**Информационная система «KbsCrypt»\***

Инструкция администратора

Версия 1.0

АО «Социальная Карта»

2025 г.

**АННОТАЦИЯ**

Настоящий документ является руководством администратора по работе с Системой «KbsCrypt» (далее по тексту – Система), которая включает в себя следующие модули, которые могут функционировать как совместно, так и по отдельности:

* + модуль «KbsСrypt.Сlient» – модуль предназначен для отправки запроса и верификации ответа в целевую систему по защищенному КС1 каналу связи;
  + модуль «KbsCrypt.Server» – модуль обеспечивает верификацию полученных запросов на наличие корректной открепленной подписи;
  + модуль «KbsCrypt.Android» – модуль предназначен для отправки запроса и верификации ответа в целевую систему по защищенному КС1 каналу связи.

В данном руководстве приводится следующая информация:

* + Общие сведения о Системе;
  + Требования к администратору Системы;
  + Инструкции для администраторов по выпуску и установке сертификата;

Оглавление

[1.Область применения 4](#__RefHeading___83)

[2.Краткое описание возможностей 4](#__RefHeading___91)

[3.Требования к уровню подготовки администратора Системы 4](#__RefHeading___85)

[4.Выпуск сертификата 6](#__RefHeading___86)

[5. Установка сертификата 7](#__RefHeading___87)

[6.Обработка ошибок с подписью и сертификатом 8](#__RefHeading___88)

[7.Термины и определения 10](#__RefHeading___89)

# 1.Область применения

Автоматизированная система «KBSCrypt» включает в себя:

* + Создание защищаемой информации;
  + Обработка защищаемой информации;
  + Передача защищаемой информации с указанием используемых протоколов и их версий;
  + Отправка запроса в Stunnel для добавления шифрования, в случае если требуется ГОСТ TLS.

# 2.Краткое описание возможностей

Система предоставляет следующие возможности локальным сервисам и целевым сервисам:

* + Подписание входящего запроса;
  + Проверка подписи;
  + Отправка проверенного запроса;

Сценарии возможного применения:

* + Создание регистрационной ссылки;
  + Проверка работоспособности определенных сервисов и модулей;
  + Получение доступных типов биометрии, то есть позволяет проверить вектора какого класса биометрии есть в КБС у клиента;
  + Передача фото для последующей идентификации;
  + Передача фото для последующего создания платежа.

# 3.Требования к уровню подготовки администратора Системы

Администратору Системы не предъявляется дополнительных требований к уровню подготовки.

Знания следующих инструментов являются преимуществом, но не являются обязательными:

* + Visual Studio Code
  + JSON
  + Helm charts
  + Yaml
  + PSQL или DBeawer
  + Astra Linux;
  + Ubuntu.

В перечень задач, выполняемых администратором Системы, должны входить:

* + задача поддержания работоспособности технических средств;
  + задача установки (инсталляции) и поддержания работоспособности системных программных средств - операционной системы;
  + задача установки (инсталляции) и поддержания работоспособности «KbsCrypt».

# 4.Выпуск сертификата

В рамках тестирования ПО «KbsCrypt» возможно использование тестового удостоверяющего центра. Для промышленной среды рекомендуется использование стандартного сертификата.

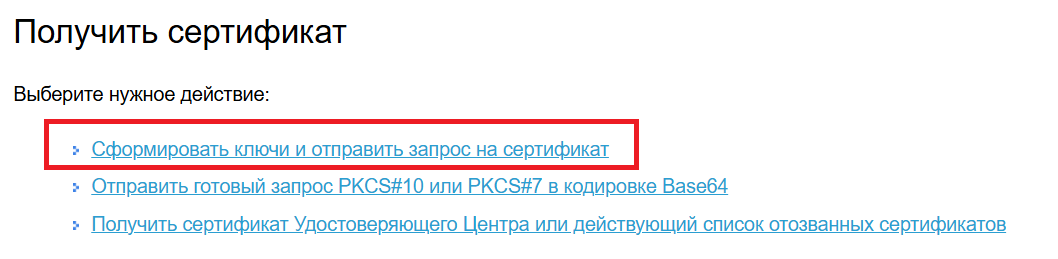
Выпуск сертификатов происходит с помощью тестового удостоверяющего центра.

Перед выпуском сертификата необходимо:

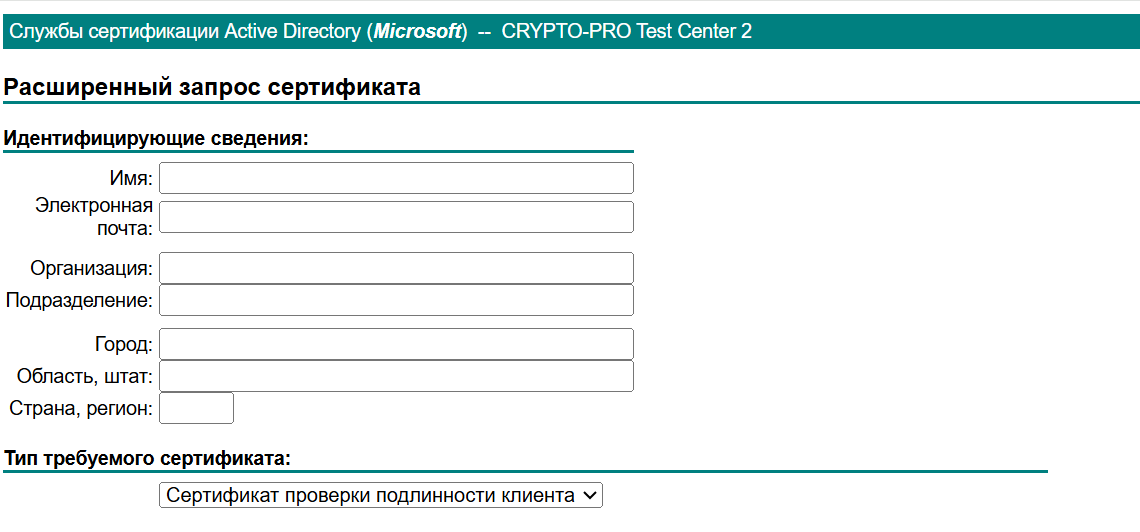
* установить КриптоПро ЭЦП Browser plug-in перейдя по [ссылке](https://www.cryptopro.ru/products/cades/plugin) выбрав соответствующую операционную систему;
* для проверки подписи тестового центра сертификации необходим криптопровайдер с поддержкой алгоритмов ГОСТ - КриптоПро CSP или аналогичный. Криптопровайдер можно загрузить по [ссылке](https://cryptopro.ru/user/?destination=node/148).

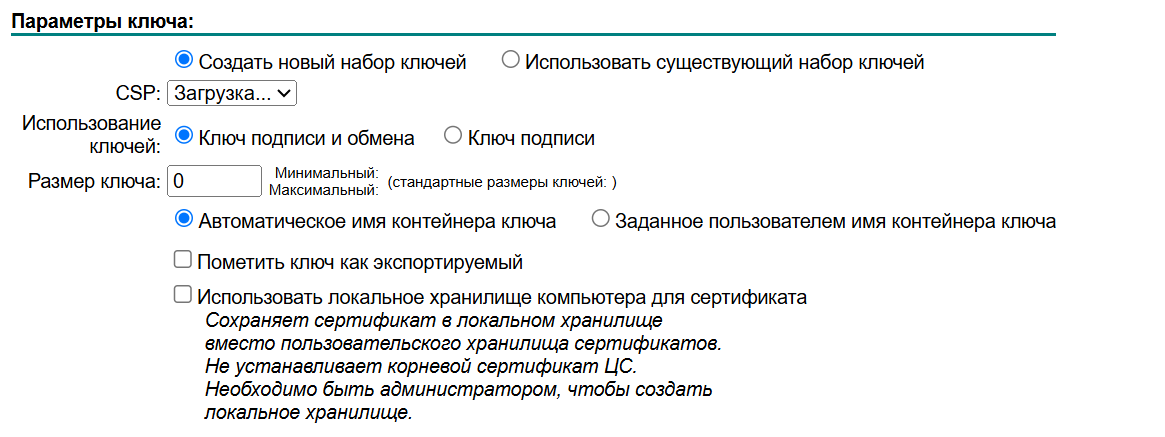
После установки КриптоПро ЭЦП Browser plug-in и КриптоПро CSP перейдите к выпуску сертификата.

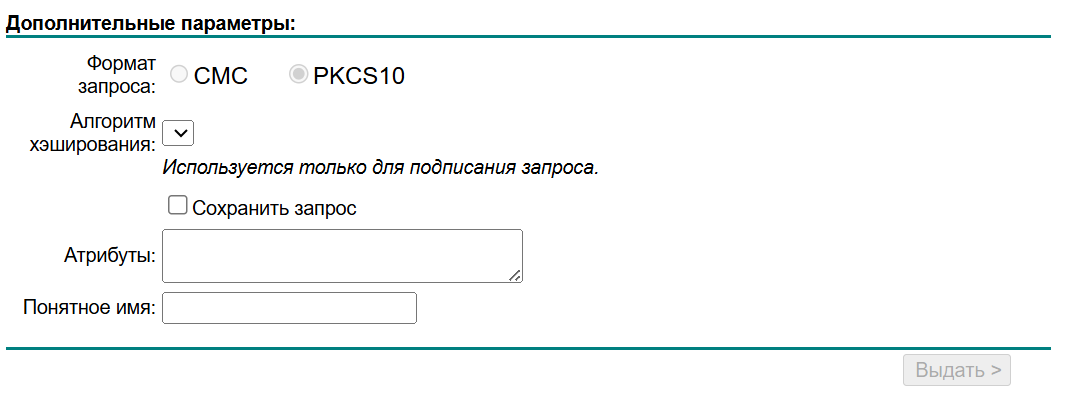
Для старта процесса выпуска необходимо перейти на сайт [тестового удостоверяющего центра.](https://testgost2012.cryptopro.ru/certsrv/) Далее необходимо перейти на «Сформировать ключи и отправить запрос на сертификат»:



Необходимо заполнить форму «[Расширенный запрос сертификата](https://testgost2012.cryptopro.ru/certsrv/certrqma.asp)» указав все необходимые необходимые данные







После выпуска сертификата необходимо скачать корневой сертификат центра сертификации по [ссылке.](https://testgost2012.cryptopro.ru/certsrv/certcarc.asp)

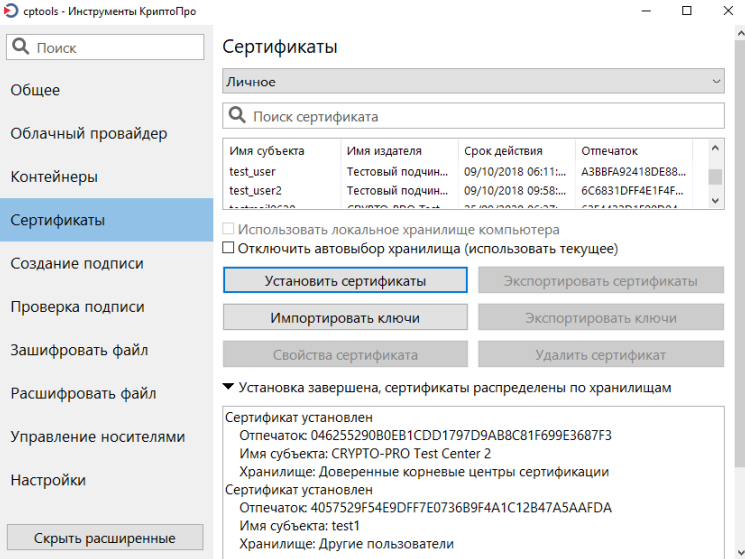
# 5. Установка сертификата

После выпуска сертификата необходимо установить его в соответствующее хранилище сертификатов.

Чтобы установить сертификат из файла в хранилище:

* нажмите кнопку Установить сертификат;
* в открывшемся окне выберите файл сертификата для установки.

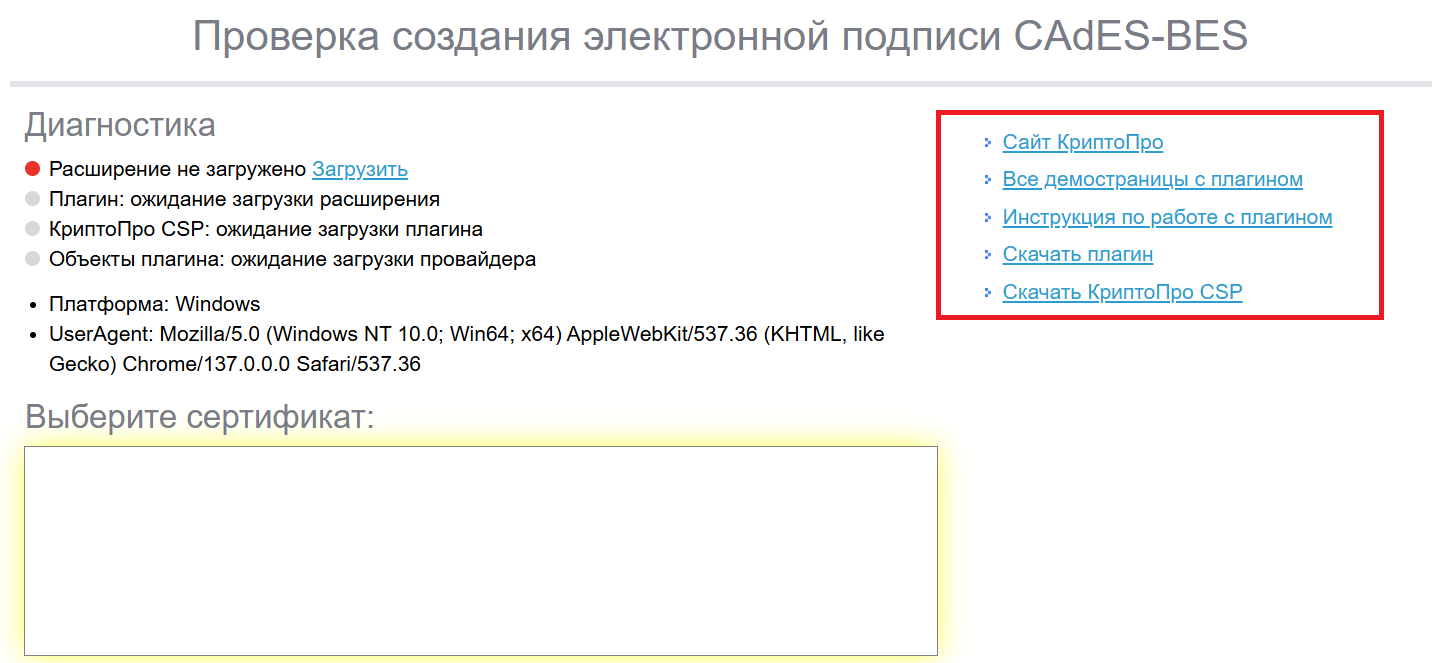
В случае успешного выполнения операции перечень установленных сертификатов в соответствующих хранилищах можно развернуть по кнопке с сообщением об успешной установке внизу окна



# 6.Обработка ошибок с подписью и сертификатом

В процессе работы с подписью и сертификатом самыми распространенными ошибками является то, что сроки действия подписи и сертификата истекли. Для проверки и подписания используется КриптоПро [https://www.justsign.me/verifyqca/#/signature.](https://www.justsign.me/verifyqca/#/signature)

Для просмотра расширенной информации можно перейти на сайт <https://www.cryptopro.ru/sites/default/files/products/cades/demopage/cades_bes_sample.html> и при возникновении ошибок перейти в соответствующие разделы с информацией в правом верхнем углу.



# 7.Термины и определения

Термины, сокращения и определения, используемые в инструкции для администратор ПО «KbsCrypt»:

* ГОСТ TLS - протокол TLS (Transport Layer Security), который использует российские криптографические алгоритмы, стандартизированные в ГОСТ (Государственных стандартах).
* TLS (Transport Layer Security) - это криптографический протокол, который обеспечивает безопасную передачу данных между двумя взаимодействующими приложениями, например, между вашим браузером и веб-сервером.
* Закрытый ключ (контейнер закрытого ключа) - это защищенное хранилище, в котором находится закрытый ключ электронной подписи.
* Корневой сертификат - это электронный документ, которым центры сертификации подписывают SSL-сертификаты при выдаче;
* SSL-сертификат - это цифровой документ, который подтверждает подлинность веб-сайта и обеспечивает безопасное соединение между сервером и браузером пользователя. Он шифрует данные, передаваемые между ними, предотвращая несанкционированный доступ к информации. Аббревиатура SSL расшифровывается как Secure Sockets Layer, или уровень защищенных сокетов.
* КриптоПро – комплекс программных инструментов для обеспечения информационной безопасности, разработанных в одноимённой компании.
* КриптоПро CSP (Cryptography Service Provider) – это конкретный продукт, криптопровайдер, который обеспечивает безопасность и целостность при работе с электронными документами и другими данными. Он необходим для работы с усиленной квалифицированной электронной подписью (КЭП), обеспечивая ее юридическую значимость.
* Сертификат подписи (Сертификат ключа проверки электронной подписи)- цифровой документ, который подтверждает принадлежность электронной подписи конкретному лицу или организации.