Удостоверяющий центр

Федеральная кадастровая палата

ИНСТРУКЦИЯ

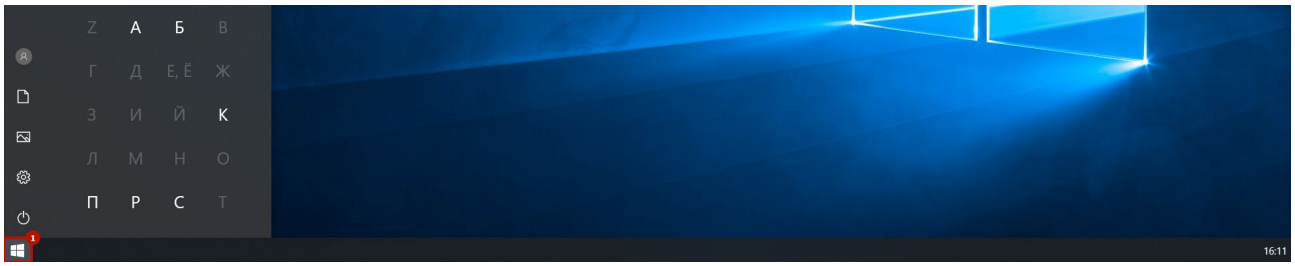
Определение алгоритма подписи сертификата ключа проверки электронной подписи (в среде операционной системы Microsoft Windows)

1. Подключение ключевого носителя

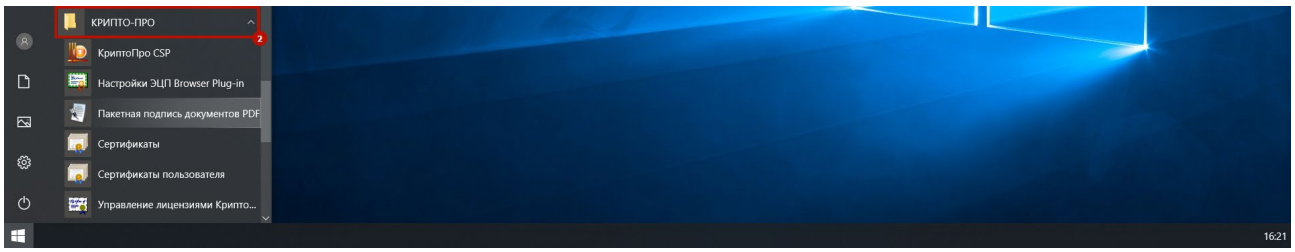
1.1. Перед началом работы необходимо подключить к компьютеру ключевой носитель, содержащий контейнер закрытого ключа и сертификат ключа проверки электронной подписи. В случае, если ранее контейнер закрытого ключа был записан в реестр операционной системы, перейдите к следующему шагу.

2. Запуск приложения КриптоПро CSP

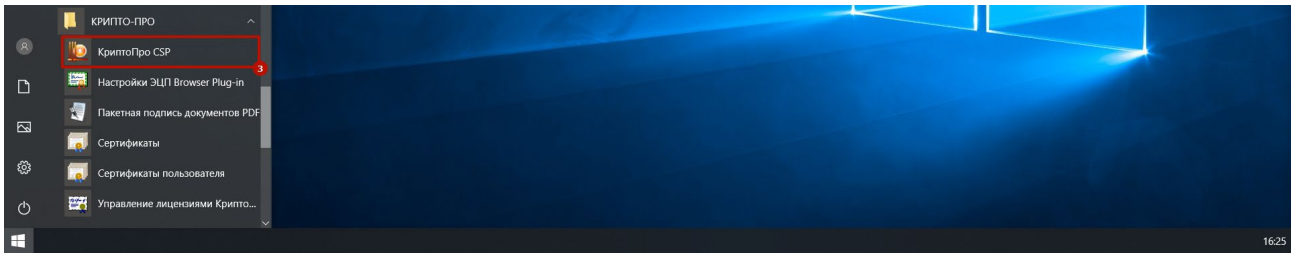
2.1. Раскройте меню «Пуск» в левом нижнем углу рабочего стола и перейдите к списку установленных приложений:



2.2. Найдите и раскройте каталог программных продуктов «КРИПТО-ПРО»:

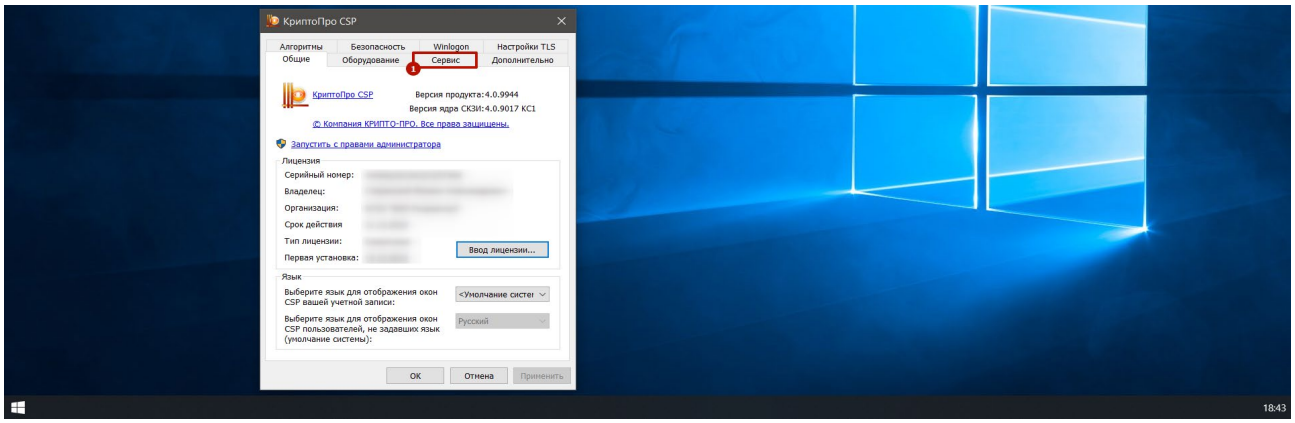


2.3. Запустите приложение КриптоПро CSP:

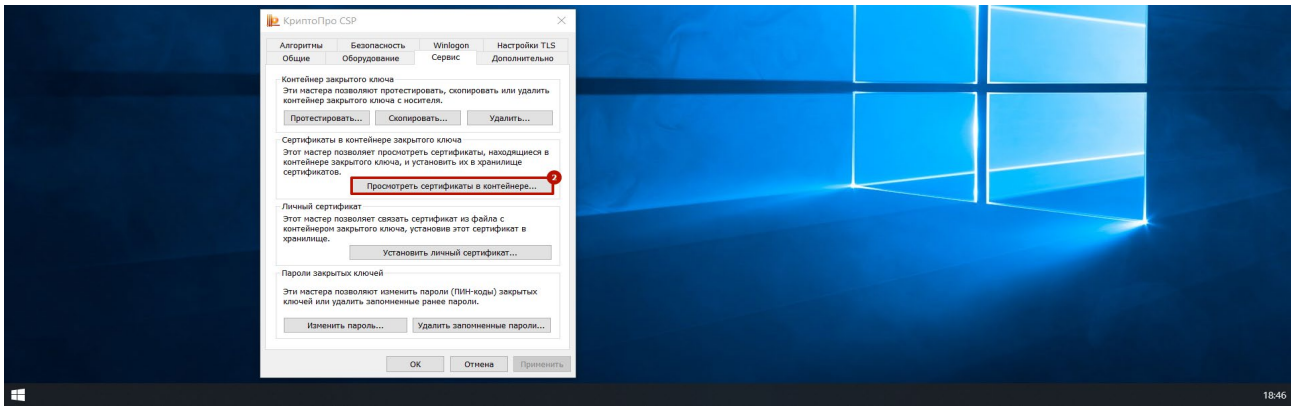


3. Поиск сертификата ключа проверки электронной подписи

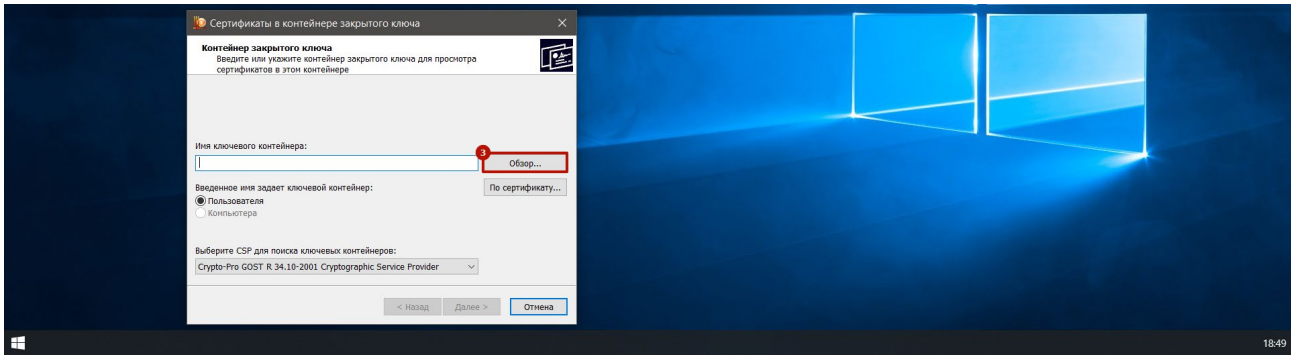
3.1. В интерфейсе приложения КриптоПро CSP перейдите во вкладку «Сервис»:



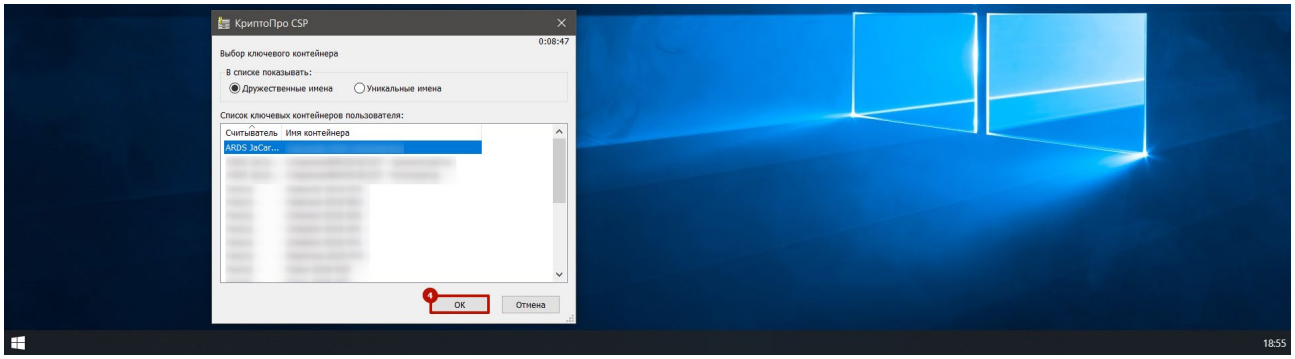
3.2. Во вкладке «Сервис» запустите мастер просмотра сертификатов:



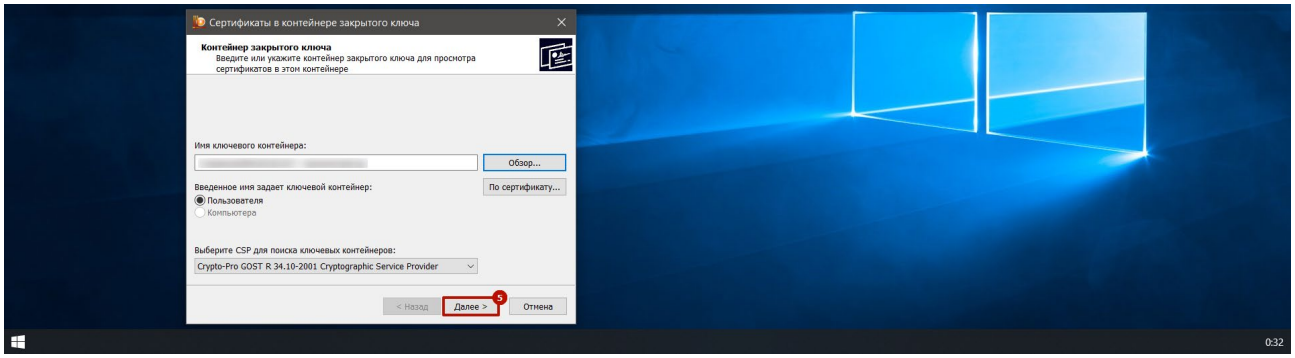
3.3. Выберите категорию пользователя и нажмите кнопку «Обзор…»:



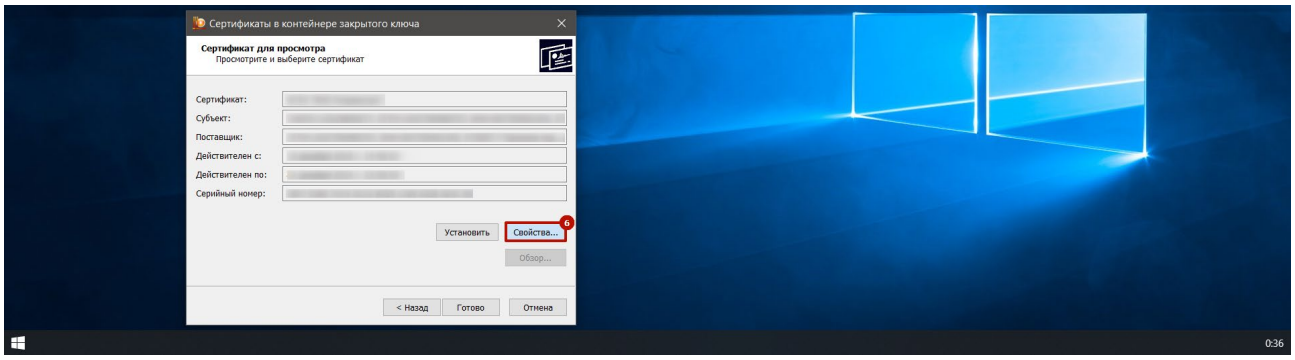
3.4. Выберите подлежащий анализу ключевой контейнер и нажмите кнопку «ОК»:



3.5. Для перехода к следующему шагу нажмите кнопку «Далее >»:

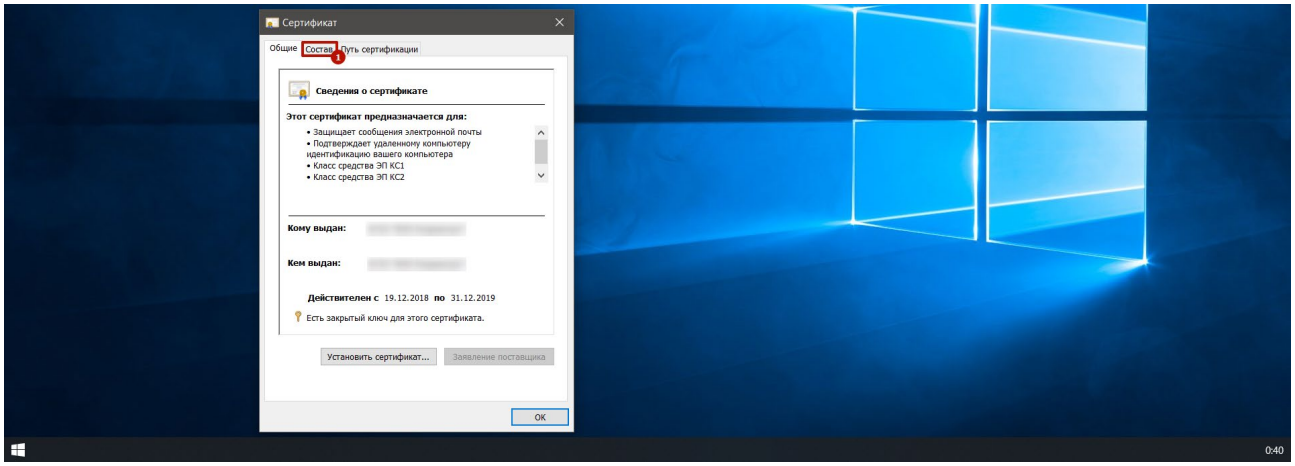


3.6. Для просмотра установленного в ключевой контейнер файла сертификата ключа проверки электронной подписи в электронном виде нажмите кнопку «Свойства…»:

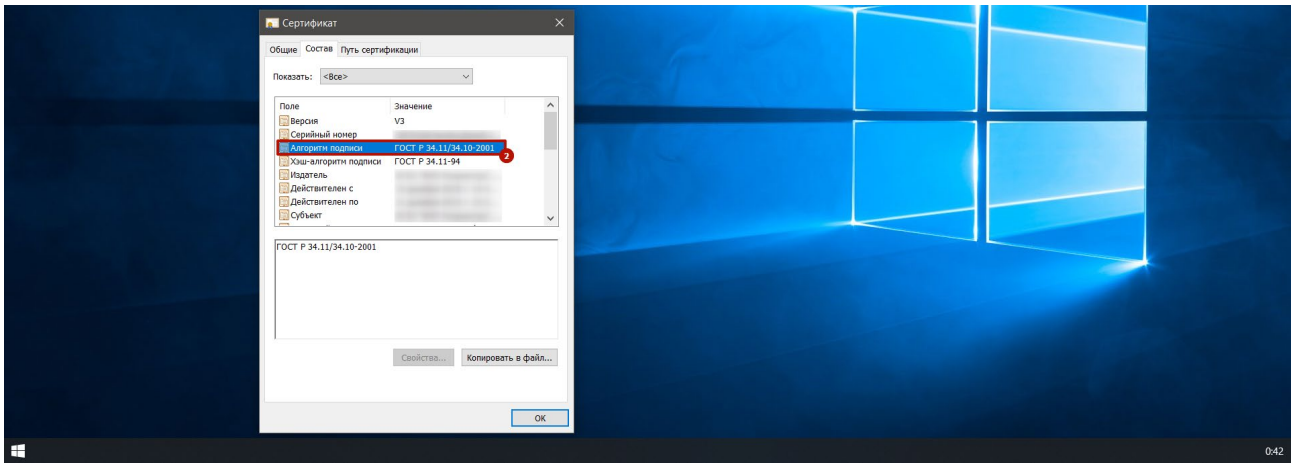


4. Анализ состава сертификата ключа проверки электронной подписи

4.1. В открывшемся окне свойств сертификата ключа проверки электронной подписи перейдите во вкладку «Состав»:



4.2. Активируйте просмотр расширения «Алгоритм подписи» и проанализируйте его значение:



4.3. В случае, если значением расширения «Алгоритм подписи» является «ГОСТ Р 34.11/34.10-2001», такой сертификат нельзя использовать после 31.12.2019 для создания электронных подписей.