Цифровые технологии

# КриптоАРМ Server

# Документация продукта

## Релиз v1.2

> Архивная документация. Актуальный релиз: v1.3

Исходная документация на CryptoARM.ru

Редакция от 26.11.2026

Правообладатель и разработчик
ООО «Цифровые технологии»

# Содержание

Общие сведения

- О продукте ... 3
- Глоссарий ... 5
- Часто задаваемые вопросы ... 12

Установка

- Инструкции по установке ... 15
- Настройка переменной REPORT_INFO_MESSAGE ... 22

Варианты использования

- Введение в форматы и стандарты электронной подписи ... 26
- Сервис проверки и улучшения электронных подписей ... 31
- Telegram-бот для проверки электронной подписи ... 37
- Сервис для настройки рабочего места ... 43

Открыть статью на сайте

# О продукте

**КриптоАРМ Server** — программный продукт, предназначенный для интеграции и автоматизации криптографических операций в информационных системах организаций. Он включает в себя набор криптографических библиотек и средства разработки (SDK), позволяющие встраивать функции шифрования данных, проверки электронных подписей и их создания в автоматизированных процессах обработки информации.

---

## Функции продукта

**Проверка электронной подписи**:

- Автоматизируйте проверку электронной подписи для поступающих документов
- Создавайте и храните протоколы проверки электронной подписи
- Визуализируйте электронную подпись для PDF документов

**Автоматизация электронной подписи**:

- Создайте свой собственный сервис электронной подписи
- Поддержка стандартов CMS, CAdES, PAdES
- Используйте КриптоАРМ на рабочих станциях и мобильных устройствах как клиент для электронной подписи

**Защита исходящих документов**:

- Отправка конфиденциальных документов
- Автоматическое шифрование файлов перед отправкой по e-mail
- Автоматическая обработка входящих писем: расшифрование, проверка подписи и категоризация

---

## Функциональные модули

| Модуль | Описание |
|---|---|
| trusted-crypto | Формирование электронной подписи,<br>Проверка подписи, шифрование и расшифрование,<br>Сведения о сертификатах,<br>Генерация ключевой пары и создание запросов на получение сертификата,<br>Подключение защищенных носителей |
| trusted-pdf | |

| Модуль | Описание |
| --- | --- |
| | Подпись и проверка электронной подписи встроенной в pdf,<br>Разметка областей для оттисков подписи,<br>Добавление графических штампов с информацией о подписи,<br>Пакетная подпись,<br>Сертификация подписанных документов с защитой от изменений,<br>Конвертация pdf-файлов в формат pdf-a/2b |
| trusted-mailcore | Сбор, разбор и отправка электронных писем,<br>Поддержка IMAP, SMTP, POP3, S/MIME,<br>Контакты и адресные книги vCard, CardDAV |
| trusted-curl | Обеспечение защищенного соединения к веб-серверам с поддержкой ГОСТ TLS |
| trusted-xml-crypto | Проверка электронной подписи формата XMLDSig (XML Digital Signature) |

Открыть статью на сайте

# Глоссарий


- Сертификаты
- Подпись и шифрование
- Почта


## Сертификаты

### Сертификат электронной подписи

Электронный документ, который подтверждает владение ключом электронной подписи

### Сертификат усиленной квалифицированной электронной подписи (УКЭП)

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

### Самоподписанный сертификат

Сертификат, изданный самим пользователем, без обращения к Удостоверяющему центру.

### Открытый ключ электронной подписи

Ключ проверки электронной подписи. Содержит содержит уникальный код, с помощью которого можно проверить подлинность электронной подписи. Сертификат открытого ключа содержит сведения о подписанте (ФИО, СНИЛС и др.), об удостоверяющем центре, который выдал ЭП и срок действия ключа.

### Закрытый ключ электронной подписи

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

### Запрос на сертификат

Электронный документ, который содержит информацию для получения сертификата электронной подписи в Удостоверяющем центре

## Ключевой контейнер

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

## Статус сертификата электронной подписи

Информация о действительности сертификата

## Удостоверяющий центр (УЦ)

Доверенная организация, которая имеет право выпускать сертификаты электронной подписи (ЭП) юридическим и физическим лицам

## Корневой сертификат

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

## Промежуточный сертификат

Сертификат, выданный удостоверяющим центрам

## Сертификат другого пользователя

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

## Список отзыва сертификатов

Список сертификатов, которые удостоверяющий центр пометил как отозванные.

## Цепочка сертификации или цепочка доверия

Иерархическая коллекция сертификатов. Для квалифицированных сертификатов ЭП, как правило, состоит из 3 звеньев. Верхнее звено - корневой сертификат. Среднее звено - сертификат удостоверяющего центра. Конечное звено - сертификат пользователя.

### Сервис DSS

Сервис электронной подписи. Предназначен для шифрования и расшифрования электронных документов, формирования запросов на создание и управление сертификатами ключей проверки электронной подписи, создания и проверки электронной подписи различного формата криптографических сообщений.

## Подпись и шифрование

### Электронная подпись (ЭП)

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

### Усиленная неквалифицированная электронная подпись (УНЭП)

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

### Усиленная квалифицированная электронная подпись (УКЭП)

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

### Профили подписи в КриптоАРМ

Заранее подготовленные наборы настроек, которые можно применять для выполнения подписи, архивирования и шифрования.

### Алгоритмы подписи

Криптографические алгоритмы, которые используются для создания электронной цифровой подписи

### Алгоритмы шифрования

Криптографические алгоритмы, которые используются для шифрования файлов

### Криптопровайдер

Провайдер криптографических услуг, криптопровайдер специализированный программный модуль или набор модулей, предоставляющих средства шифрования и дешифрования данных, цифровой подписи, а также генерации и хранения ключей.

## Присоединенная подпись

Подпись, в процессе создания которой формируется специальный контейнер, в котором находятся как подписываемый документ, так и файл подписи.

## Отсоединенная подпись

Файл подписи формируется и хранится отдельно от подписываемого документа.

## Стандарт подписи CAdES-BES (Basic Electronic Signature)

Основной и простейший формат электронной подписи, описываемый в стандарте CAdES. Он обеспечивает базовую проверку подлинности данных и защиту их целостности

## Стандарт подписи CAdES-T (Timestamp)

Формат электронной подписи, в которую автоматически добавляется штамп времени на подпись.

## Стандарт подписи CAdES-X Long Type 1

Формат электронной подписи, включающий дополнительные атрибуты certificate-values и revocation-values, которые представляют собой полные данные сертификатов и списки отзыва сертификатов. А также штампы времени на подпись и ссылки на сертификаты и списки отзыва сертификатов.

## Стандарт подписи CAdES-A (Archival)

Формат электронной подписи, сформированный на основе CAdES-X Long Type 1 или Type 2 путём добавления одного или нескольких атрибутов archive-time-stamp, представляющих собой архивные штампы времени.

## Машиночитаемая доверенность

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

## Сертификация PDF документа

Позволяет защитить PDF документ от изменений путем его подписания электронной подписью, с указанием типа изменений, разрешенных для документа.

## Конвертация PDF документа

При конвертации PDF документа происходит удаление скриптов, форм и прочих элементов, влияющих на безопасность и целостность документа.

### Формат подписи CadES

Стандарт электронной подписи, представляющий собой расширенную версию стандарта электронной подписи CMS. Эту электронную подпись можно прикрепить к любому типу файла : текстовым файлам ( .doc, .docx ), электронным таблицам ( .xls, .xlsx ), изображениям ( .jpg, .png, .gif ) и PDF-файлам.

### Формат подписи PadES

Формат, при котором подпись встраивается в PDF-документ. «Встроенная» подпись позволяет подписывать электронные документы без изменения формата файла и без создания отдельного файла подписи, как это происходит при использовании присоединенной и отсоединенной подписи соответственно. Подпись встраивается в электронный документ, и получатель может проверить документ на действительность электронной подписи.

### Видимая подпись PDF документа

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

### Невидимая подпись PDF документа

«Встроенная» подпись, которая визуально на страницах не видна.

### Область для штампа подписи в PDF документе

Область на странице PDF документа, размеченная для видимой подписи.

### Произвольная область в PDF документе

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

## Почта

### Адрес электронной почты

Название электронного почтового ящика, который может получать (и отправлять) электронные письма в сети (например, в интернете или в локальной сети, не подключённой к интернету).

### Почтовый сервер

Это программа, работающая у интернет-провайдеров и на крупных сайтах и используемая для передачи почты. Обычно пользователи не взаимодействуют с почтовыми серверами напрямую: электронная почта отправляется с помощью почтового клиента на почтовый сервер, который доставляет её в почтовый клиент получателя.

## Почтовый клиент

Это программа (например, на компьютере или мобильном устройстве), которая используется для чтения и отправки электронных сообщений.

## IMAP

Протокол, который используется для получения сообщений электронной почты с сервера. IMAP позволяет почтовым программам получать доступ не только к новым сообщениям, но и к папкам на сервере. Действия синхронизируются между несколькими почтовыми программами, подключёнными через IMAP.

## POP

Протокол, который используется для получения сообщений электронной почты с сервера. В отличие от IMAP, POP позволяет почтовому клиенту загружать только последние сообщения, которыми можно управлять в клиенте и на устройстве.

## SMTP

Протокол, который используется для передачи электронной почты. Он определяет формат сообщений и процедуру их передачи через Интернет от отправителя к получателю с помощью почтовых серверов.

## S/MIME

Стандарт для шифрования и подписи электронных писем с помощью открытого ключа.

## SSL

Протокол, который обеспечивает безопасное соединение между клиентом и сервером.

## Логин (имя пользователя)

Имя почтового ящика — комбинация из букв и цифр, которая, как правило, находится в адресе перед именем домена.

## Пароль

Набор символов, предназначенный для подтверждения личности.

## Скрытая копия

Копия электронного письма, отправленного получателю, адрес электронной почты которого не указан (в качестве получателя) в сообщении

## Копия

Копия электронного письма, отправленного получателю, адрес электронной почты которого указан в поле заголовка «Копия».

## Тело письма

Основная часть электронного письма, которая содержит текст, изображения и другие данные (например, прикреплённые файлы).

## LDAP

Протокол быстрого доступа к каталогам. Он позволяет получать и принимать через сеть данные из каталогов с иерархической структурой.

## ALD Pro

Служба каталога для Linux, программный комплекс централизованного управления компьютерами с помощью групповых политик, а также прикладными сервисами для ИТ-инфраструктур организаций различного масштаба. Комплекс создан «Группой Астра».

## CardDAV

Протокол адресной книги, предназначенный для предоставления пользователям доступа к данным на сервере.

## vCard

текстовый формат для обмена электронными визитными карточками. В карточке может содержаться имя, номера телефонов, адрес электронной почты, адрес проживания, дата рождения, фотография, сертификат и другие данные контакта.

## Gravatar

Сервис компании Automattic, позволяющий интернет-пользователям хранить свой аватар на специальном сервере.

Открыть статью на сайте

# Часто задаваемые вопросы

## Для чего нужен КриптоАРМ Server

КриптоАРМ Server — программный продукт, предназначенный для интеграции и автоматизации криптографических операций в информационных системах организаций. Он включает в себя набор криптографических библиотек и средства разработки (SDK). Подробнее читайте в статье О продукте.

## Какие криптографические операции поддерживает КриптоАРМ Server

- Формирование электронной подписи, проверка подписи, шифрование и расшифрование, сведения о сертификатах, генерация ключевой пары и создание запросов на получение сертификата, подключение защищенных носителей.
- Подпись и проверка электронной подписи встроенной в pdf, разметка областей для оттисков подписи, добавление графических штампов с информацией о подписи, пакетная подпись, сертификация подписанных документов с защитой от изменений, конвертация pdf-файлов в формат pdf-a/2b.
- Сбор, разбор и отправка электронных писем, поддержка IMAP, SMTP, POP3, S/MIME, контакты и адресные книги vCard, CardDAV.
- Обеспечение защищенного соединения к веб-серверам с поддержкой ГОСТ TLS.
- Проверка электронной подписи формата XMLDSig (XML Digital Signature).

## Как интегрировать КриптоАРМ в свою систему

КриптоАРМ предлагает два инструмента для интеграции и автоматизации: API и SDK. Оба варианта упрощают автоматизацию криптографических операций, но имеют разные области применения.

## Где посмотреть документацию и примеры для API или SDK?

1. Документация КриптоАРМ API и КриптоАРМ SDK.
2. Ссылка на видеодемонстрацию работы API от наших партнеров.

Мы готовы помочь вам с интеграцией API и SDK в вашу систему, по всем вопросам обращайтесь на sales@cryptoarm.ru.

# Требуется ли оценка влияния?

Для использования КриптоАРМ в некоторых сценариях может потребоваться проведение исследований по оценке влияния (СФ).

В КриптоАРМ возможны следующие варианты применения:

1. Использование графических интерфейсов СКЗИ. В данном варианте использования СКЗИ дополнительных исследований **не требуется**.
2. Программный вызов КриптоАРМ API. В данном варианте использования СКЗИ **требуется проведение исследований** по оценке влияния СФ на СКЗИ.
3. Использование КриптоАРМ SDK рассматривается как встраивание СКЗИ во вновь разрабатываемое или существующее прикладное программное обеспечение, программно-аппаратные и аппаратные решения. В данном случае **требуется проведение тематических исследований** СФ со встроенным СКЗИ как самостоятельного шифровального (криптографического) средства.

Если вам требуется помощь в оценке влияния, оставьте заявку на sales@cryptoarm.ru.

# Какие лицензии нужны

Для использования КриптоАРМ SDK необходима серверная лицензия.

КриптоАРМ API может работать как с клиентскими, так и серверными лицензиями на КриптоАРМ. С актуальными ценами можно ознакомиться в интернет-магазине cryptoarm.ru и в прайс-листе.

Для API будет доступен дополнительный вариант лицензирования — транзакционный. В этом случае оператор информационной системы приобретает пакет лицензий и распространяет своим клиентам клиентские лицензии вместе с параметрами операции. Пользователю не надо покупать КриптоАРМ или вручную вводить лицензии.

Также потребуется лицензия на криптопровайдер КриптоПро CSP.

# Как интегрировать проверку подписи в свою систему

С помощью КриптоАРМ Server можно легко интегрировать проверку электронной подписи во внешние системы. КриптоАРМ предлагает два инструмента для интеграции и автоматизации: API и SDK. Оба варианта упрощают автоматизацию криптографических операций, но имеют разные области применения.

# Можно ли создать протокол проверки подписи

С помощью КриптоАРМ Server можно создать протокол (отчет) проверки электронной подписи. Кроме того, для PDF-файлов доступно создание копии с визуальным штампом.

# Можно ли создать копию документа с визуальным штампом

С помощью КриптоАРМ Server можно проверить электронную подпись и визуализировать штамп на PDF-документе.

# Как интегрировать электронную подпись в свою систему

С помощью КриптоАРМ Server можно автоматизировать процессы подписания электронных документов. Для этого КриптоАРМ предлагает два инструмента: API и SDK. Оба варианта упрощают автоматизацию криптографических операций, но имеют разные области применения.

# Какие стандарты подписи поддерживаются

В КриптоАРМ Server реализована поддержка стандартов CMS, CAdES, PAdES.

# Можно ли улучшить электронную подпись с помощью КриптоАРМ Server

С помощью КриптоАРМ Server можно улучшить любую электронную подпись с формата CAdES-BES до CAdES-A.

# Как защитить документы с помощью КриптоАРМ Server

С помощью КриптоАРМ Server можно автоматизировать процессы шифрования и расшифрования файлов.

Кроме того, с помощью КриптоАРМ Server (модуль trusted-mailcore2) можно реализовать интеграцию электронной почты в вашем проекте на Node.js.

Основные преимущества такой интеграции:

- Криптографическая защита писем: поддержка стандарта S/MIME с использованием ГОСТ-алгоритмов,
- Надежные TLS соединения: благодаря интеграции с cpcurl от КриптоПро обеспечена поддержка ГОСТ TLS для безопасных соединений с почтовыми серверами.
- Работа с сертифицированным криптопровайдером КриптоПро CSP.

Открыть статью на сайте

# Инструкции по установке


- Требования к системе
- Технологический стек
- Установка
- Вход в сервис
- Проверка работы сервиса
- Установка сертификатов
- Настройка отчета
- Подпись данных


## Требования к системе

| Характеристика | Минимальное значение | Дополнение |
|---|---|---|
| Информационная емкость ОЗУ | 4 Гб | |
| Информационная емкость HDD | 50 Гб | |
| Процессор | x86_64 (или amd64) | |
| Поддерживаемые ОС | Ubuntu 18.04 LTS (Bionic Beaver), Ubuntu 20.04 LTS (Focal Fossa), Debian 11 (Bullseye), Astra Linux CE 2.12.45 (Orel) | Другие Linux дистрибутивы, поддерживающие запуск Docker |
| Дополнительно | Средство автоматизации развертывания и контейнеризации Docker | |

## Технологический стек

Node.js, NestJS, КриптоПро CSP 5.0, КриптоАРМ ГОСТ SDK, Docker

## Установка

### Установка Docker и Docker Compose

Для запуска проекта необходимо установить **Docker** и **Docker Compose**.

> 🔍 Подробную инструкцию по установке можно найти в официальной документации Docker.
>
> 📌 Минимально необходимые версии компонентов: Docker Engine: **19.03** или выше

## Установка и первый запуск сервиса

1. Создайте и перейдите в рабочую директорию:

```
mkdir cryptoarm-server && cd cryptoarm-server
```

2. Загрузите конфигурационные файлы:

```
curl -O https://git.digtlab.ru/trusted/cryptoarm/server/-/raw/main/docker/docker-compose.yml
curl -O https://git.digtlab.ru/trusted/cryptoarm/server/-/raw/main/docker/Dockerfile
curl -O https://git.digtlab.ru/trusted/cryptoarm/server/-/raw/main/.env
```

3. Создайте директорию cryptopro:

```
mkdir cryptopro
```

4. Скачайте актуальную версию КриптоПро CSP 5.0 для Linux (x64, deb) и скопируйте файл linux-amd64_deb.tgz в каталог `cryptoarm-server/cryptopro`.

> 📌 Для скачивания требуется пройти авторизацию на сайте КриптоПро.

```
cryptoarm-server/cryptopro/linux-amd64_deb.tgz
```

5. Отредактируйте настройки конфигурации:

   Откройте файл **.env** для редактирования.

   - Укажите серверную лицензию КриптоПро CSP в переменной **CRYPTOPRO_LICENSE**: `CRYPTOPRO_LICENSE=XXXXXXXXXXXXXXXXXXXXXXXXX`
   - Укажите лицензию КриптоАРМ Server в переменной **TRUSTED_LICENSE**: `TRUSTED_LICENSE=XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`

   Опционально настройте переменные окружения:

   **Переменные для настройки TSP-сервиса:**

   - `TSP_SERVICE_ADDRESS` - адрес сервиса штампов времени (по умолчанию: `<http://qs.cryptopro.ru/tsp/tsp.srf>`)

**Переменные для настройки PDF-отчетов:**

- `REPORT_TITLE` - заголовок PDF-отчета (по умолчанию: `Отчет о проверке электронной подписи`)
- `DATA_STAMP_TITLE` - заголовок штампа на подписанном документе (по умолчанию: `Документ подписан электронной подписью`)
- `STAMP_COLOR` - цвет штампа в формате HEX (по умолчанию: `#4c40d2`)
- `REPORT_INFO_MESSAGE` - нижний колонтитул (по умолчанию: `{align:left}© {COMPANY_NAME} || {align:right}Страница {pageNumber} из {totalPages}\n{WEBSITE_URL}`)

**Поддерживаемые переменные:**

- `{pageNumber}` - номер текущей страницы
- `{totalPages}` - общее количество страниц
- `{COMPANY_NAME}` - название компании (по умолчанию: `ООО Цифровые технологии`)
- `{WEBSITE_URL}` - URL сайта компании (по умолчанию: `www.cryptoarm.ru`)
- `{VARIABLE_NAME}` - любая переменная окружения

**Поддерживаемые директивы выравнивания:**

- `{align:left}` - выравнивание по левому краю
- `{align:center}` - выравнивание по центру
- `{align:right}` - выравнивание по правому краю
- `{align:justify}` - выравнивание по ширине

6. Запустите сборку:

```
docker compose build --pull
```

7. Запустите сервис:

```
docker compose up -d
```

**Дополнительно:**

- Просмотр логов:

```
docker compose logs -f
```

- Остановка:

```
docker compose stop
```

- Обновление версии образа сервиса до актуальной:

```
docker compose build --pull
docker compose up -d
```

### Сборка из исходников

1. Склонируйте репозиторий:

```
git clone https://git.digtlab.ru/trustednet/cryptoarm/server
```

2. Выполните п. 3-5 из **Установка и первый запуск сервиса**

3. Запустите сборку:

```
docker compose build
```

## Вход в сервис

Для входа в web интерфейс сервиса откройте в браузере: `http://SERVER:PORT`

- Пример: **http://172.17.1.115:3037**

Swagger документация по REST API: `http://SERVER:PORT/docs`

- Пример: **http://172.17.1.115:3037/docs**

## Проверка работы сервиса

Проверить работу сервиса можно следующими способами:

1. С помощью **Swagger** документации `http://SERVER:PORT/docs`
2. С помощью утилиты **curl**:

```
   curl -X 'POST' \
  'http://172.17.1.115:3037/cms/verify' \
  -H 'accept: application/json' \
  -H 'Content-Type: application/json' \
  -d '{
  "cms": "MIAGCSqGSIb3...==,MSMwIQYJKoZI...==",
  "data": "dGVzdA==",
  "enhancedType": "CAdES-X Long Type 1"
}'
```

В запросе передаются следующие параметры:

- **cms**: откреплённая (либо прикреплённая) подпись, закодированная в Base64
- **data**: подписанные данные в формате Base64 (для откреплённой подписи)
- **enhancedType**: формат улучшения подписи (CAdES-T|CAdES-X Long Type 1|CAdES-A)

**Пример ответа:**

```http HTTP/1.1 201 Created Vary: Origin Access-Control-Allow-Credentials: true Content-Type: application/json; charset=utf-8 Content-Length: 136101 ETag: W/"213a5-+⅛qQ+hWCfJ0yGRz0/fQGpbTbk" Date: Thu, 26 Sep 2024 12:40:04 GMT Connection: keep-alive Keep-Alive: timeout=5
{ "status": 200, "message":"OK", "isValid": true, "isValidSign": true, "signs": [ { "cadesTypeName": "CAdES-BES", "certificate": { "version": 3, "status": true, "subjectFriendlyName": "esia test3", "issuerFriendlyName": "CRYPTO-PRO Test Center 2", "subjectName": "CN=esia test3", "issuerName": "E=support@cryptopro.ru\r\nC=RU\r\nL=Moscow\r\nO=CRYPTO-PRO LLC\r\nCN=CRYPTO-PRO Test Center 2", "notAfter": "2024-10-26T16:25:37.000Z", "notBefore": "2024-08-26T16:15:37.000Z", "serialNumber": "120064ECE1352507757C00A08B00020064ECE1", "thumbprint": "29063cd", "signatureAlgorithm": "1.2.643.7.1.1.3.2", "signatureDigestAlgorithm": "1.2.643.7.1.1.2.2", "publicKeyAlgorithm": "1.2.643.7.1.1.1.1" }, "certificateData": "MIIDEz...", "issuerName": "E=support@cryptopro.ru, C=RU, L=Moscow, O=CRYPTO-PRO LLC, CN=CRYPTO-PRO Test Center 2", "serialNumber": "120064ECE1352507757C00A08B00020064ECE1", "signatureAlgorithm": "1.2.643.7.1.1.3.2", "signatureDigestAlgorithm": "1.2.643.7.1.1.2.2", "certs": [ { "status": true, "subjectFriendlyName": "esia test3", "issuerFriendlyName": "CRYPTO-PRO Test Center 2", "subjectName": "CN=esia test3", "issuerName": "E=support@cryptopro.ru\r\nC=RU\r\nL=Moscow\r\nO=CRYPTO-PRO LLC\r\nCN=CRYPTO-PRO Test Center 2", "notAfter": "2024-10-26T16:25:37.000Z", "notBefore": "2024-08-26T16:15:37.000Z", "serialNumber": "120064ECE1352507757C00A08B00020064ECE1", "thumbprint": "29063cd", "signatureAlgorithm": "1.2.643.7.1.1.3.2", "signatureDigestAlgorithm": "1.2.643.7.1.1.2.2", "publicKeyAlgorithm": "1.2.643.7.1.1.1.1" } ], "isCertChainValid": true } ], "dataStamp": "JVBERi0xLjcKJ...=", "report": "JVBERi0xLjcKJ...="
}
```

```
**Атрибуты ответа:**

- **status**: Http статус
- **message**: Если произойдет ошибка, то причина ошибки будет указана здесь
- **isValid**: Общий результат проверки
- **isValidSign**: Результат математической корректности подписи
- **signs**: Информация о сертификатах
- **dataStamp**: Подписанные данные с визуализацией штампов подписей в формате Base64 (для PDF документов)
- **report**: PDF-отчет проверки в формате Base64

**Пример неуспешного ответа:**

```http
HTTP/1.1 400 Bad Request
Vary: Origin
Access-Control-Allow-Credentials: true
Content-Type: application/json; charset=utf-8
Content-Length: 101
ETag: W/"65-ykHUL2wV5KLzsDntQL70C94heK8"
Date: Thu, 26 Sep 2024 12:42:04 GMT
Connection: keep-alive
Keep-Alive: timeout=5
{
    "message": "Запрошена проверка прикрепленной CMS подписи, но подпись не содержит исходного документа",
    "error": "Bad Request",
```
```

```
    "statusCode": 400
}
```

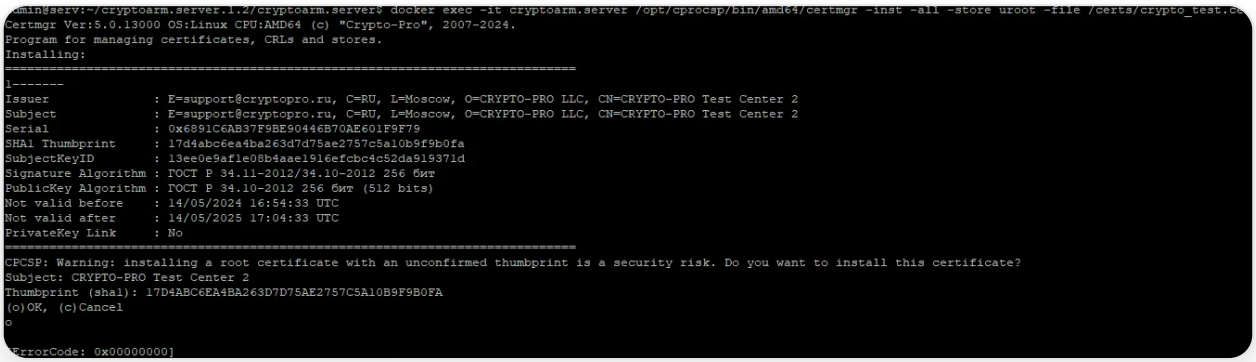
# Установка сертификатов

Скопируйте файлы сертификатов в каталог `cryptoarm-server/certs`.

## Установка корневого сертификата

Для установки корневого сертификата `certs/crypto_test.cer` выполните команду:

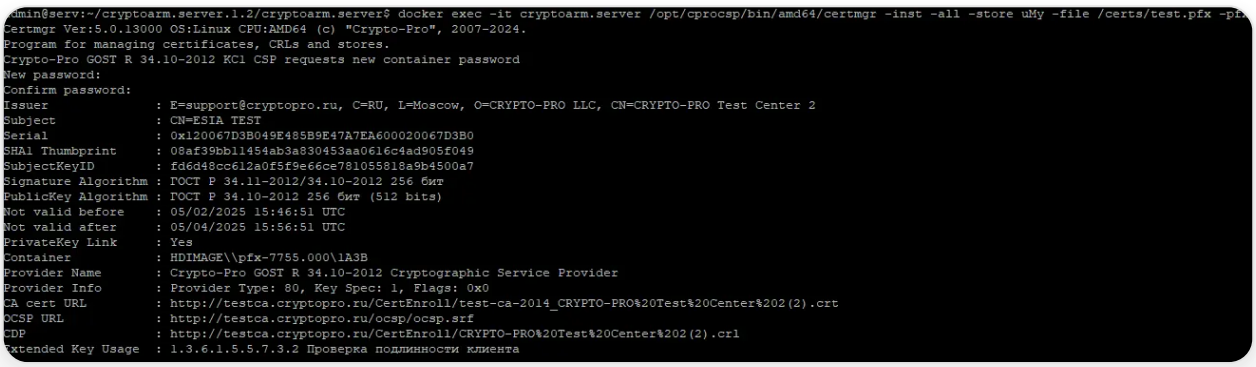
```
docker exec -it cryptoarm.server /opt/cprocsp/bin/amd64/certmgr -inst -all -store uroot -
file /certs/crypto_test.cer
```




## Установка сертификата пользователя

Для установки пользовательского сертификата `certs/test.pfx` выполните команду:

```
docker exec -it cryptoarm.server /opt/cprocsp/bin/amd64/certmgr -inst -all -store uMy -file /
certs/test.pfx -pfx
```



# Настройка отчета

## Настройка сообщения в колонтитуле

В переменной окружения `REPORT_INFO_MESSAGE` можно настроить сообщение, которое будет отображаться в колонтитуле PDF-отчета. Поддерживается замена переменных в формате `{VARIABLE_NAME}` и выравнивание текста с помощью директив `{align:direction}`.

Подробная документация доступна в файле Переменные окружения.

---

# Подпись данных

```
curl -X 'POST' \
  'http://172.17.1.115:3037/cms/sign' \
  -H 'accept: application/json' \
  -H 'Content-Type: application/json' \
  -d '{
    "cert": "MIIDEjCCAr+gAwI...==",
    "data": "dGVzdA==",
    "password": "password"
}'
```

## Параметры

- `cert`: Сертификат в Base64
- `data`: Подписываемые данные в Base64
- `password`: Пароль от контейнера (если требуется)

## Пример ответа

```
{
  "cms": "MIAGCSqGSIb3DQEHAq...AAAAAAAA"
}
```

Открыть статью на сайте

# Настройка переменной REPORT_INFO_MESSAGE


- Описание
- Поддерживаемые переменные
- Поддерживаемые директивы выравнивания
- Поддерживаемые директивы отступов
- Разделитель для одной строки
- Примеры использования
- Приоритет замены
- HTML-поддержка
- Комбинирование выравнивания и HTML
- Комбинирование отступов, выравнивания и HTML


## Описание

В переменной окружения `REPORT_INFO_MESSAGE` поддерживается замена переменных в формате `{VARIABLE_NAME}` и выравнивание текста с помощью директив `{align:direction}`.

## Поддерживаемые переменные

### Специальные переменные

- `{pageNumber}` - номер текущей страницы
- `{totalPages}` - общее количество страниц

### Переменные окружения

Любая переменная окружения может быть использована в формате `{VARIABLE_NAME}`.

Предустановленные переменные:

- `{COMPANY_NAME}` - название компании (по умолчанию: "ООО Цифровые технологии")
- `{WEBSITE_URL}` - URL сайта компании (по умолчанию: "www.cryptoarm.ru")

Переменные для настройки PDF-отчетов:

- `REPORT_TITLE` - заголовок PDF-отчета (по умолчанию: "Отчет о проверке электронной подписи")
- `DATA_STAMP_TITLE` - заголовок штампа на подписанном документе (по умолчанию: "Документ подписан электронной подписью")
- `STAMP_COLOR` - цвет штампа в формате HEX (по умолчанию: "#4c40d2")

Переменные для настройки TSP-сервиса:

- `TSP_SERVICE_ADDRESS` - адрес сервиса штампов времени (по умолчанию: "http://qs.cryptopro.ru/tsp/tsp.srf")

# Поддерживаемые директивы выравнивания

- `{align:left}` - выравнивание по левому краю (по умолчанию)
- `{align:center}` - выравнивание по центру
- `{align:right}` - выравнивание по правому краю
- `{align:justify}` - выравнивание по ширине (пока работает как left)

# Поддерживаемые директивы отступов

- `{left-margin:N}` - отступ слева в пикселях (N - число)
- `{right-margin:N}` - отступ справа в пикселях (N - число)

Директивы отступов можно комбинировать с директивами выравнивания на одной строке.

# Разделитель для одной строки

Используйте `||` для разделения строки на левую и правую части:

```
REPORT_INFO_MESSAGE="{left-margin:50}{align:left}Текст слева || {right-margin:50}{align:right}
Текст справа"
```

Это создаст эффект: `Текст слева Текст справа`

# Примеры использования

## Базовый пример

```
REPORT_INFO_MESSAGE="© Цифровые технологии
Страница {pageNumber} из {totalPages}
www.cryptoarm.ru"
```

## С использованием переменных окружения

```
# Установка переменных окружения (опционально)
COMPANY_NAME="ООО Цифровые технологии"
WEBSITE_URL="www.cryptoarm.ru"

# Использование в REPORT_INFO_MESSAGE
REPORT_INFO_MESSAGE="© {COMPANY_NAME}
Страница {pageNumber} из {totalPages}
{WEBSITE_URL}"
```

**Примечание:** Переменные `COMPANY_NAME` и `WEBSITE_URL` имеют значения по умолчанию, поэтому их установка необязательна.

## Настройка PDF-отчетов

```
# Настройка заголовков и цветов
REPORT_TITLE="Отчет о проверке подписи"
DATA_STAMP_TITLE="Документ подписан"
STAMP_COLOR="#0066cc"

# Использование в REPORT_INFO_MESSAGE
REPORT_INFO_MESSAGE="© {COMPANY_NAME}\nСтраница {pageNumber} из {totalPages}\n{WEBSITE_URL}"

# Настройка TSP-сервиса
TSP_SERVICE_ADDRESS="http://your-tsp-server.com/tsp/tsp.srf"
```

**Описание переменных PDF-отчетов:**

- `REPORT_TITLE` - отображается в верхней части PDF-отчета как главный заголовок
- `DATA_STAMP_TITLE` - отображается в штампе на подписанном документе
- `STAMP_COLOR` - используется для цвета рамки и текста штампа (формат HEX: #RRGGBB)

**Описание переменных TSP-сервиса:**

- `TSP_SERVICE_ADDRESS` - используется для подключения к сервису штампов времени при создании расширенных подписей (CAdES-BES, CAdES-T, CAdES-C, CAdES-X-Long)

## С выравниванием текста

```
REPORT_INFO_MESSAGE="{align:center}© Цифровые технологии
{align:left}Страница {pageNumber} из {totalPages}
{align:right}www.cryptoarm.ru"
```

## С отступами и выравниванием

```
# Разделенные строки
REPORT_INFO_MESSAGE="{align:center}© Цифровые технологии
{left-margin:50}{align:left}© ООО Цифровые технологии
{right-margin:50}{align:right}Страница {pageNumber} из {totalPages}"

# Одна строка с разделителем ||
REPORT_INFO_MESSAGE="{left-margin:50}{align:left}© ООО Цифровые технологии || {right-margin:
50}{align:right}Страница {pageNumber} из {totalPages}"
```

**Примечание:** Директивы должны быть в начале строки. Для создания эффекта "текст слева, текст справа" используйте разделитель `||` в одной строке.

## С дополнительной информацией и выравниванием

```
# Дополнительные переменные окружения
VERSION="1.0.0"
```

```
BUILD_DATE="2024-01-01"

# Использование в REPORT_INFO_MESSAGE
REPORT_INFO_MESSAGE="{align:center}© {COMPANY_NAME}
{align:left}Страница {pageNumber} из {totalPages}
Версия: {VERSION} | Сборка: {BUILD_DATE}
{align:right}{WEBSITE_URL}"
```

# Приоритет замены

1. Специальные переменные (`pageNumber`, `totalPages`)
2. Переменные окружения
3. Если переменная не найдена, текст остается без изменений

# HTML-поддержка

Переменные поддерживаются внутри HTML-тегов:

```
REPORT_INFO_MESSAGE="© {COMPANY_NAME}
Страница {pageNumber} из {totalPages}
<a href='{WEBSITE_URL}'>Сайт компании</a>"
```

# Комбинирование выравнивания и HTML

Директивы выравнивания можно комбинировать с HTML-тегами:

```
REPORT_INFO_MESSAGE="{align:center}© {COMPANY_NAME}
{align:left}Страница {pageNumber} из {totalPages}
{align:right}<a href='{WEBSITE_URL}'>Сайт компании</a>"
```

# Комбинирование отступов, выравнивания и HTML

Все директивы можно комбинировать:

```
REPORT_INFO_MESSAGE="{align:center}© {COMPANY_NAME}
{left-margin:50}{align:left}© {COMPANY_NAME}
{right-margin:50}{align:right}Страница {pageNumber} из {totalPages}
{align:center}<a href='{WEBSITE_URL}'>Сайт компании</a>"
```

Открыть статью на сайте

# Введение в форматы и стандарты электронной подписи


- Обзор форматов PadES, CadES и XadES
- Стандарт и формат подписи CAdES
- Политика подписи
- Дополнительные данные проверки


## Обзор форматов PadES, CadES и XadES

### 1. Формат PAdES (PDF Advanced Electronic Signature)

**PAdES** - специализированный стандарт для электронного подписания PDF-документов, разработанный с учетом особенностей этого формата.

**Технические особенности**:

- Встраивание подписи непосредственно в структуру PDF-файла
- Сохранение всех свойств исходного документа после подписания

**Ключевые преимущества**:

- Совместимость - подписанные документы открываются в любом PDF-ридере без дополнительного ПО
- Многоуровневое подписание - возможность последовательного добавления подписей без потери предыдущих
- Визуализация - поддержка графического представления подписи (штамп, подпись, печать)
- Юридическая сила - соответствие требованиям ГОСТ Р и другим регуляторным нормам

**Ограничения применения**:

- Работает только с PDF-файлами
- Ограниченные возможности для сложных бизнес-процессов, требующих работы с разными типами файлов

### 2. Формат CAdES (CMS Advanced Electronic Signature)

**CAdES** - универсальный стандарт электронной подписи на основе криптографического синтаксиса сообщений (CMS).

**Особенности реализации**:

- Создание контейнера, который содержит:
  - Исходный документ в неизменном виде
  - Криптографические данные подписи
  - Метаданные и атрибуты подписания
- Поддержка различных уровней защиты (BES, EPES, T, C, X, A, LT)

**Области применения**:

- Офисные документы (Word, Excel)
- Графические файлы (JPG, PNG)
- Мультимедийный контент (MP3, MP4)
- PDF-документы
- Исполняемые файлы и архивы

**Основные недостатки**:

- Необходимость специального ПО для просмотра файлов
- Сложности при множественном подписании ("эффект матрешки")
- Отсутствие встроенной визуализации подписи в документе

## 3. Формат XAdES

**XAdES** (XML Advanced Electronic Signature (расширенная электронная подпись XML)) - стандарт для подписания XML-документов.

**XAdES** считывается как человеком, так и компьютером и используется для подписи электронных документов, таких как изображения (. jpeg, .png ), звуковые файлы .mp3 , двоичные данные (.exe ), PDF-файлы.

**Варианты реализации**:

1. Отделенная подпись:
   - Подпись хранится в отдельном файле
   - Исходный документ остается неизменным
2. Включенная подпись:
   - Подпись встраивается в XML-структуру документа
   - Создается единый файл, содержащий и данные, и подпись

**Преимущества**:

- Машинно-читаемый формат - удобен для автоматической обработки
- Поддержка множественных подписей - без эффекта матрешки

---

# Стандарт и формат подписи CAdES

Стандарт **CAdES** (CMS Advanced Electronic Signature) определяет **8 профилей**, обеспечивающих различные уровни защиты для подписанных данных в формате CMS. Эти профили гарантируют, что документы с электронной подписью остаются **действительными в течение длительного времени**.

Согласно спецификации **ETSI TS 101 733 V2.2.1 (2013-04)**, подписывающая сторона должна создавать подпись в одном из двух форматов:

- **CAdES-BES (Basic Electronic Signature)** – базовая электронная подпись.
- **CAdES-EPES (Explicit Policy Electronic Signature)** – подпись с явной политикой.

Подпись **CAdES-BES** включает:

1. Обязательные элементы:
    - **Подписанные данные** (документ или хеш документа).
    - **Обязательные подписанные атрибуты:**
    - `Тип контента (Content-Type)`
    - `Хеш сообщения (Message Digest)`
    - `Сертификат подписи ESS (ESSCertID) или ESS-v2`
2. Дополнительные подписанные атрибуты (опционально):
    - `Время подписания (Signing-Time)`
    - `Комментарии (Content-Hints)`
    - `Ссылки (Content-Reference)`
    - `Идентификатор (Content-Identifier)`
    - `Тип обязательства (Commitment-Type-Indication)`
    - `Местоположение подписавшего (Signer-Location)`
    - `Атрибуты подписчика (Signer-Attributes)`
    - `Штамп времени (Content-Time-Stamp)`
    - `Тип кодировки MIME (MIME-Type)`

Формат **CAdES-EPES** расширяет **CAdES-BES**, добавляя:

- **Атрибут** `sigPolicyID` – явное указание политики подписи (например, соответствие eIDAS, ГОСТ или корпоративным стандартам).
- **Дополнительные атрибуты проверки**, обеспечивающие соответствие нормативным требованиям.

# Политика подписи

Политики подписи, связанные с **CAdES**, могут использоваться для установления согласованности проверенных электронных подписей. Когда проверяющий использует комплексную политику подписи, указанную подписывающим или подразумеваемую подписанными данными, он получит согласованный результат при попытке проверки электронной подписи.

Однако, если подписывающий или подписанные данные не указывают, какая политика подписи была использована, или если политика подписи выглядит неполной, результаты, достигнутые проверяющими, могут быть непоследовательными. Рекомендуется, чтобы для поддержания согласованности и подписывающий, и проверяющий согласовали одну и ту же всеобъемлющую политику подписи.

# Дополнительные данные проверки

Дополнительные данные проверки могут быть добавлены в форматы **CAdES-BES** и **CAdES-EPES** для дальнейшей проверки электронной подписи. Эти данные собираются подписывающим лицом или проверяющим лицом, или обоими. Эти дополнительные данные включают:

- Сертификаты открытых ключей (PKC);
- Информация о статусе отзыва для отдельных PKC;
- Доверенная временная метка в дополнение к временной метке по умолчанию;
- Если применимо, информация о политике подписи, используемой для проверки электронной подписи.

В зависимости от выбранных выше проверочных данных при использовании форматов **CAdES-BES** или **CAdES-EPES** для создания электронной подписи применяются форматы **CAdES**:

## CAdES-T

**CAdES-T** – электронная подпись со временем. Этот формат применяется, когда доверенное время связано с электронной подписью либо путем добавления неподписанного атрибута временной метки, либо поставщик доверенных услуг предоставляет временную метку.

## CAdES-C

**CAdES-C** – электронная подпись с полными ссылками на данные проверки. Этот формат добавляет атрибуты `complete-certificate-references` и `complete-revocation-references` к **CAdES-T**.

## CAdES-C– расширенные форматы электронной подписи

Форматы этой категории расширяют проверку **CAdES-C**, добавляя неподписанные атрибуты к электронной подписи, которые используются, когда требуется проверка подписанного документа в течение очень длительного периода.

- **CAdES-X Long** – расширенная длинная электронная подпись. Эта опция добавляет атрибуты `certificate-values` и `revocation-values`, которые предоставляют информацию о сертификате и отзыве для проверки и средства предотвращения потери этой информации.
- **CAdES-X Type 1** – расширенная электронная подпись с типом времени 1. Эта опция добавляет атрибут временной метки, основанный на токене временной метки, созданном с помощью `CAdES-C`, и может защитить ключи от компрометации.
- **CAdES-X Type 2** — расширенная электронная подпись с типом времени 2. Этот параметр добавляет атрибут `CAdES-C-time-stamped-cert-crls-reference`, который предоставляет токен временной метки в отношении пути сертификации и информации об отзыве для защиты ключей от будущей компрометации.
- **CAdES-X Long Type 1** или **2** – расширенная электронная подпись со временем. Этот вариант объединяет `CAdES-X Long` либо с `CAdES-X Type 1`, либо с `CAdES-X Type 2`.

## CAdES-A

- **CAdES-A** – архивная электронная подпись. Форматы этой категории обеспечивают обратную совместимость и сохранение долгосрочной проверки подписи для архивных документов.
- **CAdES-A** – архивная электронная подпись с атрибутом `archive-time-stamp (ATSv2)`. Эта опция добавляет один или несколько атрибутов `archive-time-stamp` к **CAdES-X Long** или **CAdES-X Long Type 1** или **2**.
- **CAdES-A** – архивная электронная подпись с атрибутом archive-time-stamp (ATSv2). Может применяться к любой существующей CAdES подписи (включая BES, EPES, T, C, X, XL или даже другую CAdES-A).

> 🔍 Полное техническое описание расширенных электронных подписей CMS описано в документе ETSI TS 101 733 Электронная подпись и инфраструктура (ESI) – Расширенная электронная подпись CMS (CAdES).

Открыть статью на сайте

# Сервис проверки и улучшения электронных подписей


- О решении
- Практические сценарии использования
- Заключение


## О решении

**КриптоАРМ Server** и модуль **trusted-crypto** обеспечивают проверку и улучшение электронных подписей в серверных приложениях.

Решение предлагает два варианта использования:

- Разработка собственного веб-интерфейса с использованием SDK,
- Использование готового сервиса.

> 🚀 Готовый сервис: sign.kloud.one
> 📚 Документация SDK доступна на портале cryptoarm.ru

### Основные возможности

1. **Проверка электронных подписей**
    - Поддержка форматов PAdES и CAdES (CMS/PKCS#7, CAdES-T, CAdES-X Long Type 1, CAdES-A)
    - Проверка присоединённых и отделённых подписей
    - Верификация квалифицированных и неквалифицированных подписей
2. **Формирование отчетности**
    - Автоматическая генерация PDF-отчётов
    - Создание печатных форм с визуализацией подписи
    - Экспорт сертификатов подписантов
3. **Улучшение подписей**
    - Преобразование до CAdES-T (подпись со штампом времени)
    - Преобразование до CAdES-X Long Type 1 (долговременная подпись)
    - Преобразование до CAdES-A (архивная подпись)

# Практические сценарии использования

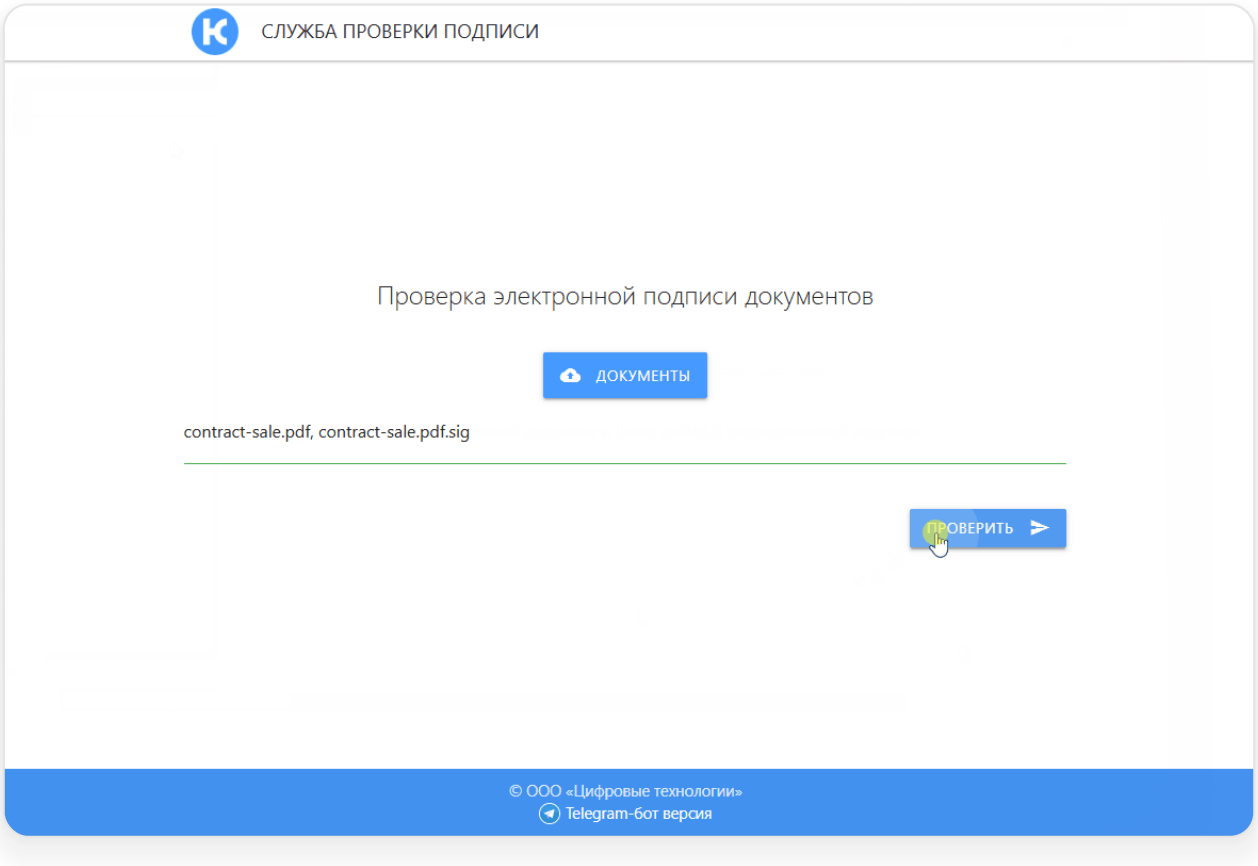
## 1. Проверка подписи документа

> 📚 Примеры запросов описаны в статье Автоматизация проверки электронной подписи с использованием КриптоАРМ Server.

Процесс проверки

1. Загрузка документа:
    - Для присоединенной подписи - сам документ
    - Для отделенной подписи - документ и файл подписи
2. Автоматический анализ:
    - Определение типа и формата подписи
    - Проверка целостности документа
    - Верификация сертификата
3. Формирование результатов:
    - Отображение статуса проверки (валидна/невалидна)
    - Вывод технических параметров подписи и сведений о сертификате

Демонстрация работы Sign.kloud.one




Статичный кадр демонстрации. Открыть анимацию

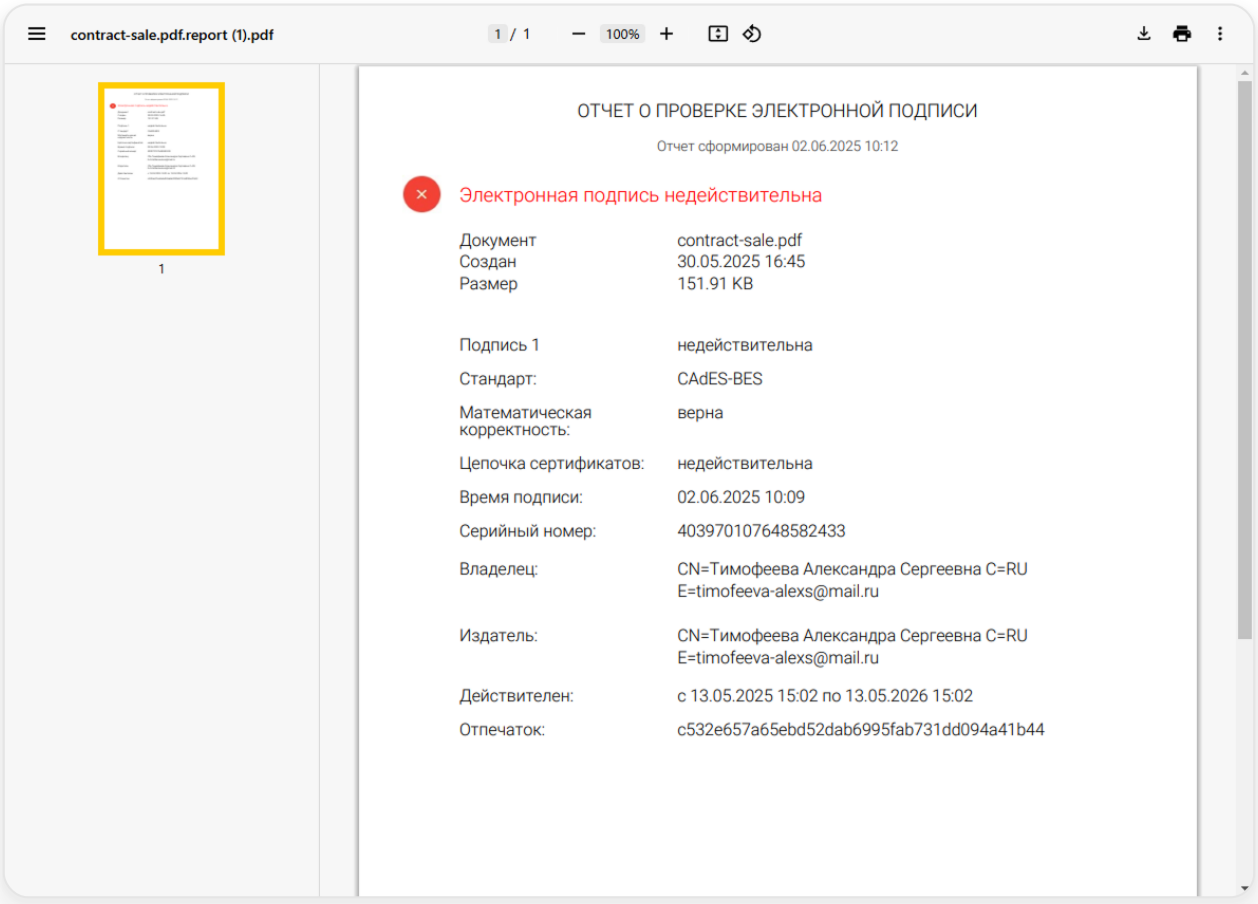
> 💡 При необходимости сертификат подписанта можно экспортировать для дальнейшего использования, например, для шифрования документов.

## 2. Создание отчета о проверке подписи

Решение автоматически формирует PDF-отчеты, содержащие:

- Технические параметры подписи
- Сведения о сертификате
- Результаты проверки цепочки доверия

Пример отчета

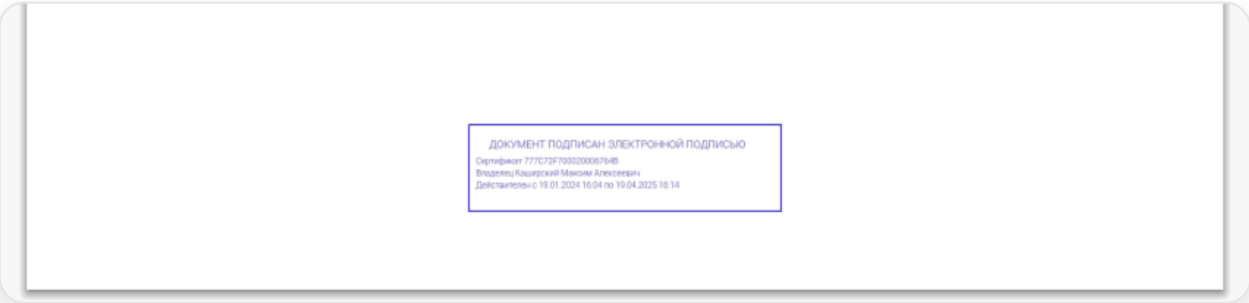



## 3. Создание печатной формы с визуальным штампом

**Печатная форма** - копия исходного документа с графическим штампом подписи. В такой копии присутствует только визуальное представление штампа, а сама электронная подпись отсутствует.

> 🚨 **Важно понимать!** Печатная форма предназначена для ознакомления, но не имеет юридической силы оригинала.
>
> 📌 **Ограничение**: В текущей версии поддерживается только для PDF-документов.

**Пример печатной формы**:




## 4. Улучшение подписи

**Улучшение подписи** — это процесс преобразования подписи в более защищенный и долговременный формат, например, CAdES-T, CAdES-X Long Type 1 или CAdES-A.

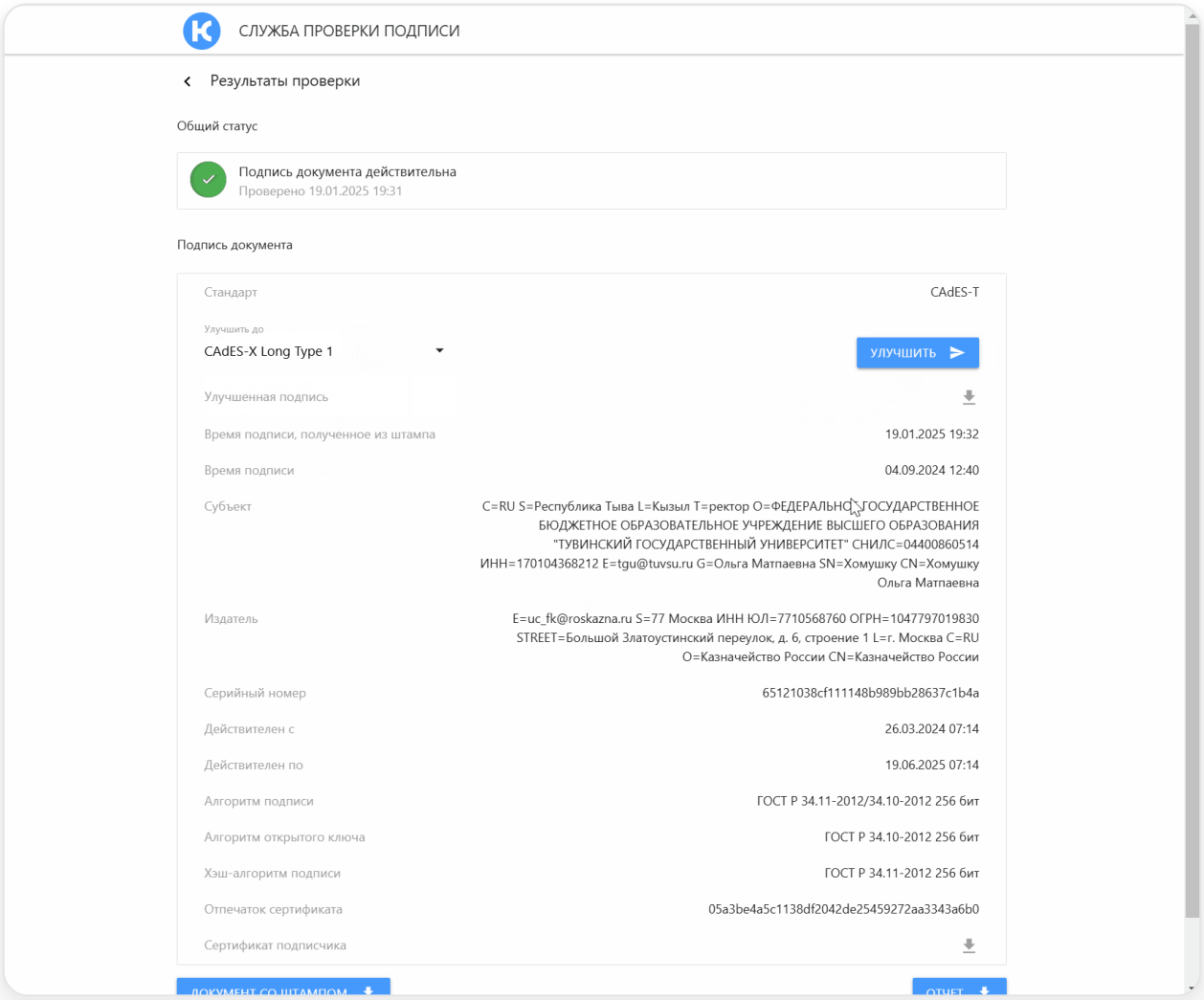
Улучшение подписи до более продвинутых форматов дает следующие преимущества:

- до **CAdES-T** (Подпись со штампом времени). Фиксируется момент подписания документа с привязкой к доверенному источнику времени.
- до **CAdES-X Long Type 1** (Долговременная подпись). Обеспечивает проверяемость подписи на протяжении 10 лет и более. Включает штамп времени, OCSP-штамп, подтверждающий действительность сертификата на момент подписи, и полную цепочку доверия.
- до **CAdES-A** (Архивная подпись). Разработана для долговременного хранения документов. Содержит специальные атрибуты, которые придают юридическую силу подписи на срок более 15 лет. Предусматривает добавление новых архивных меток в процессе хранения.

Процесс улучшения

1. Выбор целевого формата.
2. Добавление необходимых атрибутов:
    - Метки времени
    - Данные о статусе сертификата
    - Архивные атрибуты
3. Сохранение улучшенного документа

Демонстрация работы Sign.kloud.one




Статичный кадр демонстрации. Открыть анимацию

---

# Заключение

Сервис на базе **КриптоАРМ Server** предлагает комплексное решение для:

- Юридически значимой верификации подписей
- Документирования процесса проверки
- Долговременного сохранения юридической силы документов

Это решение особенно актуально для:

- Финансовых организаций
- Государственных учреждений
- Организаций с большим объемом документооборота
- Юридических служб и архивов

Открыть статью на сайте

# Telegram-бот для проверки электронной подписи


- О решении
- Описание использования
- Интерфейс @SignKloudOne_bot

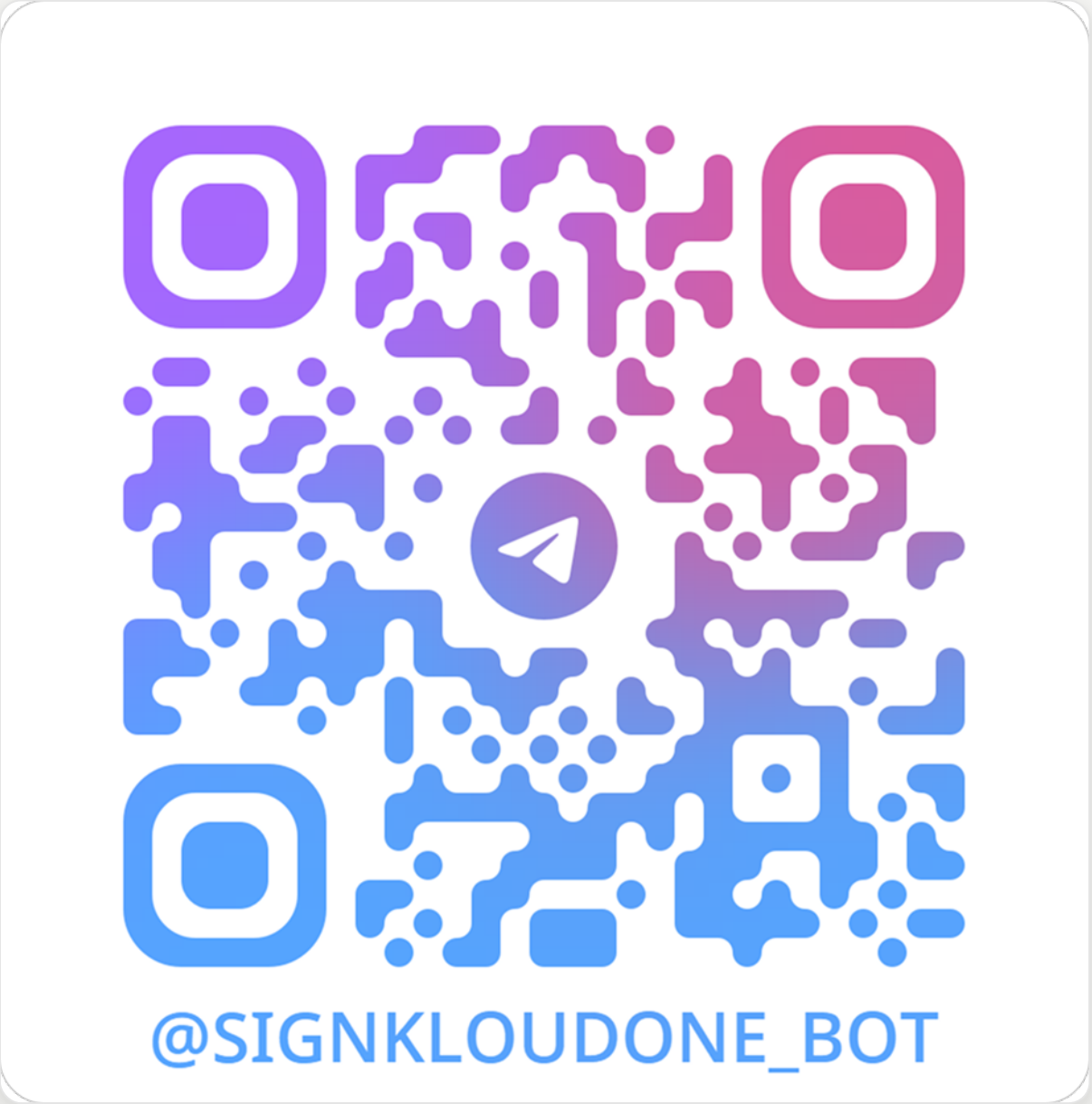

## О решении

**Telegram-бот с интеграцией КриптоАРМ Server** — это современное решение для автоматизированной проверки электронных подписей прямо в мессенджере.

### Как это работает?

Вы создаете собственного Telegram-бота и подключаете его к КриптоАРМ Server, получая мощный инструмент для проверки ЭП без сложных интерфейсов.

> 🚀 Пример готового решения: **@SignKloudOne_bot**




## Основные возможности решения

1. **Проверка электронных подписей**
    - Проверка электронных подписей в форматах PAdES и CAdES
    - Поддержка CMS (PKCS#7), CAdES-T, CAdES-X Long Type 1, CAdES-A
    - Проверка как присоединенных, так и отделенных подписей
    - Проверка квалифицированных и неквалифицированных подписей
2. **Формирование отчетности**
    - Создание отчетов о проверке в PDF-формате
    - Создание печатных форм с визуальным отображением подписи

> 📌 Для работы требуется интернет-подключение к сервису проверки.

---

# Описание использования

1. Начало работы:
   - Найдите бота в Telegram через поиск и запустите его.
   - Нажмите кнопку **СТАРТ**, чтобы активировать.
2. Отправка документов:
   - Если подпись отделенная, то отправьте два файла: исходный документ и файл подписи.
   - Если подпись прикрепленная, загрузите файл с расширением `.sig`, `.sgn`, `.p7s`.
   - Если подпись встроенная (формат PAdES), загрузите PDF-документ.

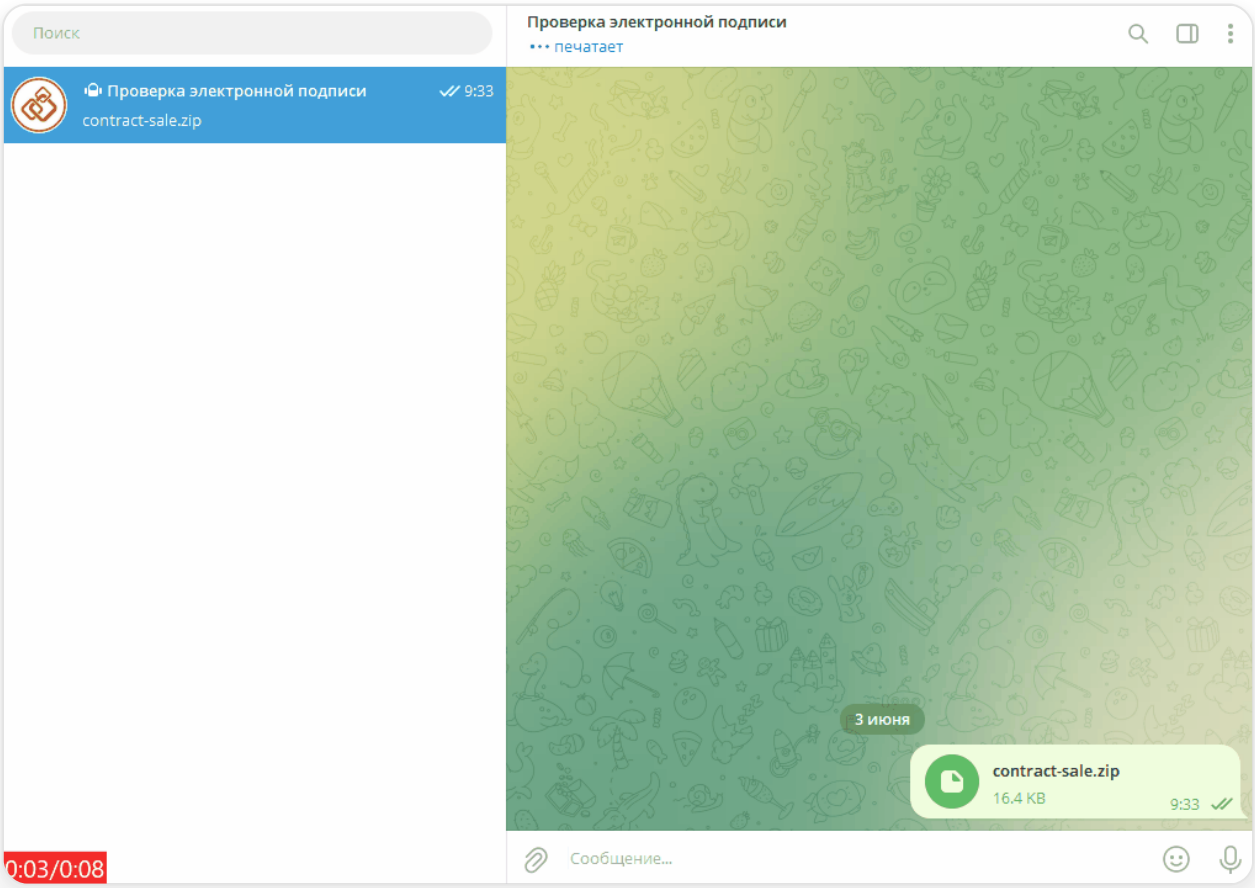
   > 💡**Альтернативный способ**: Можно загрузить в бот zip-архив, содержащий исходный документ и файл подписи.
3. Получение результатов:

   КриптоАРМ Server автоматически проверит:

   - Действительность сертификата ЭП, отозван он либо нет.
   - Соответствие подписи документу, не были ли изменения после подписания.
   - Наличие и валидность штампов времени (для CAdES-T, CAdES-A).

---

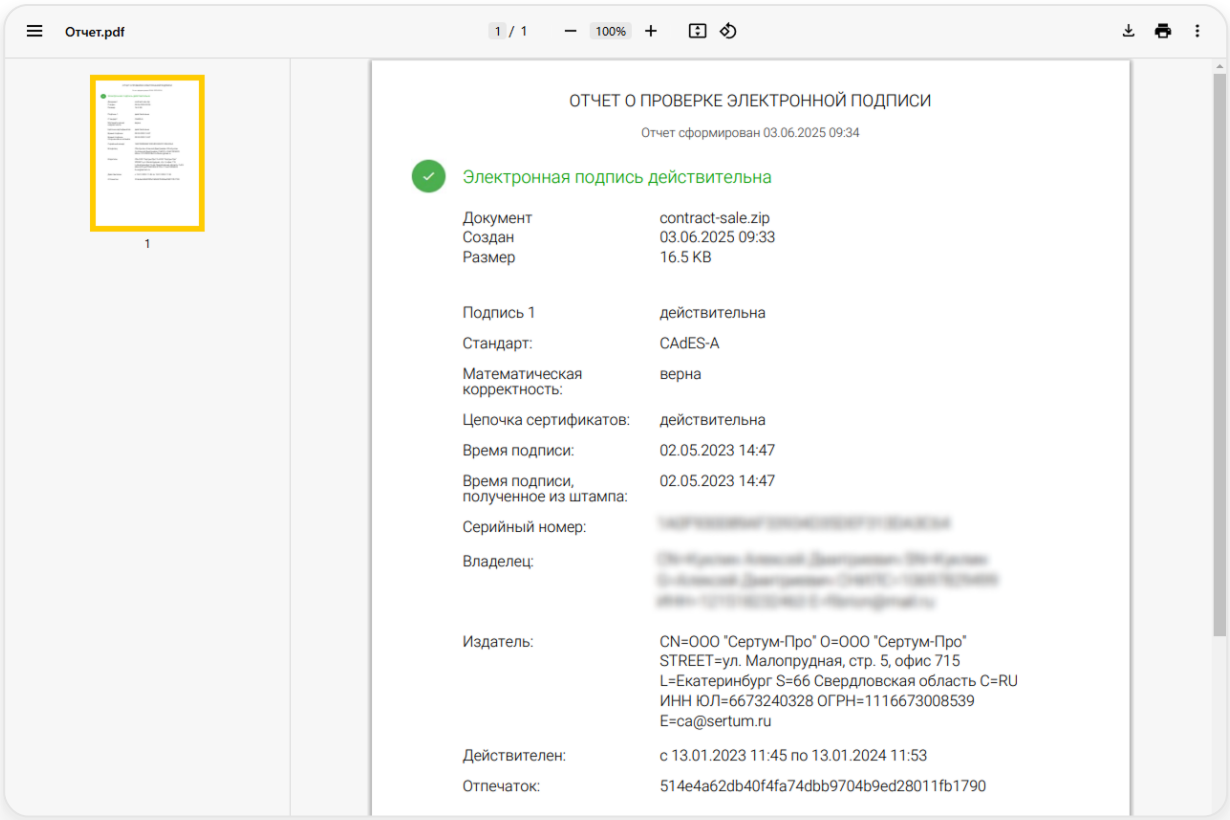
# Интерфейс @SignKloudOne_bot



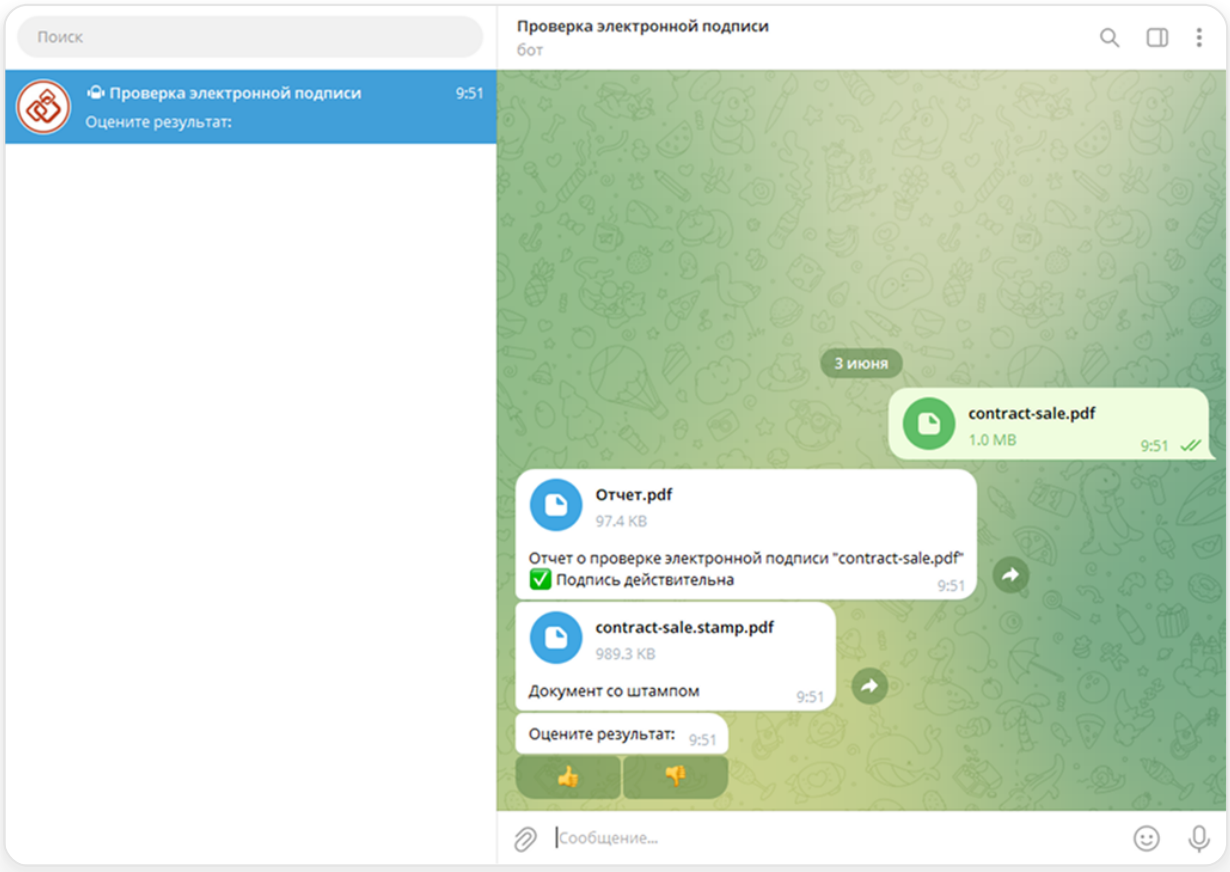

Статичный кадр демонстрации. Открыть анимацию

## Результаты проверки в @SignKloudOne_bot

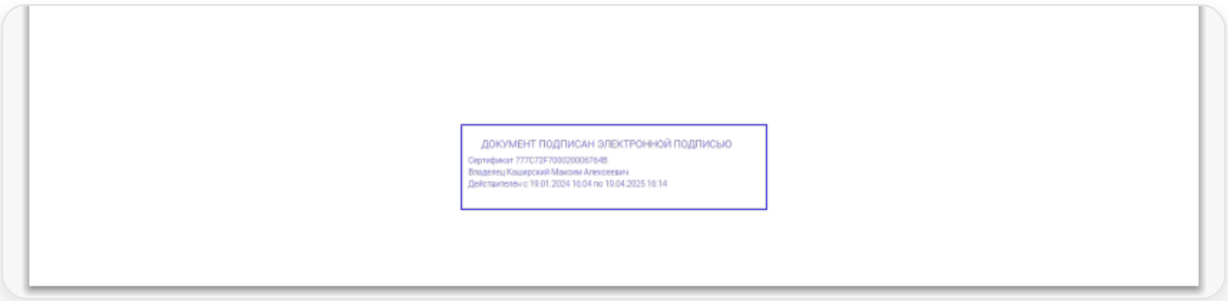
1. Общий статус подписи:
    - ✅ Подпись действительна
    - ❌ Подпись недействительна
2. PDF-отчет с детализацией




3. Для PDF-документов создается печатная форма с визуальным отображением подписи:



Пример визуализации:



Открыть статью на сайте

# Сервис для настройки рабочего места


- О решении
- Описание использования


## О решении

С помощью **КриптоАРМ Server** можно реализовать сервис для проверки рабочего места. Это проверка позволяет убедиться, что рабочее место пользователя готово для работы с электронной подписью.

Решение предлагает два варианта использования:

- Разработка собственного веб-интерфейса с использованием SDK
- Использование готового сервиса

> 🚀 Готовый сервис: sign.kloud.one

### Основные возможности

Доступно выполнение проверок **в разрезе юрисдикции**:

**Российская Федерация (63-ФЗ «Об электронной подписи», ГОСТ)**:

1. Проверка установки и версий **КриптоАРМ** и **КриптоПро CSP**.
2. Проверка действующих лицензий **КриптоАРМ** и **КриптоПро CSP**.
3. Проверка наличия личного сертификата с алгоритмом ГОСТ
4. Предоставление ссылки на скачивание дистрибутива **КриптоАРМ**.
5. Поддержка авторизации через Trusted.ID для журналирования загрузок.

**Открытая криптография (RSA/ECDSA, DES/AES)**:

1. Проверка установки и версии **КриптоАРМ**.
2. Проверка действующей лицензии **КриптоАРМ**.
3. Проверка наличия личного сертификата с алгоритмом **RSA/ECDSA**.45. Предоставление ссылки на скачивание дистрибутива **КриптоАРМ**.
4. Поддержка авторизации через Trusted.ID для журналирования загрузок.

## Описание использования

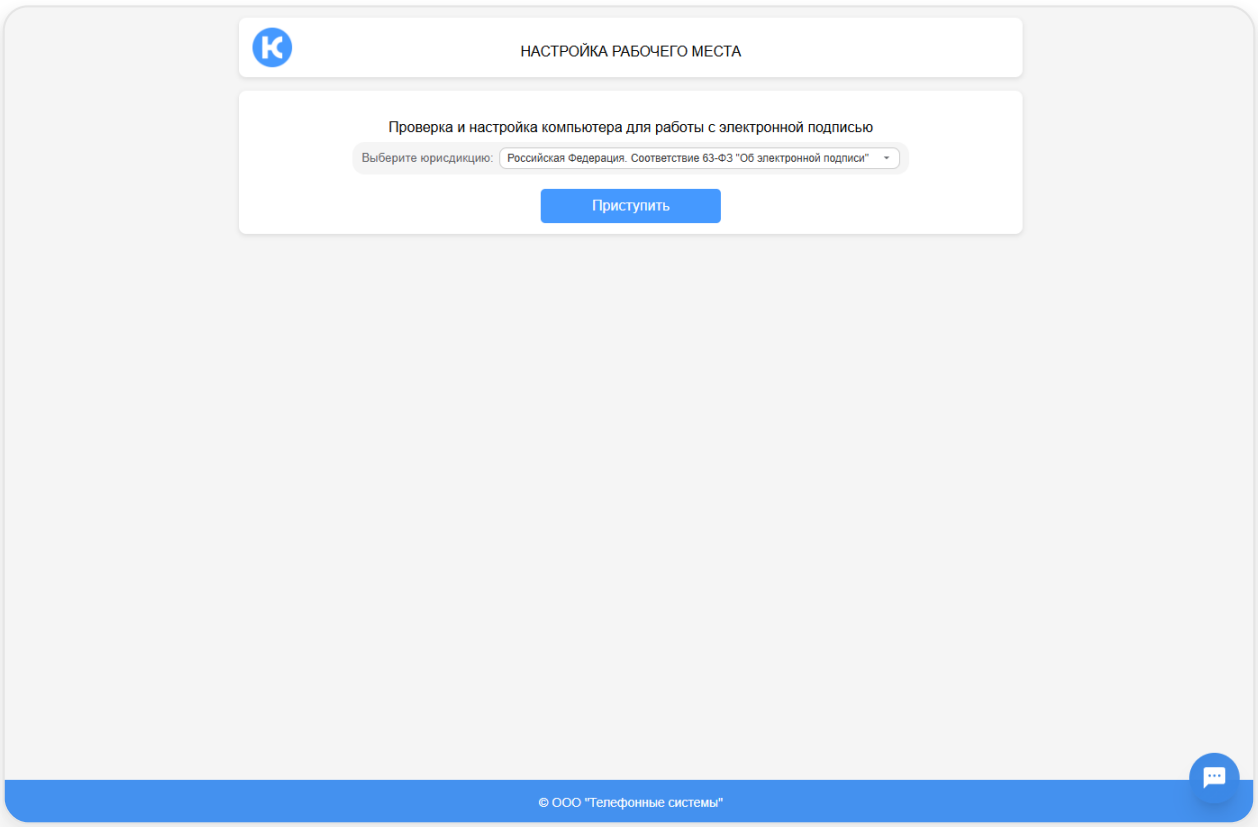
1. Запустите проверку рабочего места.

> 💡 Для проведения проверки требуется установленное приложение КриптоАРМ. В случае его отсутствия, сервис предложит его скачивание.

2. Предоставьте разрешение на открытие приложения в окне браузера.
3. Подтвердите запуск диагностики в окне приложение КриптоАРМ.
4. Дождитесь окончания проверки.

---

# Демонстрация работы Sign.kloud.one




В результате проверки сервис Sign.kloud.one отображает:

1. Общий статус:
   - ✅ Ваше рабочее место может быть использовано для формирования и проверки электронной подписи.
   - ❌ Необходимо установить недостающие компоненты.
2. Статус по каждому из проверяемых компонентов.