцию безопасно невозможно.

Статусы операции

`status`	**Значение**
`Completed`	Операция завершена; результат может описывать недействительную подпись
`Error`	Техническая или операционная ошибка
`Canceled`	Пользователь отказался от выполнения или отменил операцию

Для `Error` дополнительно передаются `Error: true` и `ErrorDescription`. Частичный успех проверки подписи сохраняет доступные результаты и сообщает ошибку для неуспешной части. Остальные операции `signAndEncrypt` частичных результатов не отправляют — см. Необработанные файлы.

`ErrorDescription` содержит стабильные коды приложения — например, `x509.sign.failed` или `x509.verify.invalidSignature`. Сообщения криптографических библиотек в контракт не входят: они остаются в лог-файле и в журнале приложения.

> 💡 **Примечание**: недействительная подпись — это результат проверки, а не ошибка. Конверт имеет `status: "Completed"`, а `signValid` и `signers[].isValid` — значение `false`.

Ошибки и отмена

Если поддерживаемая сетевая команда уже прошла проверку доверия, приложение отправляет сообщение об ошибке, чтобы сервис не оставался в ожидании.

Если обработчик команды ещё не сформировал результат, сообщение уходит на исходный адрес — тот, с которого получены параметры, а не на `uploader`, — методом `<команда>.parameters`. Статус в нём всегда `Canceled`, какой бы ни была причина, а сама причина передаётся в `ErrorDescription`:

```
{
  "jsonrpc": "2.0",
  "method": "signAndEncrypt.parameters",
  "id": "tx-42",
  "params": {
    "status": "Canceled",
```

```
    "Error": true,
    "ErrorDescription": "Operation failed"
  }
}
```

Метод и текст сообщения зависят от этапа и причины:

Когда	`method`
Параметры не получены или не прошли проверку	`<команда>.parameters`
`certificates`: ошибка или отмена после чтения параметров	`certificates.base64`, `certificates.import` или `certificates.information` — по операции
`signAndEncrypt`: ошибка или отмена после чтения параметров	`signAndEncrypt.outDirectResults` или `signAndEncrypt.verifySignResults`
Приложение закрыто до завершения вызова	Метод текущего этапа: до чтения параметров `<команда>.parameters` (для `signAndEncrypt` — `signandencrypt.parameters`), после — метод результата

Причина	`ErrorDescription`
Пользователь отменил операцию или закрыл её окно	`Operation canceled`
Пользователь отказал в `diagnostics` или отменил `certrequests`	`Access denied`
Пользователь не доверил сервис	`Access denied`
Пользователь закрыл приложение до завершения вызова	`App closed`
Остальные ошибки	Описание причины

Отказ в доверии сообщается только сервису, который обратился впервые: пользователь нажал **Отмена**, закрыл окно подтверждения или не ответил за 5 минут. Сервис от этого доверенным не становится. Если у уже доверенного сервиса сменился сертификат и пользователь отказал, сообщение не отправляется.

На вызов команды, которой в приложении нет, приложение отвечает только доверенному сервису, чей сервер по-прежнему предъявляет сохранённый ключ. Окно подтверждения при этом не показывается. Сервис получает `<команда>.parameters` со статусом `Canceled` и `ErrorDescription: "Command is not supported: <команда>"`. Для `sendMail`, `saveDocuments`, `authorize` и `mtlsAuthorization` метод — `sendMail.parameters`, `documents.parameters`, `authorize.parameters` и `mtlsAuthorization.parameters`.

При выходе из приложения `App closed` получают выполняемый вызов и локальные вызовы, ждущие в очереди. Сетевой вызов получает сообщение, только если уже прошёл проверку доверия и вход пользователя; сетевые вызовы в очереди завершаются без сообщения. Доставка не гарантируется: приложение не ждёт её завершения.

Ошибка TLS или сертификата при проверке доверия, неизвестная команда от недоверенного сервиса и недоступный адрес завершаются без сообщения. Вызывающая сторона должна иметь собственный таймаут и обрабатывать повторный вызов идемпотентно.

При закрытии или перезагрузке окна операция отменяется до обращения к криптопровайдеру. Уже запущенная операция не отменяется.

Завершение вкладки операции

Если задан `uploader` и результат успешно доставлен, вкладка операции закрывается автоматически, а временные файлы удаляются. Исключение — `VERIFYSIGN`: результат проверки остаётся на экране. В остальных случаях результат остаётся во вкладке, пока пользователь её не закроет.

Смотрите также

- Описание и возможности API — общий формат вызова.
- Транспорт и доверие — проверка сервиса и адресов.
- Команда signAndEncrypt — форматы результата операции.