Цифровые технологии

КриптоАРМ Подпись и шифрование

Документация продукта

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 ... 11
- Глоссарий ... 14

Установка

- Установка на Windows ... 21
- Установка на Linux ... 32
- Установка на macOS ... 44
- Активация лицензий ... 49

Начало работы

- Быстрый старт ... 55
- Интерфейс приложения ... 59
- Общие настройки ... 63
- Уведомления и журнал событий ... 68
- Проверка и установка обновлений ... 74

Документы

- Обзор операций и выбор раздела ... 78
- Профили подписи ... 84
- Подпись и шифрование ... 90
- Проверка и расшифрование ... 108
- Подпись и защита PDF ... 122
- Настройки подписи и шифрования ... 139
- Контекстное меню Проводника и открытие файлов ... 155
- Выполнение операций в командной строке ... 165

Сертификаты

- Раздел «Сертификаты» ... 185
- Установка сертификатов ... 193
- Создание запроса и самоподписанного сертификата ... 199
- Экспорт и удаление сертификатов ... 205

Контейнеры и списки отзыва ... 209
Группы сертификатов ... 214
Сетевой профиль доверия ... 218

OpenPGP

О разделе OpenPGP ... 224
Создание и импорт сертификатов ... 229
Действия с сертификатами ... 235
Экспорт и резервное копирование ... 242

API

Описание и возможности API ... 246
Приложение и пользователь ... 252
Транспорт и доверие ... 256
Аутентификация ... 260
Команда signAndEncrypt ... 262
Подпись PDF: штамп, готовое поле и мастер ... 278
Команда certificates ... 284
Команда certrequests ... 289
Команда diagnostics ... 295
Команда startView ... 300
Лимиты, статусы и ошибки ... 302

Открыть статью на сайте

Документация КриптоАРМ Подпись и шифрование

КриптоАРМ Подпись и шифрование — приложение 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 лицензий — лицензионный ключ КриптоАРМ и серийные номера КриптоПро.
- Быстрый старт — первая подпись, проверка и шифрование.

Разделы документации

- **Общие сведения** — о продукте, криптопровайдеры, глоссарий.
- **Установка** — Windows, Linux, macOS, активация лицензий.
- **Начало работы** — быстрый старт, интерфейс приложения, общие настройки, уведомления и журнал событий, проверка и установка обновлений.
- **Документы** — обзор операций, профили подписи, подпись и шифрование, проверка и расшифрование, подпись и защита PDF, настройки подписи и шифрования, контекстное меню и открытие файлов, командная строка.
- **Сертификаты** — раздел «Сертификаты», установка, запрос и самоподписанный сертификат, экспорт и удаление, контейнеры и списки отзыва, группы, сетевой профиль доверия.
- **OpenPGP** — обзор, создание и импорт, действия с сертификатами, экспорт и резервное копирование.
- **API** — описание и возможности, приложение и пользователь, транспорт и доверие, аутентификация; команды signAndEncrypt и подпись PDF, certificates, certrequests, diagnostics, startView; лимиты, статусы и ошибки.

Открыть статью на сайте

КриптоАРМ Подпись и шифрование

КриптоАРМ Подпись и шифрование — приложение 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.

С чего начать работу — в инструкции Быстрый старт.

Содержание:

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

Основные возможности КриптоАРМ

Электронная подпись

- создание и проверка подписи файлов любого типа;
- присоединённая и отсоединённая подпись, соподписи;
- стандарты CAdES-BES, CAdES-T, CAdES-X Long Type 1, CAdES-A;
- подпись и проверка подписи с машиночитаемой доверенностью (МЧД);
- отчёты о проверке подписи в формате PDF;
- снятие, объединение и разделение подписей.

Документы PDF

- подпись и сертификация документов;
- встроенная подпись по стандарту PAdES с видимым или невидимым штампом;
- разметка областей для подписей и подписантов;
- добавление текста и изображений;
- преобразование в форматы PDF/A-2b и PDF/A-3b.

Шифрование

- шифрование и расшифрование файлов по стандарту PKCS#7;
- шифрование для одного или нескольких получателей и по группам сертификатов;
- алгоритмы ГОСТ 28147-89, ГОСТ Р 34.12-2015 «Магма» и «Кузнечик», AES-256-CBC, DES3-CBC;
- удаление исходных файлов после шифрования, если это включено в настройках.

Архивирование

- архивирование файлов перед подписью и шифрованием;
- упаковка результатов в один архив или в отдельный архив на каждый файл.

Управление сертификатами и ключами

- просмотр сертификатов и их закрытых ключей;
- проверка 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 через КриптоПро CSP;
- 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, быстрые действия Finder и меню файлового менеджера Linux с профилями;
- командная строка (CLI) для сценариев и систем обмена документами;
- внешний API для вызова операций из веб-сервисов и локальных приложений.

Журнал и уведомления

- журнал событий с фильтрацией и сортировкой;
- экспорт журнала в файл 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. Стандарт выбирается в разделе **Настройки → Криптопровайдеры** — см. Общие настройки.

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, международные алгоритмы: RSA, ECDSA, AES и др. Алгоритмы ГОСТ не поддерживает.
2. **КриптоПро CSP версии 5.0 и выше** — стандарт X.509, алгоритмы ГОСТ (ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ 28147-89 и др.). Нужен, чтобы:

- работать с сертификатами ГОСТ;
- создавать электронную подпись, отвечающую требованиям законодательства РФ;
- использовать аппаратные ключевые носители.

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

С КриптоПро CSP приложение работает с аппаратными ключевыми носителями:

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

Полный список носителей — в формуляре 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, объединение и разделение подписей;
- просмотр, импорт, экспорт и удаление сертификатов;
- операции с сертификатами встроенного провайдера OpenSSL;
- все операции OpenPGP;
- архивирование.

Лицензия бывает двух видов:

- **пробная** — на 30 дней, активируется сама при первом запуске;
- **на рабочее место** — годовая или бессрочная, активируется лицензионным ключом.

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

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

Пробная лицензия

При первом запуске КриптоАРМ автоматически активируется **пробная лицензия на 30 дней**. С ней доступны все функции приложения, включая операции с алгоритмами ГОСТ.

Если этого срока не хватило, напишите в техническую поддержку support@trusted.ru — вам выдадут дополнительную пробную лицензию.

Лицензия на рабочее место

Лицензия на рабочее место привязана к компьютеру и активируется лицензионным ключом. Она бывает **годовой** и **бессрочной**.

На серверных операционных системах нужна серверная лицензия.

Купить лицензию можно в интернет-магазине cryptoarm.ru:

- КриптоАРМ версии Подпись и шифрование, годовая

- КриптоАРМ версии Подпись и шифрование, бессрочная

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

Компонент	Минимальная конфигурация	Рекомендуемая конфигурация
Процессор	1 ГГц	2 ГГц и выше
ОЗУ	2 ГБ	4 ГБ и больше
Дисковое пространство	500 МБ	5 ГБ и больше
Дисплей	1024×768	1920×1080 и больше

Приложение выпускается для процессоров x86-64, а для macOS — также для 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, контекстное меню файлового менеджера — в Альт Рабочая станция 11, РЕД ОС 8 и Ubuntu; версии перечислены в разделе Меню файлового менеджера на Linux. В Astra Linux меню нет.

Смотрите также

- Криптопровайдеры в КриптоАРМ — какие провайдеры выполняют операции.
- Глоссарий — термины электронной подписи простыми словами.
- Быстрый старт — первая подпись, проверка и шифрование.
- Установка на Windows, Linux и macOS — установка приложения и КриптоПро CSP.
- Активация лицензий — лицензии КриптоАРМ и КриптоПро.

Открыть статью на сайте

Криптопровайдеры в КриптоАРМ

Криптопровайдер — программный модуль, который выполняет криптографические операции: создаёт и проверяет электронную подпись, шифрует и расшифровывает данные, создаёт и хранит ключи.

КриптоАРМ работает с тремя провайдерами. Какой из них выполнит операцию, зависит от стандарта операции и алгоритма сертификата — выбирать провайдер вручную не нужно.

Содержание:

- Поддерживаемые криптопровайдеры
- Когда нужен КриптоПро CSP
- Раздел «Криптопровайдеры»
- Инструкции по установке КриптоПро CSP
- Смотрите также

Поддерживаемые криптопровайдеры

Провайдер	Стандарт	Алгоритмы	Установка
КриптоПро CSP 5.0 и выше	X.509	ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ 28147-89 и др.	Отдельно
OpenSSL	X.509	RSA, ECDSA, AES, 3DES	Встроен
Провайдер OpenPGP	OpenPGP	Все алгоритмы стандарта, включая постквантовые схемы	Встроен

КриптоПро CSP нужен также для работы с ключевыми контейнерами и аппаратными ключевыми носителями — см. Поддерживаемые ключевые носители.

Стандарт операций — X.509 или OpenPGP — выбирается в настройках: см. Общие настройки.

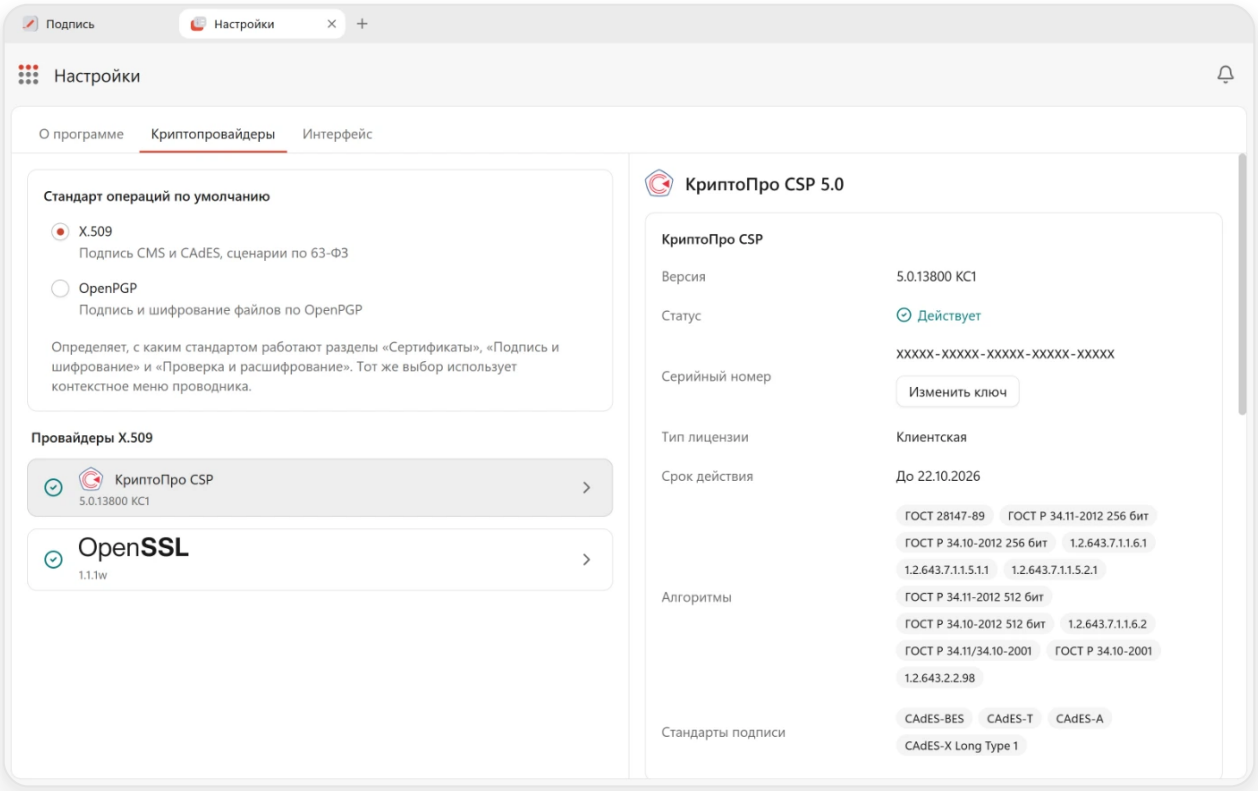
Когда нужен КриптоПро CSP

Для юридически значимого документооборота и обмена документами с государственными органами в России применяются средства криптографической защиты, которые сертифицированы ФСБ России и работают по алгоритмам ГОСТ. В КриптоАРМ это **КриптоПро CSP**: без него недоступны квалифицированная электронная подпись и сертификаты ГОСТ.

Без КриптоПро CSP приложение выполняет операции с сертификатами международных алгоритмов и все операции OpenPGP.

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 лицензий — лицензии КриптоАРМ и КриптоПро.
- Общие настройки — стандарт операций 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 связывает открытый ключ с его владельцем. Содержит сведения о владельце (ФИО, СНИЛС и др.), об удостоверяющем центре, выдавшем сертификат, и срок действия.

Квалифицированный сертификат

Сертификат, выданный аккредитованным удостоверяющим центром. Нужен для создания усиленной квалифицированной электронной подписи (УКЭП).

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. Им проверяют подпись владельца и шифруют данные в его адрес. Открытый ключ входит в сертификат и не является секретом.

Закрытый ключ

Ключ электронной подписи, доступный только владельцу. Им создают подпись и расшифровывают данные. Хранится в зашифрованном виде в ключевом контейнере — как правило, на аппаратном носителе (токене).

Запрос на сертификат

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

Ключевой контейнер

Хранилище закрытого ключа и служебных данных для его защиты. Контейнер может находиться на токене, смарт-карте, флеш-накопителе, жёстком диске или в реестре.

Статус сертификата электронной подписи

Результат проверки сертификата: не истёк ли срок действия, не отозван ли сертификат и построена ли цепочка доверия.

Удостоверяющий центр (УЦ)

Организация, которая выпускает сертификаты электронной подписи и подтверждает их действительность. Квалифицированные сертификаты выпускают только аккредитованные удостоверяющие центры.

Корневой сертификат

Сертификат удостоверяющего центра, с которого начинается цепочка доверия. Он подписан ключом самого центра, поэтому доверие к нему устанавливают явно — добавляют сертификат в хранилище доверенных корневых. В России корневой сертификат для квалифицированных сертификатов принадлежит Минцифры России.

Промежуточный сертификат

Сертификат удостоверяющего центра, выпущенный вышестоящим центром. Среднее звено цепочки доверия.

Сертификат другого пользователя

Сертификат без закрытого ключа на этом компьютере — например, сертификат контрагента или коллеги. Нужен, чтобы шифровать документы в адрес его владельца.

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)

Последовательность сертификатов от корневого до сертификата пользователя. Для квалифицированных сертификатов она, как правило, состоит из трёх звеньев: корневой сертификат, сертификат удостоверяющего центра и сертификат пользователя. Если цепочку построить не удалось, подпись считается непроверенной.

Отпечаток (thumbprint)

Хэш сертификата — короткая строка, которая однозначно его обозначает. Используется, например, для выбора сертификата в командной строке.

Подпись и шифрование

Электронная подпись (ЭП)

Данные, которые присоединены к документу или связаны с ним и позволяют определить подписавшего и убедиться, что документ после подписания не менялся.

Усиленная неквалифицированная электронная подпись (УНЭП)

Электронная подпись, созданная криптографическими средствами: позволяет определить подписавшего и обнаружить изменения документа после подписания. Равнозначна собственноручной подписи, если это предусмотрено законом или соглашением сторон.

Усиленная квалифицированная электронная подпись (УКЭП)

Усиленная подпись, созданная квалифицированным сертификатом с помощью сертифицированных средств электронной подписи. Равнозначна собственноручной подписи без предварительной договорённости сторон.

Криптопровайдер

Программный модуль, который выполняет криптографические операции: создаёт и проверяет подпись, шифрует и расшифровывает данные, создаёт и хранит ключи. См. Криптопровайдеры в КриптоАРМ.

Профиль подписи

Сохранённый набор настроек подписи, архивирования и шифрования. Профиль выбирается одним щелчком и доступен в контекстном меню Проводника на Windows, в быстрых действиях Finder на macOS и в меню файлового менеджера на Linux.

Алгоритмы подписи и шифрования

Математические правила, по которым создаётся подпись и шифруются данные. Алгоритм подписи определяется сертификатом: ГОСТ Р 34.10-2012 — у российских сертификатов, RSA и ECDSA — у международных. Алгоритм шифрования выбирается в настройках операции.

Присоединённая подпись

Подпись, которая хранится в одном файле с подписанным документом. Чтобы получить исходный документ, подпись снимают.

Отсоединённая подпись

Подпись, которая хранится в отдельном файле. Для проверки нужны оба файла — документ и подпись.

Соподпись

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

CAdES

Стандарт усовершенствованной электронной подписи для файлов любого типа. Подписи CAdES создаются сертификатами КриптоПро; сертификатом встроенного провайдера OpenSSL подпись создаётся в базовом формате CMS.

CAdES-BES

Базовая подпись CAdES: в неё вложены сведения о подписанте. Подтверждает авторство и неизменность документа.

CAdES-T

Подпись CAdES со штампом времени. Для её создания нужен адрес службы штампов времени (TSP).

CAdES-X Long Type 1

Подпись CAdES, в которую вложены штамп времени и полные сведения о сертификатах и списках отзыва. Её можно проверить и после того, как срок действия сертификата истёк.

CAdES-A

Подпись CAdES-X Long Type 1, дополненная архивными штампами времени. Предназначена для долговременного хранения документов.

Штамп времени (TSP)

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

Машиночитаемая доверенность (МЧД)

Электронная доверенность в формате XML. Подтверждает 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

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

PAdES

Стандарт подписи, встроенной в PDF-документ. Отдельный файл подписи не создаётся: результат остаётся PDF-файлом, который получатель может открыть и проверить.

Видимая подпись PDF-документа

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

Невидимая подпись PDF-документа

Встроенная подпись, которая на страницах документа не отображается.

Сертификация PDF-документа

Первая подпись в PDF-документе, которая задаёт, какие изменения разрешены после подписания.

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 на странице PDF-документа с текстом или изображением — например, комментарием, статусом или отметкой о конфиденциальности.

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 сценарии, 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

Подпись, которой один владелец подтверждает принадлежность чужого сертификата его владельцу; в OpenPGP её называют также сертификацией. 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 раздел выбрать для задачи.

Открыть статью на сайте

Установка КриптоАРМ на Windows

Инструкция описывает установку КриптоАРМ и КриптоПро CSP на Windows, обновление и удаление приложения.

Содержание:

- Подготовка к установке
- Установка КриптоАРМ
- Установка КриптоПро CSP
- Активация лицензий
- Обновление
- Мало места на системном диске
- Удаление КриптоАРМ
- Смотрите также

Подготовка к установке

Требования

- 64-разрядная Windows 10 и выше.
- Права администратора: приложение устанавливается для всех пользователей компьютера.

Скачивание установочных файлов

Дистрибутив КриптоАРМ

Скачайте установщик с одного из сайтов:

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

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

Дистрибутив КриптоПро CSP

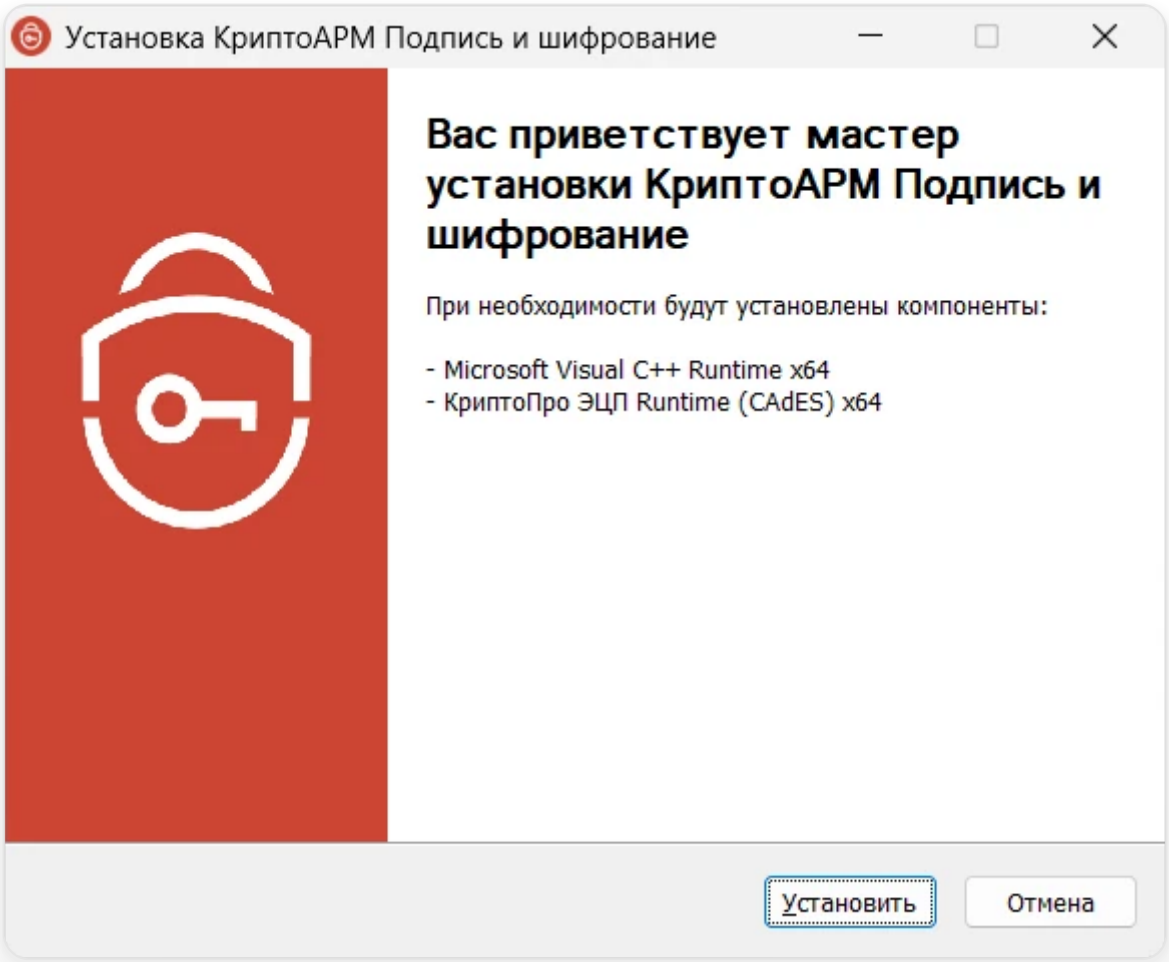
КриптоПро CSP нужен только для операций с алгоритмами ГОСТ. КриптоАРМ поддерживает КриптоПро CSP версии 5.0 и выше.

Скачайте дистрибутив для своей системы на сайте КриптоПро. Для скачивания нужно зарегистрироваться на сайте и принять лицензионное соглашение.

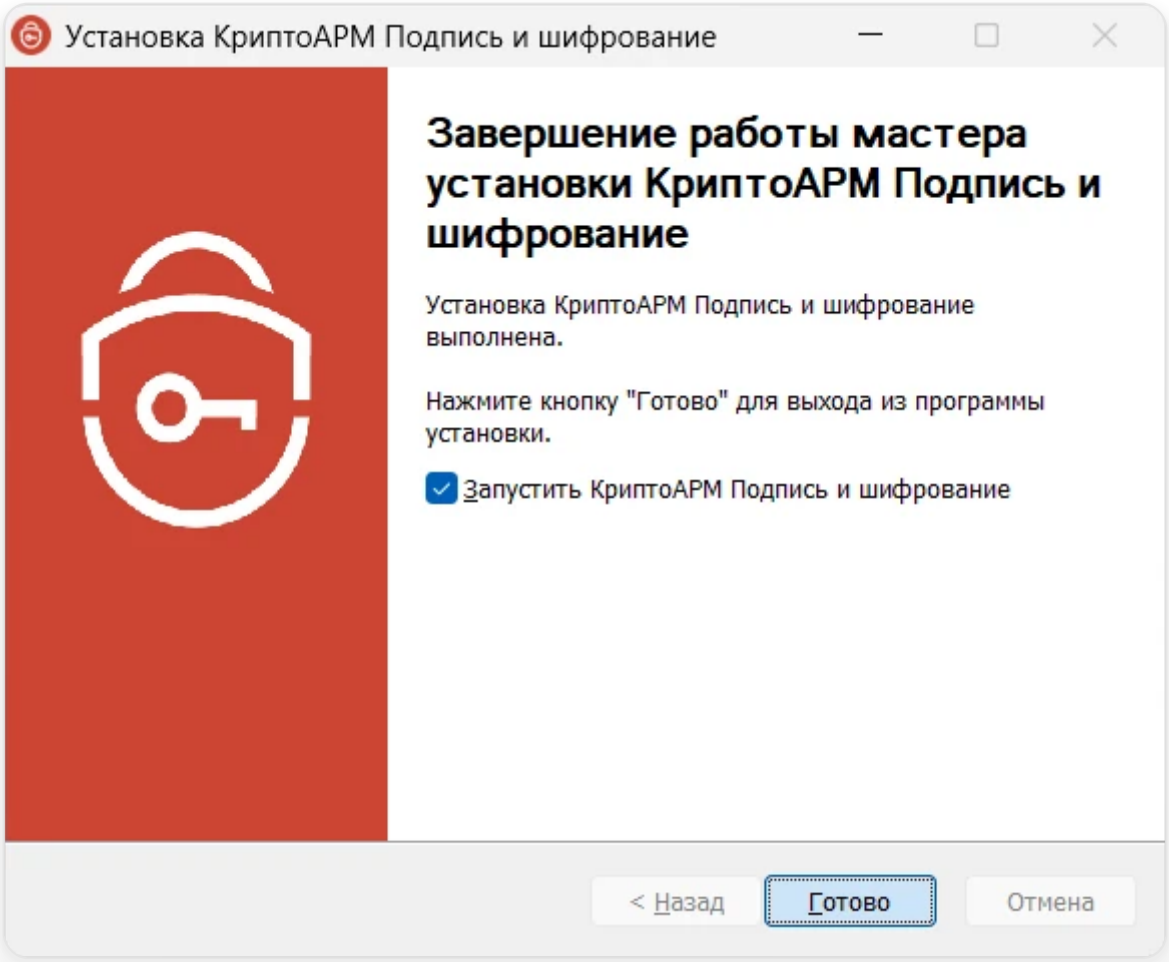
Установка КриптоАРМ

1. Запустите скачанный файл установщика.
2. На странице приветствия перечислены компоненты, которые установщик добавит, если их нет в системе:

- Microsoft Visual C++ Runtime x64;
- компоненты КриптоПро ЭЦП (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.

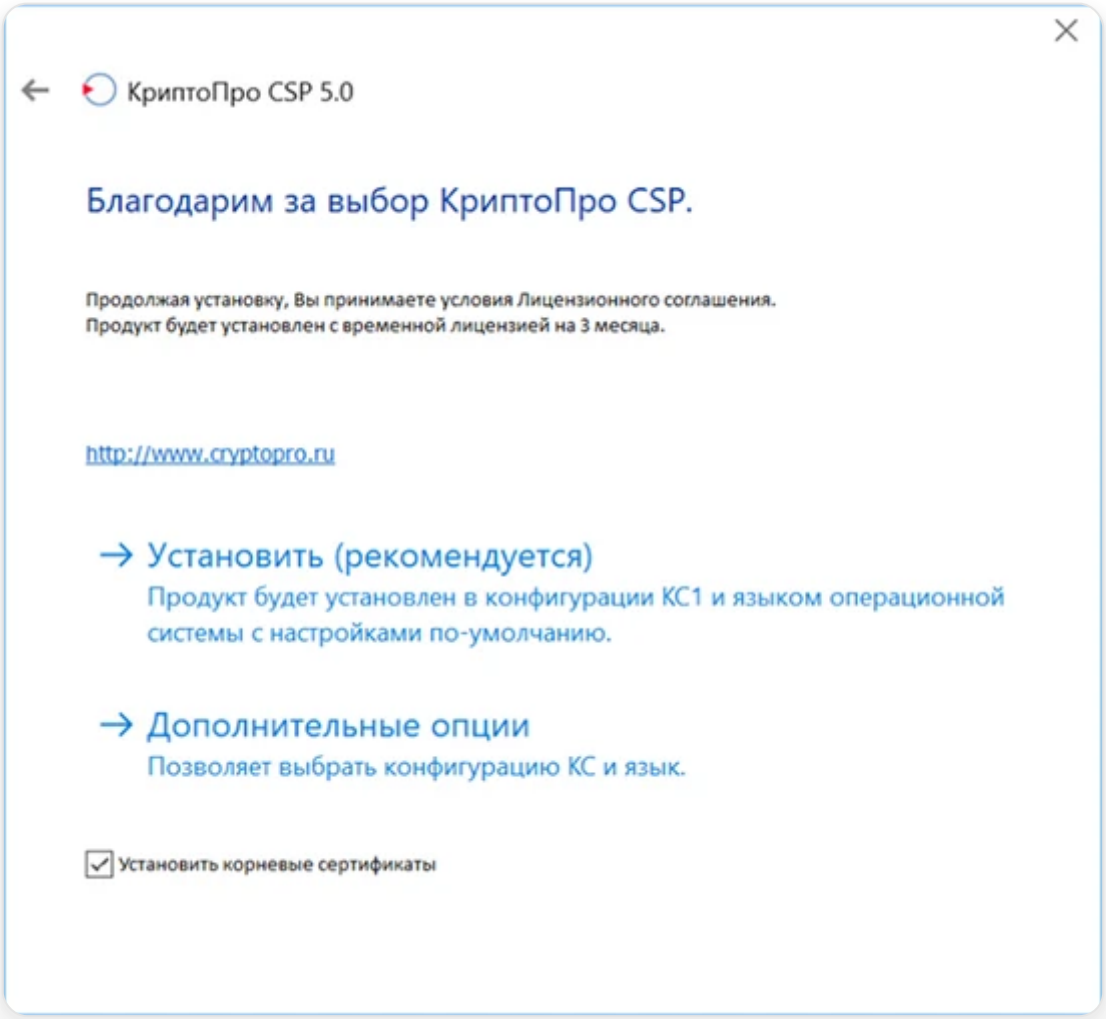


> 💡 **Примечание**: приложение устанавливается в `C:\Program Files\cryptoarm-sign`, язык установщика совпадает с языком системы. Если на диске `C:` мало места, см. Мало места на системном диске.

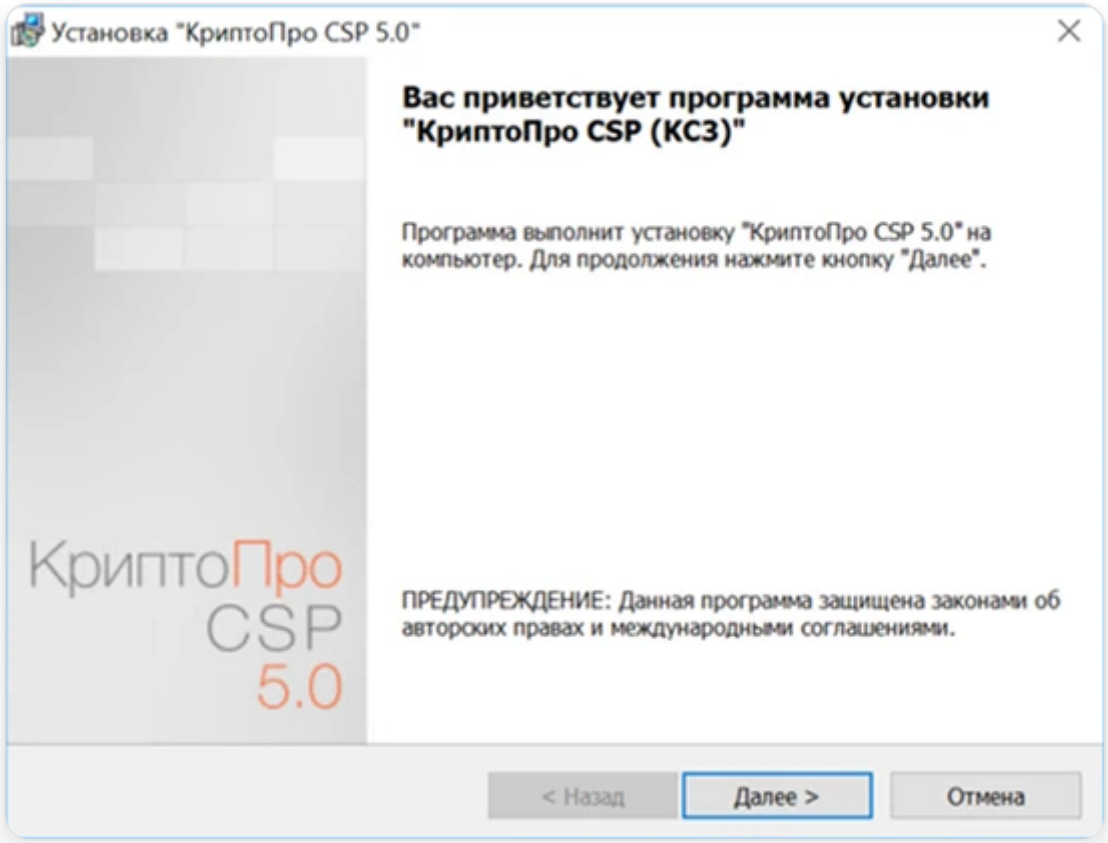
Установка КриптоПро CSP

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

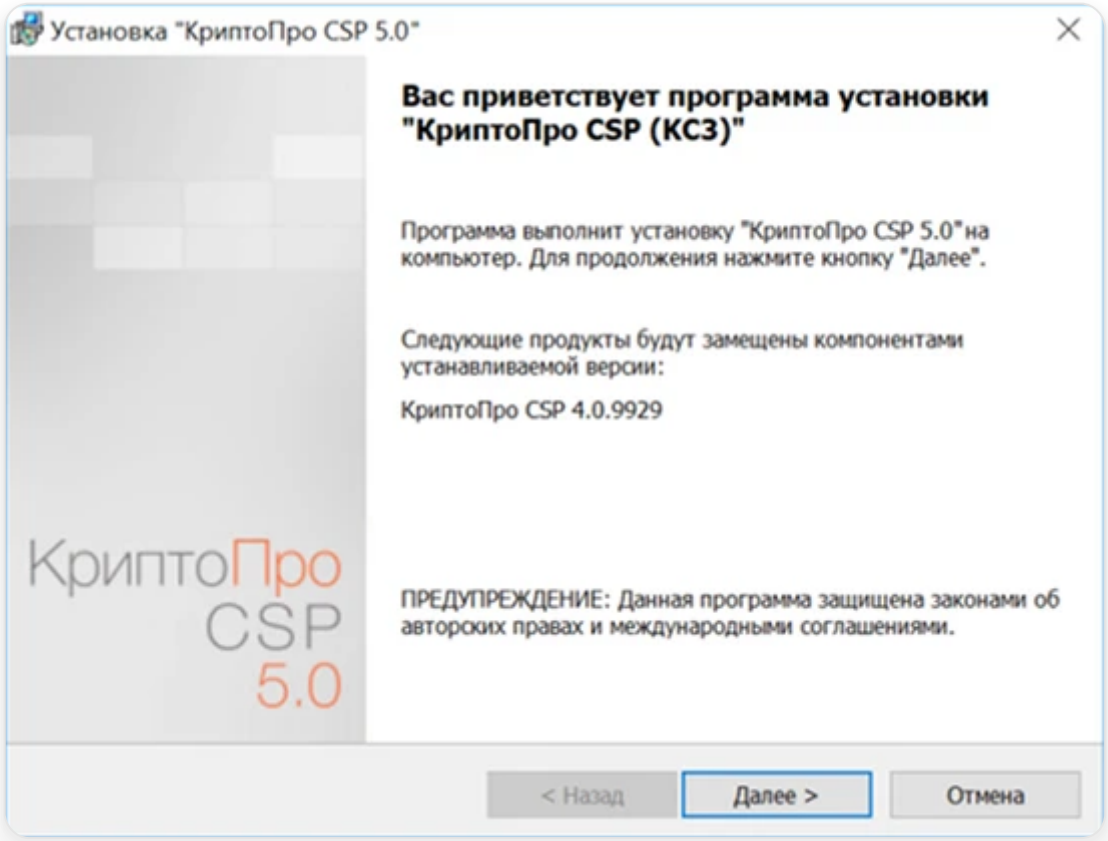
1. Запустите скачанный дистрибутив КриптоПро CSP.
2. Откроется приветственное окно мастера установки. Чтобы изменить класс защиты или язык установки, нажмите **Дополнительные опции**.



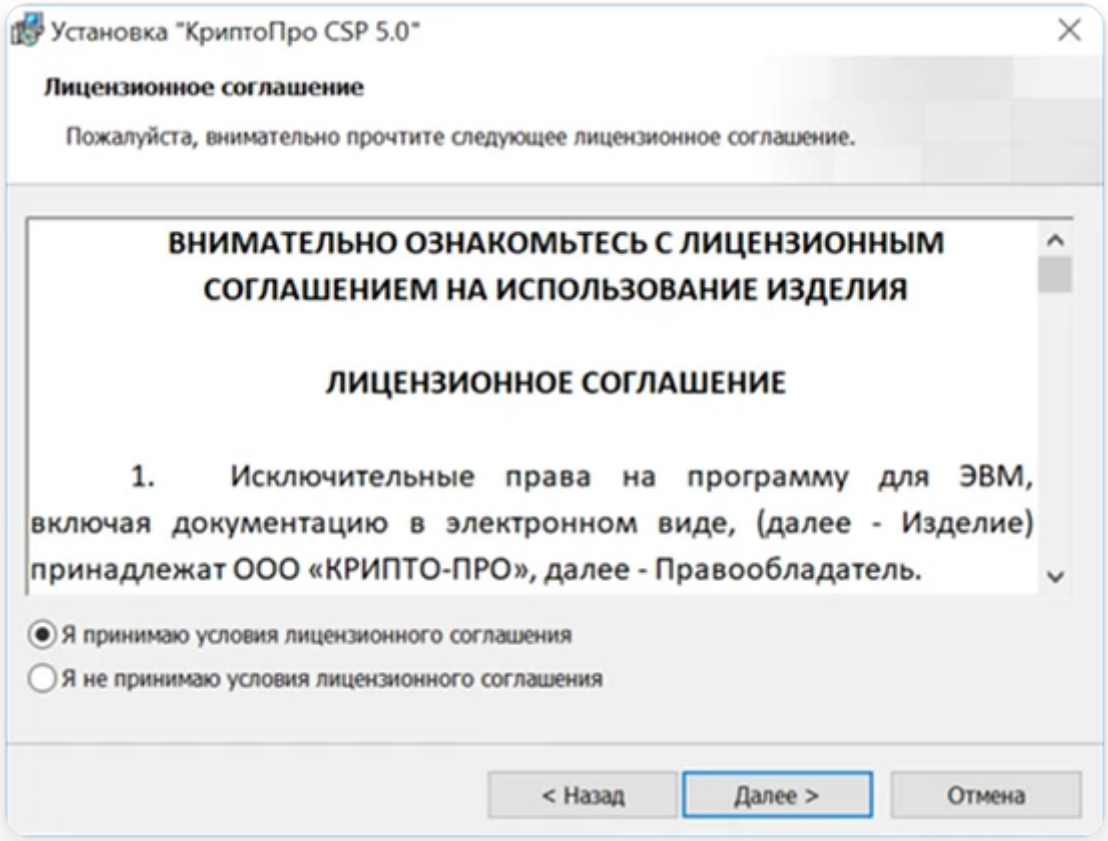
1. Дальше следуйте указаниям мастера. Он может предложить зарегистрировать дополнительные считыватели и датчики случайных чисел или включить дополнительную защиту. Чтобы продолжить, нажмите **Далее**.



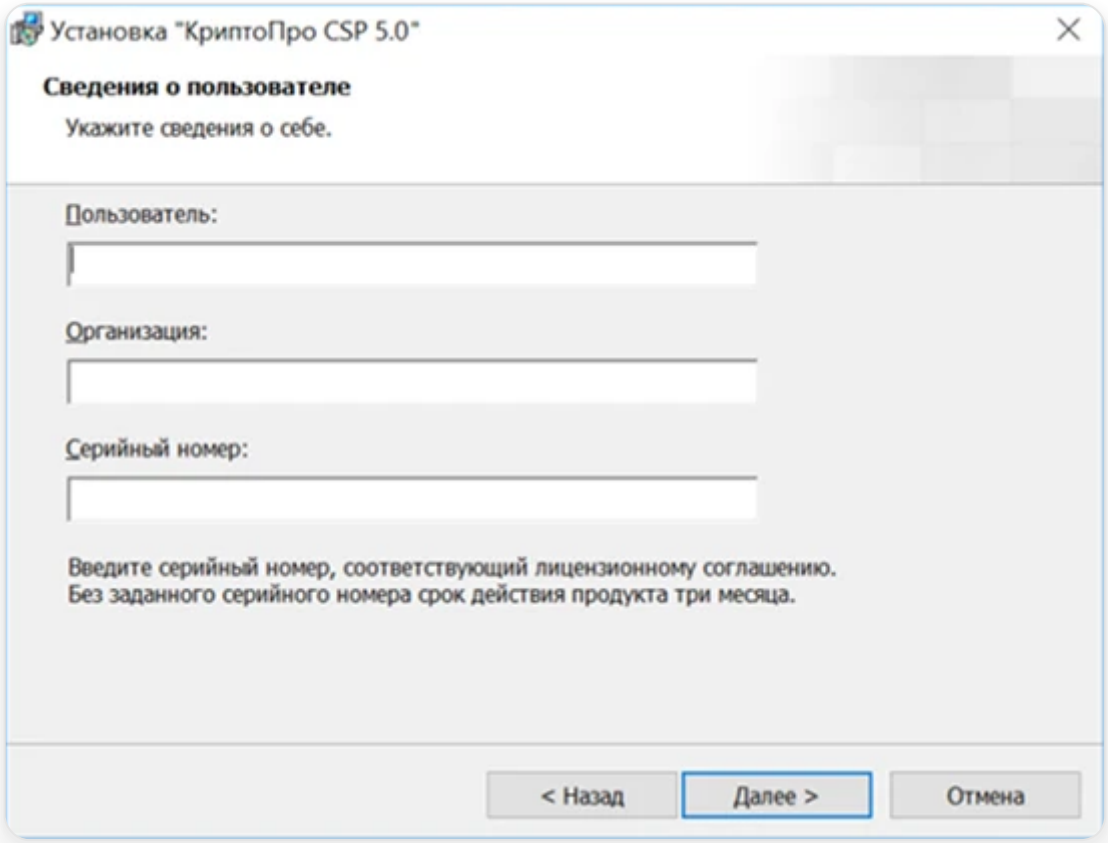
1. Если в системе уже установлена более ранняя версия КриптоПро CSP, мастер покажет сведения о ней. Нажмите **Далее**.



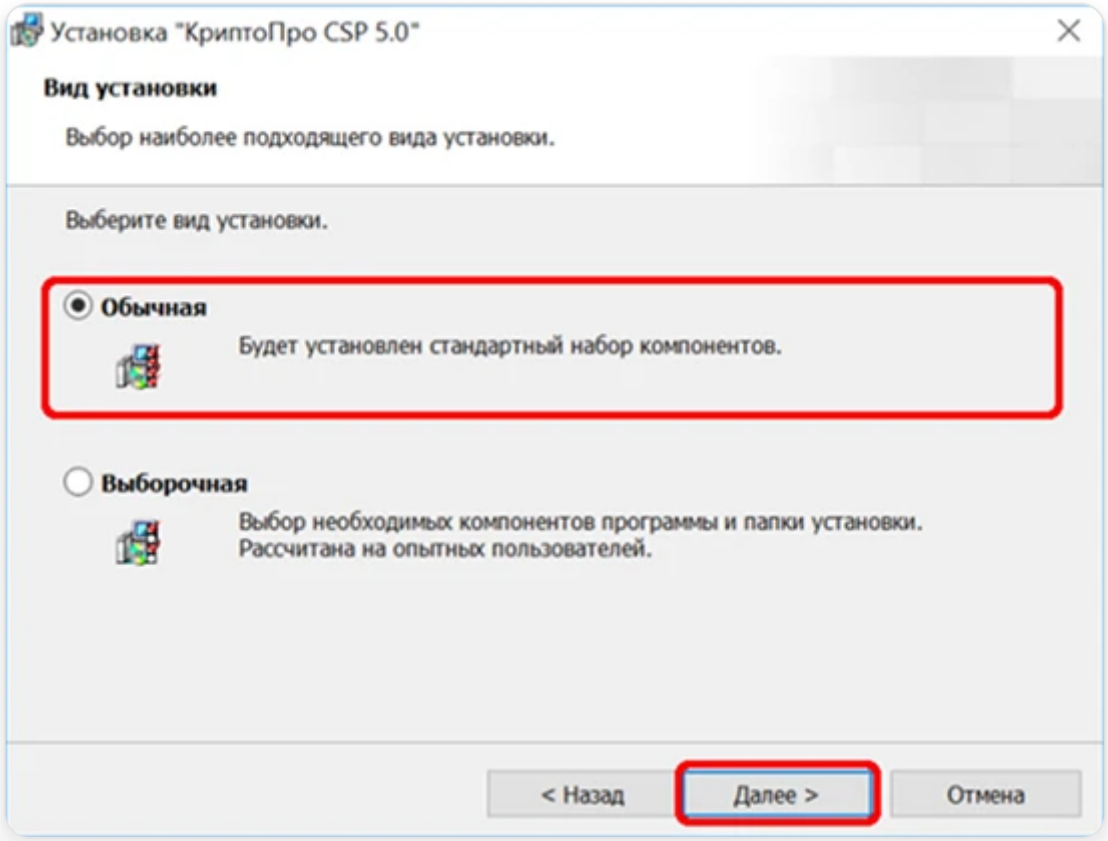
1. Выберите **Я принимаю условия лицензионного соглашения** и нажмите **Далее**.



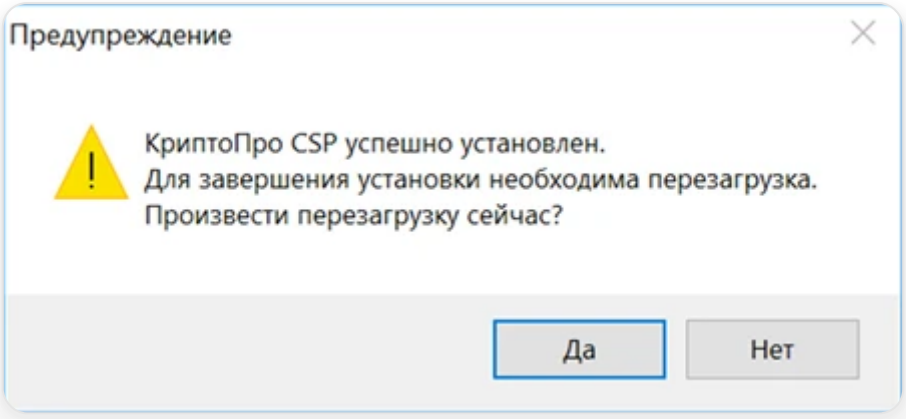
1. Введите сведения о пользователе и организации и серийный номер лицензии — или пропустите этот шаг: их можно указать позже. Нажмите **Далее**.



1. Выберите тип установки **Обычная** и нажмите **Далее**.



1. Когда установка завершится, перезагрузите компьютер.



Активация лицензий

При первом запуске КриптоАРМ действует пробная лицензия на 30 дней. Чтобы работать с алгоритмами ГОСТ после её окончания, активируйте лицензии:

- Лицензия КриптоАРМ — лицензионный ключ приложения;
- Лицензии КриптоПро — серийные номера КриптоПро CSP, TSP Client и OCSP Client.

> 💡 **Примечание**: у КриптоПро CSP свой пробный период — 90 дней после первой установки. От пробной лицензии КриптоАРМ он не зависит.

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 и установка обновлений.

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

Мало места на системном диске

Во время некоторых операций — подписи с шифрованием, расшифрования, проверки присоединённой подписи — КриптоАРМ записывает промежуточные файлы во временную папку Windows. Места им нужно примерно столько же, сколько занимают обрабатываемые файлы. Временная папка находится в профиле пользователя на диске `C:`, где бы ни было установлено приложение, поэтому при небольшом диске `C:` и крупных файлах её стоит перенести на другой диск.

1. Откройте командную строку (`cmd`) под той учётной записью, в которой работаете с КриптоАРМ, и выполните команды, заменив `D:` на нужный диск:

```
mkdir "D:\Temp\%USERNAME%"
icacls "D:\Temp\%USERNAME%" /inheritance:r /grant:r "%USERDOMAIN%\%USERNAME%:(OI)(CI)F"
*S-1-5-18:(OI)(CI)F *S-1-5-32-544:(OI)(CI)F
setx TEMP "D:\Temp\%USERNAME%"
setx TMP "D:\Temp\%USERNAME%"
```

Команда `icacls` оставляет доступ к папке только вам, системе и администраторам — как у временной папки в профиле. Это важно: туда попадают расшифрованные файлы.

1. Выйдите из системы и войдите снова.

Новая временная папка действует для всех программ этой учётной записи. Другим пользователям компьютера переменные задаются отдельно — каждому под своей учётной записью.

Удаление КриптоАРМ

1. Откройте **Параметры Windows** → **Приложения** (или **Панель управления** → **Программы и компоненты**).
2. Найдите в списке **КриптоАРМ Подпись и шифрование** и нажмите **Удалить**.

Удаление данных приложения

Каталог данных приложения при удалении сохраняется. Если он больше не нужен, удалите его вручную:

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

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

Смотрите также

- Активация лицензий — 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

Установка КриптоАРМ на Linux

Инструкция описывает установку КриптоАРМ и КриптоПро CSP на Linux из пакетов `.deb` и `.rpm`, обновление и удаление приложения.

Содержание:

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

Подготовка к установке

Требования

Для установки нужны права суперпользователя (`root`) или возможность выполнять команды через `sudo`.

Скачивание установочных файлов

Дистрибутив КриптоАРМ

Скачайте пакет с одного из сайтов:

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

Выберите пакет для своего 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

КриптоПро CSP нужен только для операций с алгоритмами ГОСТ. КриптоАРМ поддерживает КриптоПро CSP версии 5.0 и выше.

Скачайте дистрибутив для своей системы на сайте КриптоПро. Для скачивания нужно зарегистрироваться на сайте и принять лицензионное соглашение.

Для подписей со штампом времени и усовершенствованной подписи нужны также модули TSP и OCSP. В дистрибутив КриптоПро CSP они не входят — скачайте КриптоПро ЭЦП SDK для Linux.

Установка КриптоАРМ

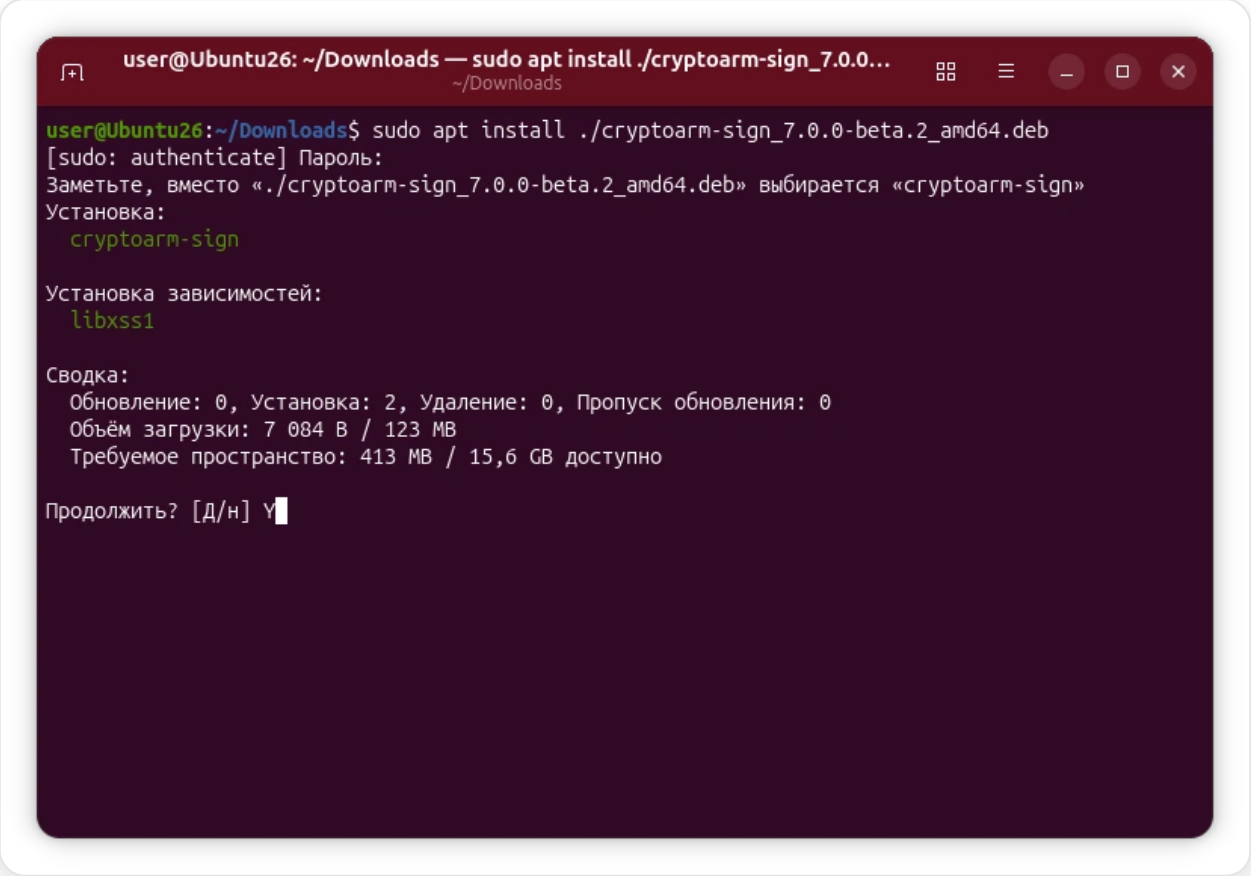
Установка DEB-пакета

Через терминал

1. Выполните в терминале команду, указав путь к пакету (`./` — текущая папка):

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

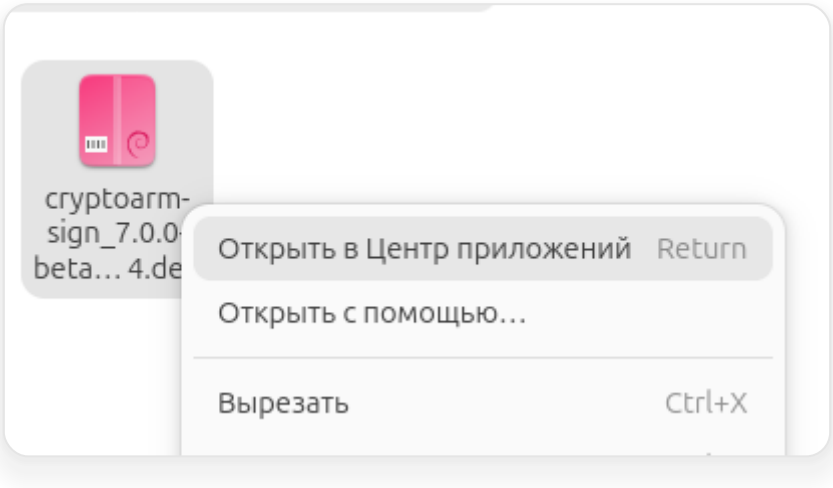
1. Введите пароль администратора, а когда `apt` покажет список устанавливаемых пакетов — подтвердите установку: `Д` (`Y`) и **Enter**.



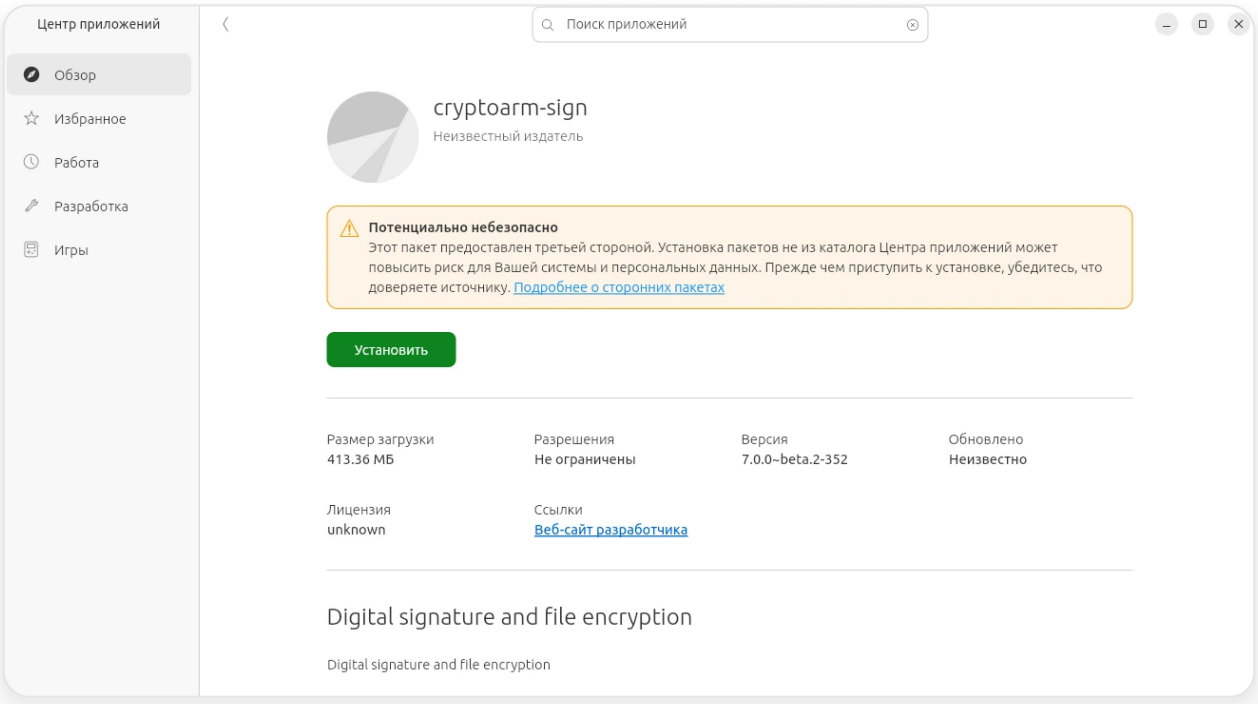
> 💡 **Примечание**: `apt` устанавливает пакет вместе с недостающими зависимостями. Команда `sudo dpkg -i` тоже установит приложение, но зависимости придётся доустанавливать отдельно командой `sudo apt install -f`.

Через графический интерфейс

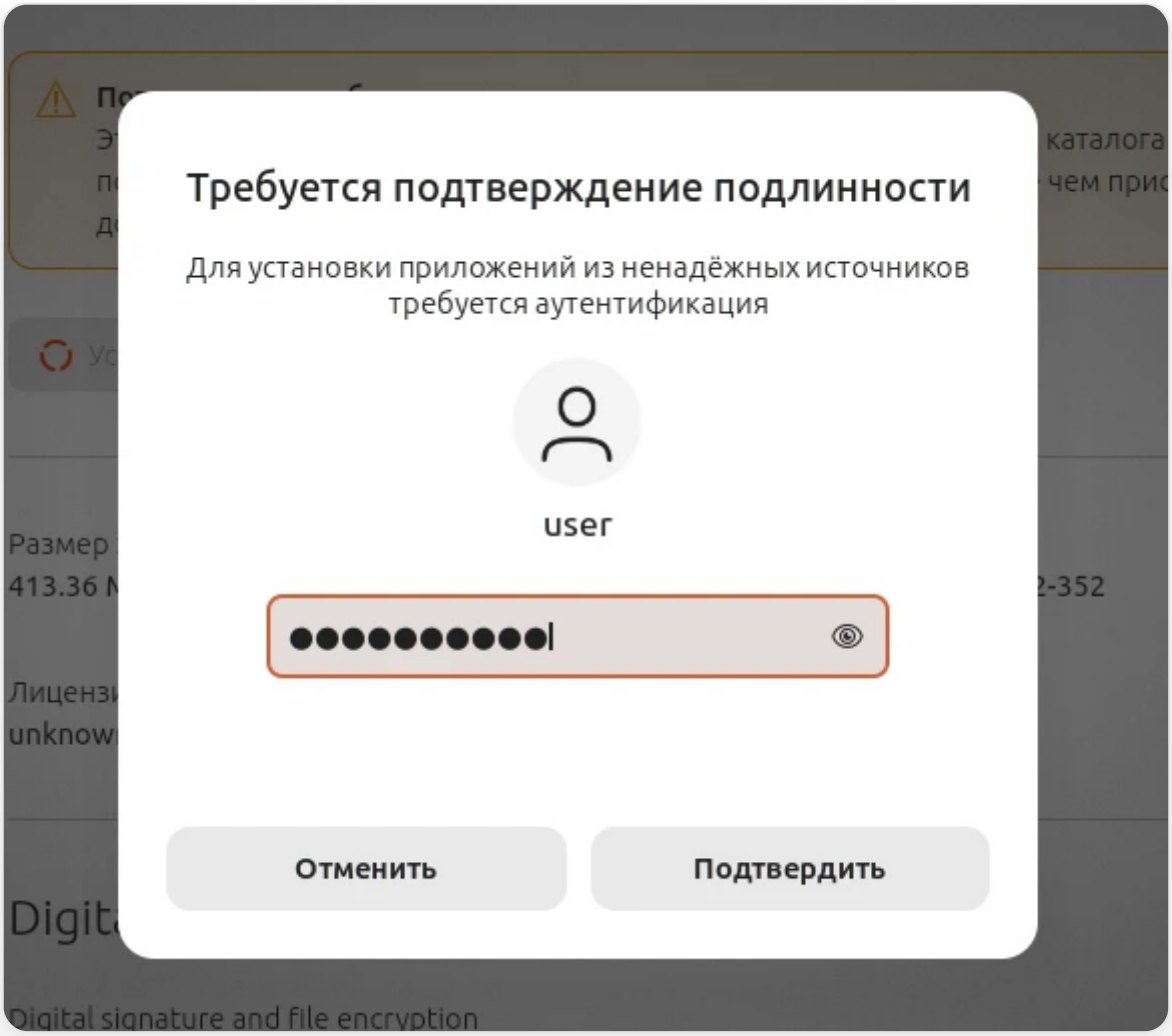
1. Дважды щёлкните по файлу `.deb` или откройте его через установщик пакетов — например, в Ubuntu это Центр приложений.



1. Нажмите **Установить**.



1. При необходимости укажите пароль администратора.



Установка RPM-пакета

Через терминал

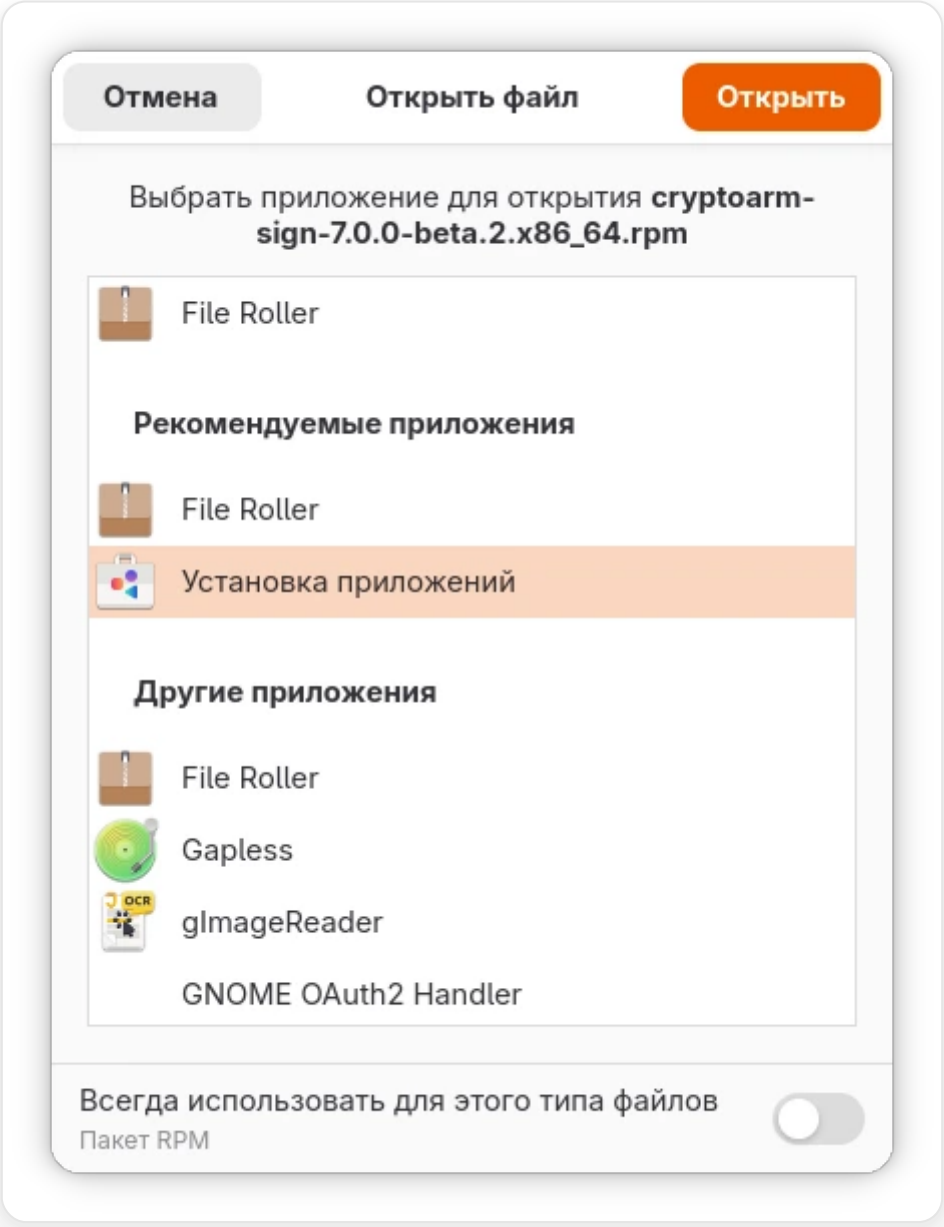
Выполните в терминале команду для своей системы, указав путь к пакету (`./` — текущая папка):

```
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
```

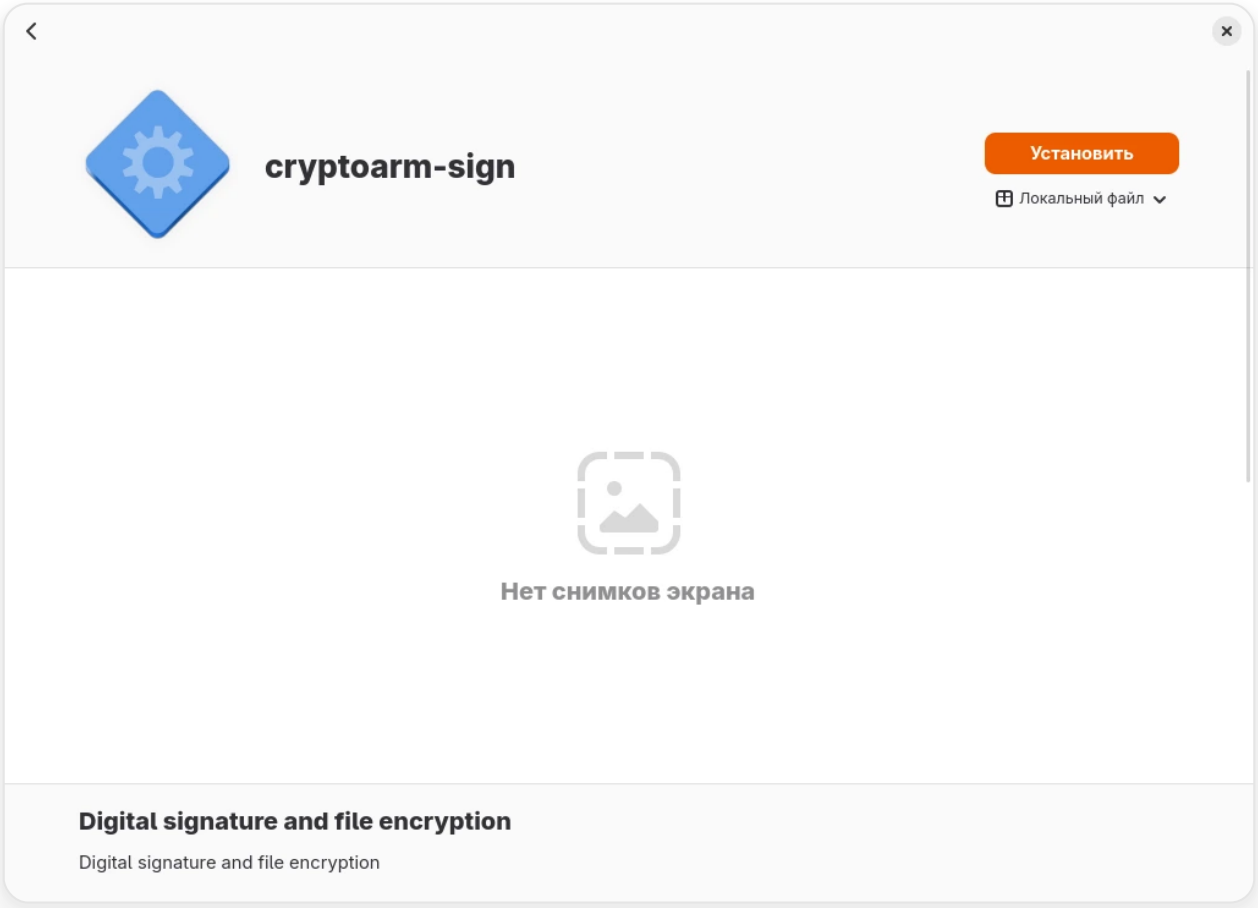
> 💡 **Примечание**: если менеджера пакетов в системе нет, пакет ставится командой `sudo rpm -i ./cryptoarm-sign-<версия>.x86_64.rpm`. Она не подтягивает зависимости: при сообщении о недостающих библиотеках установите их средствами дистрибутива и повторите команду.

Через графический интерфейс

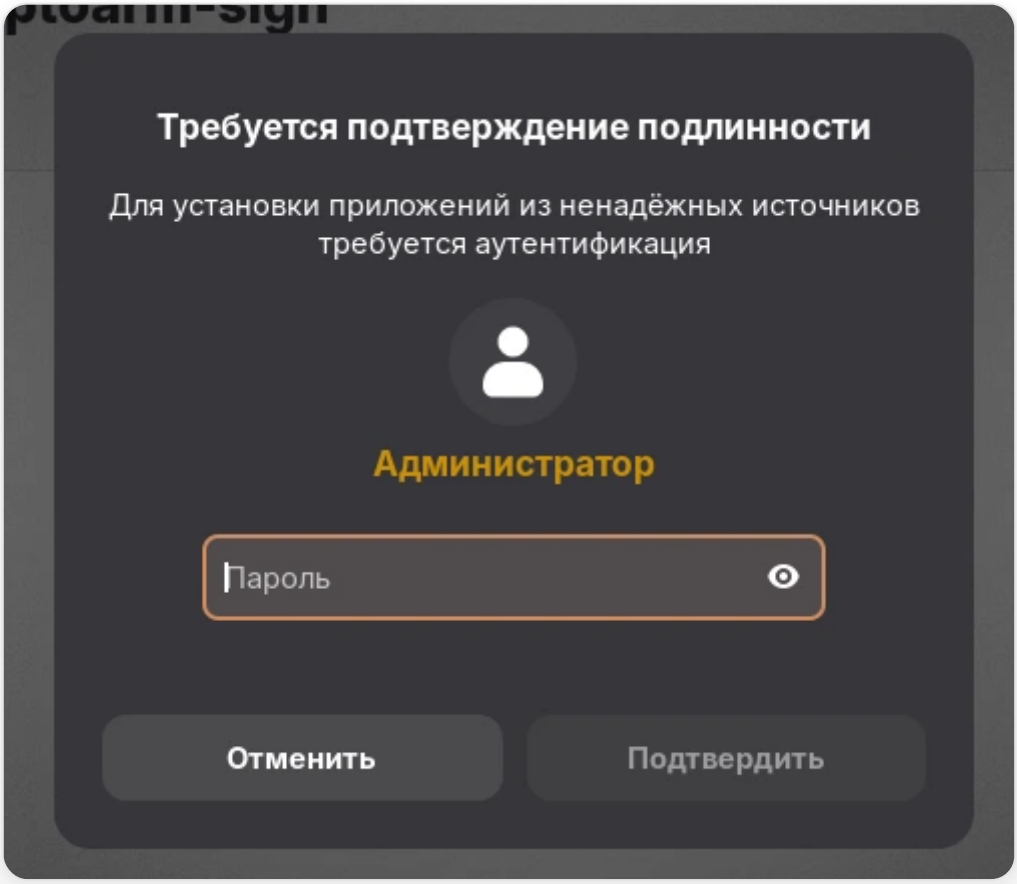
1. Откройте установочный файл `.rpm` через установщик пакетов — например, в Альт это «Установка приложений».



1. Нажмите **Установить**.



1. При необходимости укажите пароль администратора.



После установки

Приложение устанавливается в каталог `/opt/cryptoarm-sign/` и появляется в меню системы под именем **КриптоАРМ Подпись и шифрование**. Запустить его можно и из терминала:

```
cryptoarm-sign
```

Установка КриптоПро CSP

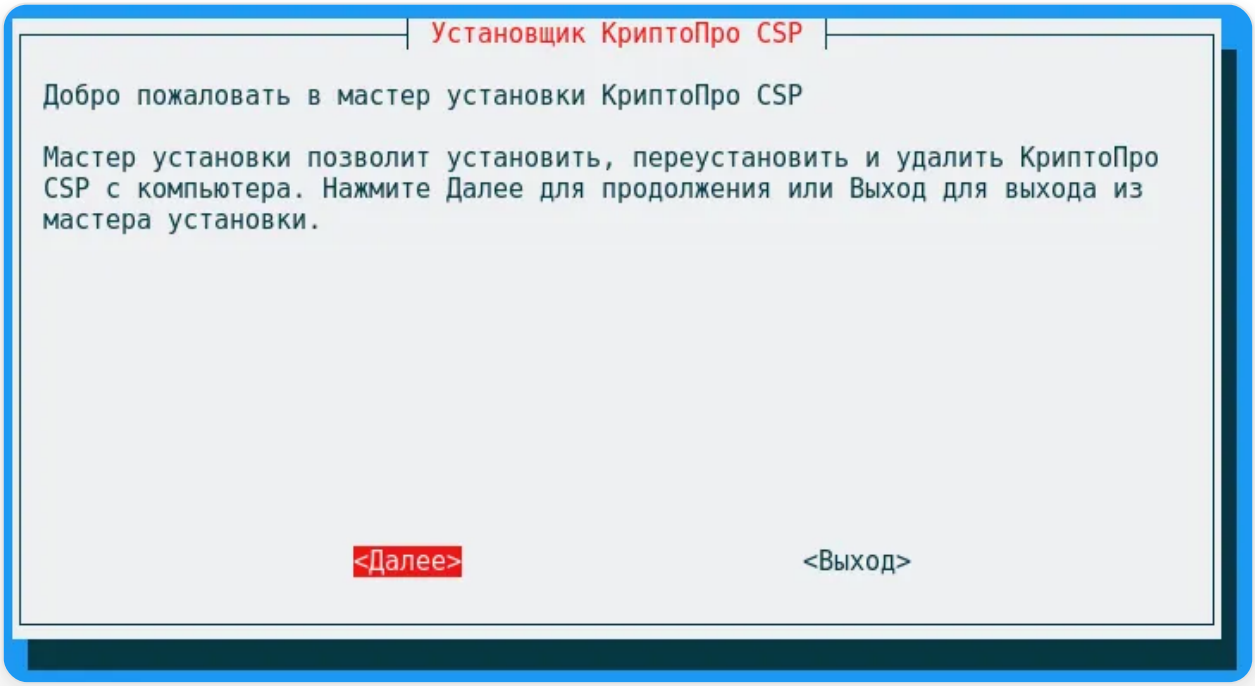
1. Распакуйте архив `.tgz` — в файловом менеджере (правая кнопка мыши → **Распаковать в эту папку** или **Извлечь здесь**) или в терминале:

```
tar -xzf <архив>.tgz
```

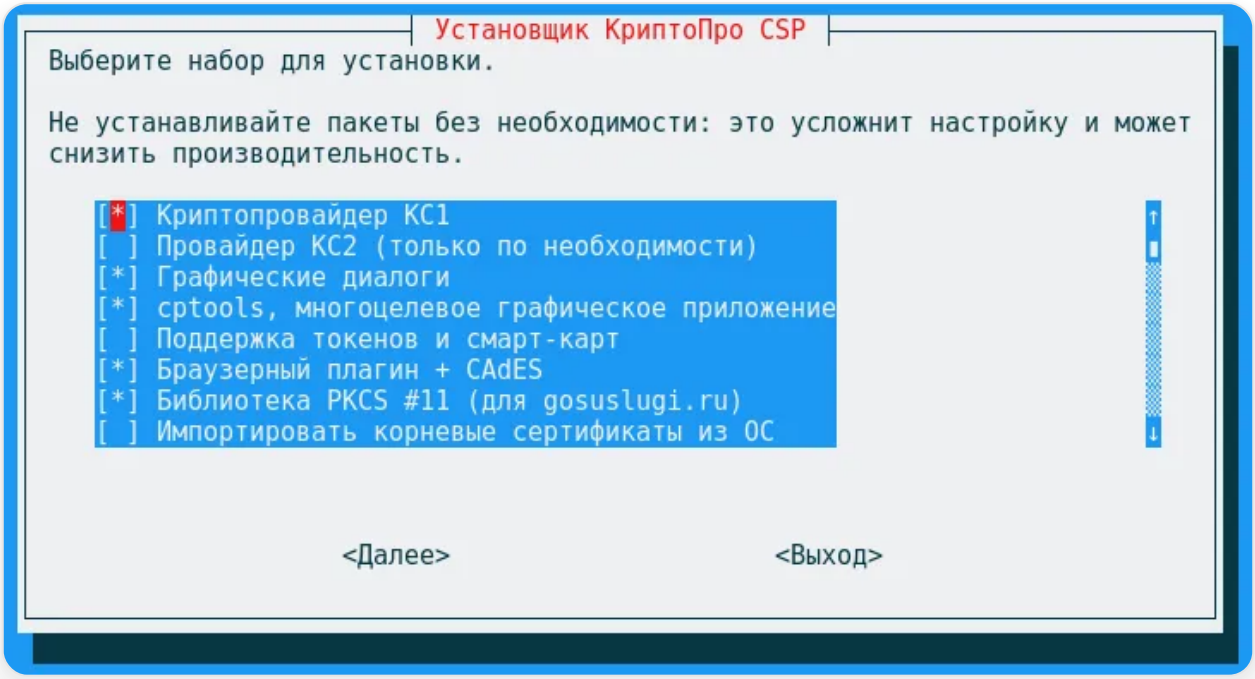
1. Запустите установщик из распакованного каталога с правами суперпользователя:

```
sudo <путь>/install_gui.sh # графический установщик
sudo <путь>/install.sh     # установка в терминале
```

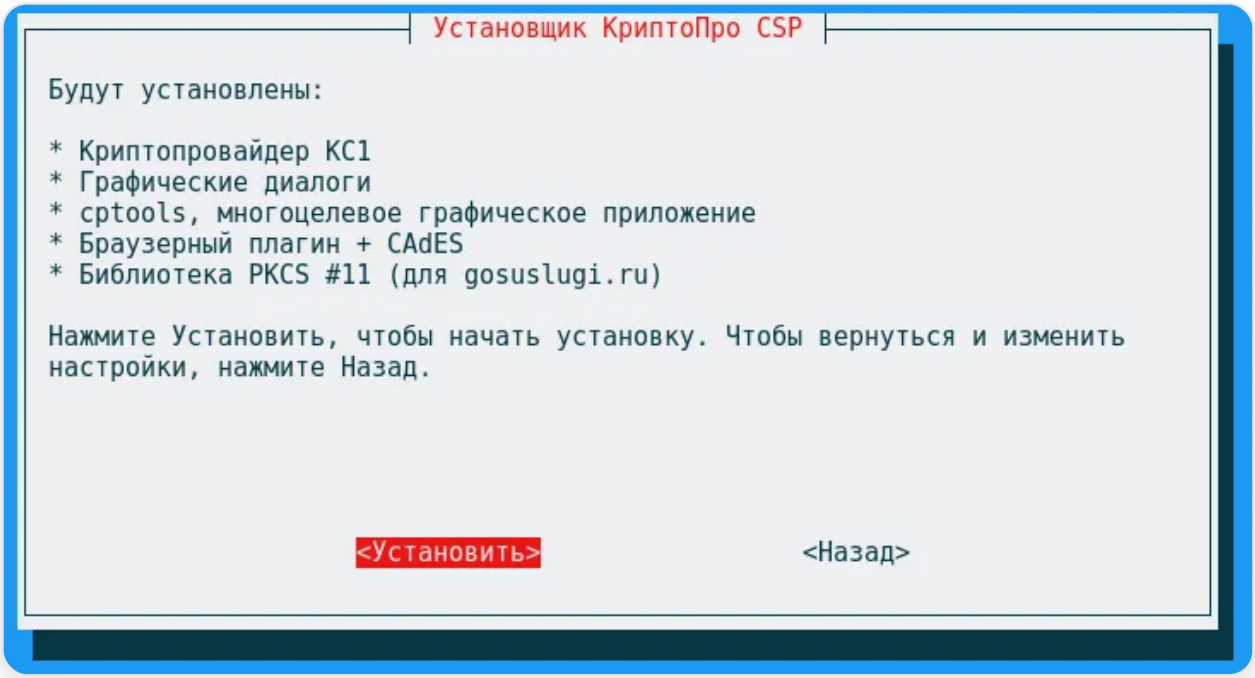
1. Если запущена графическая установка, нажмите **Далее** в открывшемся окне.



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



1. Подтвердите установку и дождитесь её окончания.



> 💡 **Примечание**: по умолчанию CSP устанавливается в `/opt/cprocsp/`.

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

> 💡 **Примечание**: в графическом установщике окно ввода пароля и поддержка ключевых носителей выбираются на шаге 4 — пункты «Графические диалоги» и «Поддержка токенов и смарт-карт». Команды ниже нужны при установке в терминале и приведены для систем с пакетами `.deb`.

Установка пакета для окна ввода пароля

Чтобы пароль контейнера закрытого ключа запрашивался в графическом окне, установите пакет:

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

Установка пакетов для работы с ключевыми носителями

> ⚠️ **Важно**: для работы с ключевыми носителями в системе должны быть установлены библиотека `libccid` версии 1.3.11 или выше и пакеты `pcscd` и `libpcsclite1`.

1. Установите пакет поддержки считывателей:

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

1. Для ключевого носителя **Рутокен**:

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

1. Для ключевого носителя **JaCarta**:

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

1. Для ключевого носителя **ESMART**:

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

Установка модулей TSP и OCSP

Модули нужны для подписей со штампом времени и усовершенствованной подписи. Для обычной подписи они не требуются.

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

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

Установка лицензий КриптоПро через терминал

> 💡 **Примечание**: установить лицензии можно и в приложении — см. Лицензии КриптоПро.

1. Установите лицензию КриптоПро CSP:

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

1. Установите лицензию модуля TSP:

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

1. Установите лицензию модуля OCSP:

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

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

Активация лицензий

При первом запуске КриптоАРМ действует пробная лицензия на 30 дней. Чтобы работать с алгоритмами ГОСТ после её окончания, активируйте лицензии:

- Лицензия КриптоАРМ — лицензионный ключ приложения;
- Лицензии КриптоПро — серийные номера КриптоПро CSP, TSP Client и OCSP Client.

> 💡 **Примечание**: у КриптоПро CSP свой пробный период — 90 дней после первой установки. От пробной лицензии КриптоАРМ он не зависит.

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 и установка 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

```
sudo apt remove cryptoarm-sign
```

RPM-пакеты

```
sudo apt-get remove cryptoarm-sign # Альт
sudo dnf remove cryptoarm-sign     # РЕД ОС, РОСА и другие системы с dnf
sudo rpm -e cryptoarm-sign         # если менеджера пакетов нет
```

Удаление данных приложения

Каталог данных приложения при удалении сохраняется. Если он больше не нужен, удалите его вручную:

```
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 лицензий — 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

Установка КриптоАРМ на macOS

Инструкция описывает установку КриптоАРМ и КриптоПро CSP на macOS 14 (Sonoma) и выше, обновление и удаление приложения.

Содержание:

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

Скачивание установочных файлов

Дистрибутив КриптоАРМ

Скачайте образ диска с одного из сайтов:

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

Образов `.dmg` 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 Apple → **Об этом Mac**.

Дистрибутив КриптоПро CSP

КриптоПро CSP нужен только для операций с алгоритмами ГОСТ. КриптоАРМ поддерживает КриптоПро CSP версии 5.0 и выше.

Скачайте дистрибутив для своей системы на сайте КриптоПро. Для скачивания нужно зарегистрироваться на сайте и принять лицензионное соглашение.

Для подписей со штампом времени и усовершенствованной подписи нужны также модули TSP и OCSP. В дистрибутив КриптоПро CSP они не входят — скачайте КриптоПро ЭЦП SDK для macOS.

Установка КриптоАРМ

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



1. Извлеките образ в боковой панели Finder.
2. Запустите приложение из папки **Программы** или через Launchpad.

> 💡 **Примечание**: приложение подписано и заверено Apple, поэтому macOS не предупреждает о неизвестном разработчике.

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 щелчком.
3. Запустите установочный пакет `.pkg` двойным щелчком.
4. Если появится предупреждение «Программа загружена из интернета», выберите **Открыть**.

5. Нажмите **Продолжить**, ознакомьтесь с лицензией и примите условия.
6. Выберите нужные пакеты и нажмите **Продолжить → Установить**.

> 💡 **Примечание**: по умолчанию CSP устанавливается в `/Applications/CryptoPro_ECP.app`. Если вы выбрали другой каталог, подставляйте его в команды терминала ниже.

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

Установка модулей TSP и OCSP

Модули нужны для подписей со штампом времени и усовершенствованной подписи. Для обычной подписи они не требуются.

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

Активация лицензий на модули TSP и OCSP через терминал

> 💡 **Примечание**: проще активировать лицензии в КриптоАРМ — см. Лицензии КриптоПро. Терминал нужен, только если графический интерфейс недоступен.

1. Выполните в терминале команды, подставив свои серийные номера:

```
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>
```

1. Введите пароль пользователя macOS.
2. Проверьте статус лицензий:

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

Активация лицензий

При первом запуске КриптоАРМ действует пробная лицензия на 30 дней. Чтобы работать с алгоритмами ГОСТ после её окончания, активируйте лицензии:

- Лицензия КриптоАРМ — лицензионный ключ приложения;
- Лицензии КриптоПро — серийные номера КриптоПро CSP, TSP Client и OCSP Client.

> 💡 **Примечание**: у КриптоПро CSP свой пробный период — 90 дней после первой установки. От пробной лицензии КриптоАРМ он не зависит.

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 и установка 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

1. Завершите КриптоАРМ сочетанием `⌘ + Q`.
2. Откройте папку **Программы**.
3. Перетащите **КриптоАРМ Подпись и шифрование** (`CryptoARM Sign and Encrypt.app`) в **Корзину**.

Удаление данных приложения

Данные приложения при удалении сохраняются. Если они больше не нужны, удалите их вручную:

1. Откройте **Finder** → **Переход** → **Переход к папке...** (или `⇧ + ⌘ + G`).
2. Открывайте по очереди и удаляйте:

- `~/Library/Application Support/cryptoarm-sign` — настройки, журнал, логи и база сертификатов и ключей OpenPGP;
- `~/Library/Preferences/ru.cryptoarm.sign.plist` — параметры окна;
- файлы быстрых действий в `~/Library/Services` — команды «Проверить и расшифровать», «Открыть для...» и профили. Удалять их вручную не обязательно: они исчезнут сами, когда вы впервые выберете такую команду после удаления приложения.

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

Смотрите также

- Активация лицензий — 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

Активация лицензий КриптоАРМ и КриптоПро

Лицензии **КриптоАРМ**, **КриптоПро CSP** и модулей **TSP Client** и **OCSP Client** активируются в приложении КриптоАРМ. Здесь же описано, как перенести лицензию КриптоАРМ на другой компьютер и где посмотреть состояние лицензий.

Содержание:

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

Лицензия КриптоАРМ

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

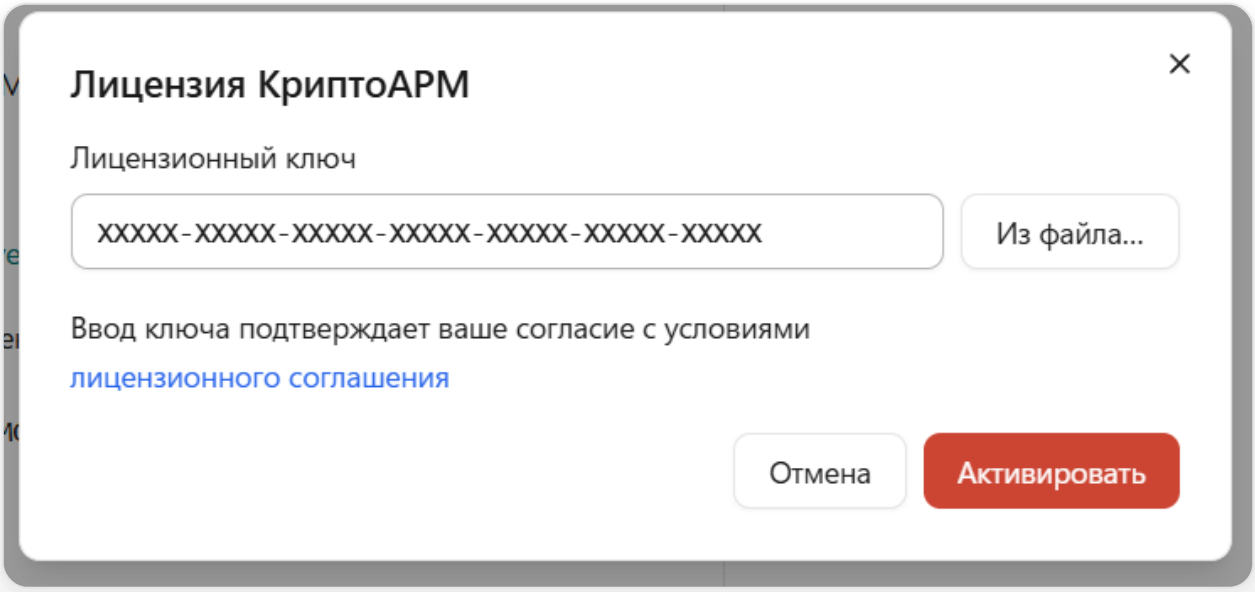
Приложению подходят ключи двух версий КриптоАРМ: **Подпись и шифрование** и **«Защищенная почта»**.

Если ключ уже установлен в приложении 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. Откройте **Настройки → 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 можно также загрузить кнопкой **Из файла...**.



1. Нажмите **Активировать**. После активации статус лицензии обновится.

> ⚠️ **Важно**: лицензионные ключи предыдущих версий КриптоАРМ не подходят. При вводе такого ключа приложение сообщит: «Ваш лицензионный ключ от версии ..., он не подходит к текущей версии». Обновление лицензии можно купить в интернет-магазине.
>
> ⚠️ **Важно**: на серверных операционных системах нужна серверная лицензия: клиентская на них не активируется.

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 другой компьютер

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

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

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

Затем активируйте лицензию на новом компьютере.

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

Лицензии КриптоПро

Лицензия КриптоАРМ не заменяет лицензии КриптоПро: серийные номера **КриптоПро CSP**, **КриптоПро TSP Client** и **КриптоПро OCSP Client** устанавливаются отдельно. Все три вводятся в КриптоАРМ.

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. Откройте **Настройки → Криптопровайдеры** и выберите **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. После установки статус лицензии обновится.

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

Сообщение	Что это значит	Что сделать
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
Лицензия записана, но её действие не удалось подтвердить	Провайдер не подтвердил установленную лицензию	Перезапустите приложение и проверьте статус
Компонент управления лицензиями КриптоПро недоступен	Приложение не может установить лицензию на этом компьютере	Установите лицензию средствами КриптоПро — например, через терминал

Активация лицензии на модули TSP и OCSP

Серийные номера модулей вводятся так же, как номер КриптоПро CSP, — кнопкой **Ввести ключ** в карточке **КриптоПро TSP Client** или **КриптоПро OCSP Client**.

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 вне приложения

Лицензии КриптоПро можно установить и без КриптоАРМ — в приложении **Инструменты КриптоПро** или в терминале:

- Linux: установка лицензий КриптоПро через терминал
- macOS: активация лицензий на модули TSP и OCSP через терминал

Терминал нужен, только если графический интерфейс недоступен.

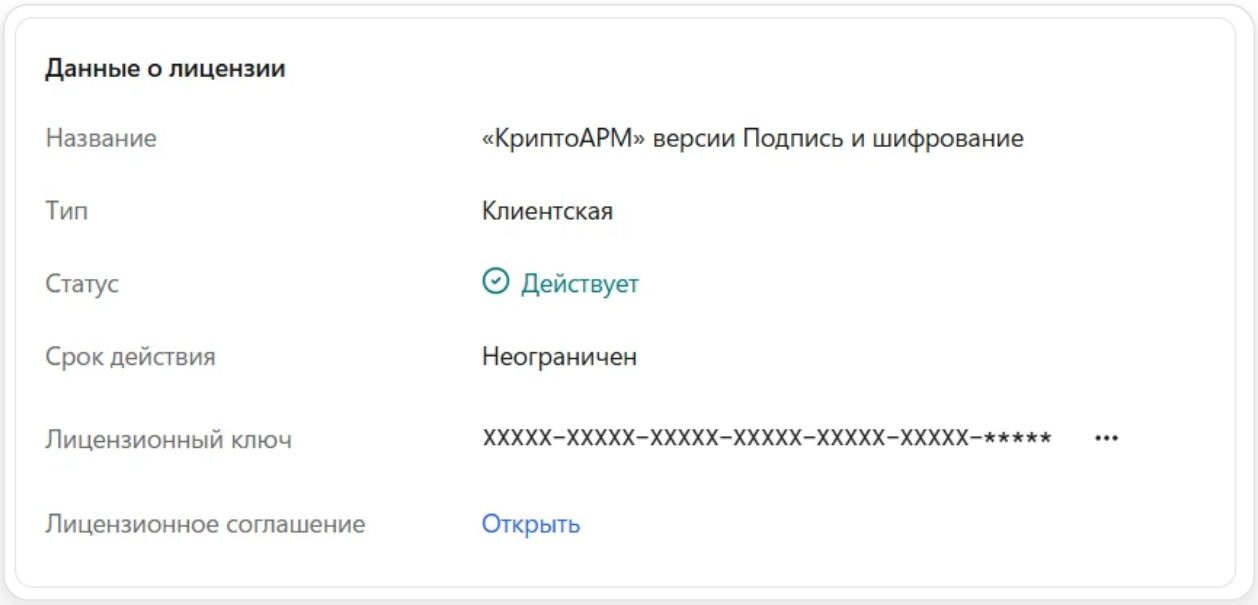
Проверка статуса лицензии

КриптоАРМ

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

Поле	Значение
Название	Продукт, для которого выдан ключ
Тип	«Клиентская» — для рабочих мест; «Серверная» — для серверных операционных систем

Поле	Значение
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. Статус **«Другая редакция»** означает, что ключ действителен, но выдан для другого продукта КриптоАРМ и этому приложению не подходит. При статусах **«Скомпрометирована»** и **«Ошибка проверки»** обратитесь в техническую поддержку support@trusted.ru.

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.

Статус **«Не удалось определить»** означает, что приложение не смогло прочитать сведения о лицензии. На выполнение операций это не влияет.

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.
- 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

Быстрый старт

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.

Ниже — как добавить сертификат, подписать и проверить документ и зашифровать файл для получателя.

Содержание:

- Подготовка сертификатов
- Работа с документами
- Работа по стандарту OpenPGP
- Если что-то пошло не так
- Что настроить дальше
- Смотрите также

Подготовка сертификатов

Добавьте сертификат 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 приложение	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.

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 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.

Работа по стандарту OpenPGP

OpenPGP — отдельный стандарт со своими ключами; для документооборота по 63-ФЗ не подходит. Выбирайте его, только если так принято у тех, с кем вы обмениваетесь файлами.

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 сертификаты других пользователей и при необходимости заверьте их.
5. Подписывайте и шифруйте файлы в том же разделе **Подпись и шифрование** — см. Особенности OpenPGP.

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.
- Контекстное меню Проводника, быстрые действия Finder и меню файлового менеджера Linux — подписывать файлы, не открывая приложение.
- 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 и установка обновлений.

Смотрите также

- Общие настройки — тема, язык, поведение окна.
- Интерфейс приложения — как устроено окно и вкладки.
- Установка сертификатов — из контейнера, из файла и вместе с закрытым ключом.
- Обзор операций и выбор раздела — какой раздел выбрать под задачу.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

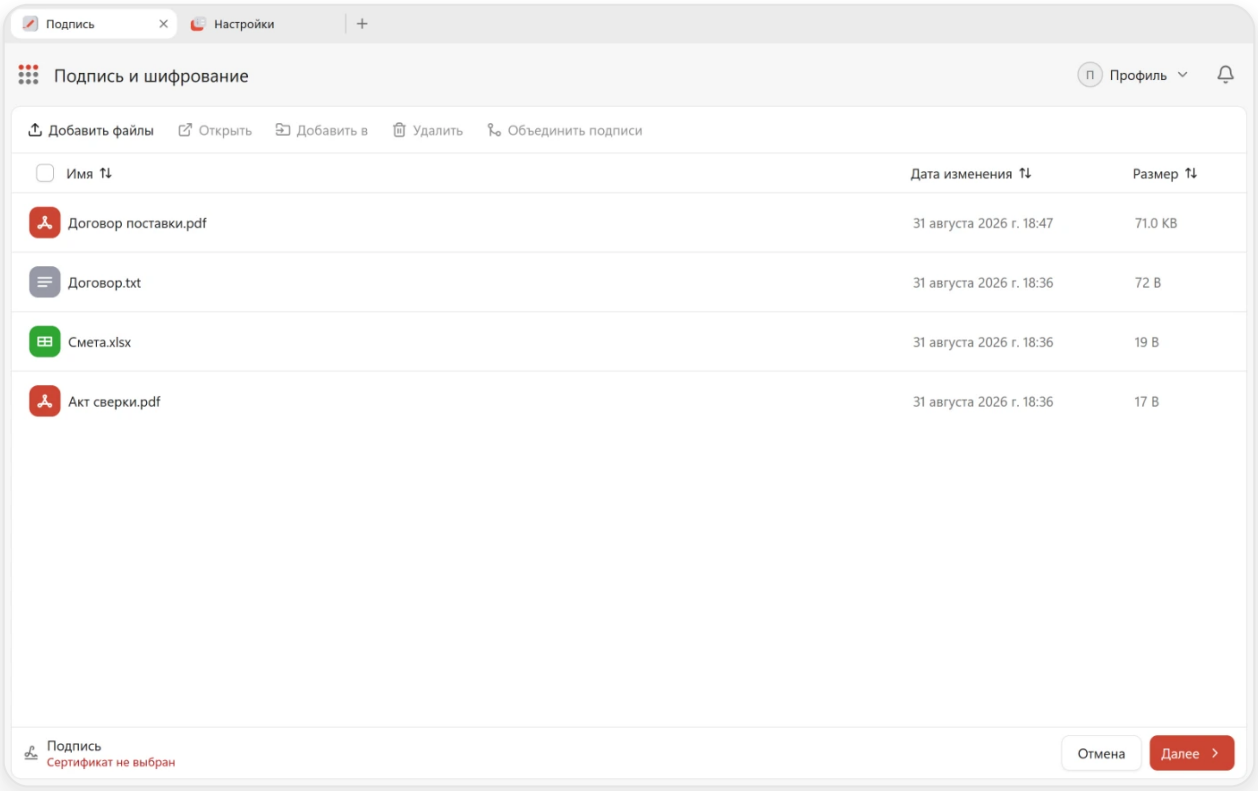
Интерфейс КриптоАРМ

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

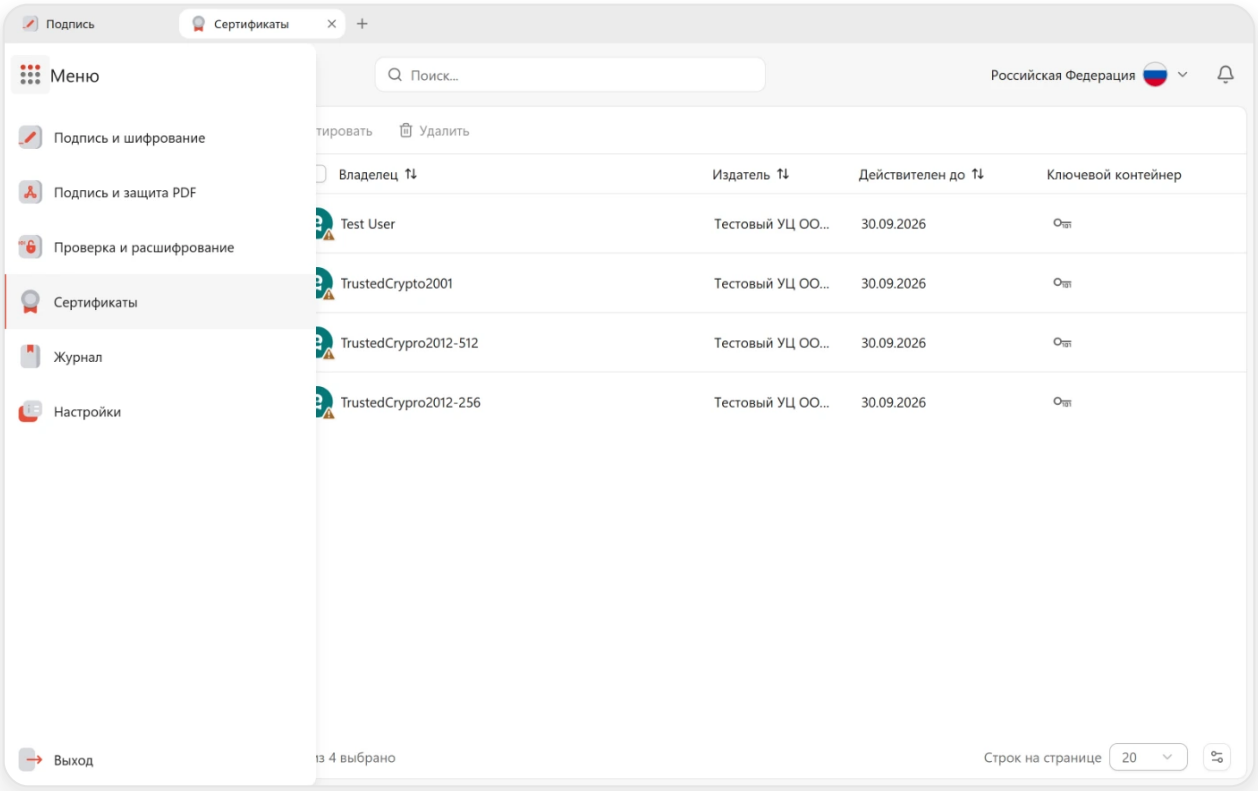
Из чего состоит окно



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.
- **Закрытие** — крестик на вкладке; закреплённую вкладку закрывает команда **«Закрыть вкладку»** в контекстном меню.
- **Прокрутка** — стрелки по краям строки, когда вкладок больше, чем помещается.
- **Закрепление** — команда **«Закрепить вкладку»** в контекстном меню вкладки. Закрепить можно вкладку любого раздела из бокового меню. Закреплённая вкладка сжимается до значка в начале строки, не закрывается вместе с остальными и открывается снова при следующем запуске — без выбранных ранее файлов.

Контекстное меню вкладки (правая кнопка мыши) содержит также команды **Открепить вкладку**, **Закрыть другие вкладки**, **Закрыть вкладки справа** и **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.

В разделе **Сертификаты** строка поиска очищается при переходе от одного списка к другому: в каждом списке поиск идёт по своим 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 скрыть нельзя. Настройки запоминаются для каждой таблицы отдельно.

Центр уведомлений

Кнопка с колокольчиком открывает центр уведомлений. В нём собраны ошибки и предупреждения, которые вы могли пропустить. Отсюда же открывается журнал — полный список 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**, **Настройки** и **Выход**. Подробнее — в разделе Сворачивание в трей при закрытии окна.

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**. Здесь описаны вкладка **Общие** и две настройки вкладки **Криптопровайдеры** — стандарт операций и проверка флага keyAgreement.

Лицензии описаны в инструкции Активация лицензий, обновления — в инструкции Проверка и установка обновлений.

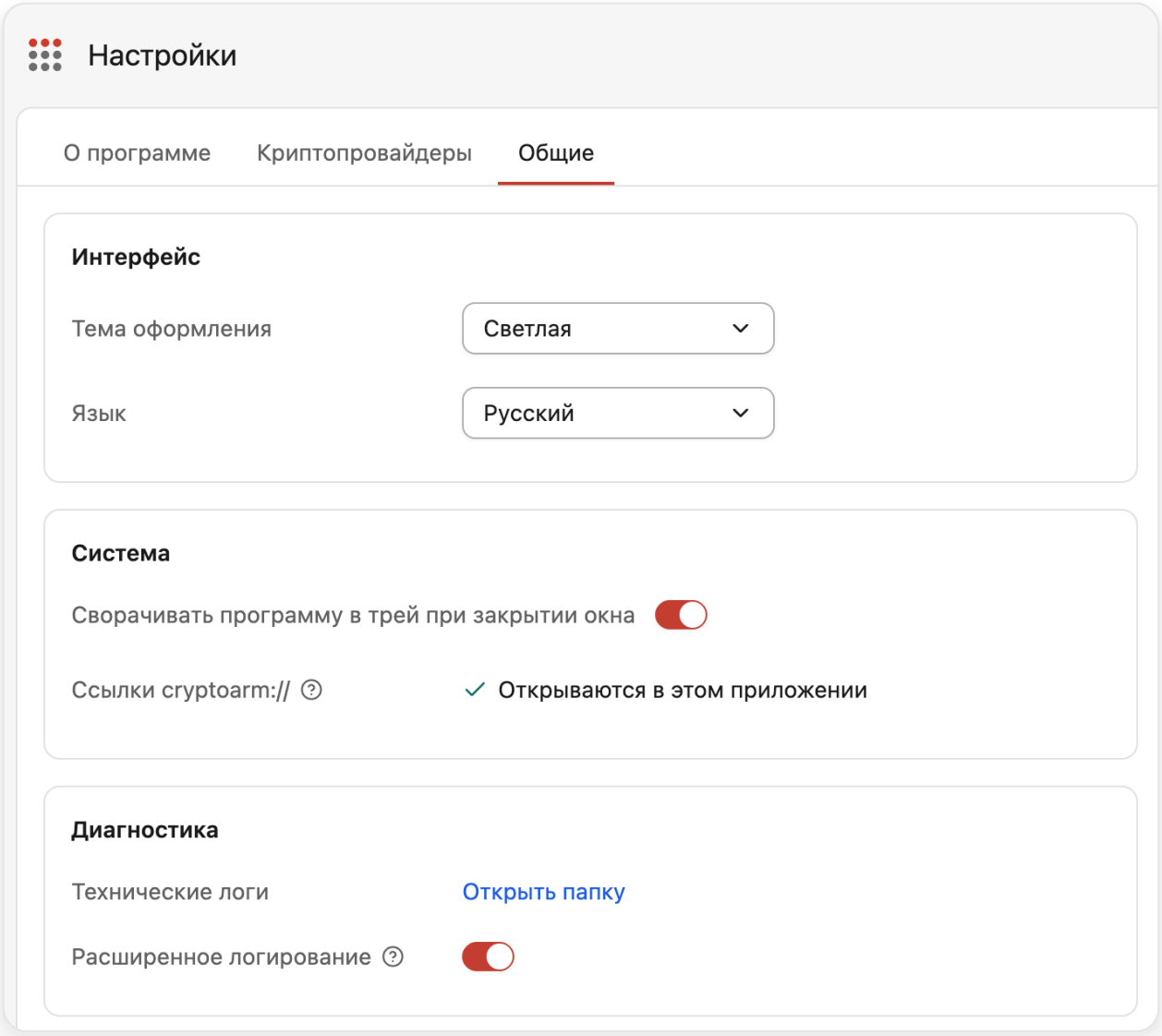
Содержание:

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

По умолчанию выбран пункт **Как в системе**: при каждом запуске приложение берёт первый язык из списка предпочитаемых языков системы, который оно поддерживает, а если такого нет — русский. В скобках рядом с пунктом показан язык, который получился.

Список предпочитаемых языков настраивается в системе:

- Windows — **Параметры → Время и язык → Язык и регион → Предпочитаемые языки**;
- macOS — **Системные настройки → Основные → Язык и регион**;
- Linux — в параметрах языка рабочего стола.

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, а его значок остаётся в области уведомлений;
- **выключена** — закрытие окна завершает работу приложения.

Свёрнутым приложением управляют через значок в области уведомлений:

- **Развернуть окно** — щёлкните по значку;
- **Открыть настройки** — щёлкните по значку правой кнопкой и выберите **Настройки**;
- **Завершить работу** — щёлкните по значку правой кнопкой и выберите **Выход**.

На macOS меню значка открывается обычным щелчком; чтобы развернуть окно, выберите в нём **Открыть**.

С включённой настройкой операции из контекстного меню Проводника выполняются быстрее: приложение уже загружено.

Технические логи

Приложение ведёт служебные записи о своей работе. Они нужны только технической поддержке при разборе неполадок; персональных данных и путей к вашим файлам в них нет.

Блок **Диагностика** на вкладке **Общие** содержит:

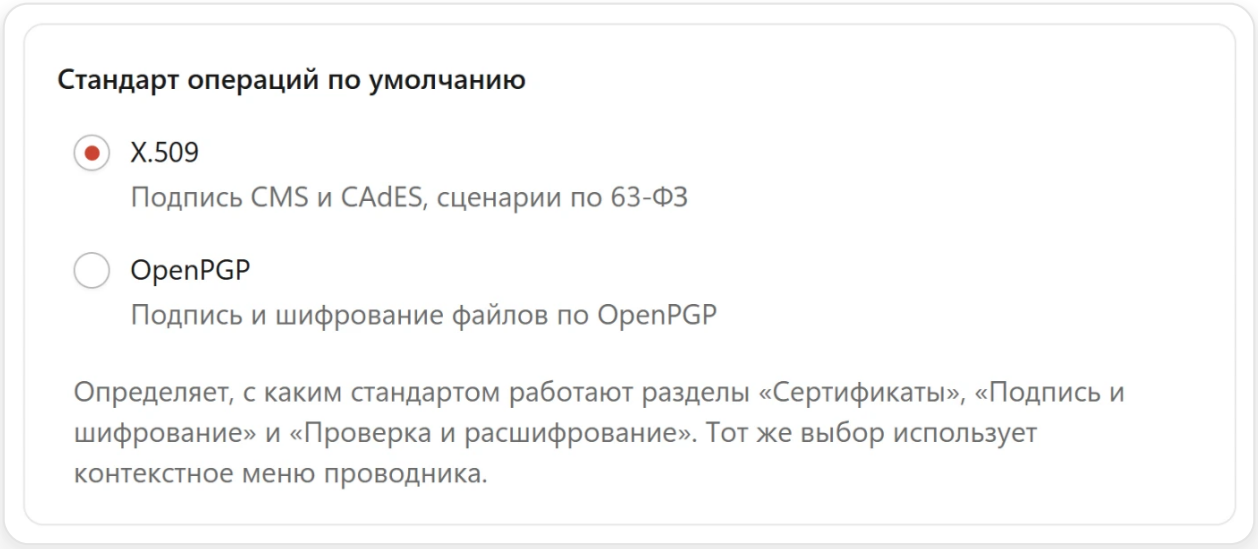
- строку **Технические логи** с кнопкой **Открыть папку** — она открывает каталог с файлами, которые просит прислать поддержка;
- переключатель **Расширенное логирование**.

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

Стандарт операций по умолчанию

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

- **X.509** — подпись CMS и CAdES, документооборот 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

Настройка **Проверять флаг keyAgreement** определяет, какие сертификаты получателей подходят для шифрования. Флаг keyAgreement в сертификате разрешает использовать его для обмена ключами.

- **включена** — шифровать можно только на сертификатах с флагом keyAgreement;
- **выключена** — подходят и сертификаты без него, если в них есть флаг keyEncipherment.

По умолчанию проверка выключена. Включайте её, если этого требует регламент организации.

Чтобы включить проверку:

1. Откройте **Настройки → Криптопровайдеры** и выберите **КриптоПро CSP**.
2. В блоке **Дополнительно** включите **Проверять флаг keyAgreement**.

> ⚠️ **Важно**: настройка действует только для КриптоПро CSP.

Смотрите также

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

Открыть статью на сайте

Уведомления и журнал событий

Уведомления сообщают о результате операции сразу, центр уведомлений хранит пропущенные сообщения, а журнал — полную историю событий, которую можно отфильтровать и передать в техническую поддержку.

Содержание:

- Уведомления
- Журнал событий
- Смотрите также

Уведомления

Всплывающие уведомления

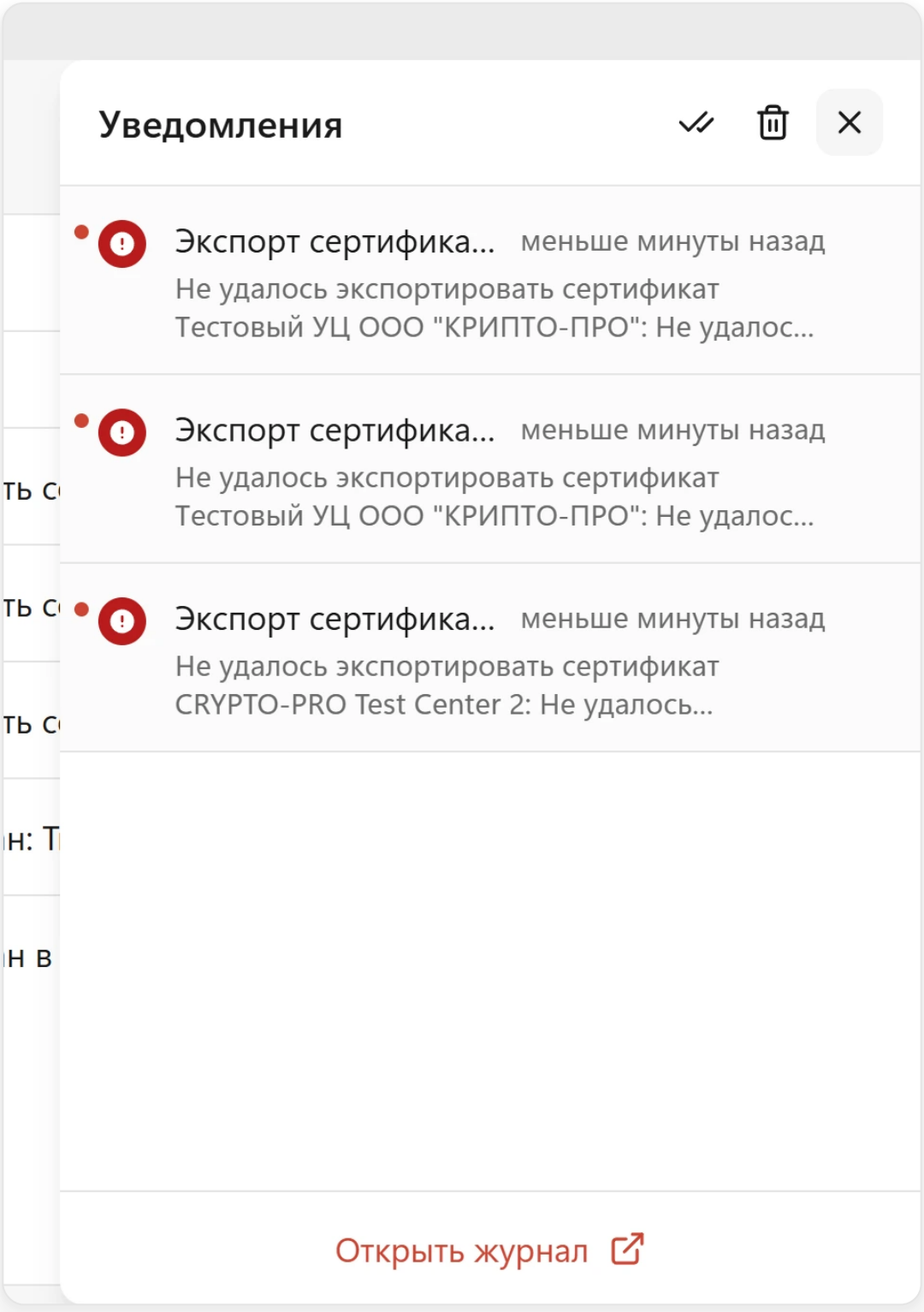
Результат действия показывается всплывающим сообщением в углу окна: «Сертификат успешно импортирован», «Сохранён 1 файл», «Не удалось сохранить файлы».

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.

Всплывающих сообщений нет там, где результат и так виден, — например, в столбце статуса разделов **Подпись и шифрование** и **Проверка и расшифрование**. Событие в любом случае записывается в журнал.

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»**.

В центр уведомлений попадают и напоминания о личных сертификатах, срок действия которых истекает в ближайшие 30 дней, — см. Проверка статуса сертификата.

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

Системные уведомления

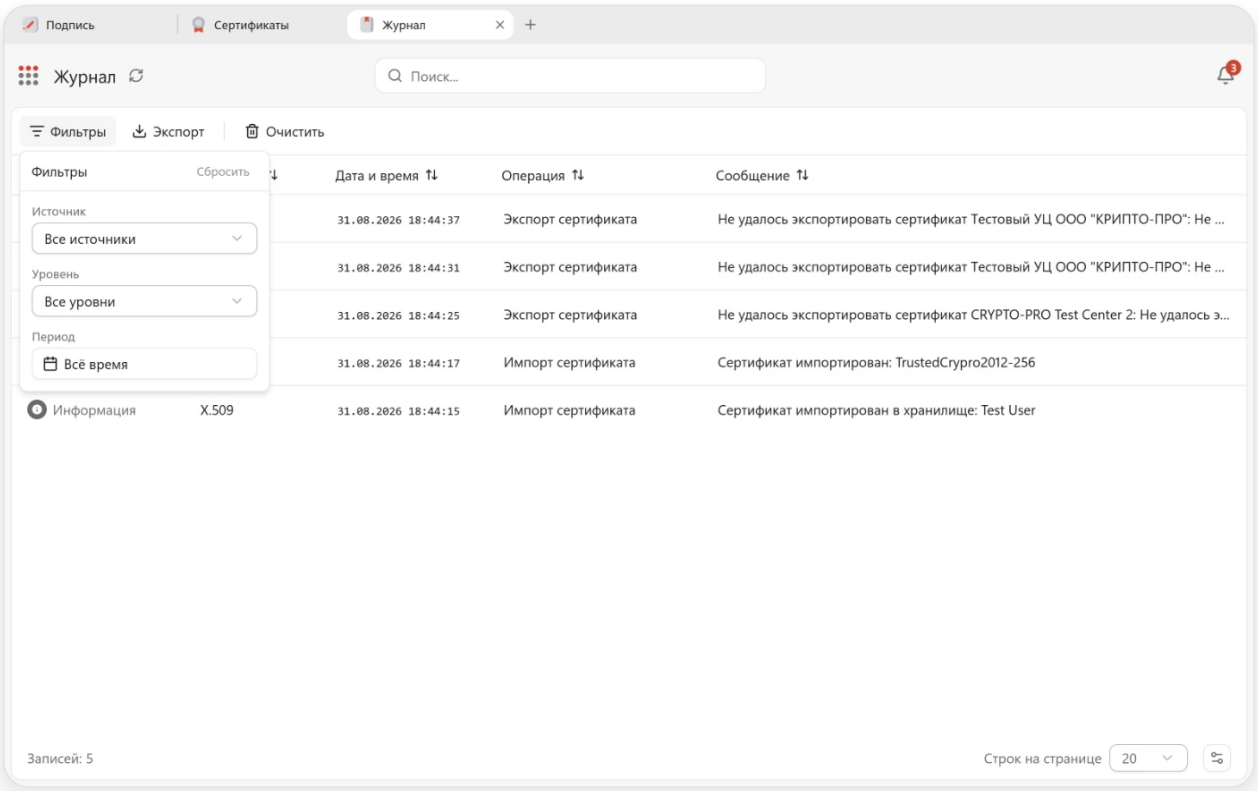
Операции, запущенные из контекстного меню Проводника или быстрых действий Finder, могут выполняться без окна приложения. Об их результате сообщает системное уведомление. Если система уведомления не показывает, ошибки и предупреждения таких операций попадают в центр уведомлений.

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

Журнал событий

В журнал записываются операции и ошибки приложения. Чтобы открыть его, нажмите кнопку **Меню** и выберите раздел **Журнал** — или нажмите **Открыть журнал** в центре уведомлений.

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.

Технические подробности отказов записываются отдельно, для технической 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.

Фильтр	Значения
Период	«Сегодня», «7 дней», «30 дней», «Всё время», «Произвольный период» — укажите даты и 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 экспортируйте журнал.

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

Проверка и установка обновлений

Приложение само проверяет, вышла ли новая версия. Загрузку — в зависимости от режима — и установку запускаете вы.

Содержание:

- Режимы обновления
- Проверка обновлений
- Установка обновления
- Предварительные версии
- Если обновление не находится
- Смотрите также

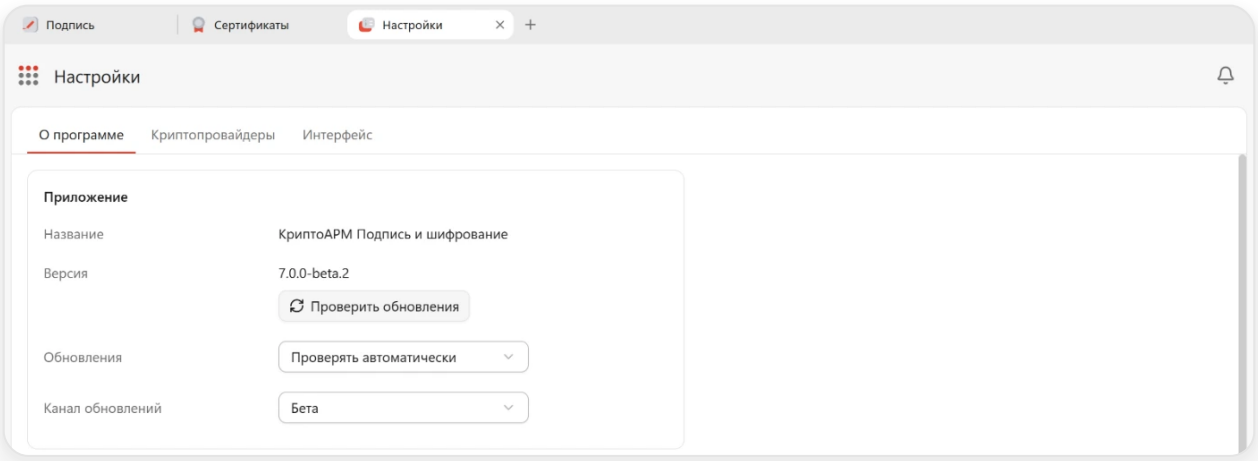
Режимы обновления

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**

Проверка обновлений

Состояние обновлений показано в строке **Версия** раздела **Настройки → О программе**. Чтобы запустить проверку вручную, нажмите там **Проверить обновления**.



Когда найдена новая версия, в правом конце строки вкладок появляется кнопка **«Доступно обновление»**. В режиме «Загружать автоматически» кнопка появляется, когда версия уже скачана, и называется **«Обновление готово»**.

Нажатие на кнопку открывает окно с номером новой версии, датой выпуска и списком изменений. Кнопка **Позже** в этом окне на время скрывает кнопку обновления; само обновление остаётся в разделе **О программе**.

Если загрузка не удалась, на кнопке появляется **«Ошибка обновления»**, а в её окне — кнопка **Проверить обновления**.

Установка обновления

1. Нажмите кнопку **«Доступно обновление»** в строке вкладок, а в её окне — **Скачать**. В разделе **О программе** та же кнопка стоит в строке **«Доступна версия X.Y.Z»**. В режиме «Загружать автоматически» этот шаг приложение делает само.
2. Дождитесь, пока кнопка в строке вкладок сменится на **«Обновление готово»**, а в разделе **О программе** появится строка **«Версия X.Y.Z готова к установке»**.
3. Нажмите **Установить** в окне кнопки или **Установить и перезапустить** в разделе **О программе**.

Приложение закроется, установит новую версию и запустится снова.

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

Предварительные версии

Предварительные версии содержат новые возможности, которые ещё проверяются, и могут работать нестабильно. Для рабочих мест, где важна предсказуемость, оставляйте стабильный канал.

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

- **Стабильный** — обычные выпуски;
- **Бета** — предварительные версии.

Сразу после установки выбран канал установленной версии: у предварительной версии — **Бета**, у обычной — **Стабильный**.

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

Если обновление не находится

Возможная причина	Что сделать
Нет подключения к интернету	Проверьте соединение и повторите проверку
Межсетевой экран или антивирус блокирует доступ к серверу обновлений	Разрешите КриптоАРМ доступ к сети
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
Уже установлена последняя версия	Обновление не требуется; номер версии показан в разделе **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** (в разделе **О программе** — **Установить и перезапустить**) ещё раз и подтвердите запрос системы

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

Если ничего не помогло, обратитесь в техническую поддержку: support@trusted.ru.

Смотрите также

- Общие настройки — остальные настройки приложения.
- Активация лицензий — состояние лицензии в том же разделе.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Обзор операций и выбор раздела

С документами в КриптоАРМ работают три раздела: **Подпись и шифрование**, **Подпись и защита PDF** и **Проверка и расшифрование**. Здесь описано, какие операции в них выполняются, чем различаются стандарты подписи и какой раздел выбрать под задачу.

Содержание:

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

Основные операции

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	Проверяет подпись, цепочку доверия, отзыв и штампы времени	«Проверка и расшифрование», «Подпись и защита PDF»
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», «Проверка и расшифрование»
Разделить подпись	Сохраняет подпись каждого подписанта отдельным файлом	«Подпись и шифрование», «Проверка и расшифрование»

Параметры операций сохраняются в профиле подписи — задавать их каждый раз заново не нужно.

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

Приложение создаёт подписи двух стандартов:

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

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		Адрес службы TSP

Стандарт	Зачем нужен	Что требуется
	Подпись останется проверяемой и после того, как сертификат истечёт: внутрь вложены доказательства, что на момент подписания он действовал	
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. 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 отдельным файлом (по умолчанию с расширением `.sig`), исходный документ не изменяется.

Печатная форма

Печатная форма — копия PDF-документа со штампом подписи, но без самой электронной подписи. Она предназначена для печати и визуального контроля и юридической силы не имеет.

Создать печатную форму можно:

- при подписи — переключатель **«Печатная копия со штампом»** у обычной подписи CMS/CAdES (см. Подпись и шифрование файлов);
- при просмотре сведений о подписи (см. Создание печатной формы).

Подпись со стандартом PAdES

PAdES — стандарт подписи, встроенной в PDF-документ. Отдельный файл подписи не создаётся: документ остаётся обычным PDF и открывается в любой программе просмотра.

Подпись PAdES может быть:

- **видимой** — отображается в виде штампа на странице;

- **невидимой** — на странице не отображается, но проверяется так же.

Сертифицирующая подпись PDF

Сертифицирующая подпись — первая подпись в PDF-документе, которая не только подтверждает авторство и целостность, но и задаёт, какие изменения разрешены после неё, — например, подписи в подготовленных местах. Любое другое изменение сделает сертифицирующую подпись недействительной.

Поставить сертифицирующую подпись может только первый подписант — см. Сертифицирующая подпись PDF-документа.

Конвертация в формат PDF/A

PDF/A — международный стандарт (ISO 19005) долгосрочного хранения PDF-документов. КриптоАРМ преобразует документы в форматы **PDF/A-2b** и **PDF/A-3b**; второй допускает вложенные файлы.

При конвертации удаляются или отключаются элементы, которые могут нарушить отображение документа или повлиять на его безопасность: сценарии (JavaScript), мультимедиа, 3D-объекты, интерактивные формы, внешние ссылки, шифрование и парольная защита.

Преобразование доступно только для неподписанных документов и выполняется вместе с подписью — см. Создание подписи с конвертацией в 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 действий разделов «Подпись и шифрование» и «Проверка и расшифрование».

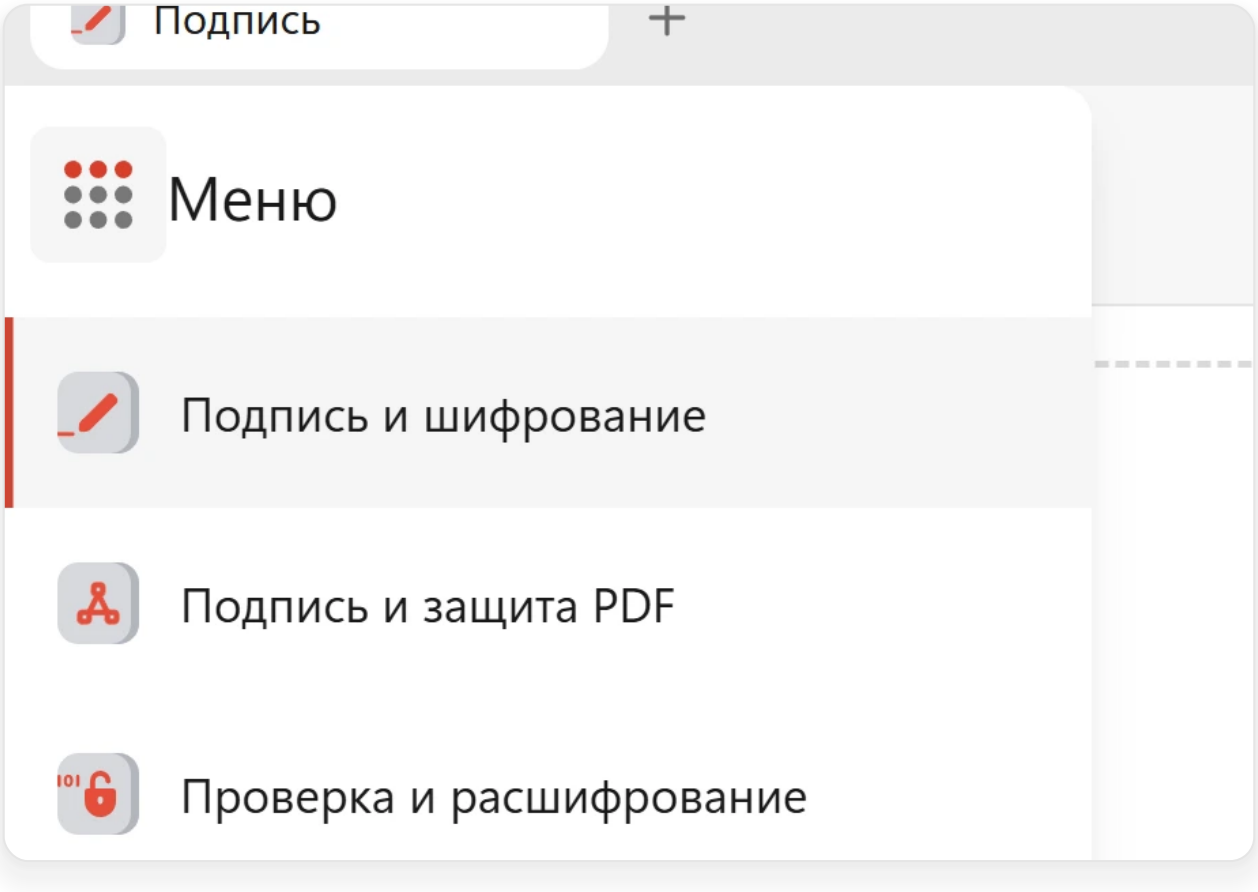
Разделение подписи

Отсоединённую подпись с несколькими подписантами можно разделить на отдельные файлы, по одному на каждого подписанта, — кнопка **Разделить подпись** на панели действий тех же разделов.

Снятие подписи

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

Выбор раздела



Задача	Раздел	Почему
Подписать или 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	Просмотр страниц, разметка, сертификация, PDF/A
Проверить подпись или расшифровать документ	Проверка и расшифрование	Сам определяет тип файла и выполняет нужные 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 действий — например, отправить только что подписанный PDF в мастер PDF или в проверку.

Смотрите также

- Профили подписи — сохранённые наборы настроек операции.
- Подпись и шифрование — подпись, архивирование и шифрование файлов.
- Проверка и расшифрование — проверка подписей и расшифрование документов.
- Подпись и защита PDF — просмотр, разметка и подпись одного PDF-документа.
- Настройки подписи и шифрования — справочник всех параметров.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Профили подписи

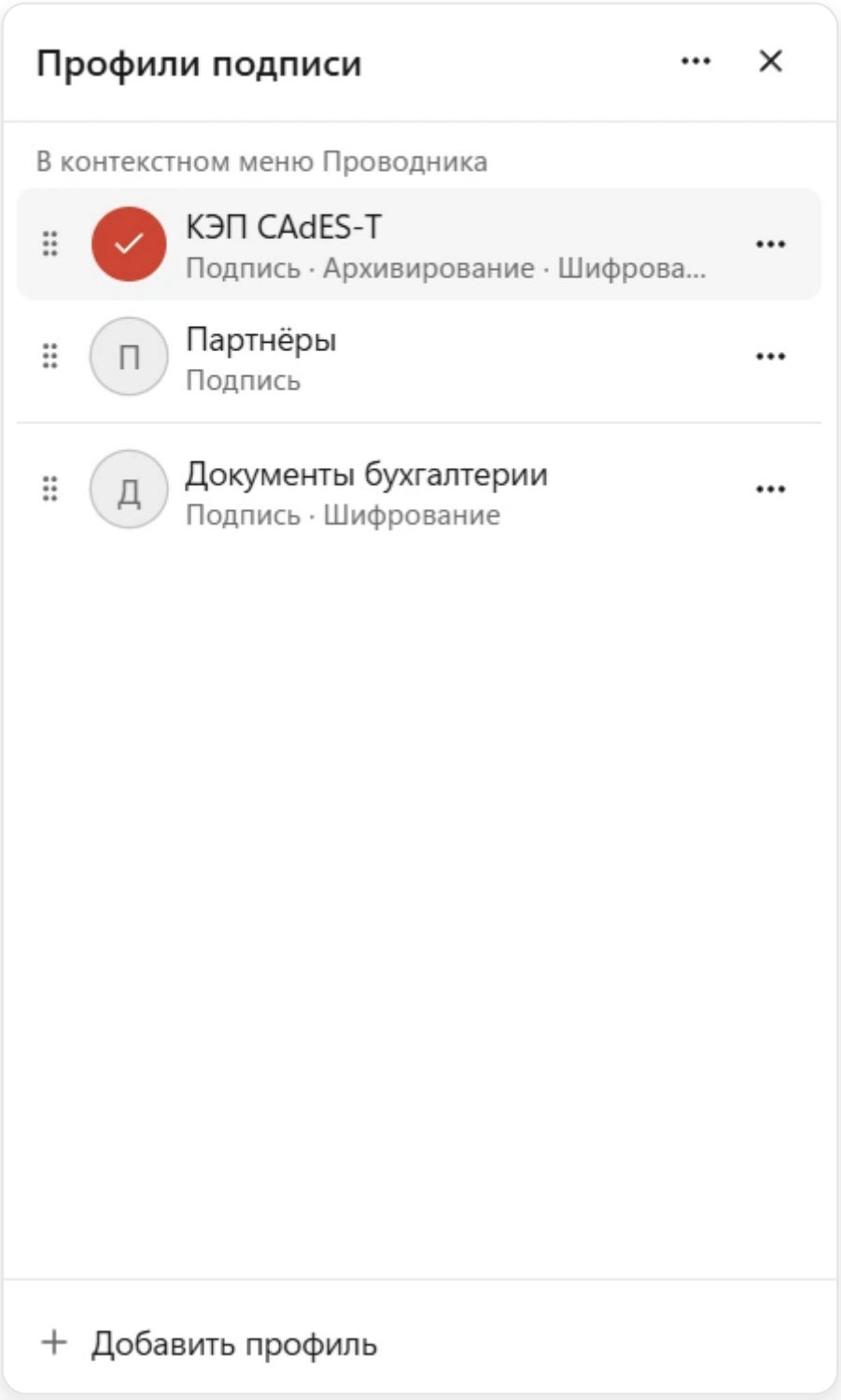
Профиль подписи — сохранённый набор настроек операции: какие действия выполнять, каким сертификатом, в каком формате и куда сохранять результат. Нужный профиль выбирается одним щелчком.

Содержание:

- Где находятся профили
- Создание профиля подписи
- Переключение между профилями подписи
- Редактирование настроек профиля подписи
- Сохранение настроек перед операцией
- Порядок профилей
- Профили в контекстном меню Проводника
- Удаление профилей подписи
- Экспорт и импорт профилей подписи
- Смотрите также

Где находятся профили

Профили доступны в разделе **Подпись и шифрование** и в мастере **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 перед операцией, сохраняются в активный профиль, поэтому создавать профиль перед первой операцией не нужно.

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

Профиль X.509 может хранить и разметку документа из мастера **Подпись и защита PDF**: место вашей подписи, места для других подписантов и рукописных подписей, произвольные области. Для каждого вида документов удобно завести свой профиль. Подробнее — в разделе Разметка по профилю.

Создание профиля подписи

1. Откройте раздел **Подпись и шифрование**.
2. Щёлкните по имени активного профиля.
3. Внизу панели нажмите **Добавить профиль** — откроется вкладка **«Редактирование профиля»**.
4. В блоке **Общие настройки** укажите **Название профиля**.
5. В блоке **Операции** отметьте действия: подпись, архивирование, шифрование. Несколько операций выполняются по порядку — см. Порядок выполнения.
6. Задайте остальные параметры — см. Настройки подписи и шифрования.
7. Нажмите **Сохранить**.

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

Переключение между профилями подписи

Активный профиль применяется при подписи. Чтобы переключить профиль, откройте раздел **Подпись и шифрование** или мастер **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.

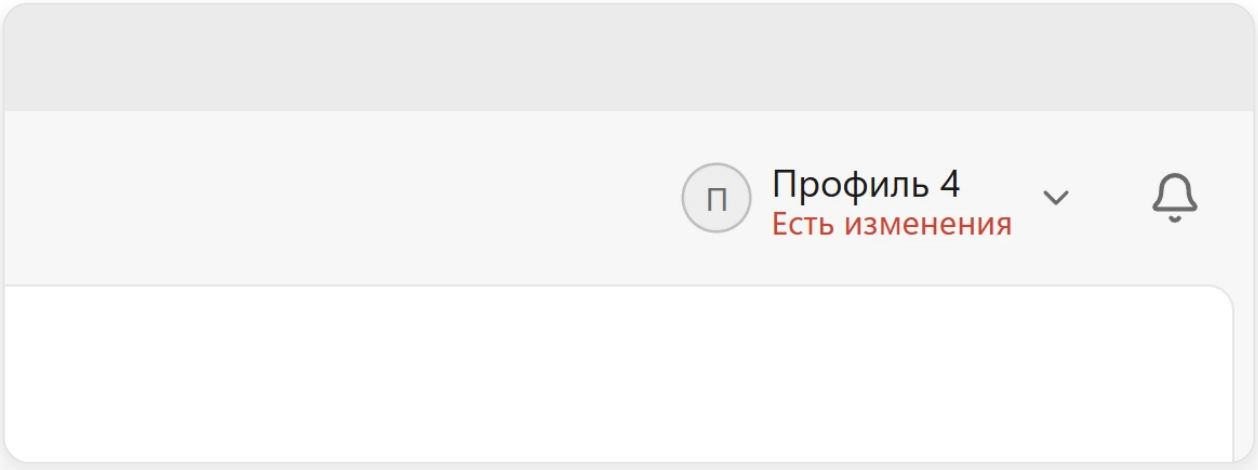
Редактирование настроек профиля подписи

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 перед операцией

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**: на macOS та же настройка называется **Показывать в быстрых действиях Finder**, а раздел панели — **«В быстрых действиях Finder»**. На Linux — **Показывать в меню файлового менеджера** и **«В меню файлового менеджера»**; в каких дистрибутивах есть меню, сказано в разделе Меню файлового менеджера на Linux.

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. Последний оставшийся профиль удалить нельзя.

Экспорт и импорт профилей подписи

Профиль можно сохранить в файл — для резервной копии или переноса на другой компьютер. Файл сохраняется с расширением `.pcarm-profile`; при импорте принимаются также файлы `.json`.

Вместе с настройками в файл попадает всё, на что профиль ссылается: логотип штампа, машиночитаемая доверенность, изображения произвольных областей и образцы рукописной подписи из разметки. При импорте образцы добавляются к образцам подписи на этом компьютере, если их там меньше пяти.

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

Раздел **Подпись и шифрование** подписывает, архивирует и шифрует файлы — по одному или сразу несколько, отдельными операциями или за один проход.

Содержание:

- Что потребуется
- Шаги операции
- Подпись со стандартом CAdES
- Подпись со стандартом PAdES
- Подпись с машиночитаемой доверенностью
- Добавление соподписи
- Объединение подписей
- Разделение подписи
- Шифрование
- Подпись и шифрование за одну операцию
- 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.

Шаги операции

Операция в разделе **Подпись и шифрование** проходит в четыре шага:

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.

Открытие раздела

Раздел **Подпись и шифрование** открывается:

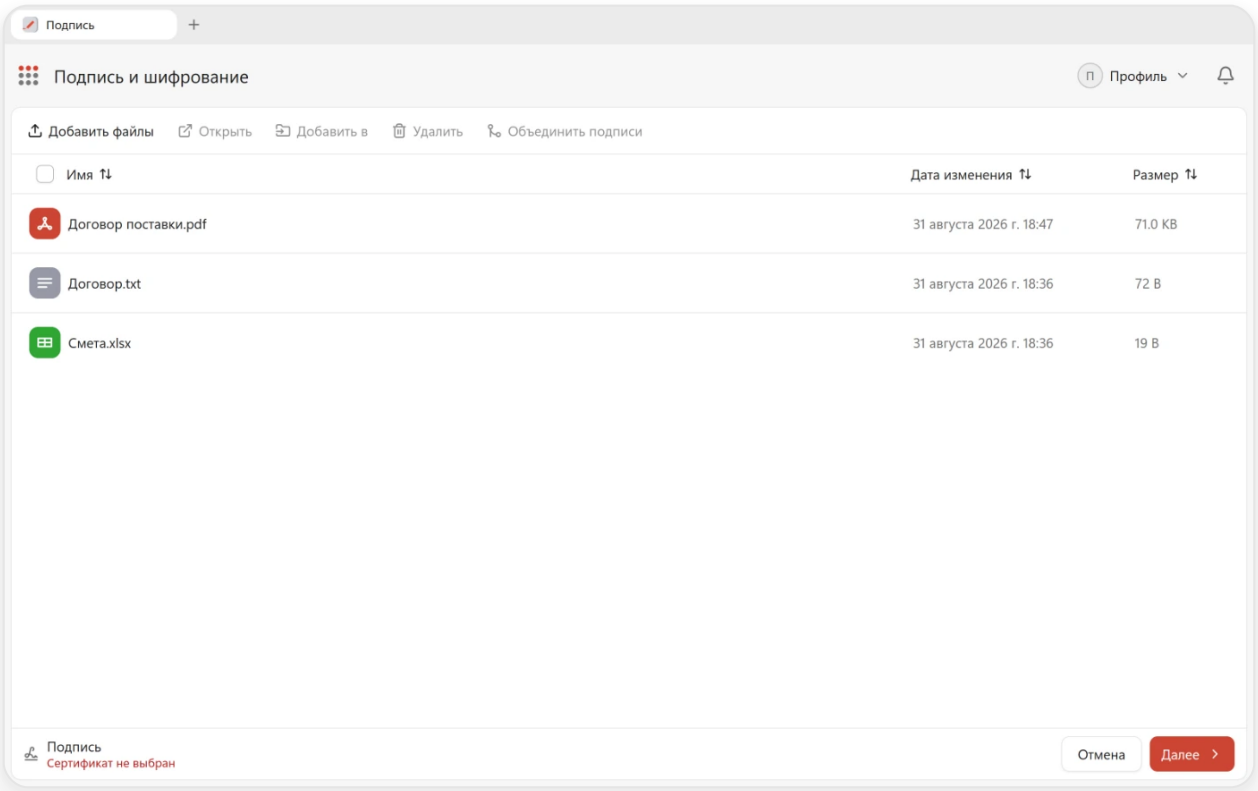
- из бокового меню — пункт **Подпись и шифрование**;
- кнопкой + в строке вкладок (правый щелчок открывает список разделов);
- из другого раздела — кнопкой **Добавить в** на панели действий;
- из контекстного меню файла — командой **Открыть для подписи и шифрования...**.

Раздел открывается в новой вкладке.

Добавление документов

Способы добавить файлы:

- перетащите их в окно раздела;
- нажмите **Добавить файлы** на панели действий;
- в пустом разделе нажмите на область **«Перетащите файлы сюда»**;
- передайте файлы из другого раздела кнопкой **Добавить в**;
- выберите файлы в файловом менеджере и воспользуйтесь командой **Открыть для подписи и шифрования...**.



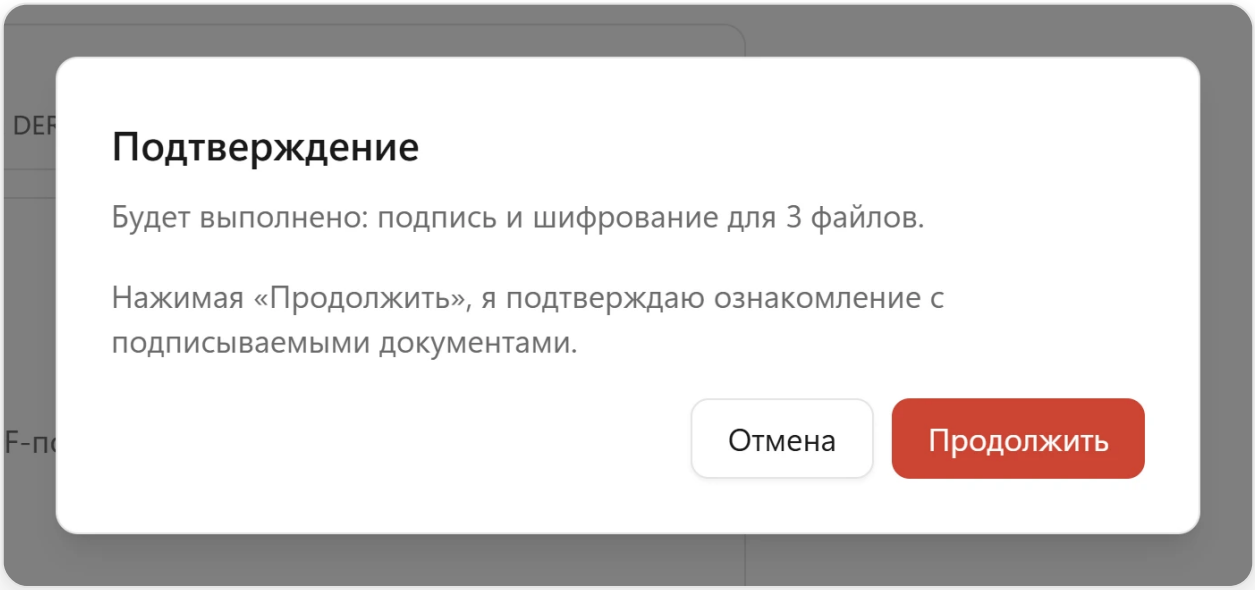
При перетаскивании папки в список попадают файлы из неё. За один раз можно добавить не более **1000** файлов — при превышении появится сообщение **«Файлы не добавлены»** с указанием количества.

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.

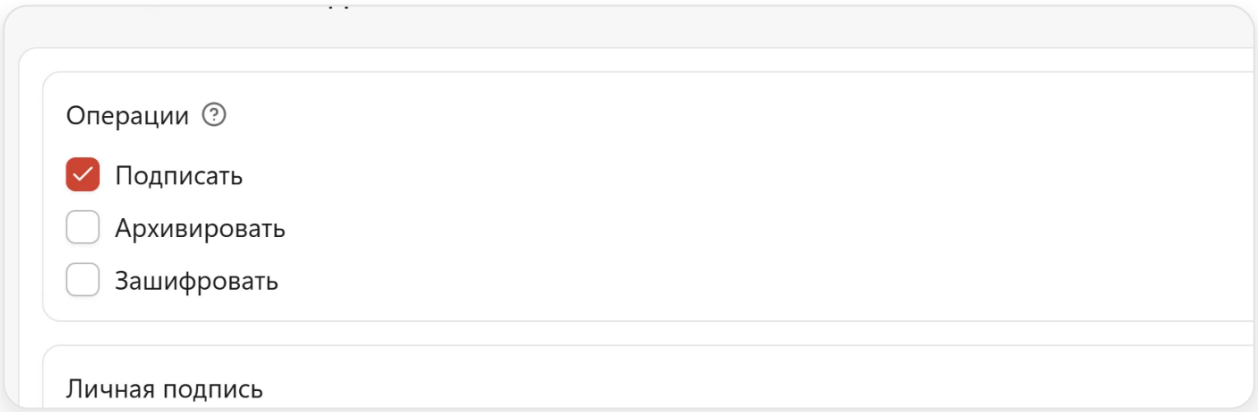
Кнопки:

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

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

Подпись со стандартом CAdES

1. Добавьте файлы в раздел — 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 и для ключа RSA или ECDSA 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 ПИН-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

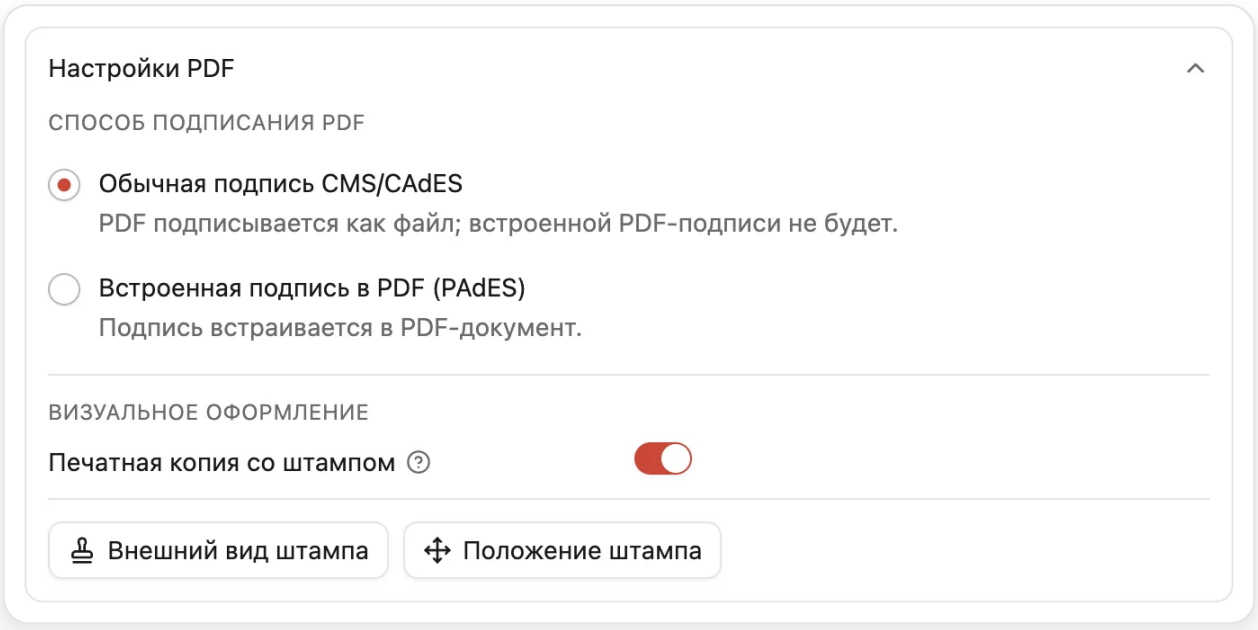
Для PDF-файлов в блоке **Настройки PDF** выбирается **способ подписания**:

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

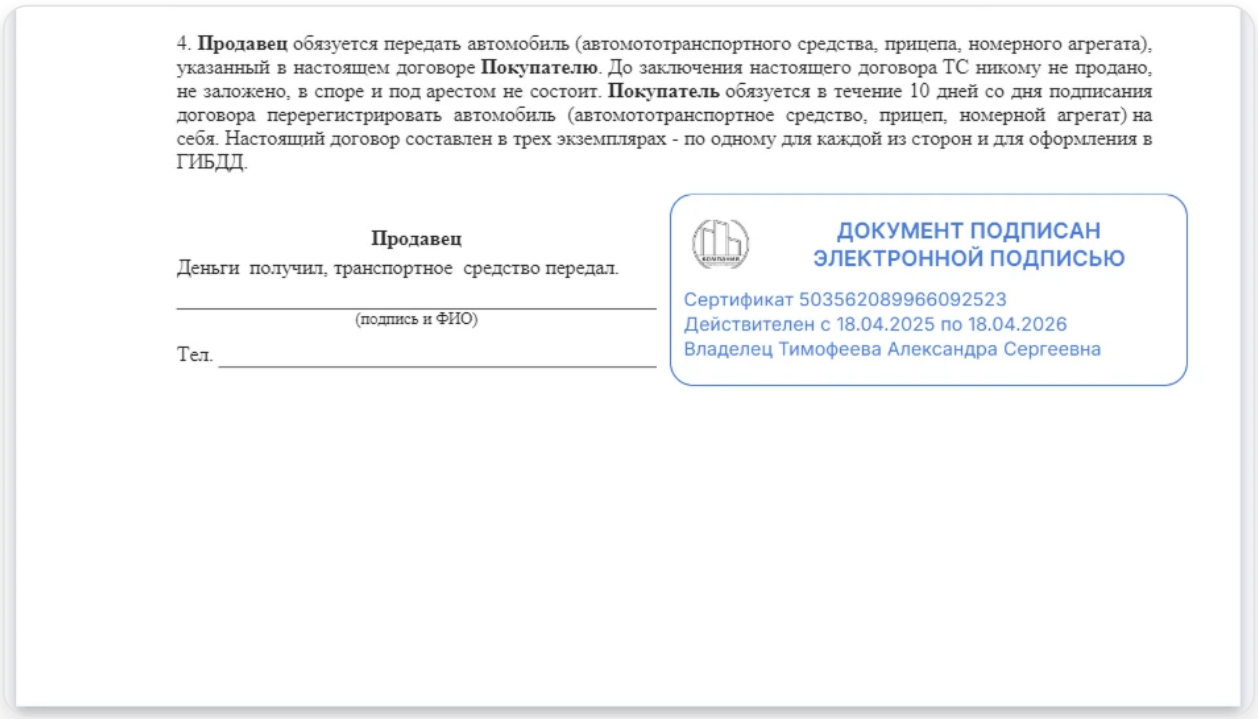
Для встроенной подписи дополнительно доступны:

- **Подготовка PDF** — преобразование в PDF/A-2b или PDF/A-3b перед подписанием;
- **Сертификация** — сертифицирующая подпись с разрешениями на последующие изменения.

В блоке **Визуальное оформление** включается штамп подписи: для встроенной подписи — **Видимый штамп подписи** на странице документа, для обычной — **Печатная копия со штампом**, отдельный неподписанный PDF рядом с файлом подписи. Оформление и положение штампа настраиваются кнопками **Внешний вид штампа** и **Положение штампа**.



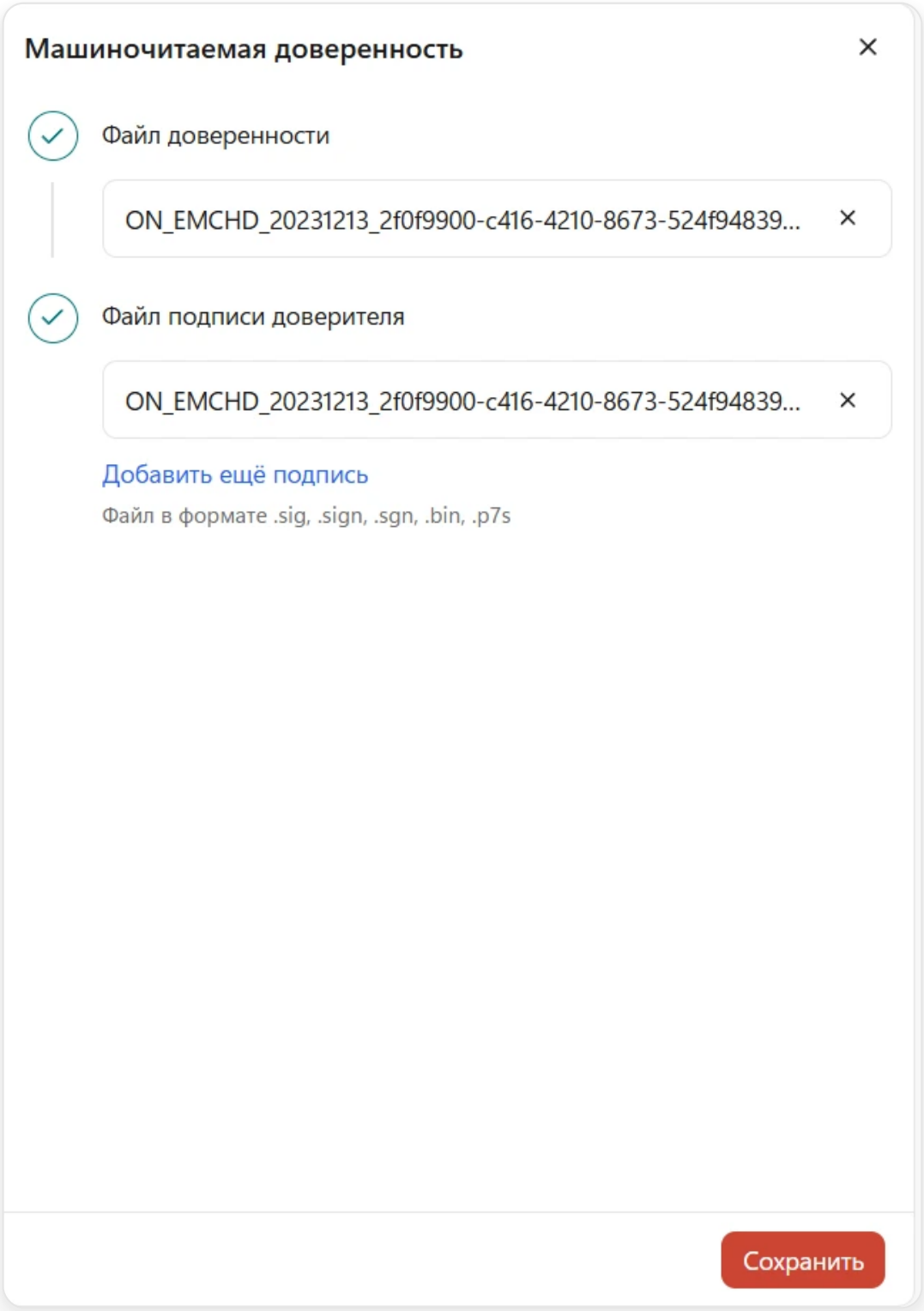
Пример визуализации штампа подписи:



> 💡 **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 действий.

Исходные файлы остаются без изменений, а новый файл сохраняется в папке первой подписи из списка. Его имя — общая часть имён подписей с суффиксом `_joined_<количество подписей>_signs`. То, чем имена различаются, в него не попадает. Например, ФИО, которое добавляет настройка **Добавлять ФИО подписанта**: из `договор_Иванов Иван Иванович.pdf.sig` и `договор_Петров Пётр Петрович.pdf.sig` получится `договор_joined_2_signs.pdf.sig`. Если общей части у имён нет, файл называется `signatures_joined_<количество подписей>_signs`. Результат прошлого объединения можно выделить вместе с новыми подписями: его подписи войдут в число, а метка `_joined_…_signs` в имени заменится, а не допишется.

Для объединения нужны как минимум две выделенные подписи и КриптоПро CSP — иначе кнопка неактивна, а подсказка на ней называет причину.

Та же кнопка есть в разделе **Проверка и расшифрование**: там объединённая подпись сразу проверяется — см. Объединение отсоединённых подписей.

Разделение подписи

Отсоединённую подпись с несколькими подписантами можно разделить на отдельные файлы — по одному на каждого подписанта. Например, чтобы передать подпись одного подписанта отдельно или исправить ошибочное объединение подписей:

1. Добавьте файл подписи в раздел.
2. Выделите его. Можно выделить несколько файлов: каждый разделится отдельно.
3. Нажмите **Разделить подпись** на панели действий.

Рядом с исходным файлом появятся его части — по файлу на каждого подписанта; в списке они заменят строку исходного файла. Исходный файл на диске не изменяется, существующие файлы не перезаписываются. Имена частей образуются от имени документа: метка `_joined_…_signs` удаляется, а если имя занято, добавляется номер. Например, `договор_joined_2_signs.pdf.sig` разделится на `договор.pdf.sig` и `договор(1).pdf.sig`, а соподписанный `акт.docx.sig` — на `акт(1).docx.sig` и `акт(2).docx.sig`. По этим именам приложение автоматически находит документ для каждой части.

Часть содержит всё, что относится к подписи этого подписанта в исходном файле: штампы времени, сведения для проверки и все сертификаты. Поэтому результат проверки части совпадает с результатом проверки этой подписи в исходном файле. Части остаются отсоединёнными подписями в той же кодировке, что и исходный файл.

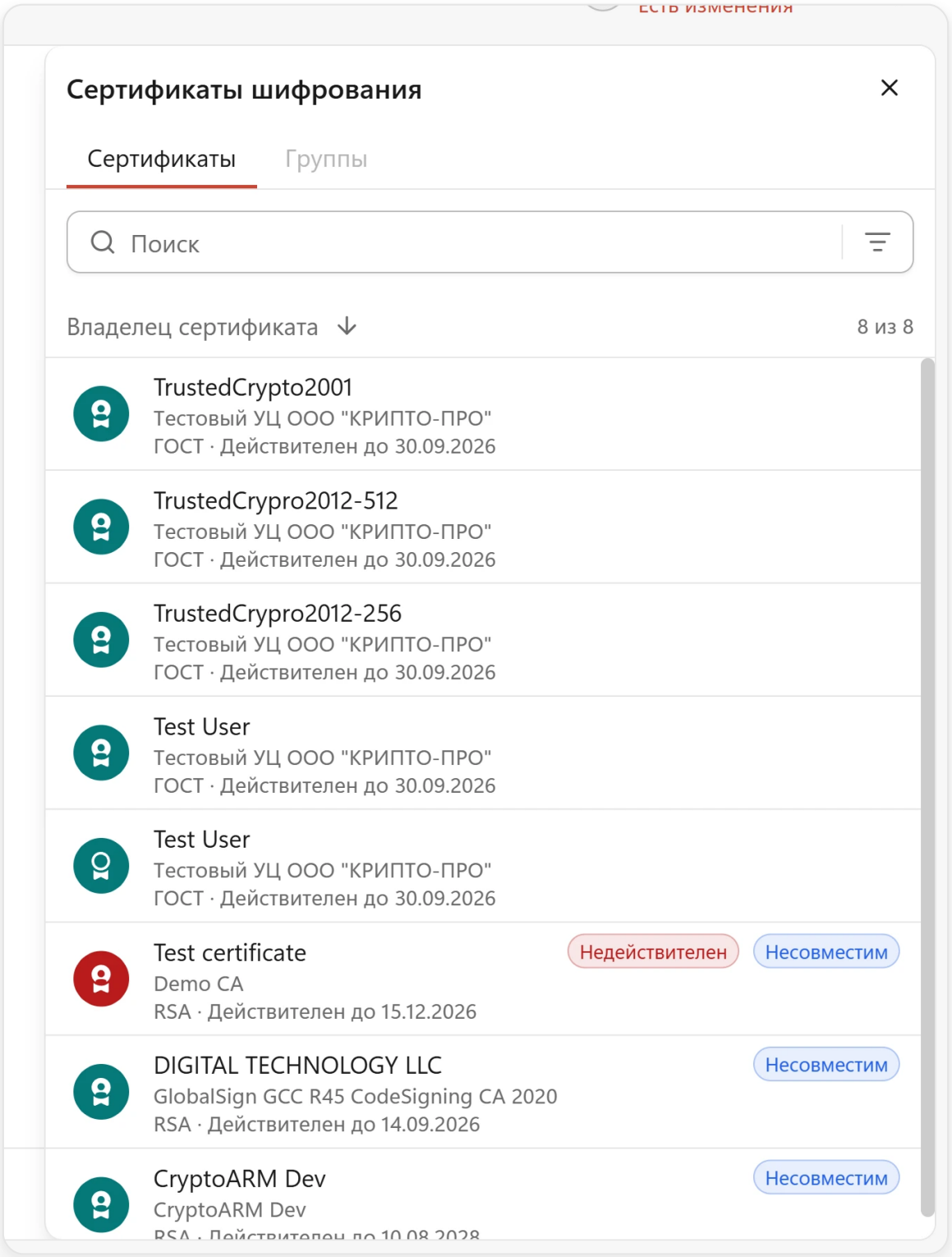
Для разделения нужен КриптоПро CSP; сертификат, ПИН-код и лицензия КриптоАРМ не требуются. Если подпись присоединённая, в ней только один подписант или выделенный файл не является подписью X.509, приложение сообщит об ошибке. Ошибка в одном файле не прерывает обработку остальных.

Та же кнопка есть в разделе **Проверка и расшифрование**: там части сразу проверяются — см. Разделение 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 исходные файлы 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.

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;
- итог записывается в журнал.

Действия на панели действий:

Действие	Что делает
Открыть	Открывает выбранные файлы средствами системы
Показать	Открывает папку с файлом
Добавить в	

Действие	Что делает
	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.

Остановка операции

Пока операция X.509 выполняется, на месте кнопки **Отменить** стоит **Остановить**. После нажатия приложение доделывает файл, который обрабатывает сейчас, и не берётся за следующие. Подтверждение не запрашивается: остановка ничего не удаляет.

- Готовые файлы остаются на диске и показаны в списке с результатом.
- Файлы, до которых очередь не дошла, возвращаются в список без статуса — такими, какими были до запуска.
- Исходные файлы не удаляются, даже если включено их удаление после шифрования.
- Если операция состоит из нескольких этапов — например, подпись, архив и шифрование, — следующие этапы не запускаются. Остановка до последнего этапа не оставляет ни подписанных, ни зашифрованных файлов: общий архив из части файлов не собирается.

Остановить можно операцию над файлами с диска. Операции OpenPGP и операции над документами из облака выполняются до конца.

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.

Сообщение	Что это значит	Что сделать
Нет сертификатов подписи	В хранилище нет сертификатов, которыми можно подписывать	Нажмите **Перейти к сертификатам** под полем и установите свой сертификат
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 хранилища **Личные сертификаты**
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. Всё равно использовать его?	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
	Папка для результатов не задана или была удалена	Проверьте блок **Сохранение результатов**

Сообщение	Что это значит	Что сделать
Укажите папку для сохранения результата / Укажите существующую папку		
Файлы не добавлены	За один раз можно добавить не больше 1000 файлов	Добавьте файлы частями

Общие ошибки

Код	Сообщение	Что сделать
—	**Не удалось подписать файл**	1. Проверьте права доступа к папке, указанной для сохранения результатов 2. Освободите место на диске 3. Точная причина записана в журнале
—	**Для операций подписи и расшифрования с использованием алгоритмов ГОСТ требуется лицензия КриптоАРМ**	1. Приобретите лицензию КриптоАРМ 2. Активируйте лицензию в настройках приложения
`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: компоненты КриптоПро ЭЦП (CAdES) входят 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
—		

Код	Сообщение	Что сделать
	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
—	**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)

Сообщение	Что это значит	Что сделать
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

Сообщение	Что это значит	Что сделать
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

Сообщение	Что сделать
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

Раздел **Проверка и расшифрование** проверяет электронные подписи и показывает сведения о них, извлекает документ из присоединённой подписи и расшифровывает файлы.

Содержание:

- Начало работы
- Проверка подписи
- Снятие подписи с документа
- Расшифрование документа
- Сохранение результатов
- Возможные ошибки
- Смотрите также

Начало работы

Открытие раздела

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 файловом менеджере — см. Открытие файлов двойным щелчком;
- из контекстного меню файлового менеджера — см. Контекстное меню Проводника.

Добавление документов

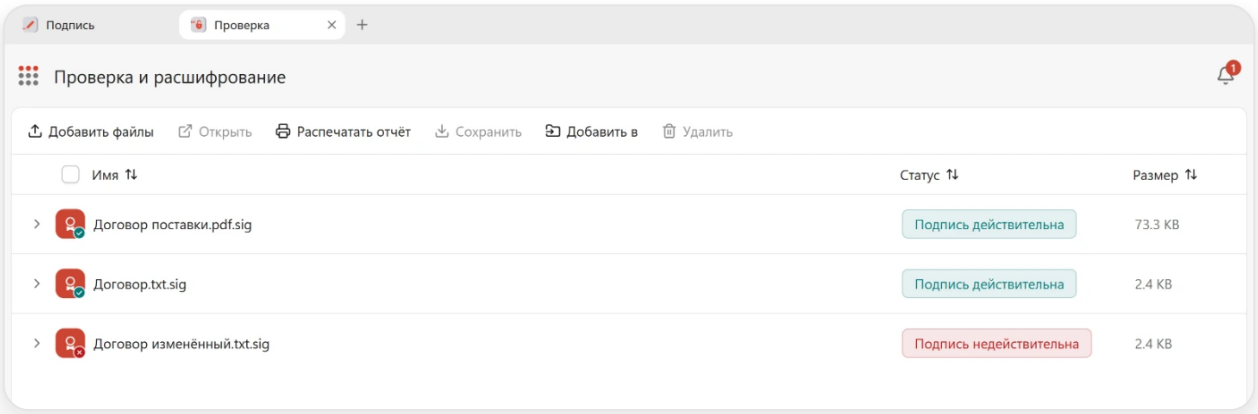
Добавьте документы одним из способов:

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

> 💡 **Совет**: в раздел 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 подписи

Откройте раздел и добавьте файлы. Проверка запускается сама: 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
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 раздел: 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 раздел — подпись проверится заново. Или нажмите кнопку поиска файла рядом со статусом либо **Указать путь к исходному файлу** в сведениях и выберите документ вручную.

Объединение отсоединённых подписей

Если документ подписали несколько человек и каждый прислал свою отсоединённую подпись, их можно собрать в один файл прямо в разделе:

1. Выделите две или более подписи X.509.
2. Нажмите **Объединить подписи** на панели действий.

Выделенные подписи X.509 в списке заменит один файл с суффиксом `_joined_<количество подписей>_signs`, и приложение сразу проверит его — с документом, если он есть в разделе или в папке подписи. Исходные файлы на диске остаются без изменений. Подробнее об именовании и ограничениях — в разделе Объединение подписей.

Кнопка показана, когда выбран стандарт X.509: подписи OpenPGP не объединяются. Если объединить подписи не удалось, приложение сообщит об ошибке, а исходные подписи проверятся заново.

Разделение подписи

Если в отсоединённой подписи несколько подписантов, её можно разделить на отдельные файлы — по одному на каждого подписанта:

1. Выделите один или несколько файлов отсоединённой подписи X.509.
2. Нажмите **Разделить подпись** на панели действий.

В списке строку каждого файла заменят его части — по одной на каждого подписанта, — и приложение сразу их проверит. Исходный файл на диске остаётся без изменений. Подробнее об именах частей и о том, что в них сохраняется, — в разделе Разделение подписи.

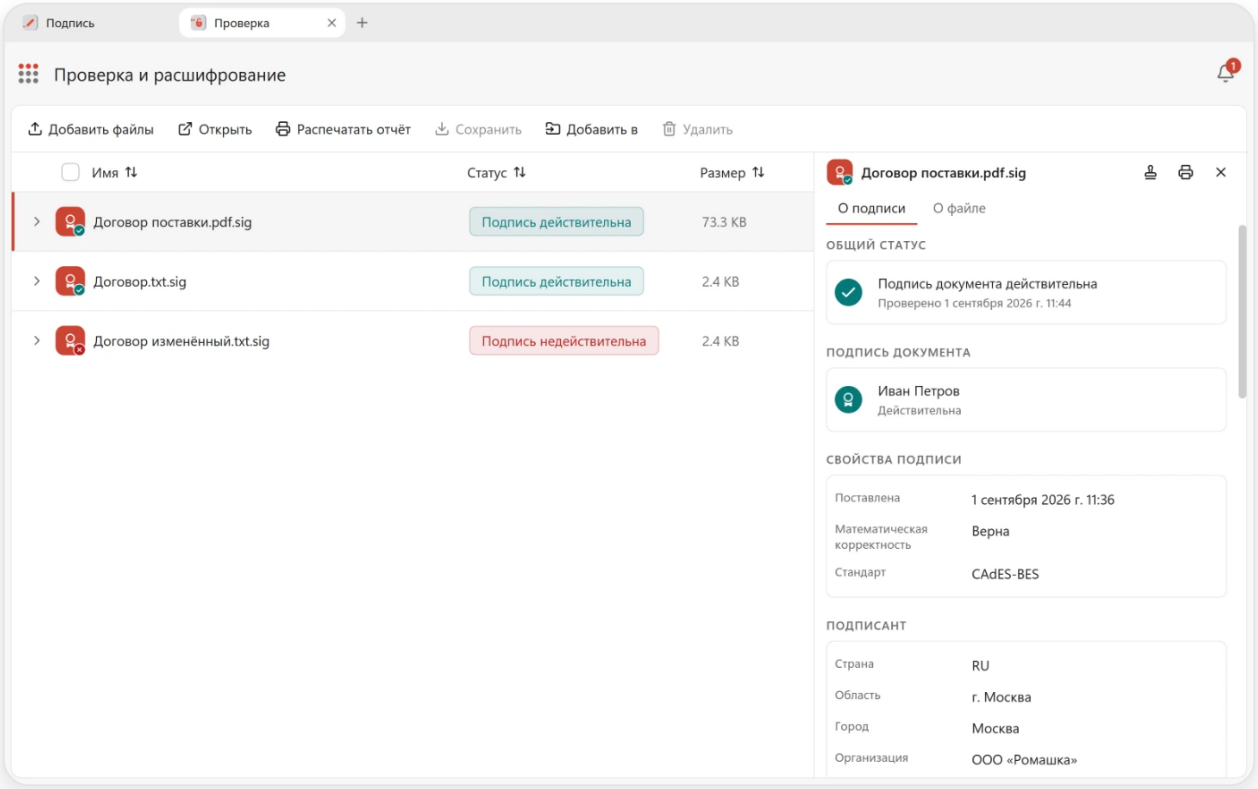
Кнопка показана, когда выбран стандарт X.509. Если разделить подпись не удалось, приложение сообщит об ошибке, а исходный файл проверится заново.

Просмотр сведений о подписи документа

Выделите проверенный файл в списке. 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. У подписей CAdES-X Long Type 1 и CAdES-A статус **«Действовал на момент подписания»** берётся из сведений, вложенных в подпись, — даже если сертификат с тех пор истёк
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»**.

Когда действует режим «Квалифицированная подпись» сетевого профиля доверия, в блоке **Свойства подписи** есть строка **Квалифицированность**:

- **Выдан аккредитованным удостоверяющим центром** — квалифицированность подтверждена;
- **Не подтверждена** с причиной — пояснением сервера, **УЦ не аккредитован** или **проверка по списку доверия завершилась отрицательно** — подпись недействительна, даже если она математически верна и цепочка действительна;
- **Не удалось проверить** с причиной, например нет связи с сервером, — подпись тоже недействительна.

В отчёте о проверке эта строка называет только результат, а пояснение стоит в строке **Причина**.

Чтобы открыть сведения о сертификате подписанта или удостоверяющего центра, нажмите на него в блоке **Цепочка сертификации**. Если этого сертификата нет на компьютере, в верхней части сведений появится кнопка **Установить сертификат**, а если есть — кнопка **Экспортировать**. Сертификат подписанта сразу попадает в хранилище **Других пользователей**. Для сертификата удостоверяющего центра и для сертификата, ключ которого есть на компьютере, приложение предложит выбрать хранилище и подставит рекомендуемое: **Удостоверяющие центры** или **Личные**. При установке корневого сертификата КриптоПро CSP попросит подтвердить действие.

Сам результат проверки после установки не меняется. Чтобы проверить подпись с новым сертификатом, вернитесь к сведениям о подписи и нажмите **Обновить** в верхней части панели. Так же можно перепроверить подпись после импорта сертификата или списка отзыва в разделе **Сертификаты** — файл не нужно добавлять заново. У расшифрованного файла этой кнопки нет.

> 💡 **Примечание**: 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

Если файл содержит соподписи, в панели сведений появляется блок **«Подписи документа»** с их количеством. Выберите в нём подпись — панель покажет сведения о ней.

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»**.

Выберите штамп в блоке **«Тип штампа»**: **на данные**, **на подпись**, **на доказательства** или **архивный**. Панель покажет 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
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 разделе Подпись и защита PDF — он показывает, где именно на странице стоит каждая подпись.

Проверка соответствия МЧД сертификату подписи

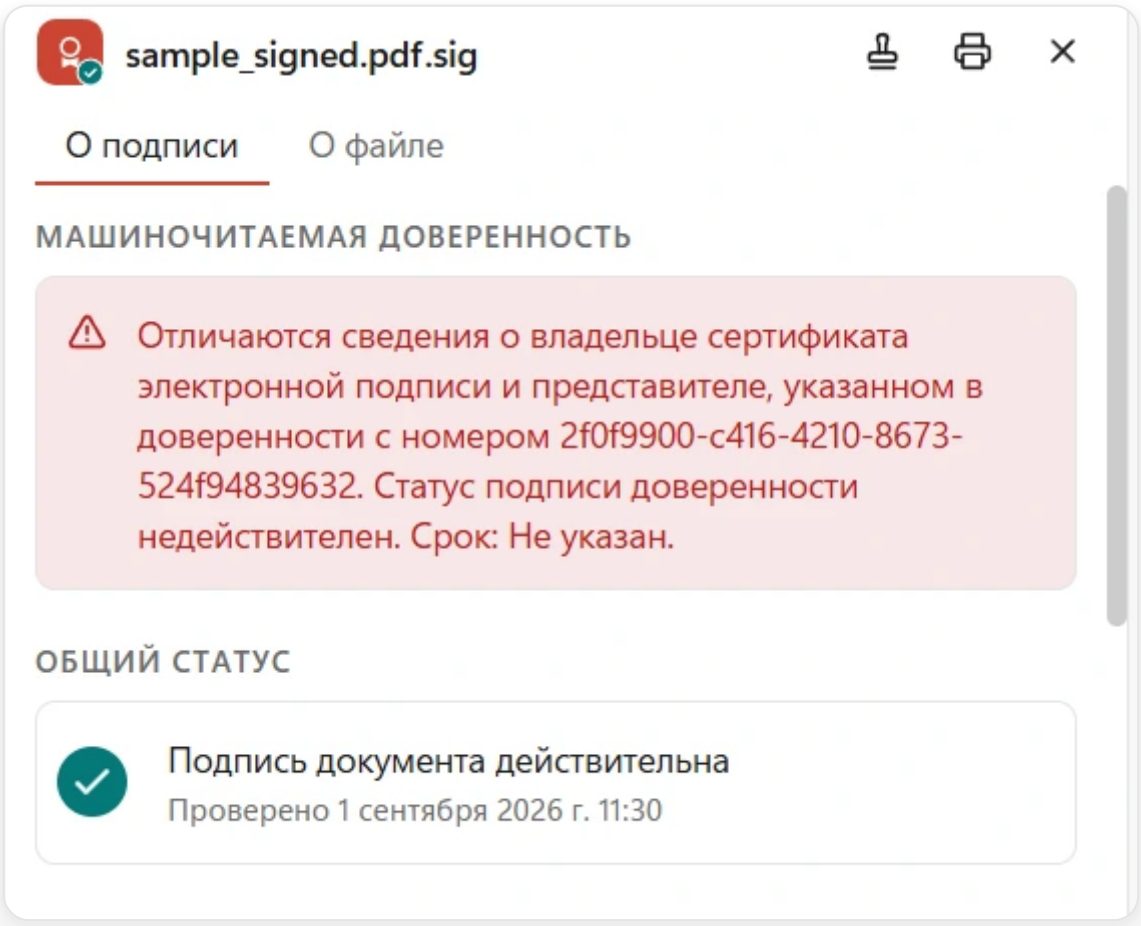
При проверке подписи приложение сравнивает ИНН владельца сертификата с ИНН представителя из машиночитаемой доверенности.

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
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.

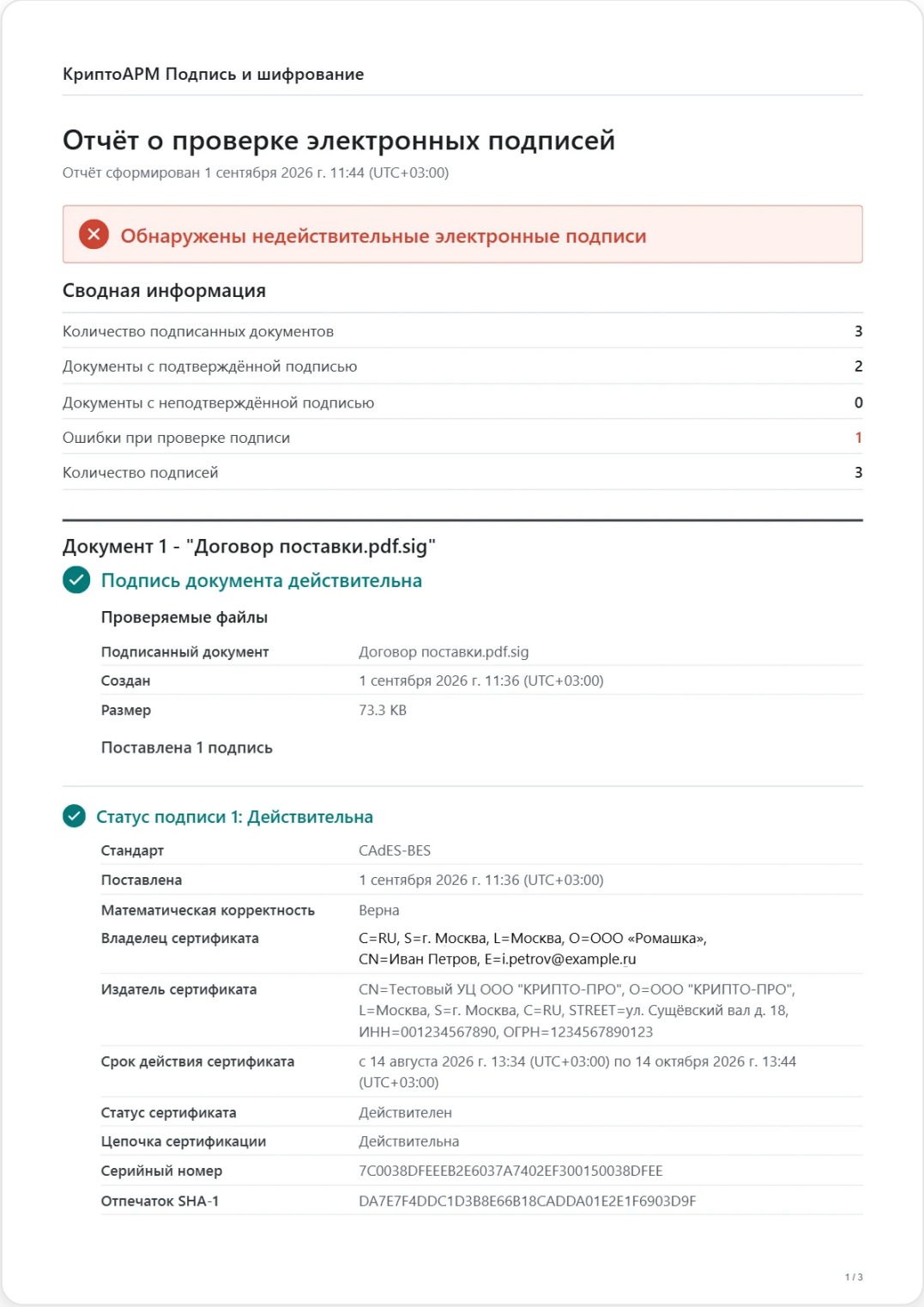
1. Выделите файлы, по которым нужен отчёт.
2. Нажмите **Распечатать отчёт** на панели действий или в панели сведений о подписи.
3. Откроется окно с отчётом о проверке электронной подписи.

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, сведения о подписанте, издатель сертификата и корневой сертификат цепочки, если цепочка построена до него. У недействительной подписи первой строкой указана **Причина**;
- дату формирования отчёта.

Отчёт можно распечатать или сохранить на устройстве.



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.

1. Откройте сведения о подписи.
2. Нажмите кнопку **Печатная форма со штампом** в панели сведений.

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

> 💡 **Примечание**: печатную форму можно создать и при подписании PDF-документа — см. Подпись со стандартом PAdES.

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
	Да	

Причина	Можно ли исправить	Что сделать
«Не удалось построить цепочку для сертификата, которым подписано сообщение»		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 и добавьте файл подписи — приложение сразу его проверит.
2. Нажмите стрелку слева от имени файла — команда **«Открыть содержимое»**. Статус файла сменится на **«Снятие подписи»**, а извлечённый документ появится вложенной строкой.
3. Сохраните документ — 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 и добавьте файлы. Приложение сразу начнёт расшифрование и проверит подпись, если она есть.
2. 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.

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 действий.
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

Сообщение	Что сделать
Не удалось открыть файл	1. Проверьте наличие и доступность файла 2. Повторите добавление файла в раздел
Файл ещё обрабатывается — повторите после завершения	Дождитесь окончания проверки и повторите действие
Не найден исходный файл для отсоединённой подписи	Добавьте в раздел 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 раздел
Архив повреждён или не является ZIP-файлом	Запросите у отправителя исправную версию архива

Ошибки при снятии подписи

Сообщение	Что сделать
Снятие подписи доступно только для совмещённой подписи	При отсоединённой подписи оригинал документа и так находится в отдельном файле

Сообщение	Что сделать
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 раздел

Ошибки при расшифровании

Сообщение	Что сделать
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 алгоритмов ГОСТ требуется лицензия КриптоАРМ	1. Приобретите лицензию КриптоАРМ 2. Активируйте лицензию в настройках приложения
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 лицензий — лицензии КриптоАРМ и КриптоПро CSP.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Подпись и защита PDF

Мастер **Подпись и защита PDF** работает с одним документом: показывает страницы, позволяет разметить место подписи, поставить рукописную подпись, подготовить места для других подписантов, сертифицировать документ, преобразовать его в PDF/A и проверить уже поставленные подписи.

Содержание:

- Что потребуется
- Начало работы
- Просмотр PDF-документа
- Создание подписи PDF-документа
- Сертифицирующая подпись PDF-документа
- Создание подписи с конвертацией в PDF/A
- Создание подписи в размеченной области
- Сохранение документа без электронной подписи
- Проверка подписи PDF-документа
- Разметка документа
- Возможные ошибки
- Смотрите также

> 💡 **Совет**: для подписи нескольких PDF-документов сразу удобнее раздел 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; не нужен, если документ сохраняется без электронной подписи. Мастер работает только по стандарту X.509: встроенной подписи PDF в OpenPGP не существует.
- **КриптоПро CSP и действующая лицензия КриптоАРМ** — для подписи ГОСТ-сертификатом.
- **Компоненты КриптоПро ЭЦП (CAdES)** — на Windows их ставит установщик приложения. Если компоненты отсутствуют, список сертификатов подписи будет пуст с пояснением **«(модуль CAdES недоступен)»**.

Начало работы

Запуск мастера

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

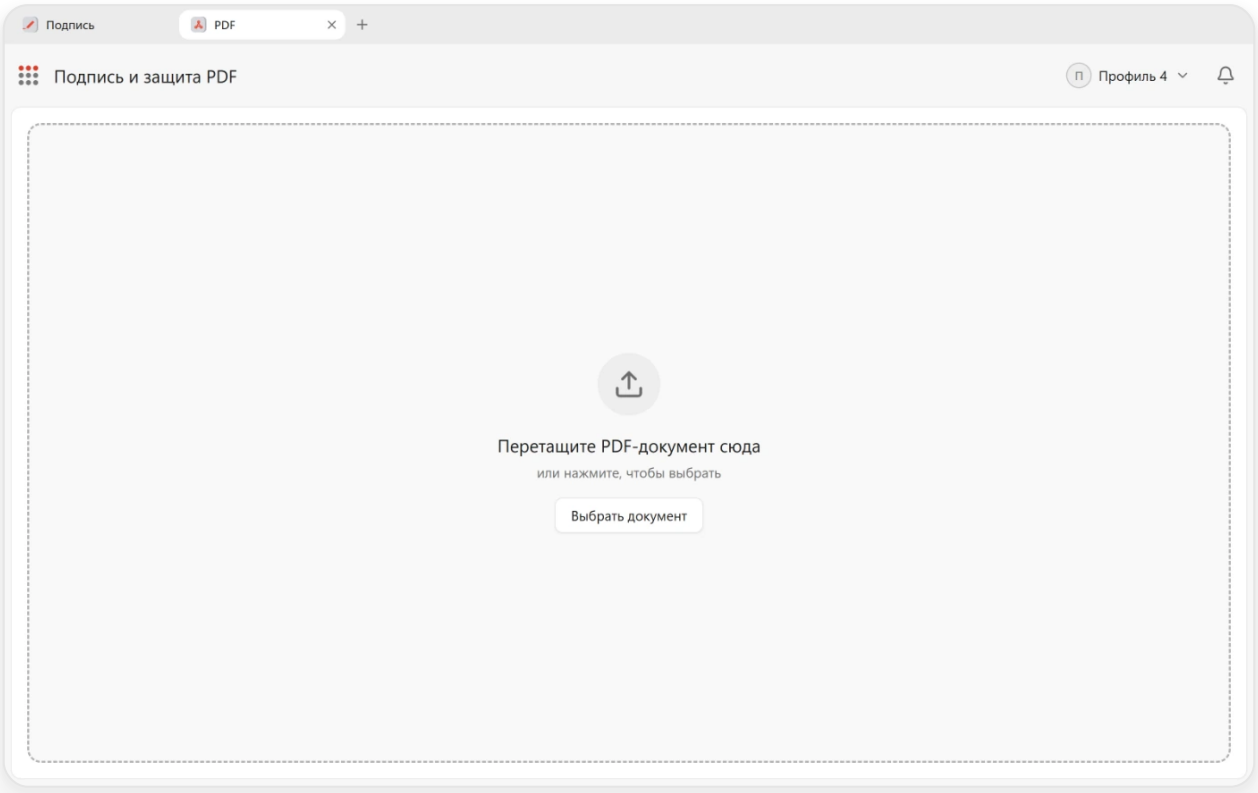
- из бокового меню: нажмите кнопку **Меню** и выберите **Подпись и защита PDF**;
- из строки вкладок: нажмите + правой кнопкой мыши и выберите раздел;
- из другого раздела: выделите PDF-документ и нажмите **Добавить в** → **Подпись и защита PDF**.

Мастер открывается 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.

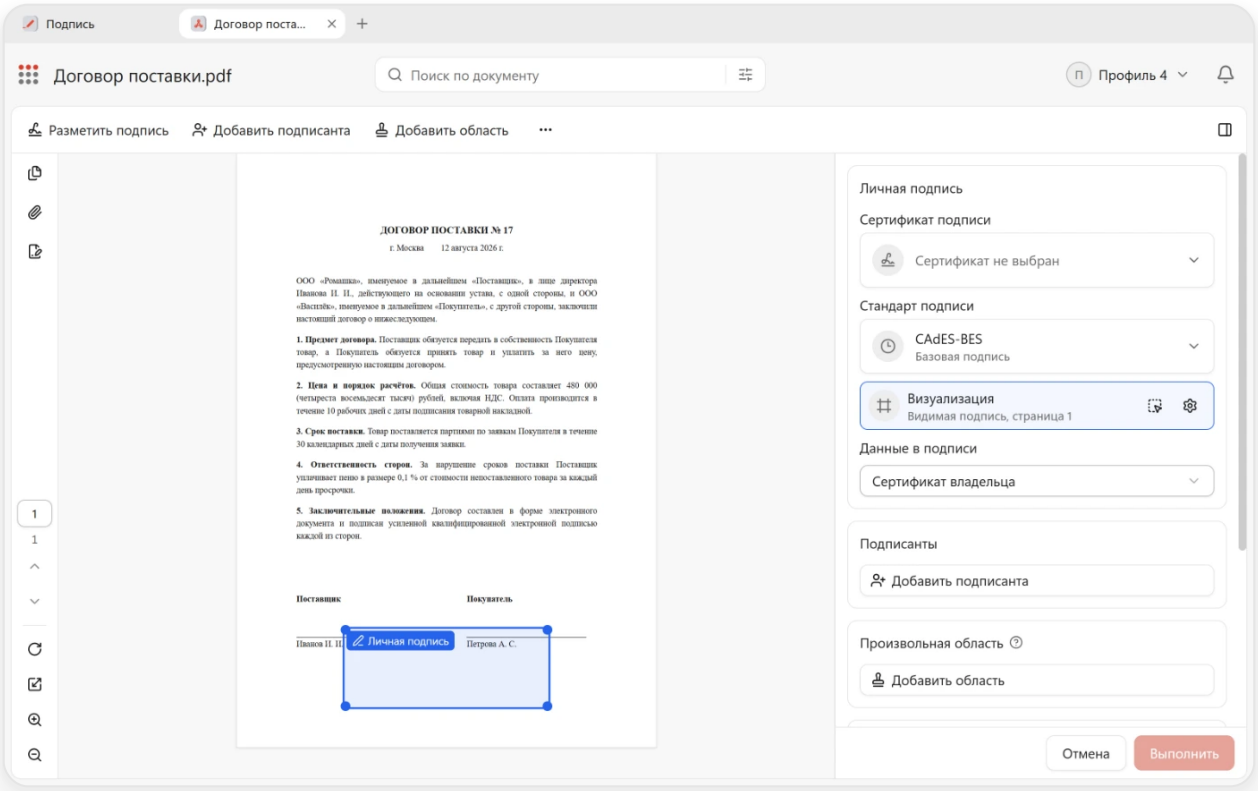


> 💡 **Примечание**: мастер открывает только файлы PDF и работает с одним документом. Если выбрано несколько файлов, откроется первый PDF из выбранных — об этом сообщит строка **«Открыт первый из выбранных PDF-файлов: одновременно открывается только один документ»**.

Просмотр PDF-документа

Добавленный в мастер документ открывается для просмотра. Если в нём есть подписи, приложение сразу их проверит (см. Проверка подписи PDF-документа).

Инструменты просмотра



Панель действий

Кнопка	Функция
Электронная подпись	Разметка места своей электронной подписи на странице
Рукописная подпись	Постановка рукописной подписи — см. Рукописная подпись
Место подписанта	Разметка места для подписи другого человека — см. Подписанты
Произвольная область	Разметка произвольной области — см. Произвольная область
Панель настроек	Открывает боковую панель с настройками подписи и разметкой мест

Кнопка	Функция
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
Сохранить разметку	Запоминание разметки в профиле для следующих документов — см. Разметка по профилю

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**

Масштаб меняется и колесом мыши с нажатой Ctrl (⌘ на macOS) или щипком на трекпаде: точка под курсором остаётся на месте. Ctrl (⌘) с клавишами «+» и «–» увеличивает и уменьшает, Ctrl (⌘) + 0 — показывает страницу целиком.

> 💡 **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.

Создание подписи PDF-документа

1. Откройте документ в мастере.
2. Нажмите **Панель настроек** на панели действий — в правой части окна появится панель настроек. По умолчанию используются параметры активного профиля подписи.

Блоки панели сворачиваются щелчком по заголовку. Свёрнутый блок кратко показывает, что в нём выбрано, и остаётся свёрнутым при следующем открытии мастера. Изначально раскрыт только блок **Электронная подпись**, остальные свёрнуты.

1. В блоке **Электронная подпись** проверьте, что переключатель в заголовке блока включён, и 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:

- рукописную подпись (см. Рукописная подпись);
- подписантов (см. Подписанты);
- произвольную область (см. Произвольная область).

1. При необходимости раскройте блок **Защита документа** и настройте параметры защиты:

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

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

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 не только подтверждает авторство и целостность документа, но и ограничивает дальнейшие изменения — см. Обзор операций.

1. Откройте документ и задайте настройки подписи, как описано в разделе Создание подписи PDF-документа.
2. Раскройте блок **Защита документа** и включите **Сертифицировать документ**.
3. Нажмите **Подписать** и подтвердите операцию.

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
Документ сертифицирован: электронные подписи разрешены, рукописные — нет	Можно подписывать, рукописную подпись — нельзя

Команды разметки, запрещённые сертификацией, недоступны, а подсказка объясняет причину.

Создание подписи с конвертацией в PDF/A

PDF/A — формат для длительного хранения документов. Что удаляется при конвертации, описано в разделе Конвертация в формат PDF/A.

> ⚠️ **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.

1. Откройте документ и задайте настройки подписи, как описано в разделе Создание подписи PDF-документа.
2. Раскройте блок **Защита документа**, включите **Преобразовать в PDF/A** и укажите дополнительные настройки:

- **Формат PDF/A** — **PDF/A-2b** или **PDF/A-3b**;
- **Если при преобразовании 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 **Подписать** и подтвердите операцию.

> ⚠️ **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.

1. Откройте документ в мастере.
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 электронной подписи приложение поясняет это строкой **«Размер и положение заданы документом — здесь их не изменить»**.

Сохранение документа без электронной подписи

Документ можно подписать от руки или разметить для других, не ставя электронную подпись: добавить рукописную подпись, места для подписантов и произвольную область и сохранить копию документа.

1. Откройте документ в мастере.
2. Выключите переключатель в заголовке блока **Электронная подпись** на правой панели. Настройки электронной подписи и переключатель **Сертифицировать документ** скроются: сертификат не нужен. Мастер запомнит выбор и в следующий раз откроет документ с выключенной электронной подписью.

> 💡 **Примечание**: пока вы ни разу не меняли этот переключатель, он включён, если на компьютере есть сертификат для подписи, и выключен, если сертификата нет.

Чтобы вернуть электронную подпись, включите переключатель снова или нажмите **Электронная подпись** на панели действий: мастер включит её и вернёт место подписи, которое было до выключения. Если места ещё не было, мастер предложит указать его на странице.

1. Добавьте рукописную подпись (см. Рукописная подпись), подписантов (см. Подписанты) или произвольную область (см. Произвольная область).
2. Если документ нужен в формате PDF/A, включите **Преобразовать в PDF/A** в блоке **Защита документа** сейчас: после первой подписи преобразовать документ уже нельзя.
3. Нажмите **Подписать**, если поставили рукописную подпись, или **Сохранить**, если только разметили документ. Подтверждение не запрашивается: исходный файл не меняется, результат сохраняется в новый файл.

Новый файл сохраняется так же, как подписанный документ: в папку из блока **Сохранение результатов**, по умолчанию — рядом с исходным, под тем же именем с номером, например `<имя>(1).pdf`. После сохранения мастер откроет новый файл. Если сохранить и его, появится следующая копия — `<имя>(2).pdf`.

Подписанты поставят подписи в размеченные места (см. Создание подписи в размеченной области). Чтобы подписать документ позже самому, добавьте место и для себя.

> 💡 **Примечание**: без электронной подписи документ нельзя сертифицировать.

Проверка подписи PDF-документа

Откройте документ в мастере — проверка подписей запустится сама.

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»**. Чтобы открыть сведения о подписи, нажмите на неё в списке или на самой странице: пока сведения открыты, подпись обведена на странице цветом статуса.

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

Откройте в боковом меню раздел **Подписи** и выберите подпись. В панели появится блок **Сведения о подписи**: подписант, время подписания, статус сертификата и цепочки, штампы времени.

Если получить сведения не удалось, панель сообщит: **«Не удалось получить сведения о подписи»**.

Разметка документа

Разметка области для штампа подписи

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

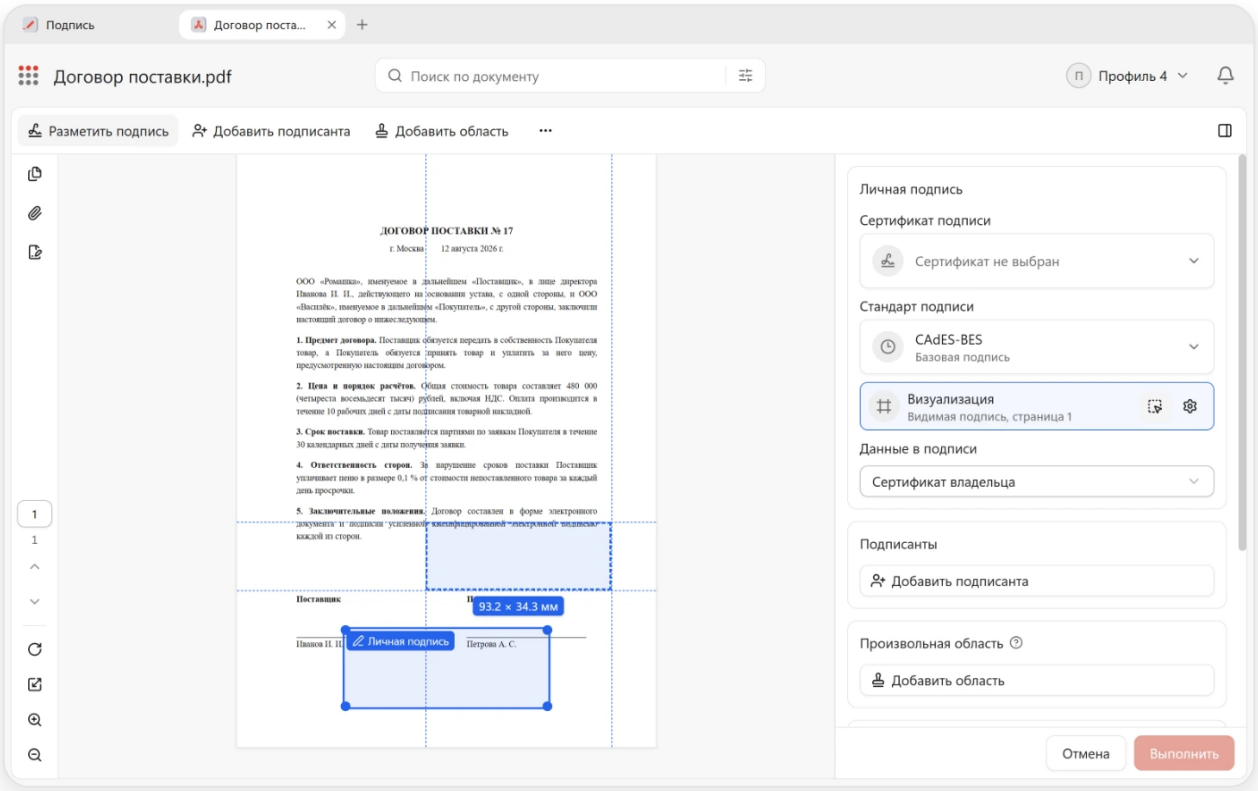
Состояние	Значение
Видимая подпись, не размечена	Место ещё не выбрано
Укажите место на странице	Разметка нажата и ждёт щелчка по странице
Видимая подпись, страница N	Штамп встанет на указанную страницу
В подготовленное место «…»	

Состояние	Значение
	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 подпись вставала на новое место во всех следующих документах, сохраните разметку в профиль.

Чтобы разметить место заново:

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



1. Нажмите кнопку свойств в той же строке. На вкладке **Внешний вид** настраивается оформление штампа: реквизиты, шрифт, цвета, рамка и логотип. На вкладке **Положение** — размер, положение и то, видима ли подпись.

Штамп занимает всю рамку. Если растянуть рамку, текст штампа останется прежнего размера, а полей вокруг станет больше; если сжать — строки перенесутся. Что видно на странице, то и попадёт в документ.

Если подпись была невидимой, разметка делает её видимой.

Видимость подписи при открытии документа берётся из профиля — переключатель **Видимый штамп подписи** в настройках PDF. Если переключить видимость в мастере, у профиля появится отметка **«Есть изменения»**; после **Сохранить изменения** так же будут подписываться следующие документы — в мастере, в разделе «Подпись и шифрование» и из контекстного меню. Если в профиле выбрана обычная подпись CMS/CAdES, мастер открывает документ с видимой подписью, и её видимость относится только к текущему документу.

Место подписи, поставленное командой **Электронная подпись**, относится к текущему документу; чтобы оно действовало и для следующих, нажмите **Сохранить разметку**.

Работа с местами на странице — личной подписью, подписантом, областью, рукописной подписью:

- **свойства** — двойной щелчок по месту или Enter, когда оно выделено;
- **сдвиг** — стрелки, с Shift шаг крупнее;
- **удаление** подписанта или области — Delete или значок корзины в строке места;
- **отмена перетаскивания** — Esc: место вернётся туда, где было.

После нажатия команды разметки под курсором виден контур будущего места — щелчок поставит его там. Размер контура — как у последнего такого же места. Красный контур означает, что место наложится на другое. Чтобы отменить разметку, нажмите Esc или ту же команду ещё раз. Щелчок по строке места на панели прокручивает документ к нему.

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	Действительная подпись, которая уже есть в документе
Красная	Недействительная подпись, а у размечаемого места — наложение на другое: сдвиньте одно из них
Серая	Подпись, которая ещё не проверена или которую не удалось проверить
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. Нажмите **Место подписанта** на панели действий или **Добавить подписанта** в блоке **Подписанты**.
2. Обведите прямоугольник на странице или щёлкните по ней. Свойства места откроются сами, курсор будет в поле **Название**.
3. Укажите **Название** — например, фамилию будущего подписанта.

Чтобы добавить невидимых подписантов, нажмите **Добавить подписанта** столько раз, сколько их нужно, и завершите Esc. Каждый, кого вы не разметили на странице, останется невидимым полем: его строка покажет **«Невидимая подпись»**, а разметить место позже можно кнопкой **Разметить** в этой строке.

Такие места отображаются со статусом **«Ожидает 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 удалить подписанта из документа, нажмите **Удалить** (значок корзины) в строке с его именем или выделите его место на странице и нажмите Delete.

> 💡 **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.

В документе может быть до десяти произвольных областей.

Разметка произвольной области

1. В блоке **Произвольные области** нажмите **Добавить область**.
2. Обведите прямоугольник на странице. Свойства новой области откроются сами, на вкладке **Внешний вид**, — пока в ней ничего нет, в списке она отмечена как **Не заполнена**.
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 на вкладке **Положение** в строке **Повторять** можно задать, на каких страницах она появится: **Нет** — только на этой, **На всех** (с возможностью исключить отдельные) или **Выборочно** — списком номеров, например `1-3, 7`.

Удаление произвольной области

Чтобы удалить произвольную область из документа, нажмите **Удалить** (значок корзины) в строке области или выделите её на странице и нажмите Delete.

Рукописная подпись

Рукописная подпись — изображение вашего росчерка на странице. Это не электронная подпись: юридическую силу она имеет, только если это допускает закон или соглашение сторон. Например, её нельзя использовать в доверенностях, платёжных и кадровых документах, счетах-фактурах.

Рукописную подпись можно поставить и с электронной подписью, и без неё — это решает переключатель в заголовке блока **Электронная подпись**. Если переключатель включён, документ будет подписан и электронной подписью, и она защитит рукописную от изменений. Если выключен, сохранится копия только с рукописной подписью (см. Сохранение документа без электронной подписи).

Рукописную подпись ставит только этот мастер: при подписании в разделе «Подпись и шифрование» или из контекстного меню она не добавляется. Её место можно сохранить в профиль вместе с остальной разметкой (см. Разметка по профилю) — вместе с выбранным для неё образцом.

В документе может быть до десяти рукописных подписей.

Постановка рукописной подписи

1. Нажмите **Рукописная подпись** на панели действий или **Добавить рукописную подпись** в блоке **Рукописные подписи**.
2. Щёлкните на странице, куда поставить подпись, или обведите для неё прямоугольник.

3. Если образцов подписи ещё нет, свойства подписи откроются сами, на вкладке **Образцы подписи**, — пока образца нет, в списке подпись отмечена как **Нет образца**. Распишитесь мышью, трекпадом или пером в поле на вкладке **Нарисовать** или выберите изображение на вкладке **Загрузить** (PNG с прозрачным фоном или JPEG). Затем нажмите **Сохранить образец**: подпись встанет в рамку, а высота рамки подстроится под пропорции образца.
4. Нажмите **Подписать**. С электронной подписью мастер попросит подтверждение и подпишет документ, без неё — сразу сохранит копию.

Для следующих рукописных подписей образец не запрашивается: после нажатия **Рукописная подпись** достаточно щёлкнуть на странице, и подпись встанет последним использованным образцом, сохранив его пропорции. Другой образец выбирается в свойствах рукописной подписи на вкладке **Образцы подписи** — там же можно добавить новый или удалить ненужный. Хранится до пяти образцов. Чтобы повторить подпись на нескольких страницах, используйте строку **Повторять** на вкладке **Положение**.

Удаление рукописной подписи

Нажмите **Удалить** (значок корзины) в строке подписи в блоке **Рукописные подписи** или выделите её на странице и нажмите Delete. Образец при этом не удаляется и остаётся на вкладке **Образцы подписи**.

Разметка по профилю

Если документы одного вида подписываются одинаково, разметку можно сделать один раз и сохранить в профиль подписи: место вашей подписи, места подписантов с их названиями, места рукописных подписей и произвольные области вместе с их текстом или изображением.

1. Разметьте документ.
2. Нажмите **Сохранить разметку** на панели действий — справа от кнопок разметки. Разметка сохранится в активный профиль — он выбран в шапке окна.

Кнопка активна, только когда разметка на экране отличается от сохранённой в профиле. Пока вы ничего не меняли и сразу после сохранения она неактивна, а подсказка сообщает, что разметка уже сохранена. В разметку входит всё, что размечено на странице: если какое-то место не нужно в следующих документах, удалите его перед сохранением.

Чтобы завести разметку для нового вида документов в отдельном профиле, разметьте документ, добавьте профиль в панели профилей и нажмите **Сохранить разметку**. Разметка, которую вы изменили, при смене профиля остаётся на месте и сохранится в новый профиль.

Следующий документ, открытый в мастере с этим профилем, будет уже размечен. Места встают у того же края страницы, с теми же отступами и того же размера. Размер рамки вашей подписи сохраняется как размер штампа в профиле, поэтому и подпись без мастера — из контекстного меню или в разделе «Подпись и шифрование» — выйдет такой же. Место на последней странице встаёт на последнюю страницу документа любой длины, остальные — на страницу с тем же номером, а если документ короче — на первую. Поэтому размечайте документ обычной для этого вида длины: на одностраничном все места сохранятся как места на последней странице. Пока вы не меняли разметку, она следует профилю: если выбрать другой профиль, документ будет размечен по нему.

Рукописная подпись сохраняется вместе с образцом, которым она нарисована: на следующем документе каждое место нарисует свой образец. Если этот образец вы удалили, место нарисует последний использованный образец, а высота подстроится под его пропорции. Если образцов на компьютере нет совсем, место встанет пустым и будет отмечено как **Нет образца**: откройте его свойства и на вкладке **Образцы подписи** распишитесь или выберите изображение.

Места подписантов, рукописные подписи и произвольные области ставятся только на документ, который ещё не подписывали и не размечали, и сохранить разметку можно только с такого документа. На уже подписанном документе — электронной подписью или от руки — и на документе, сохранённом с произвольной областью, размечается только ваша подпись: остальные места уже стоят на его страницах. На документе с местами, ожидающими подписи, не размечается ничего: выберите своё место в разделе **Подписи**.

Чтобы убрать места из профиля, удалите их в документе и снова сохраните разметку.

> 💡 **Примечание**: место вашей подписи сохраняется в настройки штампа профиля и действует при любом подписании этим профилем. Остальную разметку ставит только мастер.

Подтверждение операции

Перед подписанием открывается окно **«Подтверждение»**. В нём указано, что будет выполнено и для скольких файлов, — например, **«Будет выполнено: электронная подпись для 1 файла»**. Если выбранный сертификат подписи недействителен, окно предупредит: **«Выбранный сертификат недействителен. Всё равно использовать его?»**.

Нажимая **Подписать**, вы подтверждаете ознакомление с подписываемым документом. Отказаться от операции можно кнопкой **Отмена**.

Возможные ошибки

Технические подробности отказа записываются в журнал событий.

Ошибки при открытии файла

Сообщение	Что это значит	Что сделать
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	

Сообщение	Что это значит	Что сделать
		Запросите у отправителя исправный файл либо снимите пароль в программе, где он был поставлен
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

Сообщение	Что это значит	Что сделать
Нет сертификатов подписи	В хранилище нет сертификатов, которыми можно подписывать	Нажмите **Перейти к сертификатам** под полем и установите свой сертификат
Выберите сертификат подписи	Не указано, каким сертификатом подписывать	Выберите сертификат в блоке **Электронная подпись**
Разметьте место электронной подписи на странице	Не указано, где на странице встанет подпись	Нажмите **Разметить** в строке **Визуализация** и обведите место
Разметьте рукописную подпись на странице или удалите её	Рукописная подпись добавлена, но не поставлена на страницу	Щёлкните на странице или удалите её в блоке **Рукописные подписи**
Выберите образец рукописной подписи или удалите её	Место рукописной подписи размечено, но образец для него не выбран	Откройте свойства подписи и на вкладке **Образцы подписи** выберите или создайте образец
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

Сообщение	Что это значит	Что сделать
Произвольная область запрещена сертификацией документа — удалите её	Автор документа разрешил добавлять только подписи	Уберите произвольную область и повторите подписание
Рукописные подписи запрещены сертификацией документа — удалите их	Автор документа разрешил добавлять только электронные подписи	Удалите рукописные подписи и повторите подписание
Добавьте рукописную подпись, подписанта или произвольную область	Электронная подпись выключена, а сохранять нечего	Добавьте рукописную подпись, подписанта или произвольную область
Не удалось сохранить документ без электронной подписи	Копию не удалось записать в папку результатов	Проверьте, что папка из блока **Сохранение результатов** доступна
Не удалось преобразовать PDF в PDF/A	Документ не удалось преобразовать перед сохранением	Выключите **Преобразовать в PDF/A** или смените формат
Изображение больше 8 МБ — выберите файл меньше	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
Уже сохранено пять образцов — удалите один, чтобы добавить новый	Хранится не больше пяти образцов подписи	Удалите ненужный образец на вкладке **Образцы подписи**
Не удалось сохранить изображение как образец — выберите другой файл	Файл повреждён или не является изображением	Выберите другой файл PNG или JPEG
Изображение больше 20 МБ — выберите файл меньше	Файл для образца подписи слишком велик	Уменьшите изображение или выберите другой файл

Ошибки самой операции подписи — отсутствие лицензии, недоступный модуль CAdES, отказ криптопровайдера — совпадают с ошибками раздела **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 лицензий — лицензии КриптоАРМ и КриптоПро CSP.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Настройки подписи и шифрования

Справочник настроек подписи и шифрования. Их задают перед операцией и сохраняют в профиле подписи.

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 разделе Подпись и шифрование.

Личная подпись

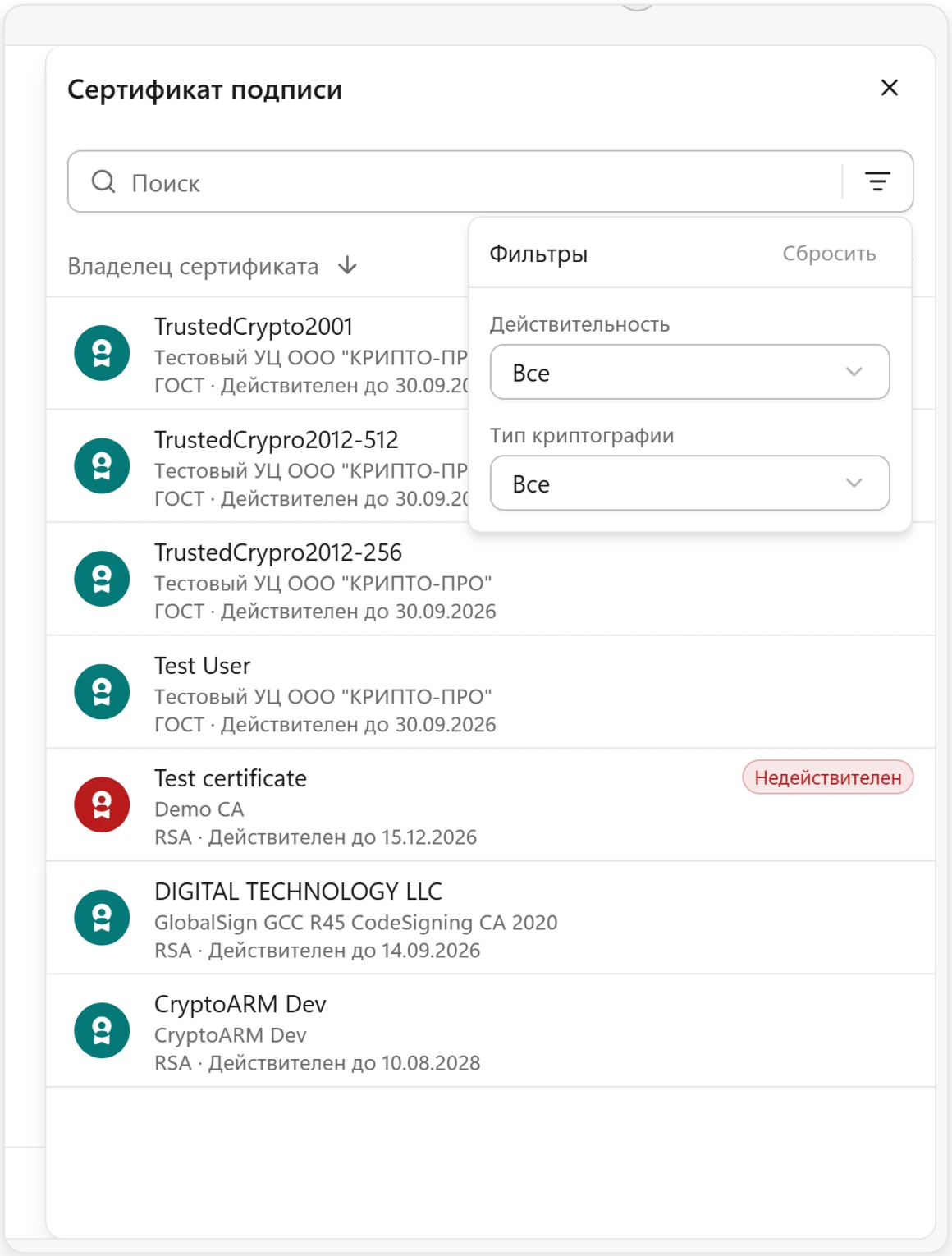
В блоке **Личная подпись** указывается сертификат, которым будет подписан документ, стандарт подписи и машиночитаемая доверенность.

Выбор сертификата подписи

Сертификат подписи — сертификат из хранилища **Личные сертификаты**, 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»**.

Сертификат, установленный не через приложение — например, средствами КриптоПро CSP, — появится в списке после нажатия кнопки **Обновить** в заголовке панели.

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 установлены компоненты КриптоПро ЭЦП (CAdES)	Запустите установщик КриптоАРМ ещё раз

> 💡 **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	`CAdES-BES`, `CAdES-T`, `CAdES-X Long Type 1`, `CAdES-A`

Название настройки	Значение по умолчанию	Описание	Допустимые значения
		подпись для долговременного хранения.	

> 💡 **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

Название настройки	Значение по умолчанию	Описание	Допустимые значения
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
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

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)
	`Выкл`		`Вкл` / `Выкл`

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Убрать служебные заголовки		Доступна для кодировки `BASE-64`. Убирает строки `-----BEGIN...` и `-----END...`	

> 💡 **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, а в блоке **Визуальное оформление** — будет ли виден штамп подписи. Какой переключатель там показан, зависит от способа.

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)`
Видимый штамп подписи	`Выкл`	Только для PAdES. Добавляет в PDF видимую область подписи. Криптографическая подпись при этом не меняется — меняется её отображение. С этой видимостью открывает документ и мастер Подпись и защита PDF	`Вкл` / `Выкл`
Печатная копия со штампом	`Выкл`	Только для CMS/CAdES. Кроме файла подписи создаётся неподписанный PDF со штампом — см. Печатная форма	`Вкл` / `Выкл`

При включённом штампе или печатной копии становятся доступны кнопки **Внешний вид штампа** и **Положение штампа**.

Внешний вид штампа подписи

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, 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	Шестнадцатеричный код 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 **Внешний вид штампа** в разделе **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.

Включённые реквизиты стоят в начале списка в том порядке, в каком выводятся в штампе. Новый реквизит добавляется последним; чтобы изменить порядок, перетащите строку за значок слева от неё.

> 💡 **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 — в палитре или шестнадцатеричным кодом.
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

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Видимость	`Невидимая`	То же, что переключатель **Видимый штамп подписи**	`Видимая`, `Невидимая`
Размер (**Ш**, **В**)	`102,3 мм`, `39,16 мм`	Ширина и высота 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`
Привязка	`Снизу, по центру`	Угол, край или центр страницы, к которому привязан штамп	Любой угол, середина любого края, центр страницы
Снизу (**Сверху**), **Слева** (**Справа**)	`20 мм` снизу	Отступ от края страницы, к которому привязан штамп	Отступ в миллиметрах
Повторять	`Нет`		`Нет`, `На всех`

Название настройки	Значение по умолчанию	Описание	Допустимые значения
		Повторяет изображение штампа на каждой странице	

Настройка размера и положения штампа подписи

1. Откройте окно настроек:

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

1. В блоке **Размер и положение** задайте:

- **Размер** — ширина (**Ш**) и высота (**В**) штампа в миллиметрах;
- **Страница** — чтобы штамп был на каждой странице, в строке **Повторять** выберите **На всех**;
- **Ориентация**;
- **Привязка** — клетка на схеме страницы: к какому углу, краю или центру привязан штамп. Цветная полоса у схемы — край страницы, от которого отсчитывается отступ: фиолетовая — сверху или снизу, бирюзовая — слева или справа;
- отступы от краёв страницы, к которым привязан штамп, — в полях рядом со схемой. При привязке по центру отступ не нужен, и поля для него нет.

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

Настройки защиты PDF-документа

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Сертифицировать документ	Выкл	Подпись становится сертифицирующей: после неё разрешены только заполнение форм и новые подписи. Такая подпись должна быть первой в документе	Вкл / Выкл
Преобразовать в 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 преобразовании возникнут ошибки	`Преобразовать страницы с ошибками в изображения`	Поведение при ошибках преобразования	`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

Переключатель **Печатная копия со штампом** в настройках PDF создаёт при подписи отдельную копию PDF-документа со штампом. Электронной подписи в копии нет: она предназначена для просмотра и печати. Переключатель доступен при способе **Обычная подпись CMS/CAdES**.

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**: добавьте в получатели свой сертификат, если файл понадобится расшифровать вам самим.

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Сертификаты шифрования	-	Сертификаты, которые будут использованы при шифровании	Сертификаты из хранилищ **Личные сертификаты** 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, фильтрами и кнопкой **Обновить** — 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

> 💡 **Примечание**: алгоритмы ГОСТ доступны, если установлен 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
Добавлять ФИО подписанта	`Выкл`	Добавляет имя подписанта (CN) из сертификата к имени файла после пользовательского суффикса	`Вкл` / `Выкл`

Название настройки	Значение по умолчанию	Описание	Допустимые значения
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»**.

Существующие файлы не перезаписываются. Если файл с именем результата уже есть, к имени добавляется номер — перед расширением документа, а расширения подписи и шифрования остаются после него: `договор(1).pdf.sig`, `отчёт-v1.0(1).pdf`. Так же нумеруются отчёты о проверке, файлы, сохранённые с экрана операций, и результаты командной строки и внешнего API.

> 💡 **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, быстрые действия Finder или меню файлового менеджера Linux (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 лицензий — 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, из контекстного меню файлового менеджера Linux или двойным щелчком по файлу подписи.

Содержание:

- Команды контекстного меню
- Быстрые действия Finder на macOS
- Меню файлового менеджера на Linux
- Подпись профилем
- Проверить и расшифровать
- Проверить и расшифровать с отчётом
- Объединить подписи
- Команды «Открыть для...»
- Как приложение выбирает интерфейс
- Уведомления о результате
- Открытие файлов двойным щелчком
- Возможные ошибки
- Смотрите также

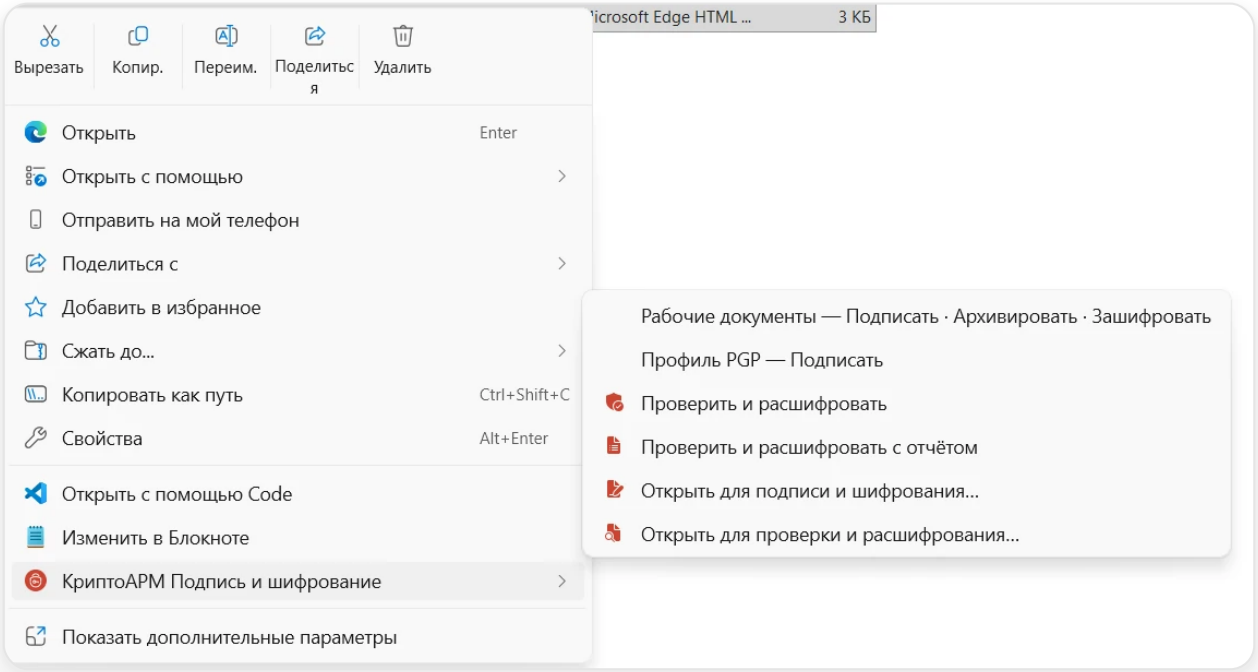
Команды контекстного меню

> 💡 **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 есть не во всех дистрибутивах — см. Меню файлового менеджера на Linux.

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
```

```
├── Объединить подписи
├── 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 команды КриптоАРМ находятся в подменю **Быстрые действия** контекстного меню Finder. Команды те же, что в Проводнике, узнать их можно по значкам:

```
Быстрые действия
├── КЭП CAdES-T — Подписать
├── Объединить подписи
├── 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.

Меню файлового менеджера на Linux

Пункт **КриптоАРМ Подпись и шифрование** с теми же командами, что в Проводнике, появляется в контекстном меню файлового менеджера в дистрибутивах:

- Альт Рабочая станция 11;
- РЕД ОС 8;
- Ubuntu 20.04, 22.04, 24.04, 26.04 и 26.10.

Меню есть и в файловом менеджере Dolphin среды KDE (Plasma 5 и 6). Команда **Объединить подписи** там показана всегда — в том числе при одном выделенном файле.

В Astra Linux меню нет — операции запускаются из окна приложения.

Если после установки пункта в меню нет, запустите приложение один раз и войдите в систему заново.

Новые версии GNOME

GNOME обновляется дважды в год, и поддержка новой версии файлового менеджера «Файлы» появляется в обновлениях приложения. Если система обновилась, а пункта в меню нет, установите последнюю версию приложения.

Можно не ждать обновления и включить меню самостоятельно:

1. Узнайте версию файлового менеджера командой `nautilus --version`. Нужно первое число — например, `52` в ответе `GNOME nautilus 52.0`.
2. Выполните команду, подставив это число:

```
mkdir -p ~/.config/cryptoarm-sign && echo 52 >> ~/.config/cryptoarm-sign/nautilus-allowed &&
nautilus -q
```

Так меню включается до следующего обновления GNOME. Если с ним файловый менеджер будет работать нестабильно, выключите меню — см. Как выключить меню в файловом менеджере GNOME.

Как выключить меню в файловом менеджере GNOME

Если файловый менеджер «Файлы» не открывается или закрывается сам, выключите в нём меню КриптоАРМ. Приложение продолжит работать, операции запускаются из его окна. Выполните в терминале:

```
mkdir -p ~/.config/cryptoarm-sign && touch ~/.config/cryptoarm-sign/nautilus-disabled &&
nautilus -q
```

Администратор может выключить меню сразу для всех пользователей компьютера:

```
sudo install -d -m 755 /etc/cryptoarm-sign && sudo touch /etc/cryptoarm-sign/nautilus-disabled
```

Настройка сохраняется при обновлении приложения. Чтобы вернуть меню, выполните:

```
rm ~/.config/cryptoarm-sign/nautilus-disabled && nautilus -q
```

Если меню выключал администратор, его возвращает команда `sudo rm /etc/cryptoarm-sign/nautilus-disabled`; меню появится после повторного входа в систему.

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.

Объединить подписи

Команда сводит отсоединённые подписи X.509 одного документа, сделанные разными подписантами, в один файл подписи — так же, как кнопка **Объединить подписи** в разделе «Подпись и шифрование». Новой подписи она не создаёт, сертификат и ПИН-код не нужны, но нужен КриптоПро CSP.

Выделите два или больше файлов подписи одного документа — например, `договор.pdf.sig` и `договор.pdf.p7s`. Файлы с другими расширениями команда пропускает. В Проводнике и в файловом менеджере GNOME при одном выделенном файле команды в меню нет.

Результат сохраняется рядом с первой из выделенных подписей под именем `договор_joined_2_signs.pdf.sig`, где число — количество подписей в получившемся файле. Имя берётся из общей части имён подписей, поэтому ФИО подписантов в него не попадают: `договор_Иванов Иван Иванович.pdf.sig` и `договор_Петров Пётр Петрович.pdf.sig` тоже дают `договор_joined_2_signs.pdf.sig`. Результат прошлого объединения можно выделить вместе с новыми подписями: его подписи войдут в число, а метка `_joined_…_signs` в имени заменится, а не допишется. Так собирают подписей больше, чем команда принимает файлов за раз. Исходные подписи остаются на месте, существующие файлы не перезаписываются. Щелчок по уведомлению показывает результат в папке.

> ⚠️ **Важно**: выделяйте подписи только одного документа. Приложение не сверяет, что подписан один и тот же файл, и подписи разных документов окажутся в одном файле — при проверке часть из них будет недействительной.

Подписи OpenPGP команда не объединяет.

Команды «Открыть для...»

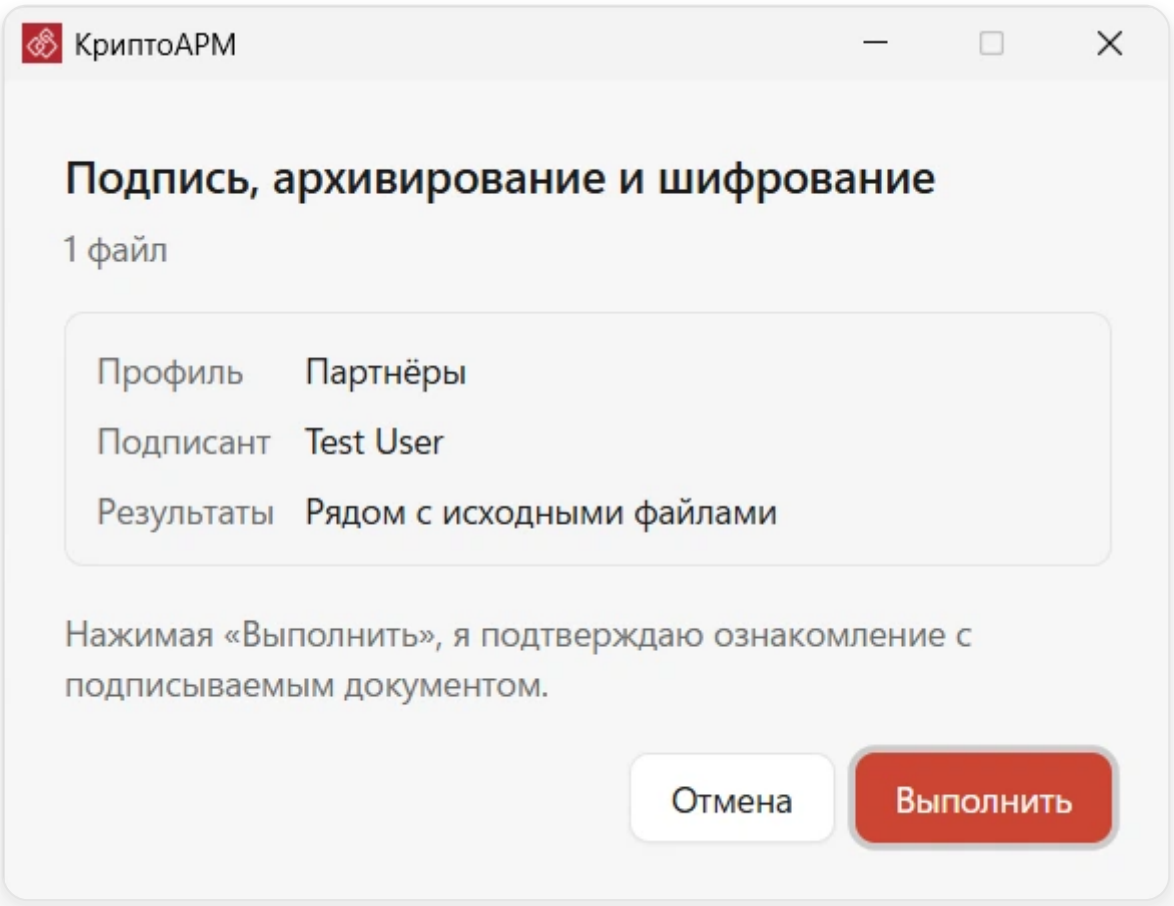
Две команды передают выбранные файлы в приложение, не запуская операцию:

- **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

Окно появляется, только если без него не обойтись:

Что вы увидите	Когда
Только уведомление о результате	Профиль не требует подтверждения, а пароль или ПИН-код не нужен либо его запрашивает КриптоПро CSP
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
Окно приложения	Профиль недоступен или заполнен не полностью — например, в нём не выбран сертификат



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.

Если закрыть окно до запуска операции, она отменяется.

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
Подписи объединены	Команда «Объединить подписи» сохранила файл с подписями, в тексте — сколько в нём подписей
Не удалось объединить подписи	Объединить подписи не получилось — причина в тексте уведомления или в журнале
Запрос не выполнен	Выделенные файлы не приняты — 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 зашифрованных данных, 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	Выделено 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
Для объединения подписей необходимо минимум два файла подписи	Среди выделенных меньше двух файлов подписи	Выделите две или больше подписи одного документа
Для объединения подписей требуется КриптоПро CSP	КриптоПро CSP не установлен	Установите КриптоПро CSP
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

Командная строка (CLI) КриптоАРМ подписывает, шифрует, расшифровывает и проверяет файлы без окна приложения. Здесь собраны команды, параметры и 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
- Лицензия
- Работа с OpenPGP
- Результат и ошибки
- Смотрите также

Общая информация

Командная строка предназначена для автоматизации — выполнения операций без участия пользователя в составе систем обмена и сценариев `.bat` и `.sh`.

Важные замечания

- Перед использованием CLI убедитесь, что приложение готово к работе с электронной подписью: сертификат установлен, лицензия активирована. Лицензию можно установить и из командной строки — см. Лицензия.

Подготовка описана в инструкции Быстрый старт.

- 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`. Сертификат, которого нет в хранилище, даёт ошибку `X.509 certificate not found` — сверьте идентификатор по выводу `certificates`.
- 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/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	—

Параметр	Описание	По умолчанию
`--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`;
- если путь файла результата — существующая папка, результат сохраняется в неё под стандартным именем, как при указании папки результата;
- 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
`--save-copy`	Принимается для совместимости и ничего не меняет: копия результата не сохраняется (`sign`, `encrypt`, `decrypt`)	Отключено
`-h, --help`	Справка по команде; без команды — список команд	—

> 💡 **Примечание**: подробный лог для обращения в поддержку включается переменной окружения `CRYPTOARM_TRACE=1` — отдельной настройки у CLI для этого нет. Записи попадают в общий файл лога `cryptoarm.log` в папке технических логов.

Список команд

Команда	X.509	OpenPGP
`sign` / `sig`	✓	✓
`encrypt` / `enc`	✓	✓
`sign-encrypt` / `se`	✓	✓
`archive` / `arc`	✓	—
`decrypt` / `dec`	✓	✓
`verify` / `ver`	✓	✓
`verify_ts` / `vts`	✓	—
`unsign`	✓	—
`certificates` / `cer`	✓	✓

Подпись

Команда: `sign` или `sig`

Команда подписывает один или несколько 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. Без `--signed-file-path` и `--folder-save-signed` соподпись записывается в тот же файл, с ними исходный файл не меняется. 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>`		—

Параметр	Описание	По умолчанию
	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
`--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	—

Объединённая подпись сохраняется рядом с первой подписью как `<имя>_joined_<N>_signs<расширение>`. С `--signed-file-path` она записывается в указанный файл, с `--folder-save-signed` — в указанную папку.

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
`--visual-copy`	Без `--pades`: сохранить рядом копию PDF со штампом без подписи — `<файл>_штамп.pdf`	Отключено
`--pades-certify`, `--certification`	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`

Параметр	Описание	По умолчанию
`--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-field <имя>`	Подписать готовое поле подписи PDF с этим именем	—
`--pades-add-signer-name`	Добавить имя подписанта в имя PDF-файла	Отключено
`--pades-signer-name <имя>`	Имя подписанта для имени PDF-файла	—
`--overwrite-original-pdf`	Заменить исходный PDF подписанным	Отключено

> ⚠️ **Важно**: параметр `--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. Если заменить файл не удалось, исходный PDF остаётся без изменений.

С `--pades-field` подпись встаёт в готовое поле документа — например, на место одного из подписантов в форме, которую подготовила система документооборота. Место и размер штампа задаёт поле: штамп вписывается в него с сохранением пропорций, а поле без размеров на странице даёт невидимую подпись. Параметры размещения (`--pades-page`, `--pades-x-mm`, `--pades-placement`, `--pades-all-pages` и аналогичные `--stamp-*`) не используются, а `--pades-width-mm` и `--pades-height-mm` задают только пропорции штампа. Имя поля указывается точно, с учётом регистра. Если поля нет или оно уже подписано, файл не подписывается.

```
cryptoarm-sign sign --source-file ./form.pdf --cert <серийный номер> \
  --pades --pades-field "Signer3"
```

К документу, в котором уже есть поля подписи, `--pades-pdfa` не применяется: преобразование испортило бы подписи и поля. Документ, сертификация которого запрещает любые изменения, не подписывается.

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	—
`--stamp-padding-bottom <мм>`	Отступ снизу	—
`--stamp-horizontal-align <x>`	По горизонтали: `left`, `center`, `right`	`center`
`--stamp-vertical-align <y>`	По вертикали: `top`, `center`, `bottom`	`bottom`
`--stamp-color <#RRGGBB>`	Цвет текста и границы	`#000000`
`--stamp-background-color <#RRGGBB>`	Цвет фона	`#ffffff`
`--stamp-title <текст>`	Заголовок штампа	«Документ подписан электронной подписью»
`--stamp-no-background`	Прозрачный фон под штампом	Отключено
`--stamp-page <номер>`	Страница размещения	Последняя

Параметр	Описание	По умолчанию
`--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`.

Отступы отсчитываются от края, к которому прижат штамп: с `--stamp-vertical-align top` значение `--stamp-padding-bottom` — это отступ сверху. Если для положения штампа указаны и `--pades-*`, и `--stamp-*`, действуют `--pades-*`.

Параметры, неприменимые к вызову, не останавливают подпись: они пропускаются, а в stderr выводится предупреждение. Так обрабатываются `--certification`, `--signer-name`, `--reason`, `--location` и `--contact-info` без `--pades`, параметры `--stamp-*` без `--pades` и `--visual-copy`, а также `--visual-copy` вместе с `--pades` — тогда создаётся только подпись PAdES. Значения штампа приводятся к допустимым: короткая запись цвета `#f00` равна `#ff0000`, неверный цвет заменяется цветом по умолчанию, заголовок обрезается до 120 символов, масштаб — до диапазона от 0,5 до 4. Параметры `--pades-*` без `--pades` по-прежнему дают ошибку.

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	—

Файлы МЧД попадают в каждый архив с результатом: в общий архив, в каждый архив при `--separate-archives` и в каждый пакет отсоединённой подписи с исходным файлом при шифровании. Рядом с результатом они копируются, только если результат не упакован в архив.

Сетевые параметры

Параметр	Описание	По умолчанию
`--tsp <url>`	Адрес службы штампов времени	—
`--ocsp <url>`	Адрес службы OCSP	—
`--proxy <адрес>`	Адрес прокси-сервера	—

Параметр	Описание	По умолчанию
`--proxy-port <порт>`	Порт прокси	—
`--proxy-login <логин>`	Логин для прокси	—
`--proxy-password <пароль>`	Пароль для прокси	—

Для стандартов `cades-t`, `cades-xlt1` и `cades-a` параметр `--tsp` обязателен. Адреса `--tsp` и `--ocsp` можно взять в одинарные кавычки — они отбрасываются.

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	—

Если файл с указанным именем уже есть, он не перезаписывается: результат получает номер перед расширением документа — `документ(1).pdf.sig`. Так же нумеруются результаты в папке и результаты остальных команд. Перезаписывается только файл подписи, к которому добавлена соподпись без `--signed-file-path` и `--folder-save-signed`.

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 шифрует один или несколько 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	—

Параметр	Описание	По умолчанию
`--folder-save-encrypted <папка>`	Папка для зашифрованных файлов	—

Алгоритм задаётся именем или OID:

Имя	OID	Алгоритм
`gost-28147`	`1.2.643.2.2.21`	ГОСТ 28147-89
`gost-2015-magma`	`1.2.643.7.1.1.5.1[.1|.2]`	Магма
`gost-2015-kuznyechik`	`1.2.643.7.1.1.5.2[.1|.2]`	Кузнечик
`aes-256-cbc`	`2.16.840.1.101.3.4.1.42`	AES-256-CBC
`des3-cbc`	`1.2.840.113549.3.7`	DES3-CBC

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 расшифровывает один или несколько 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 проверяет 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	—
`--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	—
`-r, --save-report [путь]`	Только `verify_ts`: 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`. Файлы `.bin` и `.pem`, которые не являются подписью, — например, сертификаты и ключи, — пропускаются.

Без указания пути отчёты сохраняются рядом с проверяемыми файлами: отдельные PDF — как `<файл>_report.pdf`, общий — как `merged_report_<дата и время>.pdf`. Указанная для PDF-отчётов папка создаётся, если её нет. Существующие файлы не перезаписываются: к имени добавляется номер — `<файл>_report(1).pdf`, а пути созданных отчётов возвращаются в поле `reports` итогового JSON.

JSON-отчёт сохраняется на каждый проверенный файл как `reportFile-<файл>.json` — рядом с проверяемыми файлами или в указанной существующей папке. Если указан путь, который не является существующей папкой, создаётся один файл со всеми результатами. Отчёт записывается в формате результата проверки API: `method: "verify"`, в `params` — `status` и `verifySignResults` с полями `signValid`, `signers[].isValid`, `signers[].signerCertificate` (`serial`, `subjectFriendlyName`, `notBefore`, `notAfter` и другие). Время указывается в миллисекундах с начала эпохи Unix.

С `--unsign` подпись сначала проверяется, затем извлекается исходный документ. Итоговый JSON содержит и результат проверки, и путь извлечённого файла. Документ извлекается и из недействительной подписи — тогда итоговый статус `Error` и код завершения ненулевой, поэтому полагаться на такой документ можно только при успешном результате.

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; без `--visual-copy` они пропускаются с предупреждением.

Недействительная подпись возвращает статус `Error` и ненулевой код завершения; отчёт при этом всё равно сохраняется. Если не удалось создать PDF-отчёт, ошибкой завершается вся операция.

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`

Параметр	Описание	По умолчанию
`--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 в формате JSON список личных сертификатов X.509 — из хранилища `MY`. Из него берутся идентификаторы для параметров `--cert` и `--sign-cert`. С `--all` выводятся все сертификаты: также промежуточные, корневые и сертификаты получателей — для `--recipient-cert`. С `--provider pgp` выводятся сертификаты OpenPGP.

```
cryptoarm-sign certificates
cryptoarm-sign certificates --all
cryptoarm-sign certificates --provider pgp
```

Та же команда перекодирует сертификаты и запросы на сертификат — см. Кодирование и декодирование файлов.

Лицензия

Лицензию КриптоАРМ можно установить и посмотреть без окна приложения. Эти параметры указываются без команды.

```
cryptoarm-sign --license-key <ключ>
cryptoarm-sign --license-info
```

Параметр	Описание
`--license-key <ключ>`	Проверить и установить лицензионный ключ
`--license-info`	Показать действующую лицензию, в том числе пробный период

Результат выводится в формате JSON: `status` — `Completed` или `Error`, в `license` — сведения о лицензии: состояние, редакция, срок действия, признак пробного периода. Ключ в выводе замаскирован. При ошибке установки в поле `error` указывается код, например `license.invalid`.

Лицензия устанавливается для всех пользователей компьютера, а если на это нет прав — только для текущего пользователя: тогда в выводе `fallbackUsed: true`. Ненулевой код завершения возвращается, если ключ не установлен, а для `--license-info` — если действующей лицензии нет.

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	Команды
`--cert <отпечаток...>`	Ключ подписи или получатели шифрования	`sign`, `encrypt`
`--sign-cert <отпечаток>`	Ключ подписи	`sign-encrypt`
`--recipient-cert <отпечатки...>`	Получатели	`sign-encrypt`
`--subkey <отпечаток>`	Подключ для подписи	`sign`, `sign-encrypt`
`--detached`	Отсоединённая подпись; по умолчанию — присоединённая (`--attached`)	`sign`, `sign-encrypt`
`--armor`	Сохранить результат в текстовом виде (ASCII armor)	`sign`, `encrypt`, `sign-encrypt`
`--archive`	Упаковать исходные файлы в один TAR-архив и подписать или зашифровать его	`sign`, `encrypt`, `sign-encrypt`
`--archive-name <имя>`	Имя TAR-архива	`sign`, `encrypt`, `sign-encrypt`
`--document <файл>`	Исходный файл для отсоединённой подписи	`verify`

Пути результата задаются теми же параметрами, что у X.509.

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.

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 сценариях.

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

Код	Что означает
`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 лицензий — лицензии КриптоАРМ и КриптоПро CSP.
- API КриптоАРМ — вызов операций из внешних систем.

Открыть статью на сайте

Раздел «Сертификаты»

Раздел **Сертификаты** показывает сертификаты, ключевые контейнеры, списки отзыва и запросы на сертификаты. Здесь описано, как устроен раздел, как выбрать профиль доверия и проверить сертификат.

Содержание:

- Обзор раздела «Сертификаты»
- Профили доверия
- Проверка статуса сертификата
- Сведения о сертификате
- Поиск сертификатов
- Смотрите также

Обзор раздела «Сертификаты»

Хранилища сертификатов

Хранилища перечислены в левой части окна. Выберите 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	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
Аккредитованные УЦ	Сертификаты аккредитованных удостоверяющих центров с сервера сетевого профиля 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

Хранилище	Назначение
Контейнеры	Ключевые контейнеры с закрытыми ключами

Под хранилищем **Других пользователей** располагаются группы сертификатов.

Таблица сертификатов

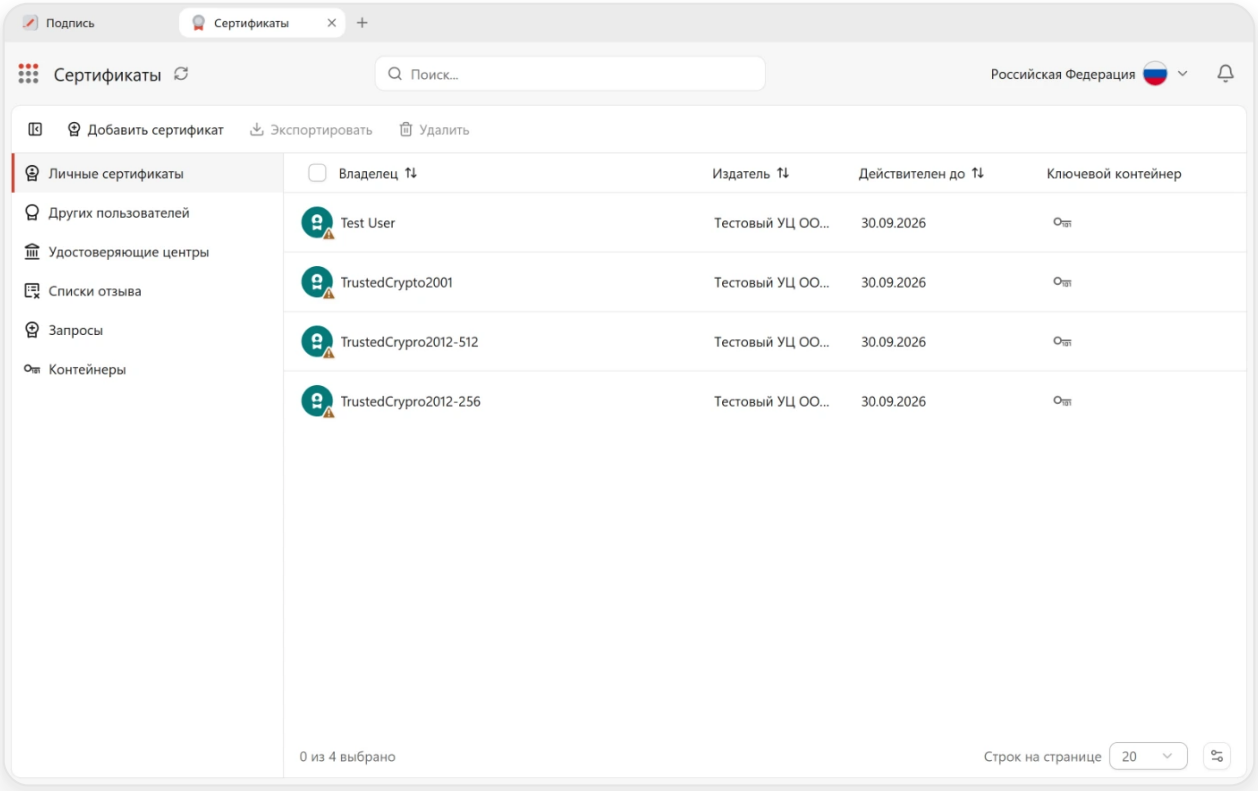


Таблица показывает владельца, издателя, срок действия, контейнер и алгоритм ключа. Набор и порядок столбцов можно поменять — см. Настройка столбцов.

Действия на панели работают и с несколькими выделенными сертификатами.

Профили доверия

Профиль доверия определяет, какие сертификаты показывает приложение:

Профиль	Отображаемые сертификаты
Российская Федерация	Сертификаты на алгоритмах ГОСТ — соответствие 63-ФЗ «Об электронной подписи»
Открытая криптография	Сертификаты на алгоритмах RSA и ECDSA
Сетевой профиль доверия	

Профиль	Отображаемые сертификаты
	Сертификаты на алгоритмах ГОСТ, как в профиле **Российская Федерация**, и сертификаты аккредитованных УЦ с сервера

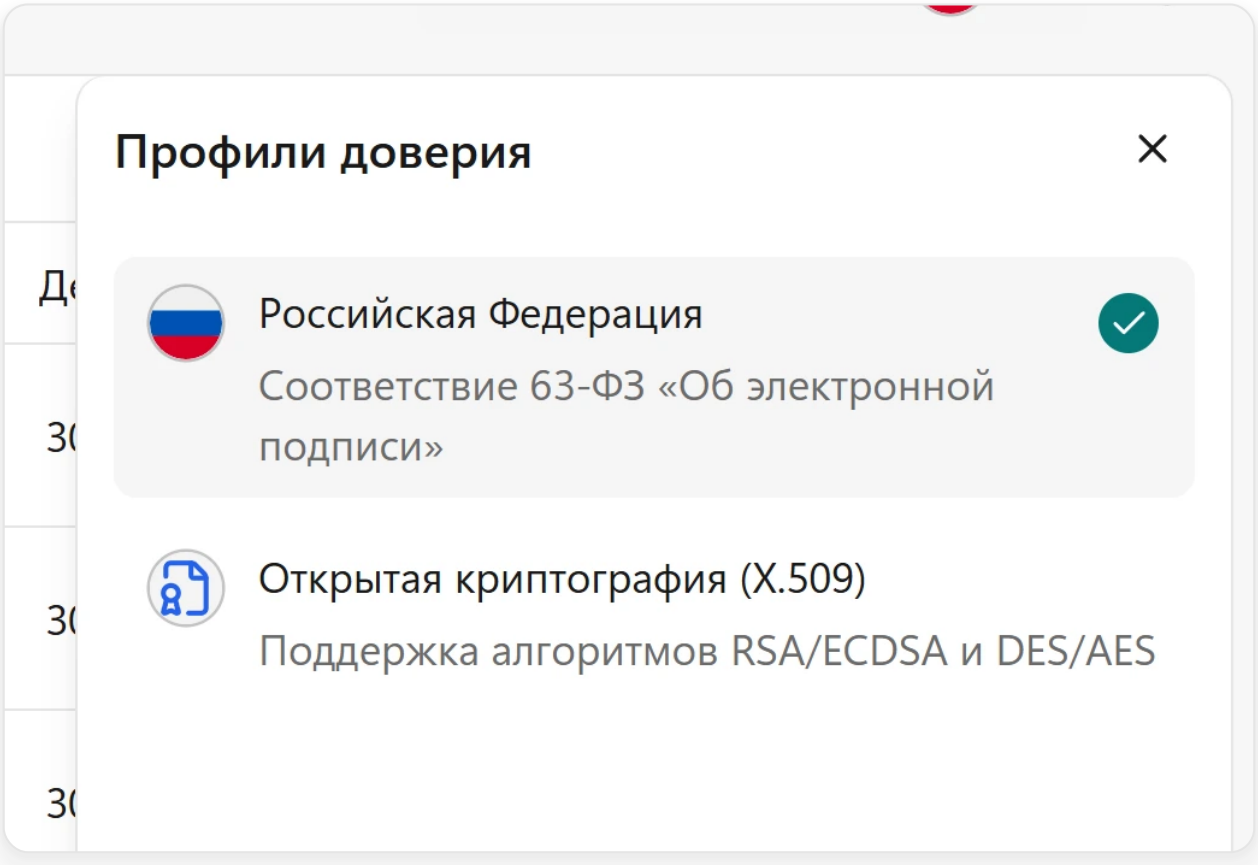
Профиль действует в разделе **Сертификаты** и в панелях выбора сертификатов при подписи и шифровании.

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.

> 💡 **Примечание**: профили «Российская Федерация» и «Открытая криптография» влияют только на отображение: сами сертификаты и операции от них не зависят. Сетевой профиль в режиме «Квалифицированная подпись» влияет и на результат проверки подписи — см. Режим «Квалифицированная подпись».

Переключение между профилями доверия

1. В разделе **Сертификаты** нажмите на название активного профиля в верхней части окна.
2. Выберите нужный профиль.



> 💡 **Примечание**: если в настройках выбран стандарт операций **OpenPGP**, раздел показывает сертификаты OpenPGP — см. О разделе OpenPGP.

Проверка статуса сертификата

Приложение проверяет срок действия сертификата, отзыв, цепочку доверия и — для личных сертификатов — связь с закрытым ключом.

Статус отображается в списке цветом значка сертификата:

Индикатор	Статус	Описание
🟢 Зелёный	Действительный	Сертификат прошёл проверку и может использоваться
🔴 Красный	Недействительный	Сертификат не прошёл проверку — 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.

О личном сертификате, срок действия которого или его закрытого ключа истекает в ближайшие 30 дней, приложение напоминает в центре уведомлений: один раз, а в последние 7 дней — ежедневно. Щелчок по напоминанию открывает личные сертификаты.

Статус сертификата и цепочка

В верхней части панели сведений 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:

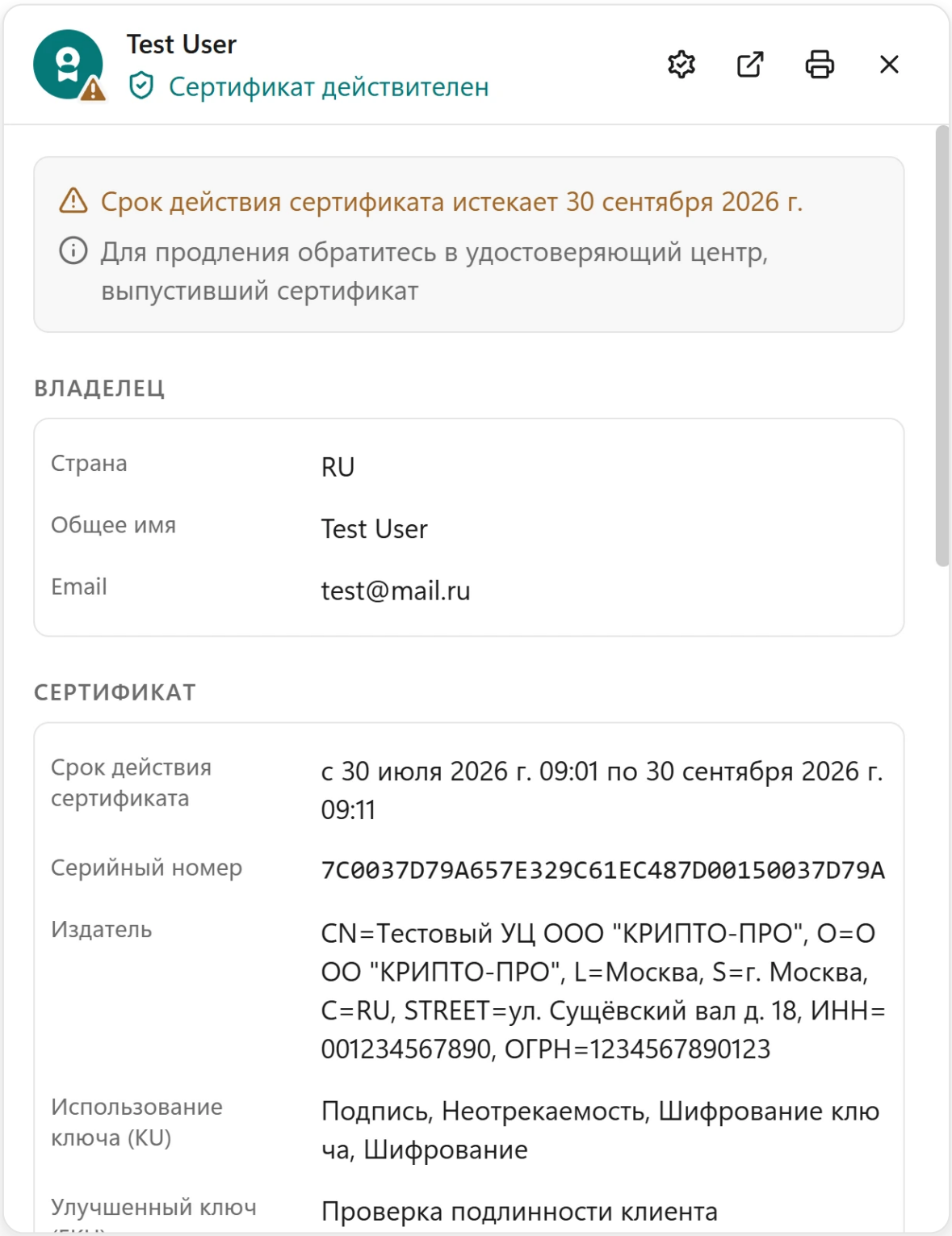
Сообщение	Значение
Срок действия сертификата истёк ...	Сертификат просрочен
Срок действия сертификата истекает ...	Сертификат скоро истечёт

Сообщение	Значение
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
Проверка цепочки доверия ещё не выполнена	Проверка не запускалась

Если срок действия личного сертификата или его закрытого ключа истёк или истекает в ближайшие 30 дней, в сведениях о сертификате появляется ссылка **Оставить заявку на сертификат**. Она открывает в браузере страницу выпуска сертификата.

Сведения о сертификате

Выделите сертификат в списке — 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 в панели сведений доступна команда **Открыть средствами Windows** — просмотр сертификата в системном окне.

Проверка контейнера закрытого ключа

Для личного сертификата в панели сведений 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** в панели сведений формирует карточку сертификата — документ со сведениями о владельце, издателе, сроке действия и отпечатке, пригодный для печати.

Поиск сертификатов

Строка поиска в заголовке окна ищет 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 — если сертификата ещё нет.
- Экспорт и удаление сертификатов — передача сертификата и перенос на другое рабочее место.
- Контейнеры и списки отзыва — работа с ключевыми контейнерами и CRL.
- Группы сертификатов — списки получателей шифрования.
- Сетевой профиль доверия — аккредитованные УЦ и проверка на квалифицированность.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Установка сертификатов в КриптоАРМ

Сертификат добавляется в КриптоАРМ двумя способами — импортом из файла или установкой из ключевого контейнера. Ниже описано, как установить личный сертификат, сертификат другого пользователя и сертификаты удостоверяющих центров.

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

Какое хранилище выбрать

Хранилище	Что в нём хранить
Личные сертификаты	Ваши сертификаты, к которым есть закрытый ключ
Других пользователей	Сертификаты других людей и организаций — для шифрования и проверки подписей
Удостоверяющие центры	Корневые и промежуточные сертификаты

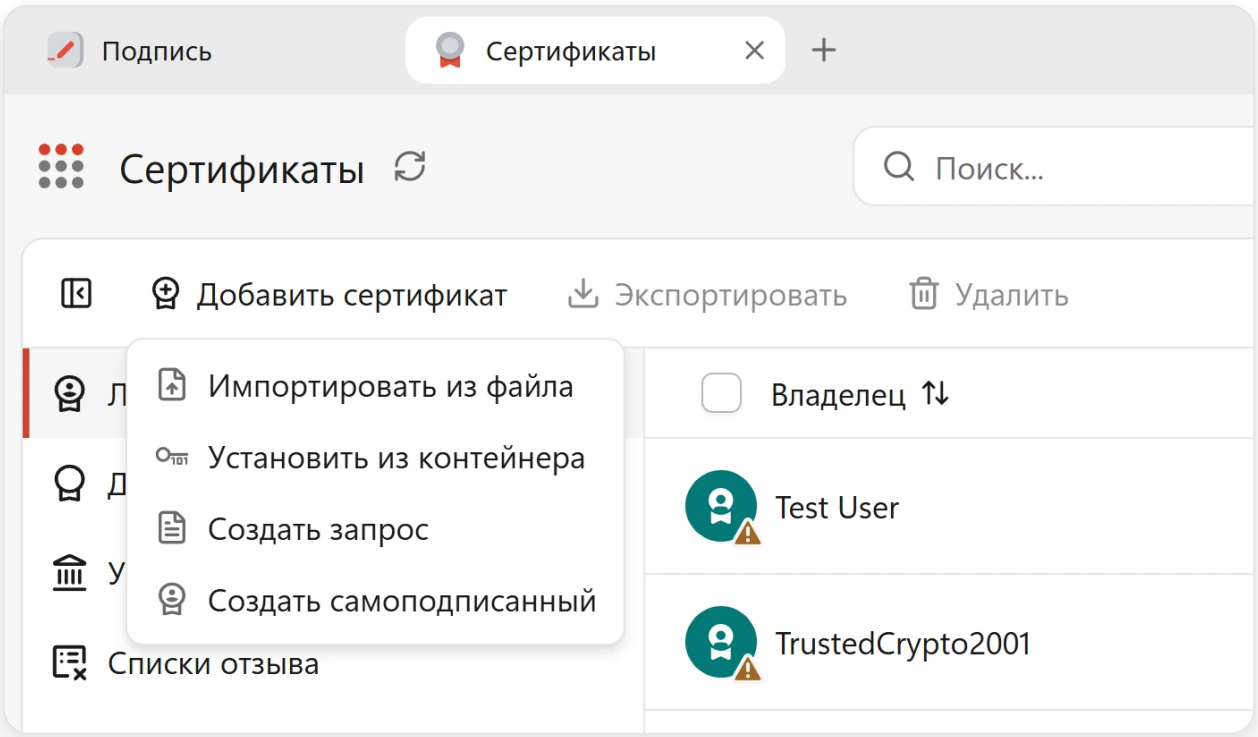
Приложение само определяет подходящее хранилище по содержимому файла и при расхождении предлагает выбрать — в окне **«Выберите хранилище для сертификата»** показаны текущее и рекомендуемое хранилища.

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 хранилище, в которое импортируете сертификат.

3. Нажмите **Добавить сертификат → Импортировать из файла**.



1. Выберите файл сертификата.
2. Если приложение предложит другое хранилище, выберите нужное и нажмите **Импортировать**.

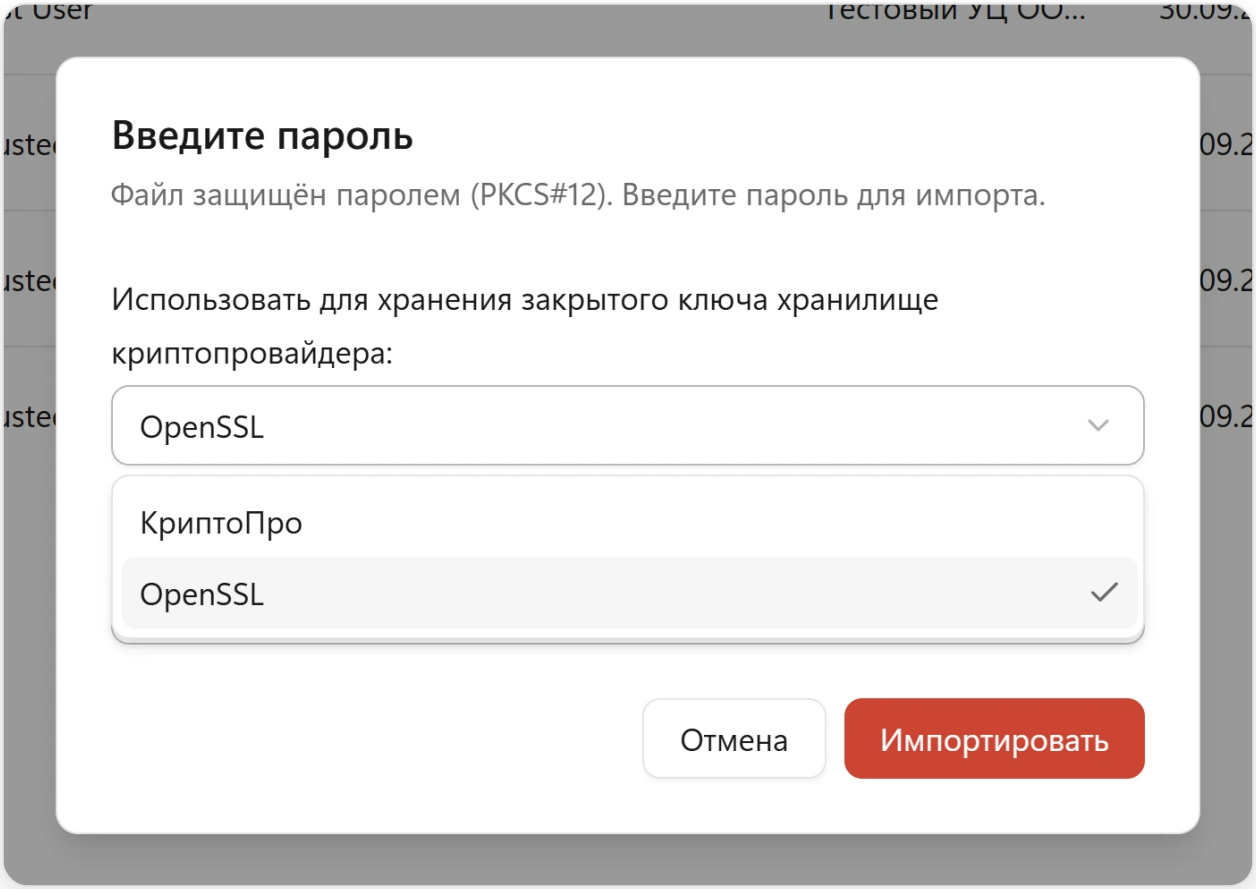
Появится сообщение **«Сертификат "..." импортирован»**.

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 хранилище **Сертификаты → Личные сертификаты**.
2. Нажмите **Добавить сертификат → Установить из контейнера**.
3. Выберите контейнер в списке и нажмите **Установить**.

Появится сообщение **«Сертификат "..." установлен из контейнера»**.

То же делает кнопка **Установить** в хранилище **Контейнеры** — см. 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 получателя.

1. Откройте хранилище **Сертификаты → Других пользователей**.
2. Нажмите **Добавить сертификат → Импортировать из файла**.
3. Выберите файл сертификата, который прислал получатель.

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. Для проверки отзыва нужен также актуальный список отзыва — см. Импорт списка отзыва.

Проверка сертификата идёт снизу вверх: **сертификат пользователя → промежуточный → корневой**. Сертификаты пользователей 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;
- в цепочке сертификации проверенной подписи — оттуда сертификат устанавливается кнопкой, см. Просмотр сведений о подписи документа.

> ⚠️ **Важно**: скачивайте сертификаты удостоверяющих центров только с их официальных сайтов. Файл, полученный из письма или стороннего архива, может оказаться поддельным.

1. Откройте хранилище **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 сертификат пользователя 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	Сертификат пользователя импортируется не в то хранилище	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 нет сертификата либо носитель недоступен	Проверьте, подключён ли носитель; если сертификата нет, запросите его в удостоверяющем центре и импортируйте 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 — передача сертификата и перенос на другое рабочее место.

- 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:

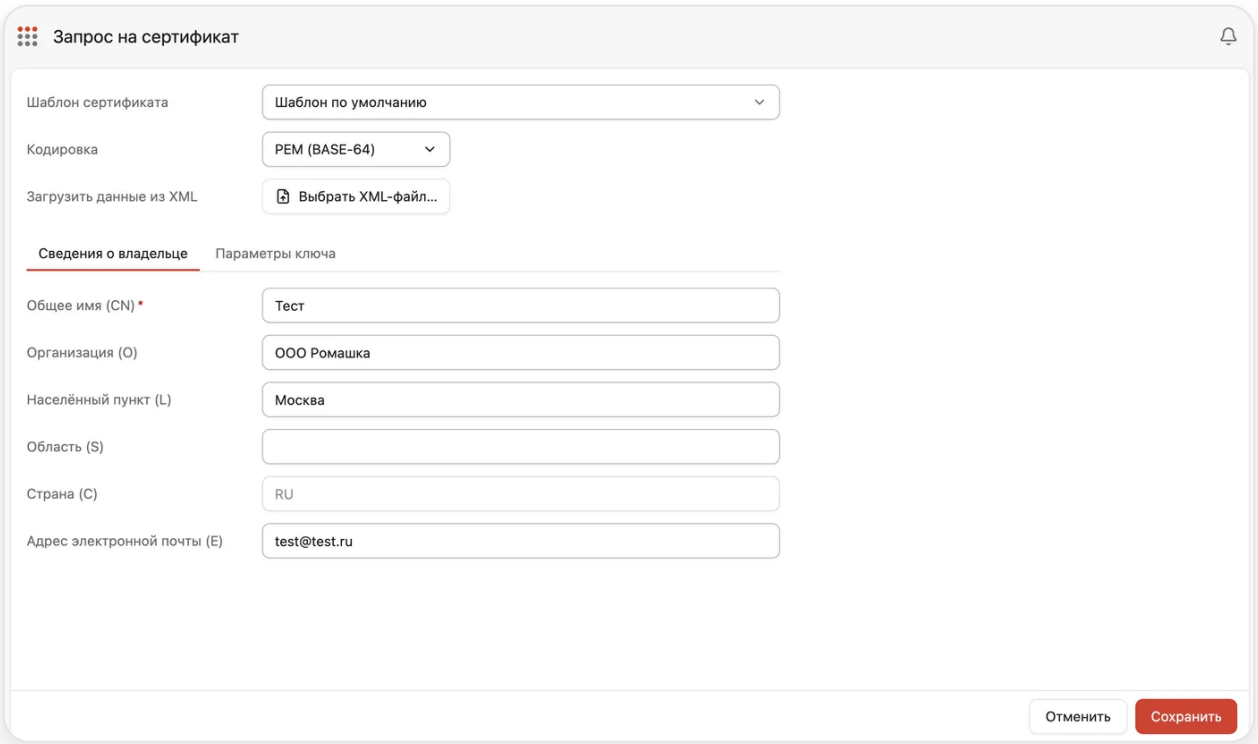
- Что потребуется
- Создание запроса на сертификат
- Создание самоподписанного сертификата
- Просмотр созданных запросов
- Возможные ошибки
- Смотрите также

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 хранилище **Сертификаты → Личные сертификаты**.
2. Нажмите **Добавить сертификат → Создать запрос** — 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. Подходят и файлы, сохранённые КриптоАРМ «Защищенная почта».

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
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. Во всех встроенных шаблонах **Общее имя (CN)** обязательно, а страна — RU, и изменить её нельзя. Если в загруженном шаблоне нет поля CN, запрос создаётся без него.

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 экспортировать 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 перечне **Расширенное использование ключа**, 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 хранилище **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 — перенос сертификата на другое рабочее место.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Экспорт и удаление сертификатов

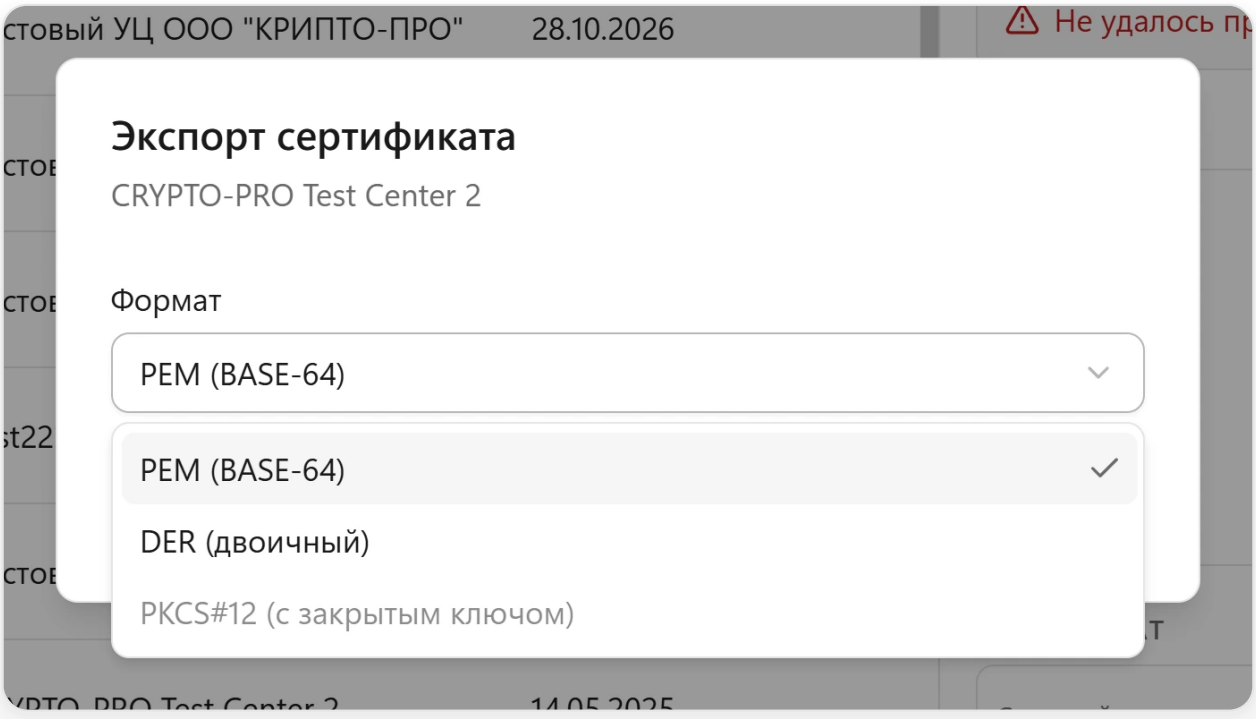
Экспорт нужен, чтобы передать сертификат другому пользователю или перенести его на другое рабочее место. Удаление убирает сертификат из хранилища.

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»**.

Та же кнопка **Экспортировать** есть в верхней части сведений о сертификате — в том числе открытых из цепочки сертификации при проверке подписи.

Выбор формата экспорта

От формата зависит, попадёт ли в файл закрытый ключ:

Формат	Что содержит	Когда использовать
DER (двоичный)	Только сертификат	Передать другому пользователю, чтобы он шифровал файлы в ваш адрес и проверял ваши подписи; импорт в другие системы
PEM (BASE-64)	Только сертификат, текстовый вид	Когда нужен текстовый файл — например, для файла настроек
PKCS#12 (с закрытым ключом)	Сертификат и закрытый ключ; файл защищён паролем	Перенести личный сертификат на другое рабочее место, где им нужно подписывать и расшифровывать

> 💡 **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**: восстановить закрытый ключ после удаления контейнера невозможно. Не удаляйте контейнер, если его ключ нужен другому сертификату.

Возможные ошибки

Сообщение	Что это значит	Что сделать
Не удалось экспортировать сертификат	Закрытый ключ запрещено экспортировать или носитель недоступен	Проверьте, подключён ли токен; ключ без разрешения на экспорт экспортировать нельзя

Сообщение	Что это значит	Что сделать
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»

Хранилище **Сертификаты → Контейнеры** показывает ключевые контейнеры, доступные КриптоПро CSP: в реестре, на флеш-накопителях, смарт-картах и токенах.

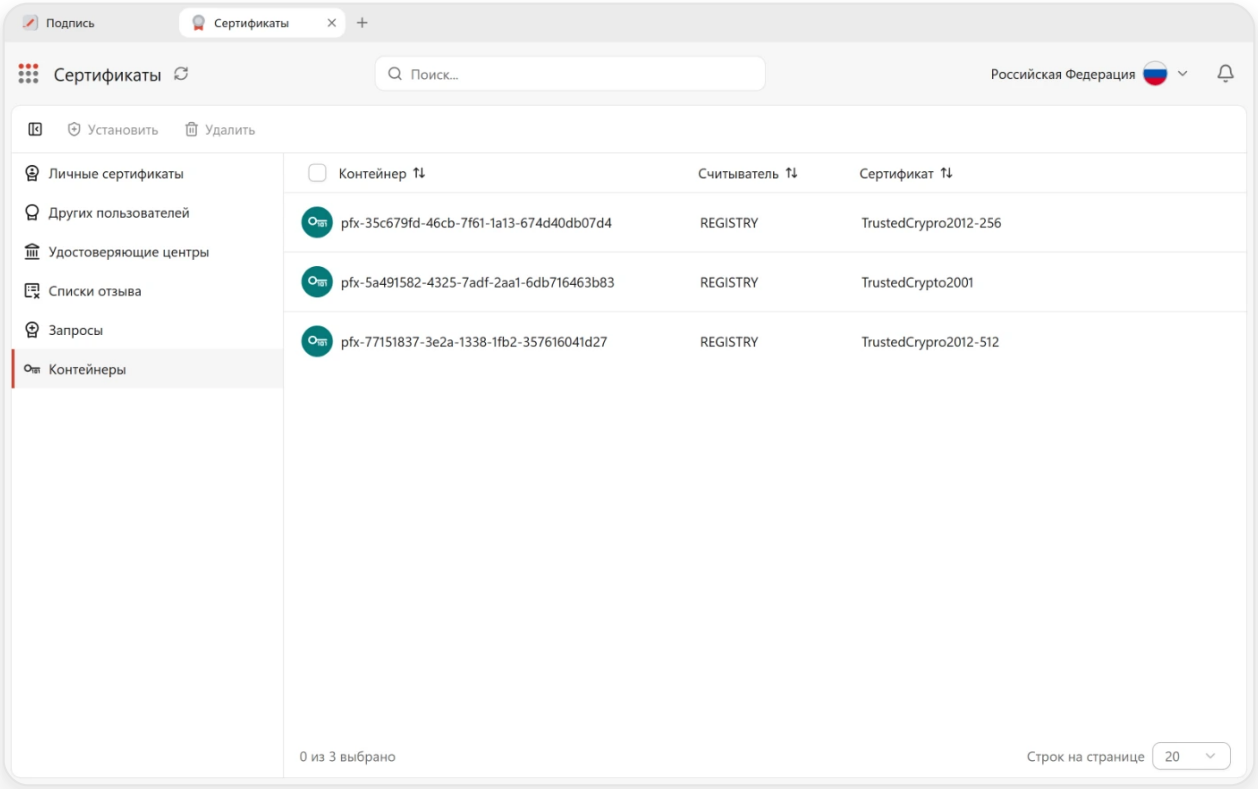


Таблица показывает имя контейнера, считыватель — где расположен контейнер — и сертификат в нём. Набор и порядок столбцов можно поменять — см. Настройка столбцов.

> 💡 **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.

Проверить закрытый ключ и распечатать сведения о сертификате можно после его установки, в хранилище **Личные сертификаты**:

- 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 хранилище **Сертификаты → Контейнеры**.
2. Выделите контейнер.
3. Нажмите **Установить**.

Появится сообщение **«Сертификат "..." установлен из контейнера»**.

Если сертификат уже установлен, кнопка **Установить** недоступна.

То же делает команда **Добавить сертификат → Установить из контейнера** в хранилище **Личные сертификаты** — см. Установка сертификатов.

Удаление контейнера

1. Выделите контейнер.
2. Нажмите **Удалить**.
3. При необходимости включите **«Удалить связанный с контейнером сертификат»**.
4. Подтвердите действие в окне **«Удаление контейнера»**.

> ⚠️ **Важно**: удаление контейнера уничтожает закрытый ключ. Восстановить его невозможно: подписать документы и расшифровать ранее зашифрованные файлы будет нельзя.

Списки отзыва (CRL)

Сертификат отзывают до окончания срока действия, если закрытый ключ скомпрометирован, изменились данные владельца, сертификат выпущен с ошибкой или владелец прекратил работу с ним. Без актуального списка отзыва 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.

Хранилище **Сертификаты → Списки отзыва** показывает установленные списки отзыва.

Таблица показывает издателя, даты выпуска и окончания действия и номер списка. 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 хранилище **Сертификаты → Списки отзыва**.
2. Нажмите **Импортировать**.
3. Выберите файл списка отзыва.

Появится сообщение **«Список отзыва "..." импортирован»**.

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 недоступен	Проверьте, подключён ли носитель; если сертификата нет, запросите его в удостоверяющем центре и импортируйте из файла
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

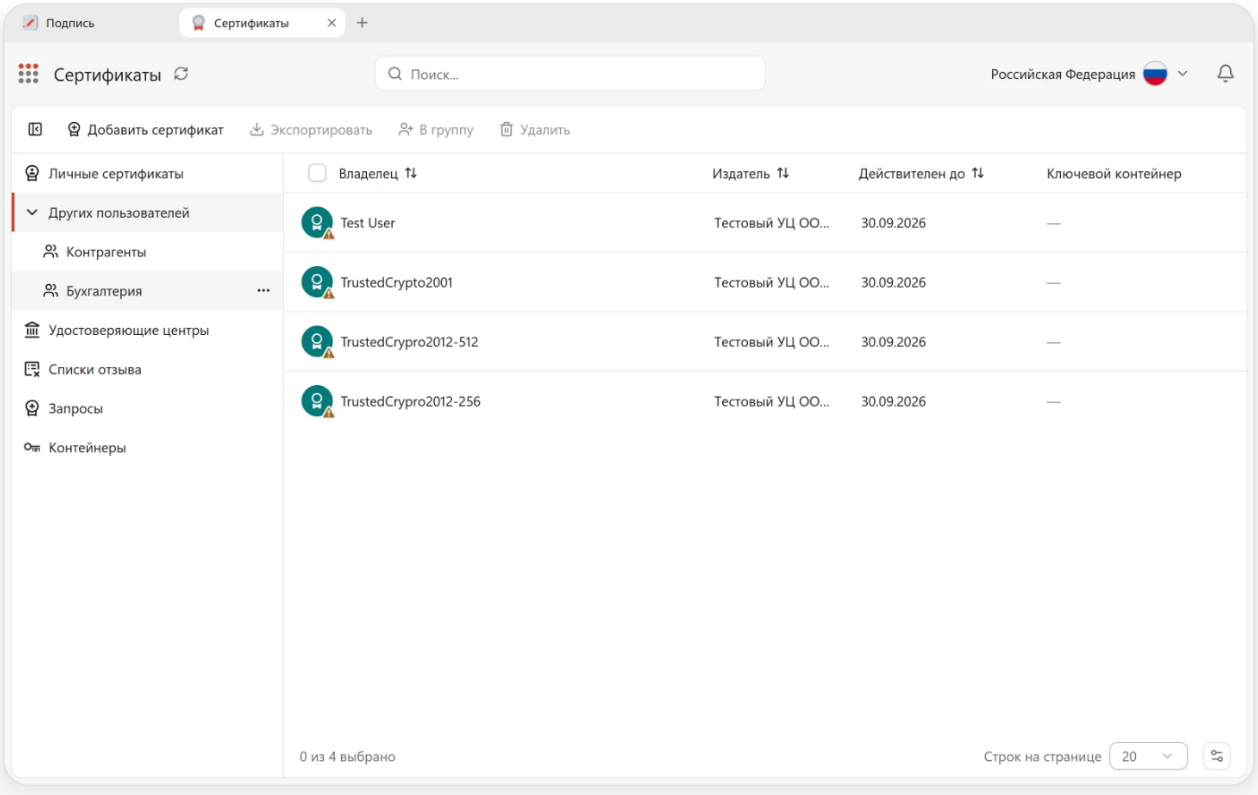
Группа — именованный список сертификатов. Она избавляет от выбора одних и тех же получателей по одному: при шифровании достаточно указать группу.

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**.



> 💡 **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»**.

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.

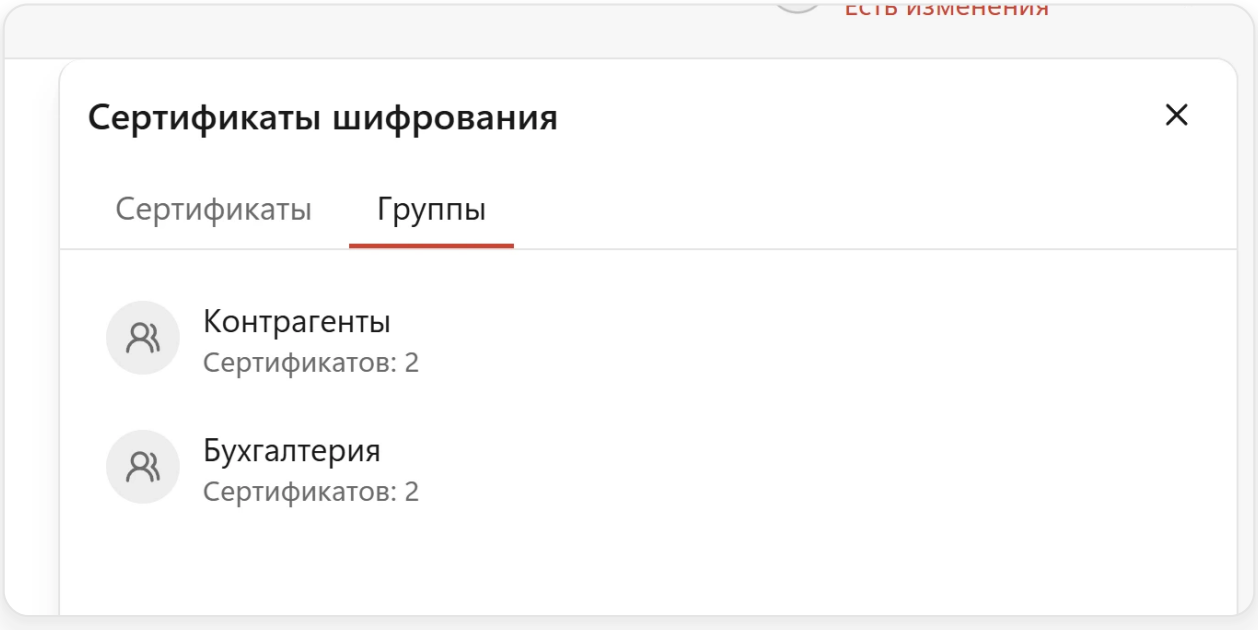
Удаление группы

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 — рядом с названием показано, сколько в группе сертификатов.



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

Сетевой профиль доверия

Квалифицированный сертификат по 63-ФЗ выпускает только аккредитованный удостоверяющий центр. Сетевой профиль доверия подключает КриптоАРМ Server с актуальным перечнем аккредитованных УЦ (TSL). С таким профилем приложение показывает сертификаты этих УЦ и проверяет сертификаты на квалифицированность.

Подключить можно любой КриптоАРМ Server: `sign.cryptoarm.ru` или сервер вашей организации.

Содержание:

- Добавление профиля
- Общий вход с сетевым профилем
- Хранилище «Аккредитованные УЦ»
- Проверка на квалифицированность
- Режим «Квалифицированная подпись»
- Настройки и удаление
- Смотрите также

Добавление профиля

1. Перейдите в раздел **Сертификаты** и нажмите на название активного профиля доверия в верхней части окна.
2. Нажмите **Добавить сетевой профиль** внизу панели.
3. В поле уже указан `sign.cryptoarm.ru`. Для сервера вашей организации введите его адрес. Нажмите **Подключить**. Параметры входа приложение получит от сервера. Если сервер передал не все параметры, заполните недостающие поля.
4. Войдите в учётную запись в открывшемся браузере.

Добавленный профиль сразу становится активным. В панели выбора он находится в группе **Сетевые профили**, под **Российская Федерация** и **Открытая криптография**. Его название — адрес сервера, изменить его можно в настройках. Под названием указана дата редакции TSL, из которой загружен список аккредитованных УЦ.

Если вход отменён или не удался, профиль не сохраняется. Второй профиль доверия для того же сервера создать нельзя: приложение сообщит, что он уже добавлен.

В хранилищах сетевой профиль доверия показывает те же сертификаты, что и профиль **Российская Федерация**.

Общий вход с сетевым профилем

Тот же сервер может быть подключён и в панели **Профили подписи** как сетевой профиль. Тогда учётная запись у профилей общая:

- если для сервера уже есть сетевой профиль со входом, профиль доверия добавляется без нового входа;
- сетевой профиль для сервера, у которого уже есть профиль доверия, тоже добавляется без нового входа;
- выход из учётной записи в настройках любого из профилей действует на оба;
- удаление одного профиля не затрагивает другой: он продолжает работать с той же учётной записью.

Профиль доверия не создаёт профиль подписи и не подключает облачные документы.

Хранилище «Аккредитованные УЦ»

Когда выбран сетевой профиль доверия, в списке хранилищ появляется **Аккредитованные УЦ** с сертификатами аккредитованных удостоверяющих центров из TSL сервера.

- Значок сертификата показывает, действует ли сертификат на текущую дату.
- Поиск, столбцы и сведения о сертификате работают так же, как в других хранилищах.
- В сведениях о сертификате доступны **Печать** и **Проверить на квалифицированность**.

Хранилище доступно только для чтения: удалить из него сертификат или добавить свой нельзя.

Обновление списка

Список хранится на компьютере. Приложение сверяет его с сервером при открытии хранилища, если списка ещё нет или последняя сверка была более суток назад. Чтобы сверить список сразу, нажмите **Обновить** в заголовке окна.

Под таблицей указаны дата редакции TSL, из которой загружен список, и время последней сверки, например: «TSL от 22.10.2026, проверен 46 минут назад». Если сверка не удалась, время не указывается.

Первая загрузка может занять несколько минут: сервер формирует список. Пока идёт загрузка, отображается сохранённый список. Если обновить список не удалось, остаётся последний загруженный, а над таблицей появляется сообщение об ошибке. Если требуется вход, над таблицей появится кнопка **Войти**.

Установка сертификата УЦ

Если цепочку сертификата не удаётся построить, потому что на компьютере нет сертификата УЦ, установите его из списка:

1. Выделите сертификат в таблице.

2. Нажмите **Установить** на панели действий.

Сертификат будет установлен в хранилище **Удостоверяющие центры** — к корневым или промежуточным, как при обычном импорте. При установке корневого сертификата КриптоПро CSP попросит подтвердить действие. Сертификаты устанавливаются по одному. Если сертификат уже установлен, кнопка **Установить** недоступна.

> ⚠️ **Важно**: сертификаты устанавливаются в том виде, в каком их передал сервер. Подключайте профиль доверия только к серверу, которому доверяете.

Проверка на квалифицированность

1. Выберите сетевой профиль доверия в разделе **Сертификаты**.
2. Откройте сведения о сертификате.
3. Нажмите **Проверить на квалифицированность** (значок с галочкой) в верхней части панели сведений.

Результат появится в уведомлении. **Выдан аккредитованным удостоверяющим центром** — квалифицированность подтверждена. Иначе — **Квалифицированность не подтверждена** с причиной: пояснение сервера, **УЦ не аккредитован** или **проверка по списку доверия завершилась отрицательно**.

Квалифицированность говорит о том, кем выпущен сертификат. Действует ли он сейчас, показывает его статус.

Так же можно проверить сертификат, открытый из сведений о подписи, — сертификат подписанта или УЦ из цепочки, даже если его нет в хранилище. Проверку выполняет сервер профиля доверия, выбранного в разделе **Сертификаты**.

> 💡 **Примечание**: без режима «Квалифицированная подпись» результат проверки не меняет ни статус сертификата, ни результат проверки подписи. Чтобы узнать его снова, повторите проверку.

При других профилях доверия кнопки проверки нет.

Режим «Квалифицированная подпись»

В режиме приложение само проверяет квалифицированность сертификата каждого подписанта: подпись действительна, только если сервер профиля подтвердил, что сертификат выпущен аккредитованным УЦ.

Чтобы включить режим:

1. Откройте настройки профиля доверия.
2. На вкладке **Настройки профиля** включите **Режим «Квалифицированная подпись»**.
3. Нажмите **Сохранить**.

Режим действует, пока этот профиль выбран в разделе **Сертификаты**. Если выбрать другой профиль доверия, подписи проверяются как обычно.

Проверка подписи

Подпись, которая без режима была бы действительной, получает итог **Подпись недействительна**, если:

- квалифицированность сертификата подписанта не подтверждена;
- квалифицированность проверить не удалось: нет связи с сервером, требуется повторный вход или сервер не ответил.

Подпись, недействительную и без режима, сервер не проверяет: её итог и причина остаются прежними.

Причина видна в строке **Квалифицированность** сведений о подписи и в отчёте о проверке.

Без связи с сервером подписи в режиме недействительны. Восстановите связь или войдите в профиль и проверьте файлы снова.

Режим действует везде, где приложение проверяет подписи, — в том числе в мастере PDF, при проверке из контекстного меню и через внешний API. Командная строка проверяет подписи без режима.

Статусы сертификатов

В хранилищах **Личные сертификаты** и **Других пользователей** статус сертификата учитывает квалифицированность:

- **Сертификат действителен** — цепочка действительна и квалифицированность подтверждена;
- **Сертификат недействителен** — цепочка недействительна или квалифицированность не подтверждена;
- **Не проверен** — проверка ещё идёт или квалифицированность проверить не удалось.

В сведениях о сертификате с действительной цепочкой вверху появляется пояснение: **Выдан аккредитованным удостоверяющим центром**, **Сертификат действителен, но квалифицированность не подтверждена** с причиной или **Сертификат действителен, но не удалось проверить квалифицированность**. Если нужен вход, рядом с пояснением есть кнопка **Войти**. Тот же результат показан в строке **Квалифицированность** после издателя.

Статусы в списке обновляются, когда вы открываете раздел или нажимаете **Обновить**, а также при смене профиля доверия и когда в хранилище **Аккредитованные УЦ** загружается новая редакция TSL. Приложение при этом обращается к серверу не чаще раза в сутки на каждый

сертификат; после проверки подписи статус её подписанта берётся из этой проверки. Чтобы проверить сертификат сразу, нажмите **Проверить на квалифицированность** в сведениях о нём.

Сведения о сертификате подписанта, открытые из сведений о подписи, показывают квалифицированность из этой проверки. В печатной форме сведений о сертификате есть строка **Квалифицированность**.

Тот же статус сертификат имеет при выборе сертификата подписи или шифрования, в том числе в мастере PDF.

Статусы сертификатов удостоверяющих центров режим не меняет.

Что проверяет режим

Сервер проверяет, что издатель сертификата есть в действующем перечне аккредитованных УЦ (TSL). Это не все условия квалифицированной подписи по статье 11 63-ФЗ: закон требует, чтобы УЦ был аккредитован на день выдачи сертификата. Поэтому подпись сертификатом, выданным до того, как УЦ лишился аккредитации, режим покажет недействительной.

Остальные проверки подписи режим не меняет.

> ⚠️ **Важно**: в режиме сертификаты подписантов отправляются на сервер профиля доверия при каждой проверке подписи, в том числе при проверке через внешний API без открытия окна. В сертификате есть персональные данные владельца, например СНИЛС и ИНН.

Настройки и удаление

Чтобы открыть настройки, нажмите **...** у профиля в панели выбора профиля доверия и выберите **Редактировать**. Настройки разделены на две вкладки:

- **Настройки профиля** — название профиля и режим «Квалифицированная подпись»;
- **Параметры ресурса** — учётная запись (вход и выход), адрес ресурса и сервер авторизации, статус соединения и сертификат ресурса.

Чтобы удалить профиль, нажмите **...** у профиля в панели выбора и выберите **Удалить**.

Если удалить выбранный профиль, выбор вернётся к **Российская Федерация**.

Смотрите также

- Раздел «Сертификаты» — профили доверия и хранилища.
- Установка сертификатов — импорт сертификатов удостоверяющих центров из файла.

- Профили подписи — сетевой профиль для того же сервера.
- Проверка и расшифрование — строка «Квалифицированность» в сведениях о подписи.
- 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.

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 с зарубежными коллегами, 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.

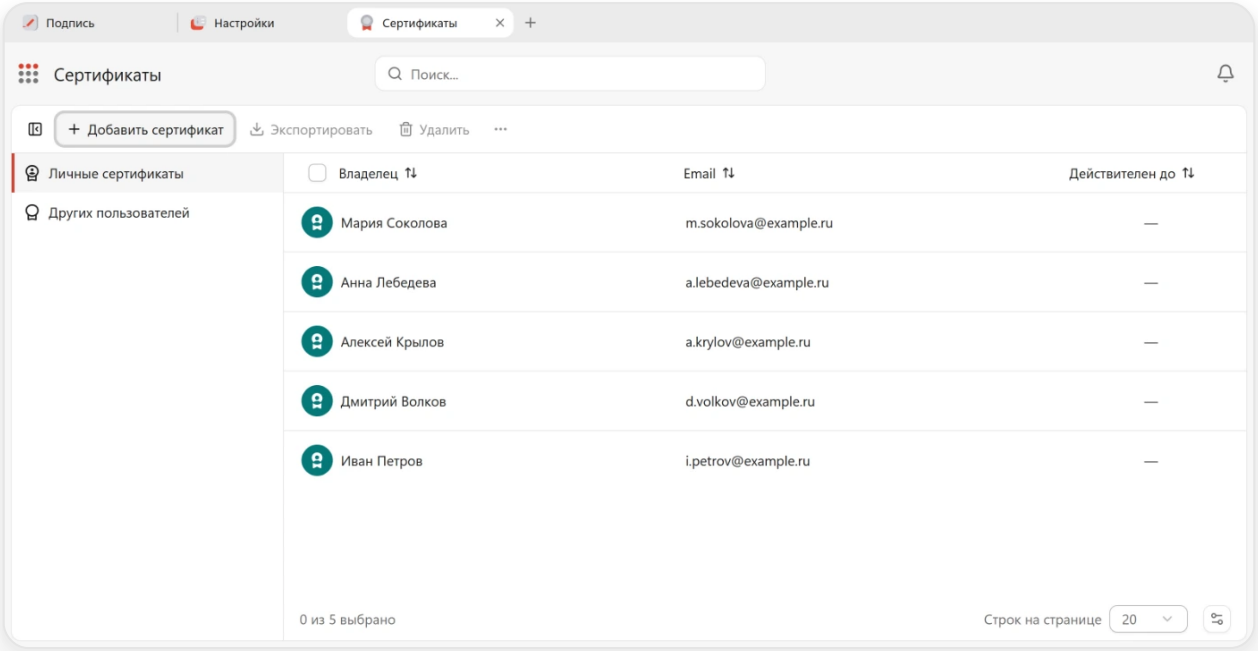
Переключение на OpenPGP

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	Сертификаты других пользователей

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, адрес электронной почты 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. Достоверность показывается и в результатах проверки подписи.

Достоверность	Когда присваивается
Абсолютная	Доверие владельцу — «Абсолютное»: это ваш собственный сертификат
Полная	Сертификат заверил владелец с полным или абсолютным доверием — либо двое владельцев с частичным
Частичная	Сертификат заверил один владелец с частичным доверием
Неизвестна	Заверений от владельцев, которым вы доверяете, нет
Недостоверна	Сертификат отозван или отключён
Не определена	Срок действия сертификата истёк, или сертификат скомпрометирован

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.

Подключи

Сертификат OpenPGP состоит из основного ключа и подключей. Основной ключ заверяет подключи и чужие сертификаты, а подключи выполняют конкретные задачи: подпись, шифрование или аутентификацию.

Подключ можно добавить или отозвать, не трогая основной ключ, — см. Добавление подключа.

Постквантовые схемы

Постквантовые схемы рассчитаны на появление квантового компьютера — их выбирают, когда данные должны оставаться защищёнными 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.

> ⚠️ **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 — свой сертификат и сертификаты других пользователей.
- Действия с сертификатами — подключи, заверение, отзыв, смена пароля.
- Экспорт и резервное копирование — передача открытого ключа и копия закрытого.
- Подпись и шифрование — операции с файлами.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Создание и импорт сертификатов OpenPGP

Свой сертификат OpenPGP создаётся в приложении или импортируется из файла вместе с закрытым ключом. Сертификаты других пользователей импортируются из файлов, которые они прислали.

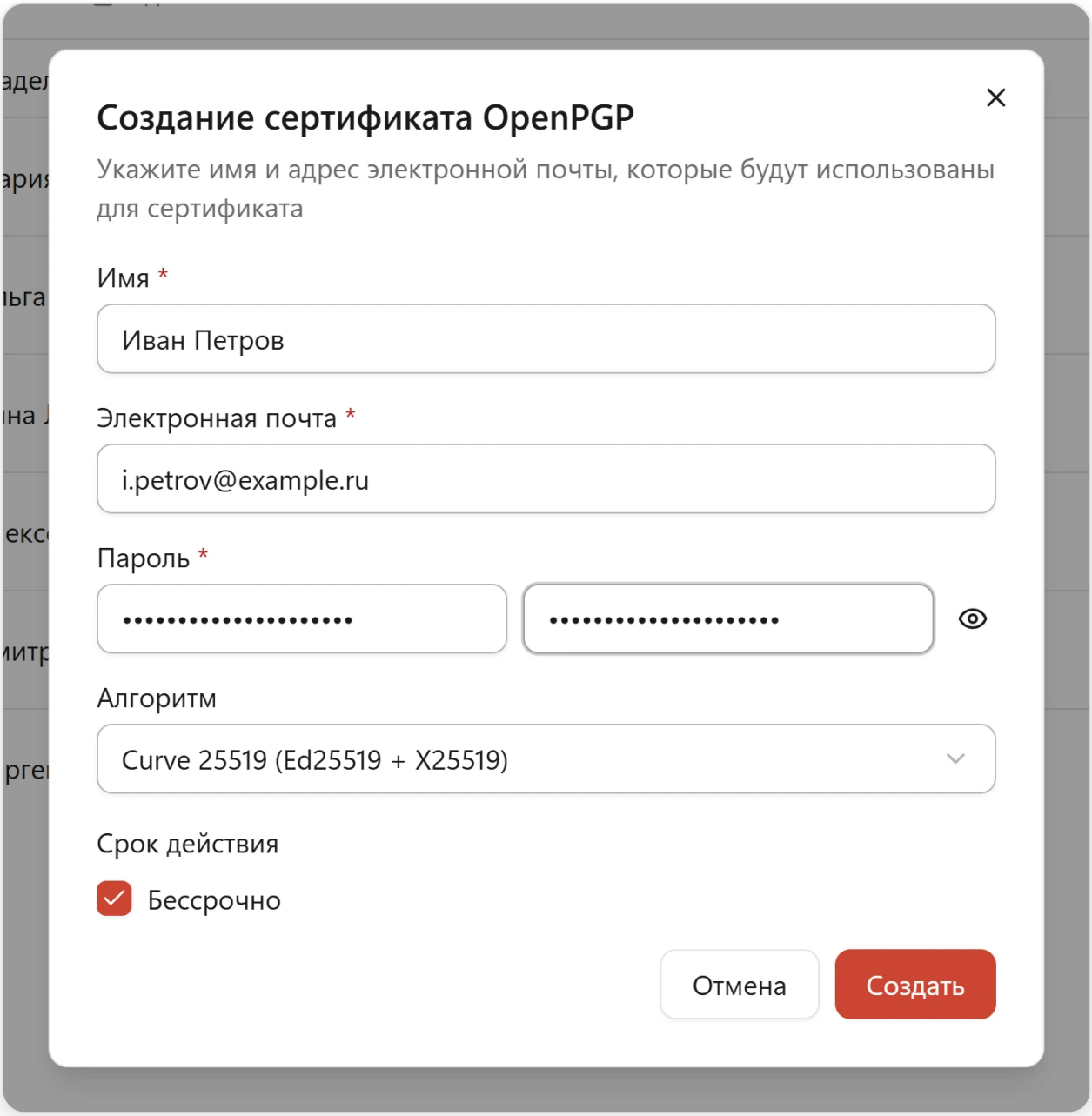
Содержание:

- Создание сертификата
- Импорт сертификата
- Импорт закрытого ключа
- Восстановление из бумажной копии
- 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 другие пользователи;
- **Алгоритм** — схема ключа;
- **Срок действия** — дата или **Бессрочно**;
- **Пароль** и его подтверждение.



1. Нажмите **Создать**.

Появится сообщение **«Сертификат успешно создан»**. Сертификат находится в хранилище **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 поддерживают нынешние программы OpenPGP. **RSA 4096** выбирают ради совместимости со старыми программами. Гибридные постквантовые схемы (в списке — группы **PQ шифрование** и **PQ подпись и шифрование**) выбирайте по договорённости с получателем: их поддерживают не все программы OpenPGP. Например, GnuPG читает постквантовое шифрование (ML-KEM) начиная с версии 2.5, а ключ с постквантовой подписью (ML-DSA) 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

Группа в списке	Схема	Описание
Классические	**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
PQ шифрование	**Curve 25519 + ML-KEM-768**, **Curve 448 + ML-KEM-1024**	Обычная подпись, постквантовое шифрование
	Brainpool P-256 + ML-KEM-768, **Brainpool P-384 + ML-KEM-1024**	То же на кривых Brainpool
PQ подпись и шифрование	**Curve 25519 + ML-DSA-65 + ML-KEM-768**, **Curve 448 + ML-DSA-87 + ML-KEM-1024**	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.

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 других пользователей и шифровать файлы в их адрес, импортируйте их сертификаты.

1. Откройте раздел **Сертификаты**.
2. Нажмите **Добавить сертификат → Импортировать из файла**.
3. Выберите файл сертификата — 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**. Чтобы подтвердить принадлежность сертификата, заверьте его.

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, экспортированный из КриптоАРМ, бумажную резервную копию и закрытый ключ в стандартном формате OpenPGP — например, экспортированный из GnuPG.

Если в файле находится закрытый ключ, приложение попросит **пароль закрытого ключа**. 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

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 владельца прислать сертификат заново. Если это ваш закрытый ключ из GnuPG, экспортируйте его заново без пароля и задайте пароль при импорте

Сообщение	Что это значит	Что сделать
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	Экспортируйте 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, удаление.
- Экспорт и резервное копирование — копия закрытого ключа.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Действия с сертификатами OpenPGP

Здесь описаны действия с уже созданным или импортированным сертификатом OpenPGP: подключи, заверение, доверие владельцу, отзыв, смена пароля и удаление.

Содержание:

- Добавление подключа
- Отзыв подключа
- Заверение сертификата
- Просмотр заверений
- Доверие владельцу
- Отзыв сертификата
- Смена пароля закрытого ключа
- Удаление сертификата
- Группы сертификатов
- Возможные ошибки
- Смотрите также

Добавление подключа

Подключ выделяет отдельную ключевую пару под конкретную задачу. Его можно отозвать, не отзывая сертификат целиком.

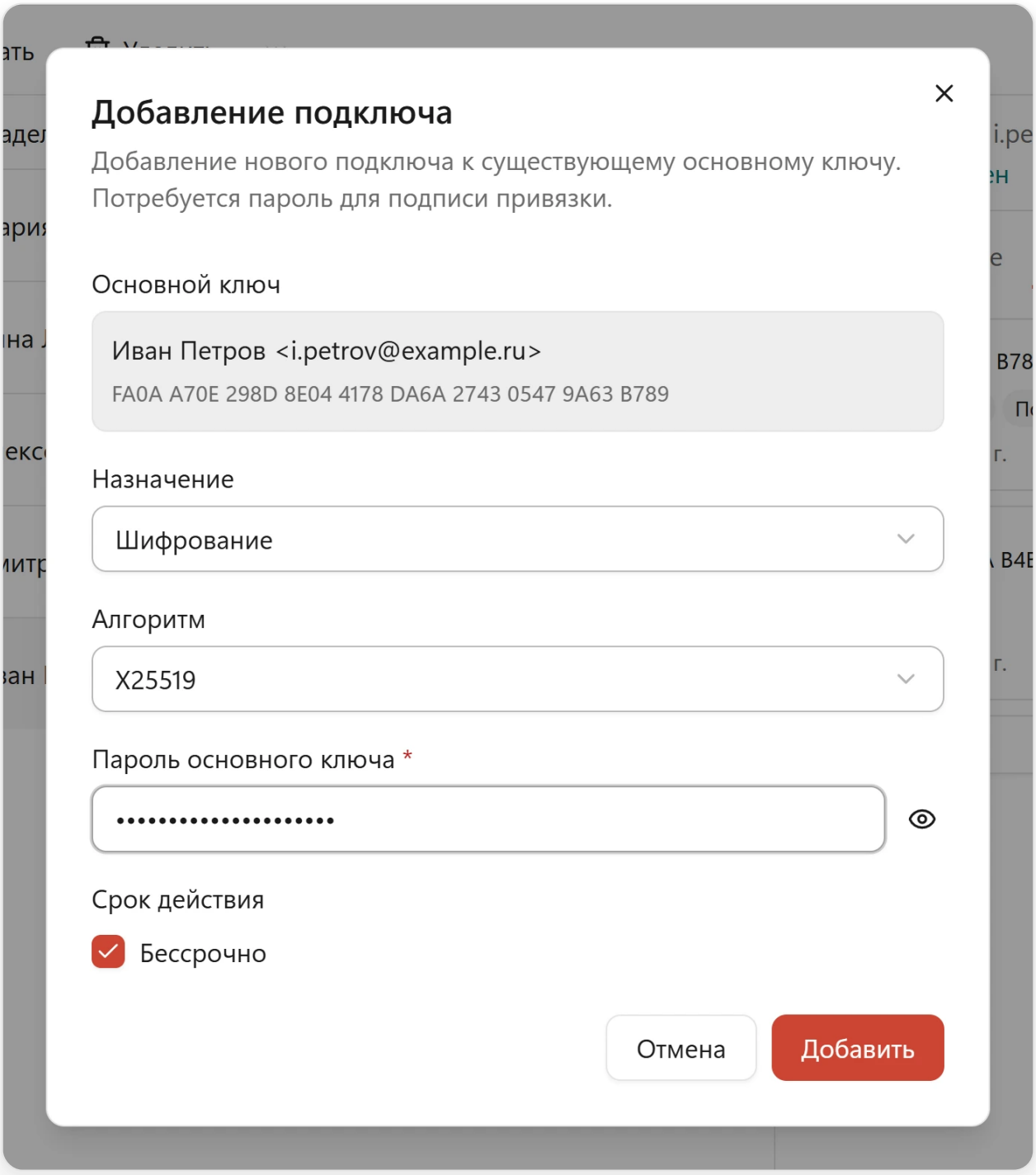
1. Выделите личный сертификат.
2. В панели сведений перейдите на вкладку **Подключи** и нажмите **Добавить подключ**.
3. В окне **«Добавление подключа»** укажите:

- **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

Назначение	Доступные алгоритмы
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.

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.

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.

> ⚠️ **Важно**: заверение — публичное утверждение о принадлежности ключа: оно попадает в экспортируемый открытый ключ и видно тем, кому вы его передадите.

Просмотр заверений

Вкладка **Заверения** в панели сведений показывает, кто заверил сертификат. Локальные заверения помечены как **«Локальное»**, неизвестные заверители — как **«Неизвестный заверитель»**.

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	Вы решили не полагаться на заверения владельца — они не учитываются
Частичное	Одного заверения владельца мало: сертификат станет достоверным после двух 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 — другие пользователи 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 другие пользователи узнают, что ключ больше использовать не следует.

1. Выделите личный сертификат.
2. Откройте меню ··· и выберите **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**.

Появится сообщение **«Сертификат отозван»**.

> ⚠️ **Важно**: отзыв необратим. После отзыва экспортируйте открытый ключ и передайте его тем, кто пользуется вашим сертификатом, — иначе они не узнают об отзыве.

Смена пароля закрытого ключа

1. Выделите личный сертификат.
2. Откройте меню ··· и выберите **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 — никому 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.

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.

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 другим пользователям.
- Подпись и шифрование — операции с файлами по стандарту OpenPGP.
- Глоссарий — термины электронной подписи простыми словами.

Открыть статью на сайте

Экспорт и резервное копирование ключей OpenPGP

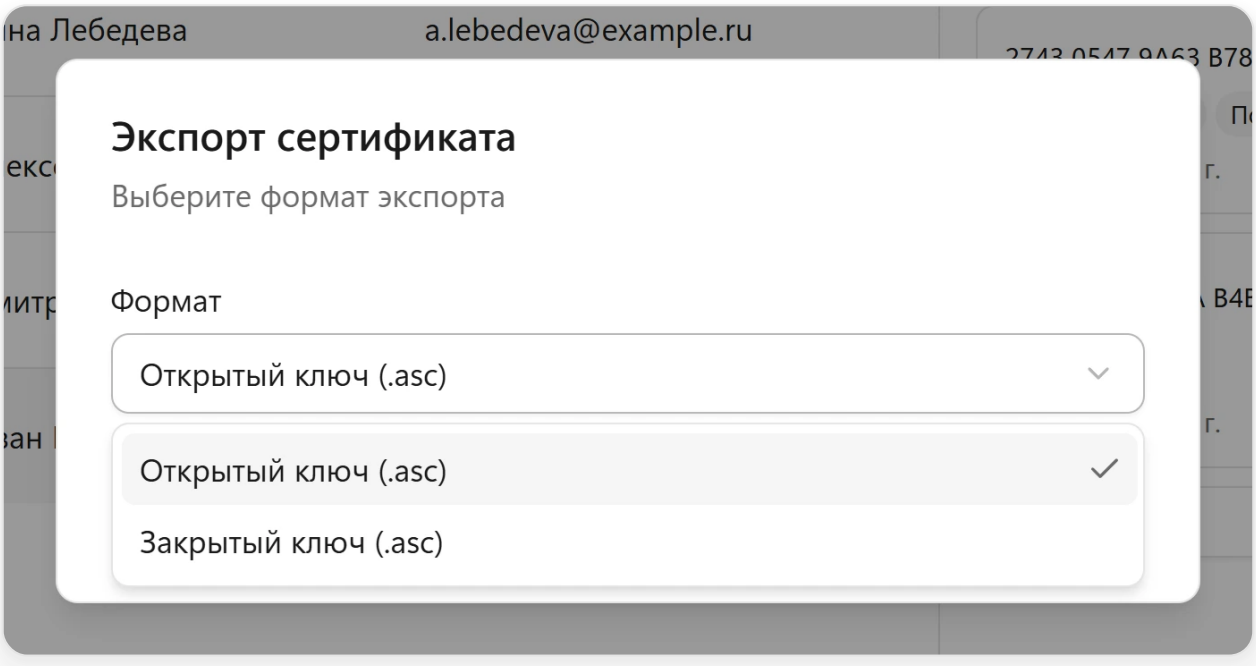
Открытый ключ передают другим пользователям, закрытый — хранят в резервной копии. Восстановить закрытый ключ OpenPGP невозможно, поэтому копия обязательна.

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. Получатель 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 на другой компьютер с КриптоАРМ, но сторонние программы OpenPGP его не прочитают, несмотря на расширение `.asc`. Открытый ключ, наоборот, сохраняется в стандартном формате OpenPGP.

> ⚠️ **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 расшифровывать файлы, зашифрованные в ваш адрес. 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.

Экспортируются только открытые ключи — по одному файлу на сертификат.

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, там, где доступ к ней есть только у вас;
- проверьте копию сразу после создания: импортируйте её на другом рабочем месте или сверьте отпечаток;
- помните, что смена пароля в приложении уже сделанные копии не затрагивает.

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; если ошибка повторяется, экспортируйте сертификаты по одному
Экспортировано N из M, ошибок: K	Часть сертификатов экспортировать не удалось	Экспортируйте оставшиеся по одному — так видно, на каком возникает ошибка
	Неверный пароль или сбой операции	Проверьте пароль и повторите

Сообщение	Что это значит	Что сделать
Не удалось подготовить резервную копию закрытого ключа к печати		

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.

Вызвать приложение можно двумя способами:

- **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, распаковка
`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, поддерживаемые команды
`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. **Уведомление о получении.** Сразу после получения ссылки приложение сообщает сервису о вызове уведомлением `<команда>.callback` — ещё до проверки доверия.
5. **Проверка сервиса.** При первом обращении с этого адреса приложение показывает сертификат сервиса и запрашивает разрешение — см. Запрос от сетевого сервиса.
6. **Запрос параметров.** Приложение отправляет на указанный адрес JSON-RPC запрос `<команда>.parameters`, чтобы получить параметры операции.
7. **Подготовка операции.** Приложение загружает нужные файлы и открывает экран операции с переданными настройками.
8. **Подтверждение пользователем.** Пользователь проверяет, что именно запрошено, и запускает операцию.

9. **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`.

Формат ссылки для локального вызова

Вариант 1 — JSON в ссылке:

```
cryptoarm://<command>/<JSON>
```

```
cryptoarm://startView/{"jsonrpc":"2.0","id":"tx-42","result":{"uiView":"SIGN_AND_ENCRYPT"}}
```

JSON в ссылке — это конверт JSON-RPC: объект с полями `jsonrpc`, `id` и `result`. Состав `result` зависит от команды и описан на её странице.

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 файла параметров в окне показывается путь к нему.

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. Вход пользователя включает сам сервис — параметром `authType=oidc` в ссылке. Доступ к файлам даёт отдельный токен в `extra.token`.

Подробности — на странице Аутентификация.

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. К файлу на узле вызова добавляется токен входа, как задаёт `customAuth`, кроме `in: "body"`. Значение `extra.token` передаётся параметром `accessToken` в адресе файла. Файл на другом узле скачивается без токена входа — 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	Поля `VERSIONS`, `PROVIDERS`, `LICENSES`, `PRODUCT` и `COMMANDS` — см. `diagnostics`.

Ответ с параметрами

В теле ответа сервис возвращает конверт JSON-RPC:

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:

- объект в `error` — ответ с ошибкой;
- флаги принимаются и строками: `"true"` равнозначно `true`, `"false"` — `false`;
- 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.

Смотрите также

- Приложение и пользователь — окна согласия на стороне пользователя.
- Транспорт и доверие — HTTPS, доверенные сервисы, локальный вызов.
- Аутентификация — вход пользователя по OIDC и токен доступа к файлам.
- 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. Разработчику сервиса она показывает, что увидит его пользователь.

Содержание:

- Запрос от сетевого сервиса
- Запрос от локального приложения
- Экран 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

Под сведениями показан результат проверки сертификата сервиса: **«Соединение защищено»** и **«Сертификат ресурса действителен»** либо **«Соединение не защищено»** и **«Сертификат ресурса недействителен»**.

> ⚠️ **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**.

Экран операции

Операция сервиса открывается в отдельной вкладке на обычном экране операции — с файлами, сертификатами и настройками. Параметры, которые сервис задал явно, показаны без возможности изменения; остальные пользователь может изменить перед запуском.

Операция запускается кнопкой на экране, как обычно. Если закрыть вкладку, не запустив операцию, сервис получит отказ.

> 💡 **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
```

Сразу после получения ссылки — до проверки доверия — приложение сообщает сервису, что вызов получен:

```
{
  "jsonrpc": "2.0",
  "method": "diagnostics.callback",
  "id": "tx-42",
  "params": {
    "status": "Received",
    "VERSIONS": { "cryptoarm": "7.4.0" }
  }
}
```

Имя команды в методе записывается в нижнем регистре — например, `signandencrypt.callback`. Ответ на уведомление не требуется, и его доставка на выполнение команды не влияет. Уведомление уходит без токена входа и до ответа пользователя в окне доверия: если следующих запросов нет, пользователь ещё не ответил.

После подтверждения доверия приложение отправляет запрос параметров:

```
{
  "jsonrpc": "2.0",
  "method": "diagnostics.parameters",
  "id": "tx-42",
  "diagnostic": {}
}
```

Для остальных команд поле `diagnostic` содержит `VERSIONS`, `PROVIDERS`, `LICENSES`, `PRODUCT` и `COMMANDS` — см. «Приложение и поддерживаемые команды».

Сервис отвечает параметрами команды:

```
{
  "jsonrpc": "2.0",
  "id": "tx-42",
  "result": {
    "operation": ["VERSIONS", "LICENSES"]
  }
}
```

Требования к ответу перечислены в разделе Описание запросов и ответов.

Результат отправляется как уведомление JSON-RPC — см. Ответ на результат.

Доверенный сервис

Сетевой вызов работает только по HTTPS. 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 привязано к адресу сервиса — схеме, узлу и порту — и к его сертификату. Смена сертификата требует нового решения пользователя; если пользователь откажет, сервис получит `Access denied`, а сохранённый сертификат останется прежним.

Сохранённый сервис отображается в группе **«Доверенные сервисы»** панели профилей подписи — см. Доверенные сервисы. После удаления профиля доверие, сохранённый сертификат сервиса и его настройки 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

Входные файлы и получатель результата могут быть на другом узле — например, в хранилище S3 или на CDN. Окно доверия для них не показывается, а токен входа на другой узел не передаётся.

Перенаправления (HTTP 3xx) выполняются только по HTTPS. Входной файл может перенаправить на любой узел, а получатель результата должен принимать его по указанному адресу: перенаправление результата на другой узел не выполняется.

Значение `extra.token` добавляется как параметр `accessToken` к адресу каждого входного файла и получателя результата, на каком бы узле они ни были.

Адреса служб штампов времени (TSP) и проверки статуса сертификата (OCSP) могут быть и HTTP, и HTTPS. Пользователь видит их в настройках 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`, `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

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.

Содержание:

- Вход пользователя: `authType=oidc`
- Токен доступа к файлам
- Смотрите также

Вход пользователя: `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/`. Выполненный вход сохраняется и продлевается без вопросов к пользователю; при смене провайдера пользователь входит заново;
4. повторяет исходную команду по адресу `nextUrl`, передавая токен так, как задаёт `customAuth`. 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. При `403` повторный вход и повтор команды не выполняются.

`nextUrl` обязан оставаться на том же origin — схеме, узле и порту, — что и исходный вызов: токен не уходит на другой узел. Если в `nextUrl` есть параметр `id`, дальше вызов идёт с этим идентификатором.

`customAuth` задаёт, где сервис ждёт токен:

in	Куда попадает токен	Имя
header (по умолчанию)	Заголовок <имя>: <scheme> <токен>; scheme по умолчанию — Bearer	headerName или key, по умолчанию Authorization
query	Параметр адреса <имя>=<токен>	key, по умолчанию token
body	Поле <имя> в корне JSON-тела запроса; в multipart/form-data — в JSON поля operation-response	key, по умолчанию token

Токен добавляется ко всем запросам на тот же origin: к запросу параметров, отправке результата, сообщению об ошибке и загрузке входных файлов — кроме in: "body": у запроса загрузки нет тела. Токен в адресе или в теле попадает в журналы сервера и прокси на стороне сервиса, поэтому заголовок предпочтительнее.

Значения authType:

authType	Что делает приложение
oidc	Вход по OIDC — см. Вход пользователя
oidc:mtls	То же, что oidc
mtls	Обычный вызов, без входа
Другое	После проверки доверия сервис получает <команда>.parameters со статусом Canceled и ErrorDescription: "Unsupported auth type: <значение>"

В локальном вызове authType не учитывается: команда выполняется без входа.

Токен доступа к файлам

Токен доступа к файлам передаётся в extra.token команды signAndEncrypt и добавляется к адресу каждого входного файла и получателя результата — см. Адреса файлов и токен.

Смотрите также

- Описание и возможности API — форматы ссылок, запросов и ответов.
- Транспорт и доверие — проверка сертификата сервиса, адреса файлов и токен.
- Лимиты, статусы и ошибки — завершение вызова при отказе.

Открыть статью на сайте

Команда signAndEncrypt

Команда запускает подпись, архивирование и шифрование документов, обратные операции — расшифрование, снятие подписи и распаковку — или проверку 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**: операции требуют действующей лицензии на КриптоАРМ — см. Общая информация.

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.

Прямые операции (можно комбинировать):

Значение	Описание
`SIGN`	Подпись
`ARCHIVE`	Архивирование
`ENCRYPT`	Шифрование

Обратные операции (выполняются по одной или вместе):

Значение	Описание
`UNSIGN`	Снятие подписи
`DECRYPT`	Расшифрование
`UNZIP`	Распаковка ZIP

Проверка подписи:

Значение	Описание
`VERIFYSIGN`	Проверка подписи

Ограничения:

- прямые и обратные операции не смешиваются;
- `VERIFYSIGN` выполняется только отдельно;
- каждая обратная операция снимает с файла один слой, в том порядке, в каком слои лежат в файле; порядок операций в массиве не важен. Например, `["DECRYPT", "UNZIP", "UNSIGN"]` для `act.pdf.sig.zip.enc` возвращает `act.pdf`;
- `DECRYPT` снимает шифрование с входного файла;
- `UNSIGN` без `DECRYPT` снимает подпись с входного файла, кроме ZIP-архива, который распаковывает `UNZIP`. Со всего остального — с расшифрованного файла и с файлов архива — подпись снимается, если у файла расширение подписи: `.sig`, `.p7s`, `.sgn`, `.sign`, `.bin` или `.pem`. Другие файлы возвращаются как есть;
- `UNZIP` распаковывает ZIP-архив: сам входной файл или то, что осталось от него после `DECRYPT` или `UNSIGN`. Если архив лежит поверх подписей, `UNSIGN` снимает подпись с файлов архива; если подпись лежит поверх архива — с самого архива. Каждый файл архива

возвращается отдельным результатом с идентификатором архива и своим `name`. Файл, который не является ZIP, после другой операции возвращается как есть, а при одной операции `UNZIP` даёт ошибку.

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`, `LICENSES`, `PRODUCT` и `COMMANDS`.

```
{
  "jsonrpc": "2.0",
  "method": "signAndEncrypt.parameters",
  "id": "tx-42",
  "diagnostic": {
    "VERSIONS": { "csp": "5.0.13000", "cryptoarm": "7.4.0", "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 }
    },
    "PRODUCT": "cryptoarm-sign",
    "COMMANDS": {
      "signAndEncrypt": { "openPdfMaster": true },
      "certificates": {},
      "certrequests": {},
      "diagnostics": {},
      "startView": {}
    }
  }
}
```

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.

Вместо `props.files` можно передать `props.archive` — 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, снятия подписи и распаковки 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

Поле	Описание
`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`	`false` — один файл результата на вызов, `true` — по файлу на каждый входной
`props.extra`	Настройки операции — см. Параметры extra

Параметры extra

Поле	Значения
`signType`	`0` — присоединённая подпись (по умолчанию), `1` — отсоединённая
`signStandard`	`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` или другое расширение, с точкой или без
`encryptionExtension`	`enc` (по умолчанию), `p7m`, `p7e`, `pem` или другое расширение, с точкой или без
`signerChainIncludeKind`	`personal` — только сертификат подписанта (по умолчанию), `full` — вся цепочка
`timestampOnSign`	`true` превращает CAdES-BES в CAdES-T; `false` стандарт не понижает
`tspURL`, `ocspURL`	Адреса служб штампа времени и проверки статуса сертификата
`isSignaturePades`	Подпись PDF в формате PAdES
`isPdfCertificationSign`	Сертифицирующая подпись PDF
`isAddStampToPdf`	Отдельная печатная копия PDF со штампом подписи

Поле	Значения
`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
`isSafeMode`	Безопасный режим преобразования в PDF/A с меньшим расходом памяти. Действует, если документ в PDF/A преобразует профиль сервиса
`openPdfMaster`	`true` открывает документ в мастере «Подпись и защита PDF» — см. Подпись PDF
`signCertificate`	Сертификат подписанта
`encryptCertificates`	Сертификаты получателей
`MCHD`	Машиночитаемая доверенность
`token`	Токен доступа к входным файлам и получателю результата: параметр `accessToken` в их адресах
`pin`	ПИН-код контейнера закрытого ключа. Хранится только в памяти операции

Числовые значения принимаются и строками: `"1"` равнозначно `1`. Флаги — тоже: `"true"` равнозначно `true`, `"false"` — `false`.

Если `signStandard` не передан, стандарт подписи берётся из профиля доверенного сервиса, а без профиля — CAdES-BES. `timestampOnSign: true` поднимает CAdES-BES до CAdES-T и требует адреса службы штампов времени — из `tspURL` или профиля.

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": "<Base64 DER или PEM>" }`

Селектор	Пример
Издатель и серийный номер	`{ "issuerName": "CN=Example CA", "serial": "01AB" }`

```
{
  "extra": {
    "signCertificate": { "hash": "b0a1c2d3e4f5a6b7c8d9e0f1a2b3c4d5e6f7a8b9" }
  }
}
```

Подписать можно сертификатом из «Личных» с закрытым ключом — ГОСТ, RSA или ECDSA, как при обычной подписи. Сертификат RSA или ECDSA, как и сертификат, ключ которого хранится не в КриптоПро CSP, подписывает в формате CMS, в том числе при `signStandard: "cades-bes"`. Стандарты CAdES-T, CAdES-X Long Type 1 и CAdES-A для него приводят к ошибке.

Если сертификата подписанта нет в хранилище пользователя или у него нет закрытого ключа, операция не отклоняется: пользователь выбирает сертификат подписи сам.

Получатели шифрования передаются в `encryptCertificates` — массивом сертификатов в Base64 DER или PEM. Без операции `ENCRYPT` поле не учитывается. Устанавливать получателей пользователю не нужно: они используются в том виде, в котором их передал сервис, и в хранилище не добавляются. Сертификат УЦ получателем быть не может.

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 на экране операции. Переданные сервисом получатели и найденный сертификат подписанта показываются без возможности изменения.

Подпись PDF и штамп

Подпись PAdES включается полем `isSignaturePades`, печатная копия со штампом — полем `isAddStampToPdf`. Оформление и размещение штампа, подпись в готовое поле документа (`signStampPAdES.fieldName`) и открытие документа в мастере «Подпись и защита PDF» (`openPdfMaster`) описаны на странице Подпись PDF.

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.

Без `extra.MCHD` подпись создаётся с МЧД из профиля сервиса, и на экране операции пользователь может выбрать другую или убрать её. Реквизит штампа `MCHDNumber` без значения показывает номер МЧД, с которой создаётся подпись.

Настройки и подтверждение

Явно переданные через API тип подписи, кодировки, расширения файлов, алгоритм шифрования, подпись PAdES, сертификация, печатная копия, видимость подписи PAdES (`pdfMarkedArea.isVisible`), МЧД и сертификаты заблокированы для изменения. Если параметр не передан, начальное значение берётся из профиля сервиса, и пользователь может его изменить. Готовое поле подписи (`signStampPAdES.fieldName`) и мастер PDF фиксируют подпись PAdES и её видимость.

Вид и положение штампа пользователь меняет, только если вызов не передал ни `PAdESStampAppearance`, ни `signStampAppearance`, ни `signStampPosition`, ни `signStampPAdES`. Штамп, который пользователь изменил, ставится таким, каким он показан на экране операции. Если пользователь штамп не менял, он ставится по правилам из раздела Оформление и размещение штампа.

Стандарт подписи, состав цепочки сертификатов в подписи и преобразование в PDF/A берутся из вызова и профиля сервиса и на экране операции не меняются. Место подписи пользователь выбирает только в мастере PDF.

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 или получить не удалось. Такой результат приходит со `status: "Error"`, а файл, который не проверен, — с полем `error`.

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. Сообщение приходит со `status: "Completed"`, а `signValid` и `signers[].isValid` — со значением `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. Архив операции `ARCHIVE` передаётся частью с именем `file`, файлы распакованного `UNZIP` архива — частями с идентификатором архива. Отчёт о проверке и печатная копия со штампом остаются полями конверта в Base64.

Значение `returnFiles: false` оставляет метаданные результата без содержимого файлов. Такой результат отправляется обычным JSON и при `uploadMethod: "multipart/form-data"`.

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.

Результаты записываются по файлу на каждый входной файл:

Каталог	Прямая и обратная	Проверка подписи
`props.localResultParams.savePath`	`direct-result-<id>.json`, затем `direct-result-<id>(1).json`, …	`verify-result-<id>.json`, затем `verify-result-<id>(1).json`, …
`props.uploader`	`direct-result-<id>-<fileId>.json`	`verify-result-<id>-<fileId>.json`

`saveResultsSeparately: true` даёт имена `<…>-result-<id>-<fileId>.json` и при `savePath`, `false` — один файл `direct-result-<id>.json` или `verify-result-<id>.json` на вызов. Существующие файлы не перезаписываются: к имени добавляется следующий 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
`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
`qualification`	Object	Квалифицированность сертификата подписанта
`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 хэширования
`extVerifyInfo`	Object	Результат проверки CAdES в КриптоПро CSP
`signerCertificate`	Object	Сертификат подписанта

`qualification` передаётся, только когда действует режим «Квалифицированная подпись», и только у подписи, действительной без него. В этом режиме `isValid` — `true`, только если квалифицированность подтверждена:

Поле	Тип	Описание
`state`	string	`passed` — подтверждена, `failed` — не подтверждена, `error` — проверить не удалось
`verification`	Object	Ответ сервера для `passed` и `failed`
`checkedAt`	string	Время проверки в формате ISO 8601
`error`	string	Код причины для `error`, например `network.unreachable` или `network.authRequired`

Поля `verification`:

Поле	Тип	Описание
`status`	boolean	Проверка по списку доверия пройдена
`isAccreditedCA`	boolean	Издатель сертификата — аккредитованный УЦ
`error`	string	Текст причины отказа от сервера, если он передан

`signatureAlgorithm` — алгоритм подписи вместе с хэшем: для RSA и ECDSA это, например, `1.2.840.113549.1.1.11` (sha256WithRSAEncryption), а не идентификатор алгоритма ключа.

`extVerifyInfo` передаётся только для подписи CAdES:

Поле	Тип	Описание
`cadesType`	number	Тип CAdES
`cadesVfyStatus`	number	Код проверки CAdES: `0` — успешно, иначе код ошибки КриптоПро CSP
`mathValidity`	boolean	Математическая корректность подписи — без учёта статуса сертификата
`successVfyType`	number	Тип CAdES, по которому подпись прошла проверку, если заявленный не прошёл

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
`provider`	string	Криптопровайдер
`notBefore`	number	

Поле	Тип	Описание
		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 PDF — штамп, готовое поле и мастер «Подпись и защита PDF».
- Подпись и шифрование — те же операции в интерфейсе.

Открыть статью на сайте

Подпись PDF: штамп, готовое поле и мастер

Страница дополняет описание команды `signAndEncrypt`: здесь собраны параметры, которые относятся только к подписи PDF-документов.

Содержание:

- Оформление и размещение штампа
- Подпись в готовое поле
- Мастер «Подпись и защита PDF»
- Смотрите также

Оформление и размещение штампа

Оформление видимого штампа задаётся объектом `PAdESStampAppearance` — для подписи PAdES — и объектом `signStampAppearance` — для отдельной печатной копии со штампом.

В сетевом вызове поля вызова накладываются на штамп из профиля доверенного сервиса: что вызов не передал, берётся из профиля, а блок `requisitesSettings` заменяется целиком. В локальном вызове недостающее — значение по умолчанию. `PAdESStampAppearance` учитывается, только если подпись PAdES включает сам вызов (`isSignaturePades: true`).

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 PNG, JPEG, GIF, WebP или BMP: `…` или Base64 PNG, JPEG и GIF без префикса. В локальном вызове — также путь или `file://` к файлу изображения
`isHiddenLogo`	Скрыть логотип

Блок `requisitesSettings` — состав реквизитов:

Поле	Значения
`centralDisplayType`	`byGost` — состав по ГОСТ, `arbitrary` — список `central`. Без значения — список `central`, а если его нет — 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": "…" }`. `editedValue` печатается вместо значения из сертификата; с `"isUsedEditedValue": false` печатается значение из сертификата. Реквизиты выводятся в штампе в порядке элементов списка. 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`	`last`, `some` или `all` — см. Выбор страницы
`pageNumbers`	Массив номеров страниц; обязателен при `some`
`pdfMarkedArea.pageNumber`	Номер страницы, если не передан `pageNumbers`
`isDisplayedOnAllPages`	Показывать штамп на всех страницах
`pdfMarkedArea.dimensionsDocument`	`width`, `height`, `horizontalPadding`, `verticalPadding`
`pdfMarkedArea.stampSize`	`width` и `height` штампа, если их нет в `dimensionsDocument`
`pdfMarkedArea.placementOnPage`	`horizontal`: `left`, `center`, `right`; `vertical`: `top`, `center`, `bottom`
`pdfMarkedArea.orientationDegrees`	Поворот: `0`, `90`, `180` или `270`
`pdfMarkedArea.isVisible`	`false` — подпись PAdES без штампа, даже если штамп задаёт профиль сервиса
`fieldName`	Имя готового поля подписи — см. Подпись в готовое поле

Размеры и отступы задаются в пунктах PDF.

Выбор страницы

Подпись PAdES стоит на одной странице: при `last` — на последней, при `some` — на первой из `pageNumbers`, а на остальные страницы списка ставятся копии её штампа. Значение `all` не означает все страницы: подпись встаёт на страницу из `pdfMarkedArea.pageNumber`, а без неё — на последнюю. Штамп на всех страницах включает `isDisplayedOnAllPages`: подпись остаётся на выбранной странице, а копии штампа ставятся на остальные.

Без `pdfMarkedArea.isVisible` подпись PAdES получает штамп, если его задаёт профиль сервиса с подписью PAdES. Если профиль не подписывает PAdES или его нет, штамп получает подпись, которую включил сам вызов (`isSignaturePades`).

Для печатной копии страницы задаются внутри `signStampAppearance`: `pageSelection` и строка `pageNumbers` вида `"1,3-5"`. Без них копия ставится на все страницы. Печатная копия, которую включил профиль сервиса, а вызов не упоминает, ставится целиком по профилю.

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.

Подпись в готовое поле

Если сервис сам готовит PDF-форму с местами для нескольких подписантов, каждое место — это пустое поле подписи с именем. `signStampPAdES.fieldName` указывает, в какое из них поставить подпись этого вызова:

```
{
  "isSignaturePades": true,
  "signStampPAdES": { "fieldName": "Signer3" }
}
```

- Место и размер подписи задаёт поле. Остальное размещение из `signStampPAdES` — страницы, отступы, привязка к краю, штамп на всех страницах — не используется. Поле без размеров на странице даёт невидимую подпись.
- Штамп вписывается в поле с сохранением пропорций своего размера — `width` и `height` из `pdfMarkedArea.dimensionsDocument` или `pdfMarkedArea.stampSize`. Чтобы он заполнил поле целиком, передайте размеры поля.
- Вид штампа определяется, как в разделе Оформление и размещение штампа: поля вызова поверх штампа профиля сервиса, без профиля — поверх штампа по умолчанию. Штамп профиля используется, даже если сам профиль подписывает без видимого штампа.
- Имя указывается точно, с учётом регистра.

- Поля подписи должны лежать в корне формы, а не внутри иерархии полей: вложенное поле (`form[0].page[0].signature[0]`) не находится. XFA и расширенные права Adobe Reader сервис должен снять до вызова: КриптоАРМ подписывает документ в том виде, в каком его получил.
- Поле требует PAdES — `isSignaturePades: true` или профиль сервиса с подписью PAdES, иначе вызов отклоняется с ошибкой. Для операций без `SIGN` поле не используется.
- Если поля с таким именем нет или оно уже подписано, файл не подписывается: сервис получает `Canceled` с кодом `x509.pdf.sign.fieldNotFound` или `x509.pdf.sign.fieldAlreadySigned` в `ErrorDescription` (см. Необработанные файлы).

Остальные поля документа не меняются, поэтому следующий подписант получает тот же файл со своим `fieldName`. Каждая подпись дописывается к файлу и не нарушает предыдущие.

Для второго и следующих подписантов:

- Сертифицирующей может быть только первая подпись. Если профиль сервиса создаёт сертифицирующую подпись, передавайте остальным `isPdfCertificationSign: false`, иначе файл не подпишется с кодом `x509.pdf.sign.certificationNotFirst`.
- PDF/A из профиля не применяется к документу, в котором уже есть поля подписи.
- Документ, сертификация которого запрещает любые изменения, не подписывается — код `x509.pdf.sign.certificationLocked`. Сертификация, разрешающая заполнять форму и подписывать, после подписи в поле остаётся действительной.

Мастер «Подпись и защита PDF»

С `openPdfMaster: true` документ открывается не на экране операции, а в мастере «Подпись и защита PDF». Пользователь видит страницы и сам выбирает, куда поставить подпись: в готовое поле или в любое место на странице. Без параметра открывается обычный экран операции.

```
{
  "operation": ["SIGN"],
  "props": {
    "files": [{ "id": "form", "name": "form.pdf", "url": "https://api.example.ru/files/
form.pdf" }],
    "uploader": "https://api.example.ru/results",
    "extra": {
      "openPdfMaster": true,
      "isSignaturePades": true,
      "signStampPAdES": { "fieldName": "Signer3" }
    }
  }
}
```

Мастер открывается только для такого вызова, иначе вызов отклоняется с ошибкой:

- операция — только `SIGN`;
- в `props.files` ровно один файл с расширением `.pdf`, без `props.archive`;

- подпись PAdES — `isSignaturePades: true` или профиль сервиса с подписью PAdES;
- без печатной копии: `isAddStampToPdf: true` не допускается.

Что задаёт вызов:

- `signStampPAdES.fieldName` — поле, выбранное для подписи при открытии. Если пустого поля с таким именем нет, место пользователь выбирает сам.
- Размещение из `signStampPAdES` — где подпись появится, если в документе нет пустых полей. Если они есть, а `fieldName` не задан, место выбирает пользователь.
- Вид штампа — по тем же правилам, что для подписи в готовое поле. Изменить его в мастере нельзя.
- Сертификат подписи — как на экране операции (см. Сертификаты).
- Стандарт подписи и сертификация — из вызова и профиля сервиса; изменить их в мастере нельзя.
- МЧД — из `extra.MCHD`, без него — из профиля сервиса; выбрать другую в мастере нельзя.

Что может пользователь:

- перенести подпись в другое пустое поле или в любое место на странице;
- разметить места для следующих подписантов — они сохраняются в документе пустыми полями подписи с введёнными названиями, и эти названия можно передавать в `fieldName`;
- добавить произвольную область с текстом или изображением;
- заполнить сведения о подписи: причину, место, контакт.

Сертификация из профиля не применяется к уже подписанному документу, а PDF/A — к документу с подписями или полями подписи. Сертификация, запрошенная в вызове (`isPdfCertificationSign: true`), так не отключается: уже подписанный документ тогда не подписывается, и сервис получает код `x509.pdf.sign.certificationNotFirst`.

`showSettingsBeforeOperation` мастер не учитывает: он сам служит экраном настроек.

Ответ сервису:

- Результат приходит в том же формате, что и с экрана операции. Если в вызове есть `uploader`, вкладка мастера после отправки закрывается.
- Подпись выполняется один раз. Если она не удалась — например, из-за неверного ПИН-кода, — сервис получает ошибку, а для новой попытки нужен новый вызов.
- Закрытие вкладки до подписи — отмена: сервис получает `Canceled`.

Поддержку мастера сервис узнаёт по `COMMANDS.signAndEncrypt.openPdfMaster` в `diagnostic` запроса параметров (см. диагностику). Этот же признак означает поддержку `signStampPAdES.fieldName`. Версия без признака оба параметра пропускает: открывает обычный экран операции и ставит подпись по размещению из `signStampPAdES`, а не в поле.

Смотрите также

- Команда signAndEncrypt — операции, файлы, параметры и результат.

- Команда diagnostics — признак поддержки `openPdfMaster`.
- Лимиты, статусы и ошибки — коды ошибок и отмена.
- Подпись и защита PDF — тот же мастер 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 DER в Base64 или PEM — 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

Неизвестное хранилище — ошибка.

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**. Если в `props.store` есть допустимое для сертификата хранилище, сертификат импортируется в первое такое без выбора: пользователь только подтверждает импорт. Если допустимого нет, пользователь выбирает хранилище сам, начиная с рекомендуемого для сертификата, и результат не сообщает, какое он выбрал.

Сертификат попадает только в это хранилище: самоподписанный пользовательский сертификат не становится доверенным корневым.

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

Поле	Тип	Описание
`issuerFriendlyName`	string	Издатель в удобочитаемом виде
`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`
`utf8name`	`true` — кириллица в сведениях о владельце в UTF8String

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`	

Поле	Описание
	Дополнительные расширенные назначения ключа, OID через ;
privateKeyUsagePeriod	Срок использования закрытого ключа в секундах от момента, когда открывается форма 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

Форма показывает только поля из RDN, обязательны в ней поля с ProhibitEmpty. Если CN в шаблоне нет, запрос создаётся без него.

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>"
      }
    }
  }
}
```

`certificateBase64` — сертификат DER в Base64 или PEM. 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. 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.

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, сведения о личных сертификатах, а также название приложения и команды, которые оно поддерживает.

Содержание:

- Общая информация
- Формат ссылки
- Параметры
- Подтверждение пользователем
- Результат
- Приложение и поддерживаемые команды
- Сведения о личных сертификатах
- Смотрите также

Общая информация

Возвращаются только запрошенные сведения: приложение не собирает и не отправляет сведения, которые сервис не запрашивал.

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

Значение	Что возвращается
`CSP_ENABLED`	Доступность КриптоПро CSP
`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
`PRODUCT`	Название приложения
`COMMANDS`	Команды протокола, которые поддерживает приложение

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", "PRODUCT", "COMMAN
DS"],
    "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. Изменить разрешение 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": "7.4.0",
      "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 }
    },
    "PRODUCT": "cryptoarm-sign",
    "COMMANDS": {
      "signAndEncrypt": { "openPdfMaster": true },
      "certificates": {},
      "certrequests": {},
      "diagnostics": {},
      "startView": {}
    }
  }
}
```

Поле `packageType` различает только платформу, на которой запущено приложение: `msi` — Windows, `pkg` — macOS, `deb` — Linux, каким бы установщиком оно ни было установлено.

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

Поле	КриптоАРМ	КриптоПро CSP
`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.

Приложение и поддерживаемые команды

Протокол `cryptoarm://` обслуживают и КриптоАРМ «Подпись и шифрование», и КриптоАРМ «Защищенная почта», а набор команд у них разный: например, `sendMail` есть только в «Защищенной почте». Версию оба приложения сообщают под одним ключом `VERSIONS.cryptoarm`.

Перед вызовом команды сервис проверяет, есть ли она среди ключей `COMMANDS`. Значение ключа — объект со сведениями о том, что поддерживает команда. Сейчас там одно поле — `signAndEncrypt.openPdfMaster: true`: приложение умеет открывать документ в мастере «Подпись и защита PDF» и подписывать готовое поле PDF. Новые сведения в объекте только добавляются, поэтому незнакомые поля сервис пропускает. `PRODUCT` называет приложение — `cryptoarm-sign` — и нужен для журналов и поддержки; набор команд по нему не определяется.

Оба поля приходят и в `diagnostic` запроса параметров каждой команды, поэтому отдельный вызов `diagnostics` для этого не нужен. Если полей нет, приложение их не поддерживает. Тогда команду можно вызвать как обычно: неподдерживаемую команду приложение отклонит с ошибкой `Command is not supported` — см. ошибки и ограничения.

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

Поле	Тип	Описание
`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 хэширования 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 — 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.

Отдельного раздела 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
Один запрос: параметры, файл или результат	600 секунд
Сообщение сервису об ошибке или отмене	10 секунд
Установка соединения с сервером	30 секунд
Ответ сервиса, встроенный JSON или локальный файл	Около 512 МиБ
Данные, встроенные в один JSON-результат в Base64	Около 383 МиБ суммарно

Вызовы выполняются по одному: следующий начинается, когда пользователь закончит с текущим. Повторный вызов той же транзакции отклоняется, пока предыдущий не завершён.

Для больших результатов используйте `multipart/form-data` или `returnFiles: false`.

Статусы операции

`status`	Значение
`Completed`	Операция завершена; результат может описывать недействительную подпись
`Error`	Техническая или операционная ошибка
`Canceled`	

status	Значение
	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.

Недействительная подпись — это результат проверки, а не ошибка: статус остаётся `Completed` — см. Проверка подписи.

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`

Когда	method
Приложение закрыто до завершения вызова	Метод текущего этапа: до чтения параметров <команда>.parameters, после — метод результата

Причина передаётся в ErrorDescription:

Причина	ErrorDescription
Пользователь отменил операцию или закрыл её окно	Operation canceled
Пользователь отказал в diagnostics или отменил certrequests	Access denied
Пользователь не подтвердил доверие сервису	Access denied
Пользователь закрыл приложение до завершения вызова	App closed
Остальные ошибки	Описание причины

Если пользователь нажал **Отмена** или закрыл окно подтверждения доверия, сервис получает отказ — и при первом обращении, и после смены сертификата у доверенного сервиса. Доверенным сервис от этого не становится, а сохранённый сертификат не меняется.

На вызов команды, которой в приложении нет, доверенный сервис получает <команда>.parameters со статусом Canceled и ErrorDescription: "Command is not supported: <команда>"; окно подтверждения не показывается.

При выходе из приложения выполняемый вызов получает App closed. 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.

Закрытие окна приложения отменяет операцию, которая ещё не запущена; 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.