

Инструкция по генерации ключей системы ДБО Corporate (для клиентов, перешедших из ДБО «Урал ФД»)

Оглавление

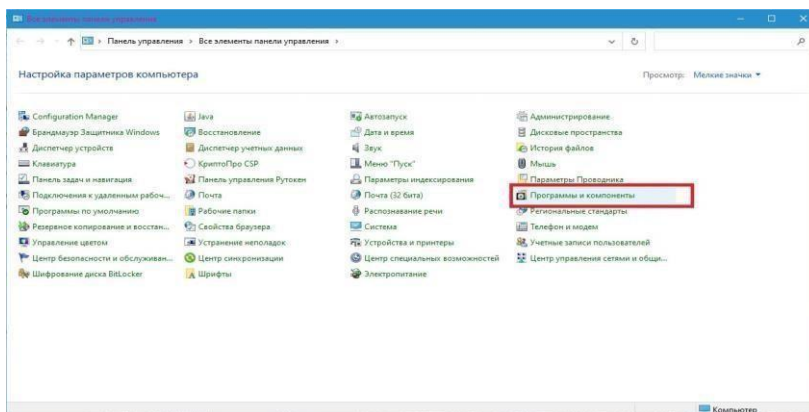
1. Запрос на новый сертификат в ДБО Corporate 1
2. Установка плагина 4
3. Установка КриптоПро CSP 5

После успешной генерации ЭЦП вам необходимо передать в банк Акт признания открытого ключа ЭП (Сертификата) для обмена сообщениями. Банк активирует ЭЦП только после получения Акта признания открытого ключа.

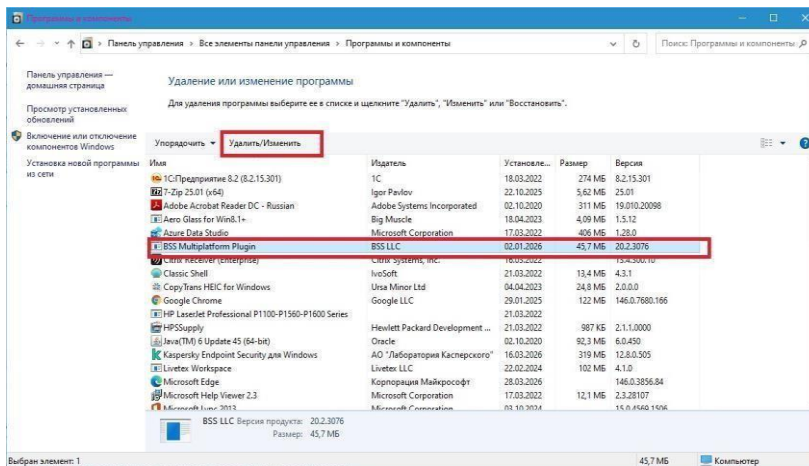
1. Запрос на новый сертификат в ДБО Corporate

Перед тем, как начать работу в ДБО, необходимо пройти процедуру начальной генерации электронно-цифровой подписи (далее – ЭЦП).

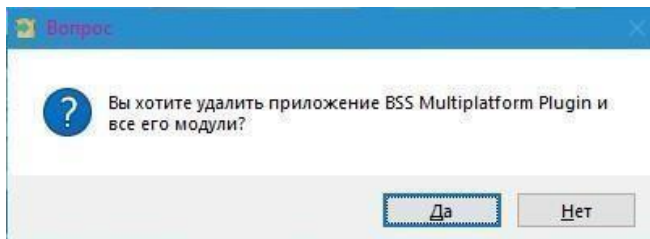
Для этого необходимо удалить старый плагин с компьютера. Чтобы это сделать нажмите «Пуск → Панель управления → Программы и компоненты».



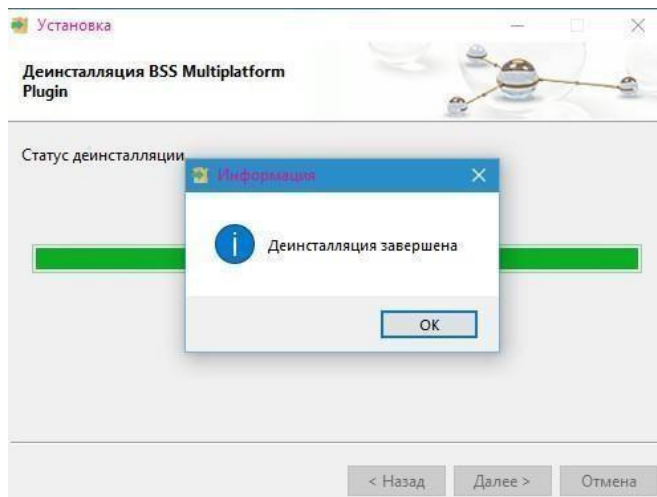
Выберите плагин для старого ДБО, он называется BSS Multiplatform Plugin и нажмите «Удалить / Изменить».



Затем нажмите согласиться, нажав на кнопку «Да».

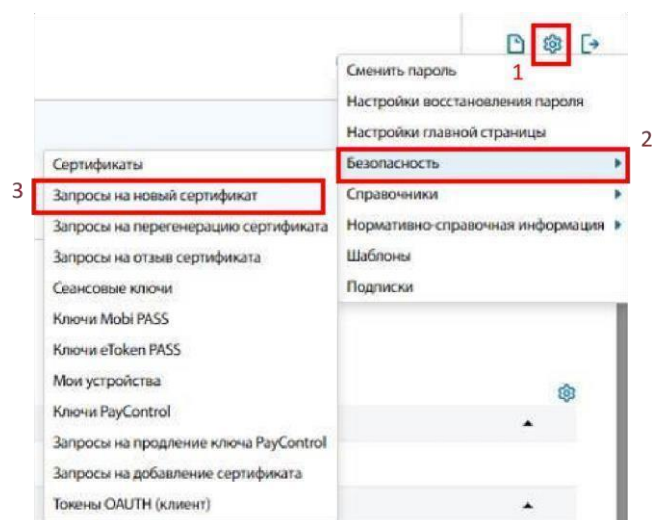


После окончания нажмите «ОК».



Далее перейдите в новое ДБО по ссылке <https://dbo.bankdom.ru> введите логин / пароль для входа в ДБО.

Перейдите в раздел «Настройки», для этого необходимо нажать на  в правом верхнем углу и перейти в раздел «Безопасность → Запросы на новый сертификат».



Чтобы создать новый запрос на выпуск сертификата, необходимо в открывшемся окне нажать на кнопку «Создать».



Далее необходимо заполнить, открывшуюся экранную форму запроса на новый сертификат:

- Выбрать уполномоченное лицо из списка, если их несколько у компании;
- Выбрать из выпадающего списка средство подписи: КристоПРО;
- В поле Подразделение обязательно указать название подразделения, где работает уполномоченное лицо, например, бухгалтерия;
- В поле Адрес электронной почты обязательно указать адрес электронной почты;
- Проверить все предзаполненные поля и при необходимости внести изменения.

Запрос на новый сертификат

Номер: 27 Дата: 25.02.2026

Уполномоченное лицо клиента: Жукова Мария Витальевна

Средство подписи: Жукова Мария Витальевна I ООО, КристоПро

Полное имя (CN): Жукова Мария Витальевна

Фамилия (SN): Жукова Имя Отчество (G): Мария Витальевна

Должность (TITLE): Генеральный директор

Адрес электронной почты (E): ooo@test.ru

Город (L): Пермь Наименование субъекта (ST): Пермский край Страна (C): RU

Адрес (Street): Ленина, д.60

Организация (O): ООО "Ромашка"

ИНН (INN): СНИЛС (SNILS): ОГРН (OGRN): ОГРНИП (OGRNIP):

ИНН (INNLE): 0000000000

Подразделение (OU): тест

Кем создан: Клиент

Сообщение из банка:

Сохранить Выгрузить запрос

Важно!

- В случае заполнения заявки под ОПФ ООО / АО, то ИНН необходимо указать в поле ИНН (INNLE):
- Для ИП в поле ИНН (INN):

Организация (O): ООО/АО

ИНН (INN): СНИЛС (SNILS): ОГРН (OGRN): ОГРНИП (OGRNIP):

ИНН (INNLE): 1234567891

Организация (O): ИП

ИНН (INN): 123456789101 СНИЛС (SNILS): ОГРН (OGRN): ОГРНИП (OGRNIP):

Вставьте ваш ключ Рутокен в порт USB, световой индикатор на устройстве должен загореться. Нажмите «Сохранить».

После чего откроется форма для выбора ключевого носителя, необходимо выбрать Рутокен ECP и нажать «ОК».

Выбор ключевого носителя - КристоПро CSP

Выберите носитель для создания контейнера Ir-019c985a-f0a4-1920-beda-1d275729faa6

Реестр
Директория
Rutoken ECP
Недоступные для данной операции
Облачный токен

Режим работы: CSP (rutoken_ecp_068f01e2)

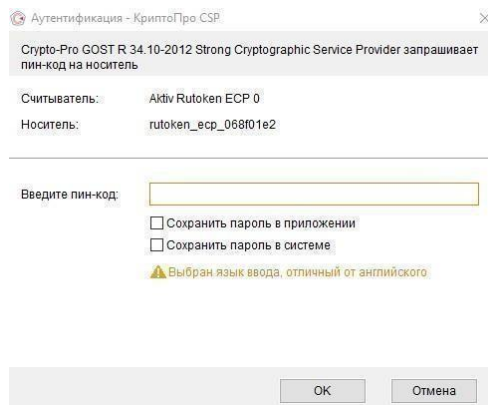
Описание: Хранилище закрытых ключей. Обеспечивает самый высокий уровень производительности.

ОК Отмена

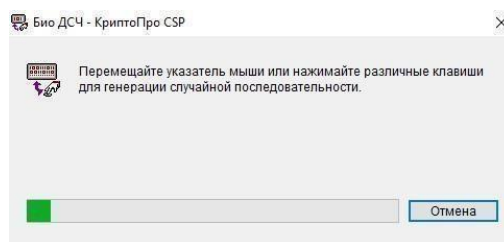
Важно!

В случае, если у вас отражается Рутокен ФКС, то необходимо выбрать «Режим работы CSP».

Далее потребуются ввести ранее установленный пин-код для Рутокен и нажать «ОК».



Перемещайте указатель мыши или нажимайте различные клавиши для генерации случайной последовательности.



Запрос на сертификат отобразится в статусе «Создан». Его необходимо выбрать и нажать «Отправить», после чего статус изменится на «Принят».

Важно!

В течение дня банк обработает запрос и при повторной авторизации в ДБО отобразится уведомление и статус самого запроса измениться на «Ожидание акта»:

Информация

Сертификат издан банком. Вам необходимо распечатать Акт признания ключа, заверить его и передать по месту заключения договора.



Это значит, что сейчас необходимо отправить в банк акт признания открытого ключа ЭП (Сертификата) для обмена сообщениями. Для этого нужно нажать на кнопку «Распечатать акт» и предоставить его любым удобным способом в банк:

- Подпишите с помощью УКЭП, направьте по системе ЭДО (например, Диадок, Тензор и другие) или в формате архива через ДБО;
- Подпишите собственноручной подписью и передайте оригинал в любой офис банка.

После получения подписанного акта признания открытого ключа ЭП (Сертификата) для обмена сообщениями банк активирует сертификат. После чего статус запроса изменится с «Принят» на «Исполнен». Это означает, что вы успешно сгенерировали ключи и банк ввел их в эксплуатацию. Теперь вы можете начать работу с системой ДБО Corporate.

2. Установка плагина

В случае, если у вас не установлен плагин, то при попытке отправить запрос на новый сертификат, система отобразит информационное уведомление: Плагин для работы с электронными подписями не обнаружен. Скачать его? Нажмите «ДА», для скачивания и «НЕТ» после запуска плагина, если он скачен, но не запущен.

Установка плагина



Плагин для работы с электронными подписями не обнаружен. Скачать его?
Нажмите Да для скачивания и Нет после запуска плагина, если он установлен, но не запущен.

Да

Нет

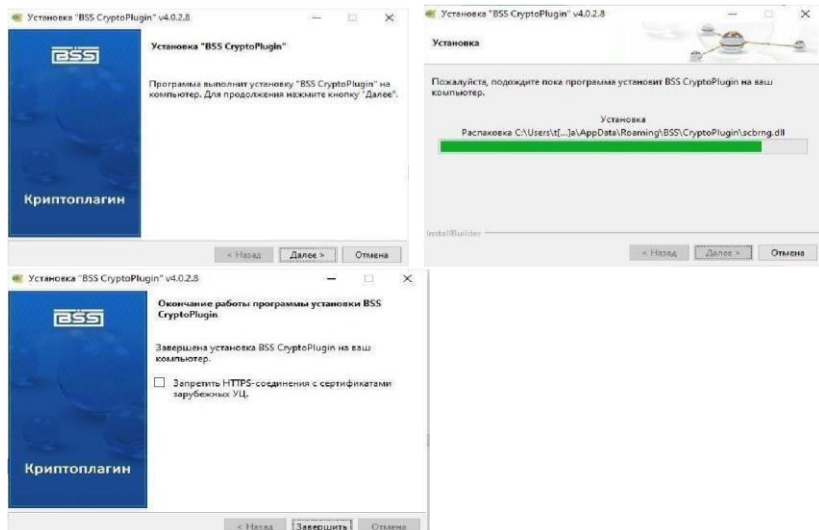
Отмена

Внимание

Работа с ЭП будет возможна только после установки плагина

ОК

После скачивания плагина, его необходимо установить, нажав на кнопку «Далее».



3. Установка КриптоПро CSP

Для работы с Рутокен на вашем компьютере должна быть установлена программа КриптоПро CSP. В случае если у вас отобразится ошибка: Алгоритм генерации сертификата устарел, это означает что КриптоПро CSP не установлен.

Чтобы установить КриптоПро CSP необходимо скачать его с официального сайта, перейдя по ссылке: <https://cryptopro.ru/products/csp>

Алгоритм генерации сертификата устарел

Вы используете алгоритм ГОСТ Р 34.10-2001. С 31.12.2017 стало невозможным создание сертификата по данному алгоритму.

ОК

КриптоПро CSP

Главная > Продукты



Ключа на сервере)

КриптоПро CSP 5.0 — новое поколение криптопровайдера, развивающее три основные продуктовые линейки компании КриптоПро: КриптоПро CSP (классические токены и другие пассивные хранилища секретных ключей), КриптоПро ФКН CSP/Рутокен CSP (неизвлекаемые ключи на токенах с защищенным обменом сообщениями) и КриптоПро Ключ (распределенное хранение ключа: часть ключа на клиенте, часть ключа на сервере).

Все преимущества продуктов этих линеек не только сохраняются, но и приумножаются в КриптоПро CSP 5.0: шире список поддерживаемых платформ и алгоритмов, выше быстродействие, удобнее пользовательский интерфейс. Но главное — работа со всеми способами хранения ключей, включая распределенный, теперь единообразна. Для перевода прикладной системы, в которой работал КриптоПро CSP любой из версий, на поддержку распределенного хранения или на новые носители с неизвлекаемыми ключами, не потребуется какая-либо переработка ПО — интерфейс доступа остается единым.

Скачать КриптоПро CSP

с ознакомительной полнофункциональной 90-дневной лицензией

Купить лицензию

После того, как КриптоПро CSP был успешно установлен, необходимо будет заново заполнить и отправить запрос на выпуск сертификата.