

# Инструкция по установке крипто-провайдера ЭЦП на сервер

## Оглавление

1. Перечень лицензий для покупки. ....	1
2. Порядок установки: .....	2

### 1. Перечень лицензий для покупки.

- 1.1 КриптоПро .NET (архив-библиотека крипто-провайдера), описание: [ссылка](#),  
требования: [ссылка](#)  
Необходимо приобрести серверную лицензию: [ссылка](#)  
Дистрибутив: [ссылка](#)
- 1.2 КриптоПро CSP 4.0 (крипто-провайдер, необходим для работы КриптоПро .NET), описание: [ссылка](#)  
Необходимо приобрести лицензию на право использования на сервере: [ссылка](#)  
Дистрибутив: [ссылка](#)
- 1.3 iTextSharp (библиотека для модификации PDF), вот одна из подходящих: [ссылка](#)  
Необходимо приобрести лицензию на один сервер: [ссылка](#)  
Дистрибутив: загружается в проект через NuGet: [ссылка](#)

## 2. Порядок установки:

### 2.1 КристоПро .NET (архив-библиотека крипто-провайдера)

Дистрибутив: [ссылка](#)

### 2.2 КристоПро CSP 4.0 (крипто-провайдер, необходим для работы КристоПро .NET)

Дистрибутив: [ссылка](#)

### 2.3 iTextSharp (библиотека для модификации PDF)

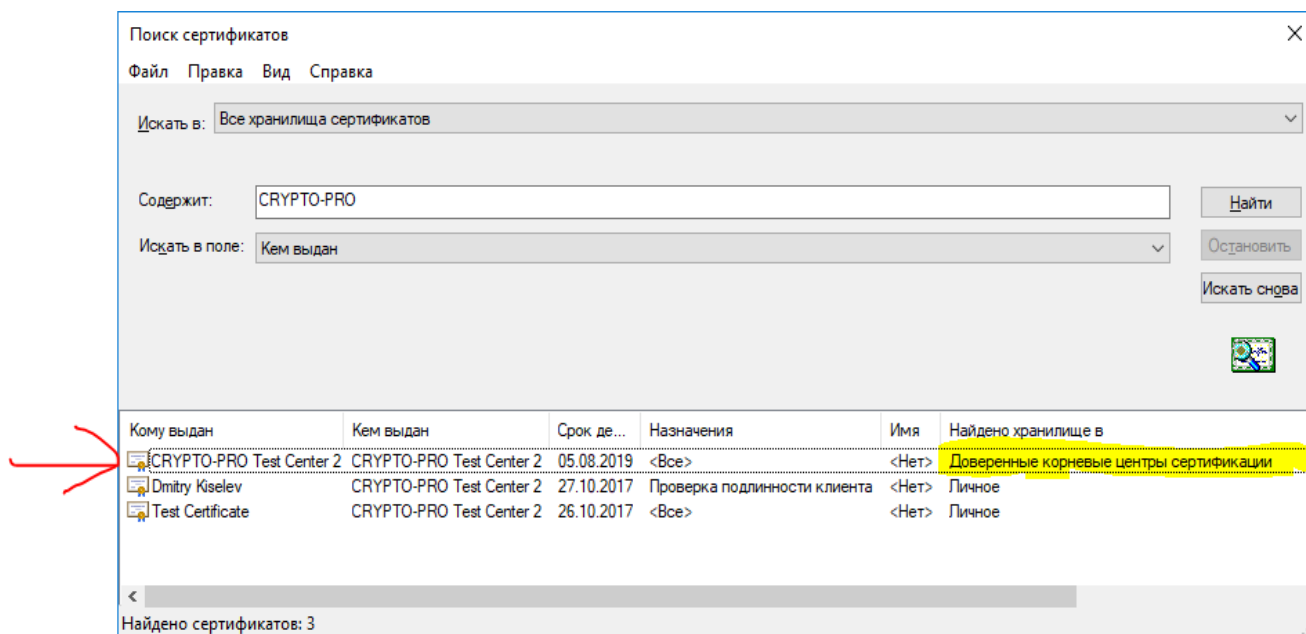
Дистрибутив: загружается в проект через NuGet: [ссылка](#)

### 2.4 Adobe Acrobat Reader

Дистрибутив: [ссылка](#)

### 2.5 Установить два сертификата:

2.5.1 Сертификат Удостоверяющего Центра «Кристо Про» и установить его в хранилище сертификатов, в узел «Доверенные корневые центры сертификации», вот пример для тестового сертификата:



Данный сертификат содержит всю необходимую информацию об удостоверяющем центре.

2.5.2 Отправить в Удостоверяющий Центр «Крипто Про» запрос на сертификат, для этого заполнить данные на форме, получив личный сертификат пользователя, уполномоченного нашей компанией подписывать документы PDF посредством ЭЦП: [ссылка](#)

Данный сертификат (в формате X.509) данные пользователя, его открытый и закрытый ключи, то есть всю информацию, необходимую для ЭЦП.

Вот пример заполнения формы запроса личного сертификата:

#### Идентифицирующие сведения:

Имя:	Dmitry Kiselev
Электронная почта:	kd.000.000.1@gmail.com
Организация:	SKDO
Подразделение:	IT
Город:	Moscow
Область, штат:	Moscow
Страна, регион:	RU

#### Тип требуемого сертификата:

Сертификат проверки подлинности клиента ▼

#### Параметры ключа:

☒ Создать новый набор ключей ☐ Использовать существующий набор ключей

CSP: Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider ▼

Использование ключей: ☐ Exchange ☐ Подпись ☒ Оба

Размер ключа: 512 Минимальный: 512 Максимальный: 512 (стандартные размеры ключей: [512](#))

☒ Автоматическое имя контейнера ключа ☐ Заданное пользователем имя контейнера ключа

☐ Пометить ключ как экспортируемый

☐ Использовать локальное хранилище компьютера для сертификата  
*Сохраняет сертификат в локальном хранилище вместо пользовательского хранилища сертификатов.  
Не устанавливает корневой сертификат ЦС.  
Необходимо быть администратором, чтобы создать локальное хранилище.*

#### Дополнительные параметры:

Формат запроса: ☐ CMC ☒ PKCS10

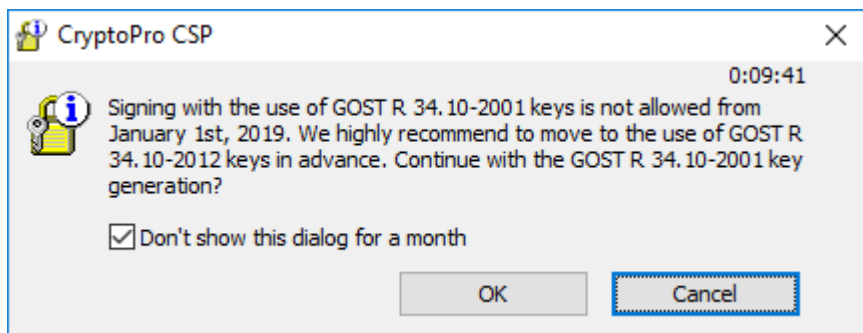
Алгоритм хеширования: GOST R 34.11-2012 256 bit ▼  
*Используется только для подписания запроса.*

☐ Сохранить запрос

Атрибуты:

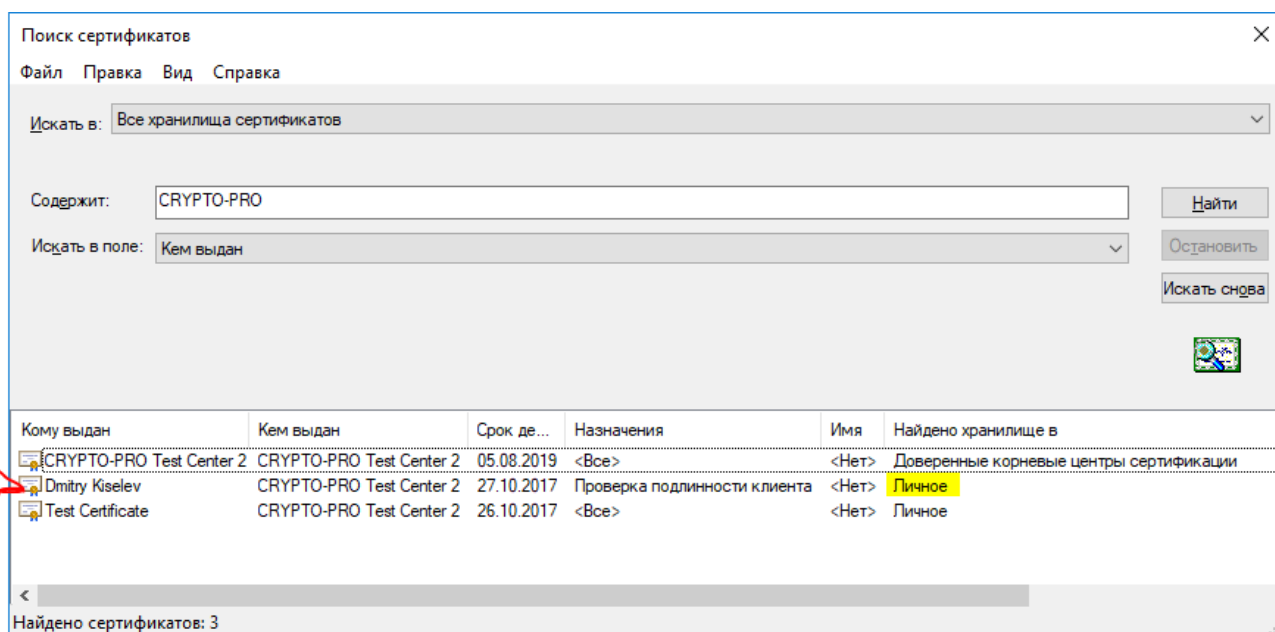
Понятное имя:

Необходимо обратить внимание на параметры ключа (поле CSP), если выбрать старый сервис-провайдер, то будет получено сообщение:



Наше ПО реализовано с учётом этого предупреждения и модифицировано именно на сервис-провайдер GOST R 34.10-2012 (CryptoPro.Sharpei.Gost3410\_2012\_256CryptoServiceProvider).

После заполнения формы Удостоверяющий Центр предложит скачать и установить сертификат, его необходимо поместить в личное хранилище:



После этого наше ПО сможет автоматически осуществлять подпись PDF-файлов ЭЦП, принадлежащей сотруднику, на имя которого получен личный сертификат.

Вот пример личного сертификата, выбрано поле с личными данными владельца (DN-поле):

