КриптоАРМ

Краткое руководство пользователя

Содержание руководства

Что такое “КриптоАРМ”?

КриптоАРМ - программа для шифрования и электронной подписи файлов любого формата и размера (в т.ч. PDF, DOCX, XLSX, JPG, PNG).

Программа соответствует всем требованиям российского законодательства в части обеспечения юридически значимого статуса и используется для подписания котировочных заявок, банковских гарантий, межевых планов, алкогольных деклараций, различных соглашений, договоров, контрактов и других документов.

Используется в информационных системах, в которых необходимо:
- надежно защитить данные от постороннего доступа;
- обеспечить подлинность и авторство электронных документов;
- согласовывать электронные документы с коллегами;
- гарантировать целостность данных при отправке по незащищенным каналам связи и т.д.

Установка «КриптоАРМ»

1. Скачать дистрибутив

Актуальная версия программы: www.trusted.ru/support/downloads/

2. Убедиться в наличии прав администратора

Установка программы «КриптоАРМ» без наличия прав администратора невозможна.

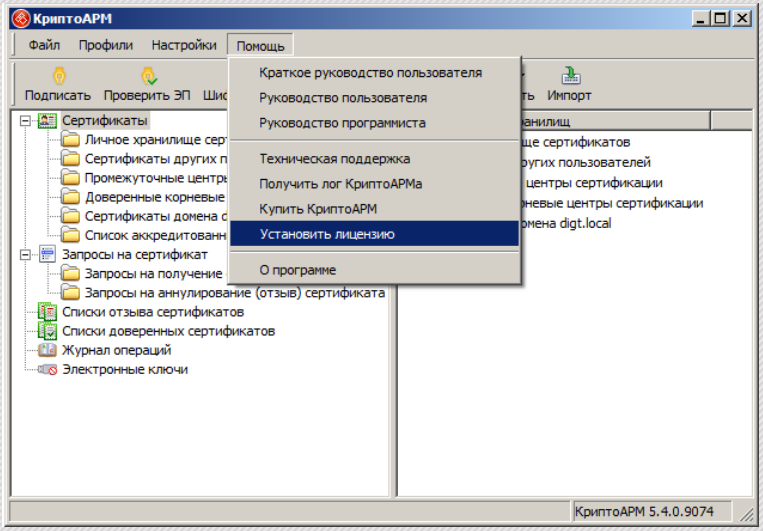
3. Установить программу

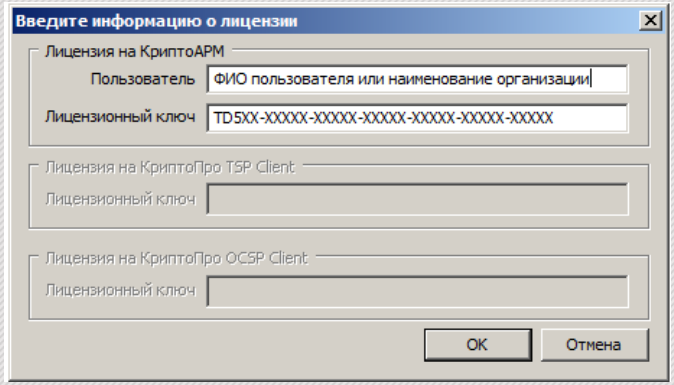
При первичной установке программы на компьютер автоматически будет активирован 14-дневный ознакомительный период «КриптоАРМ Стандарт Плюс» или «КриптоАРМ Терминал» (в зависимости от типа операционной системы).

По истечению ознакомительного периода программа автоматически переключится в режим «КриптоАРМ Старт» и предложит приобрести лицензию в официальном интернет-магазине: http://cryptoarm.ru/

Установка лицензии

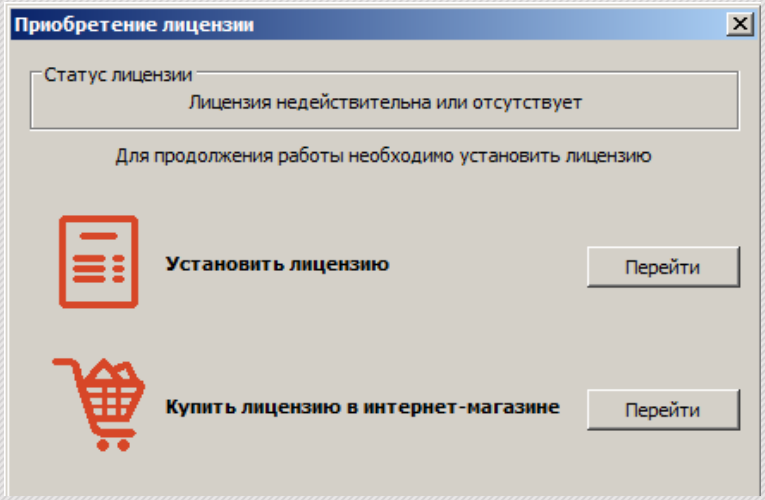
Вариант 1: Для установки лицензии зайдите в раздел **Помощь** – **Установить лицензию,** введите название вашей организации и лицензионный ключ.

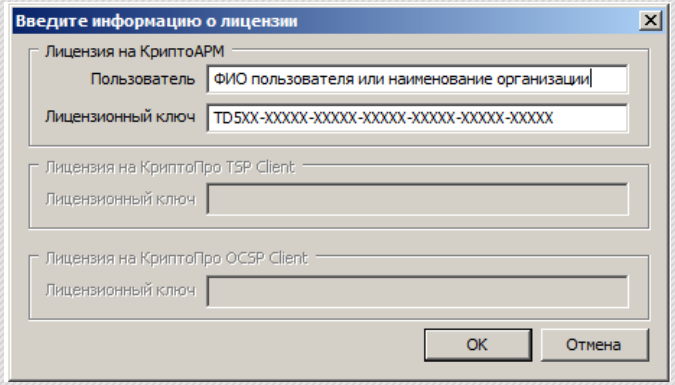




Установка лицензии

Вариант 2: Если ознакомительный период уже истек, то после каждого запуска программы вам будет предложено окно для удобной установки и покупки лицензии.





Установка сертификатов с токенов или смарт-карт

Для установки сертификата на компьютер необходимо:

1. Установить **криптопровайдер (КриптоПро CSP)** и соответствующий **драйвер** для ключевого носителя;

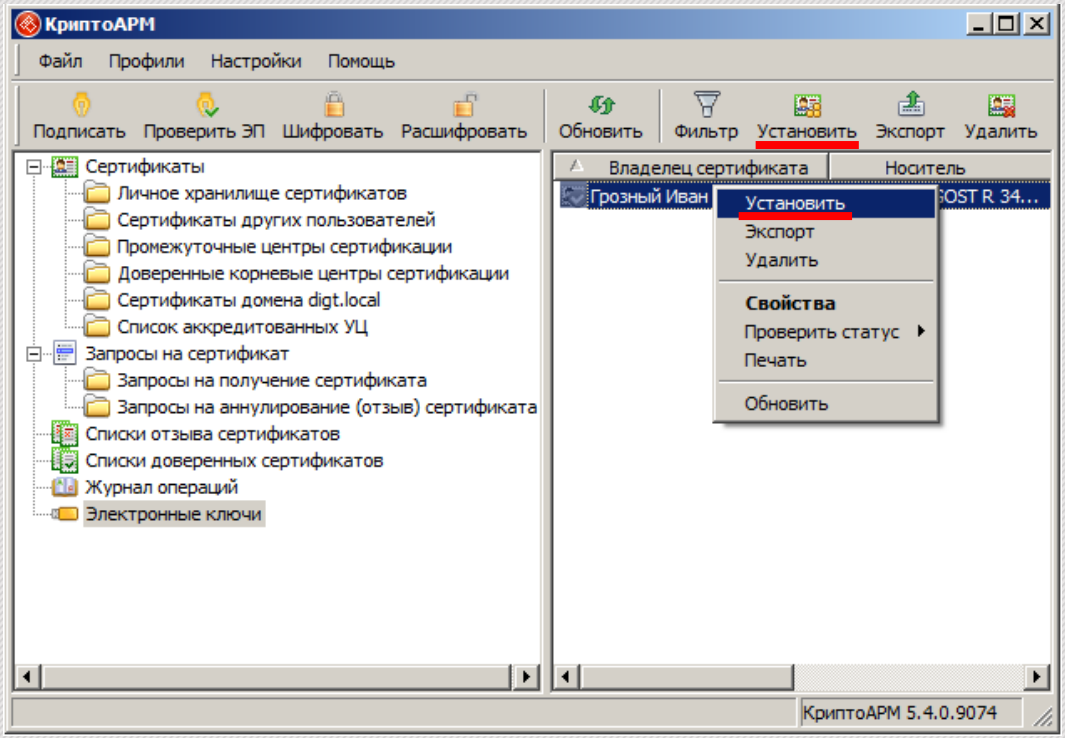
2. Подключить **токен или смарт-карту** к компьютеру (поддерживаются ключевые носители Рутокен, eToken, JaCarta, ESMART, Gemalto);

3. Зайти в ветку **«Электронные ключи»** и дождаться пока программа «КриптоАРМ» считает все сертификаты, хранящиеся на токене или смарт-карте;

4. Неустановленные на компьютере сертификаты, хранящиеся на подключенных электронных ключах, будут отображены **серым цветом (см. картинку ниже).**

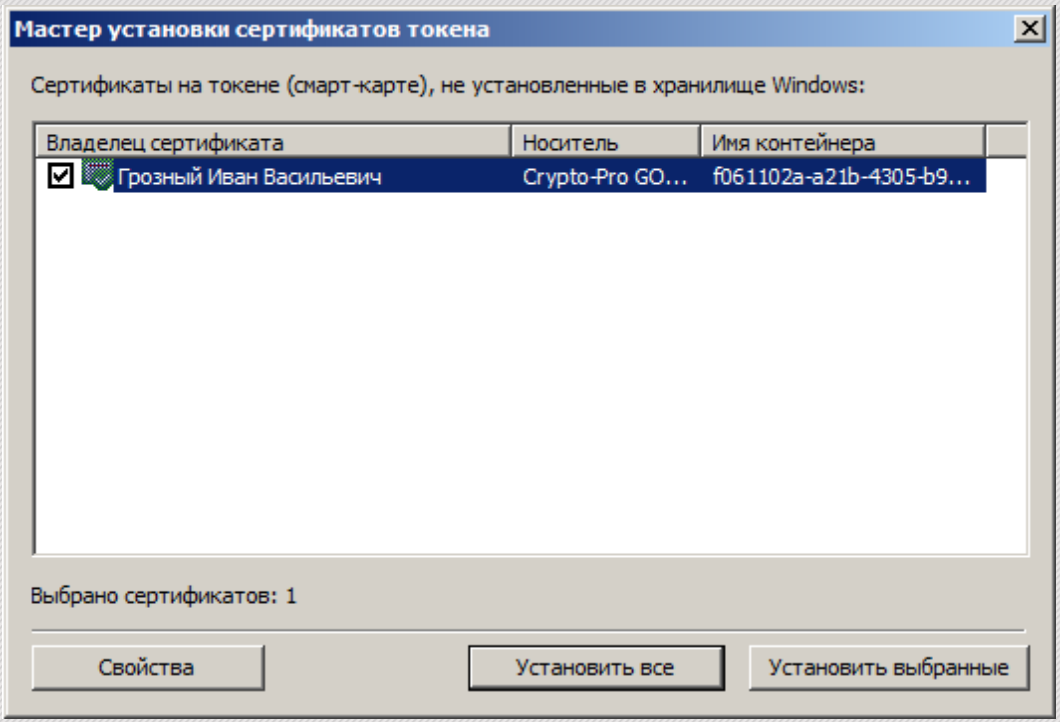
Установка сертификатов с токенов или смарт-карт

5. Выберите интересующие вас сертификаты и нажмите кнопку **Установить** на панели или в контекстном меню.



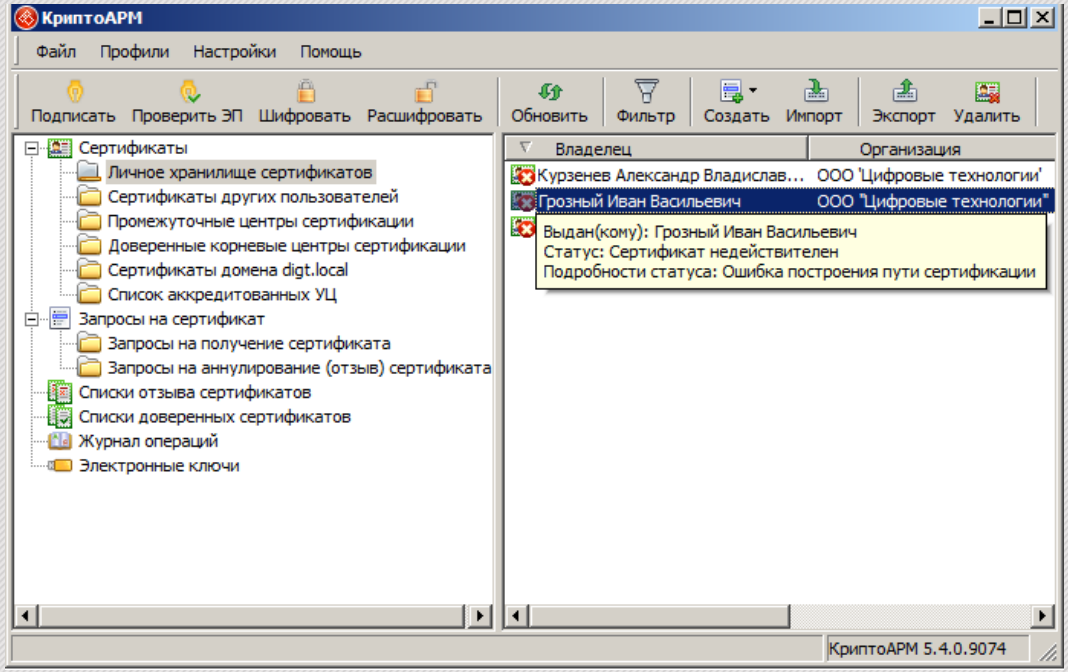
Установка сертификатов с токенов или смарт-карт

6. Выберите интересующие вас сертификаты и нажмите кнопку **Установить выбранные** или на кнопку **Установить все.**



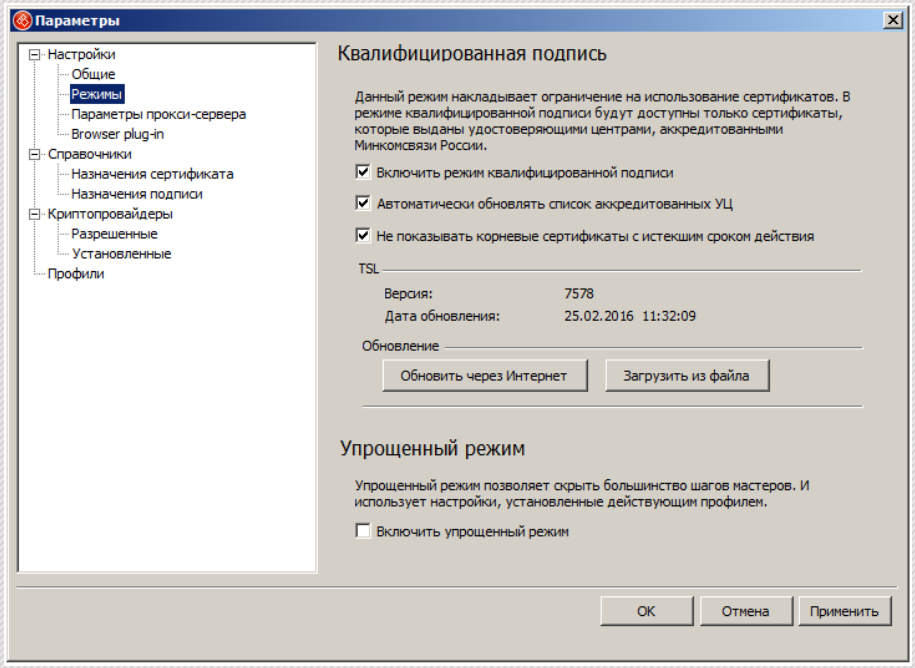
Установка сертификатов с токенов или смарт-карт

7. Ваши сертификаты будут установлены в **Личное хранилище сертификатов** со статусом **«Ошибка построения пути сертификации»**



Установка сертификатов с токенов или смарт-карт

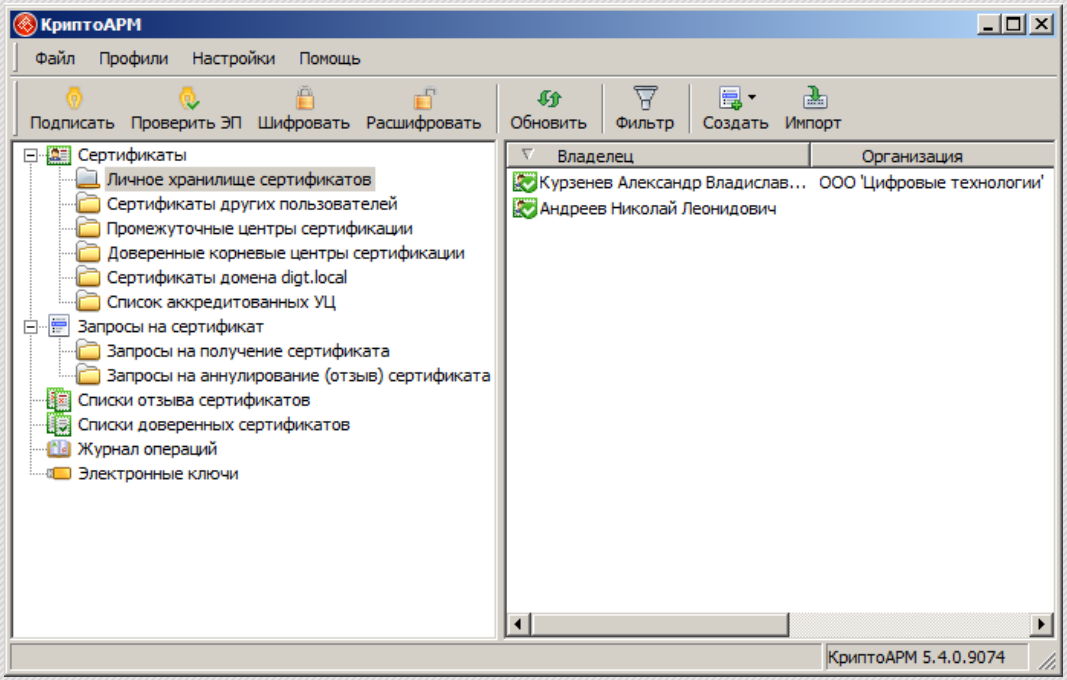
8. Для автоматического построения пути сертификации в **Настройках** программы воспользуйтесь режимом **Квалифицированная подпись**.



Примечание:
Данный режим предназначен только для квалифицированных сертификатов и требует наличия соединения с интернетом.
При включении режима неквалифицированные сертификаты будут скрыты (см. следующую страницу).

Установка сертификатов с токенов или смарт-карт

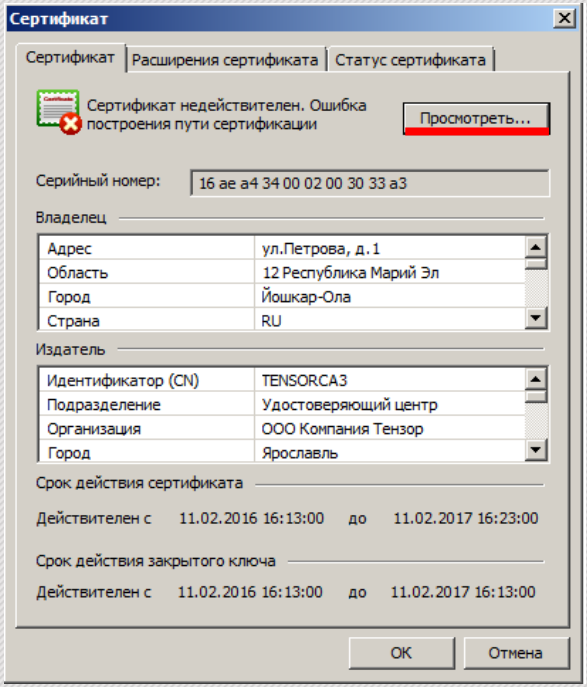
9. Поздравляем! Все необходимые сертификаты установлены!

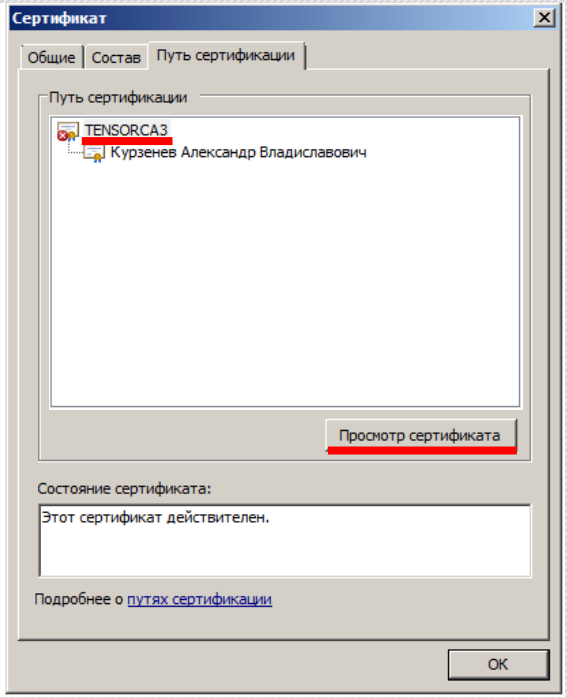


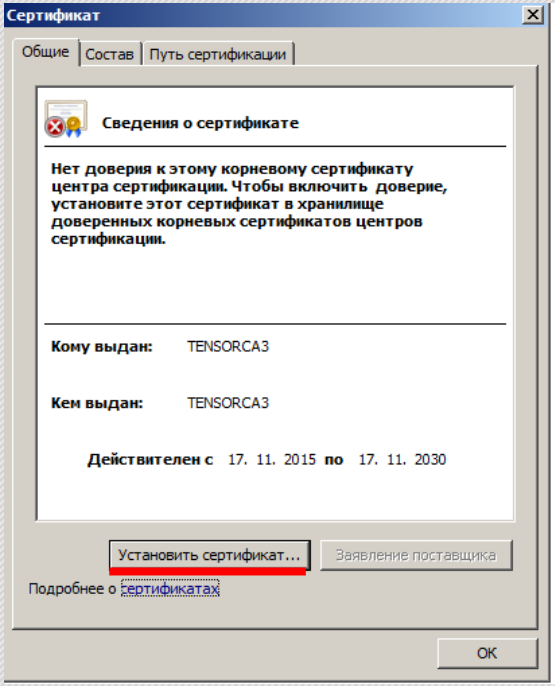
Если режим Квалифицированная подпись вам не помог, то отключите его и воспользуйтесь инструкцией для ручной установки необходимых сертификатов и списков отзыва сертификатов (шаги 10-13).

Установка сертификатов с токенов или смарт-карт

10. Для «ручного» построения пути сертификации в **Свойствах** сертификата нажмите **Просмотреть** – **Путь сертификации** – **Просмотр сертификата** – **Установить сертификат**

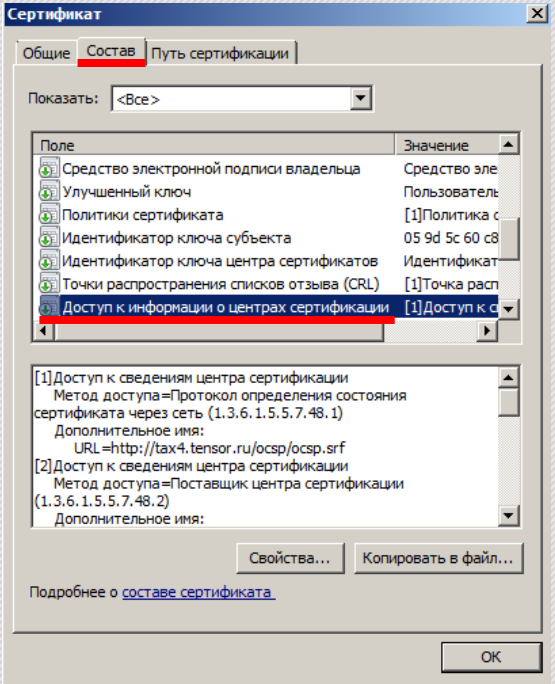


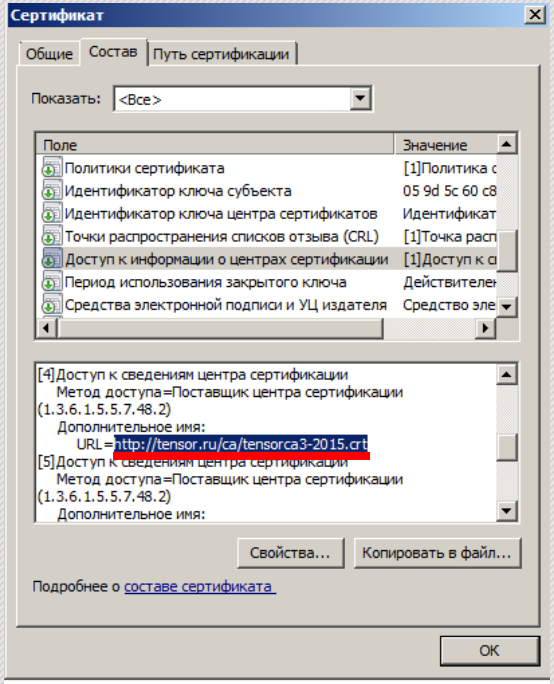


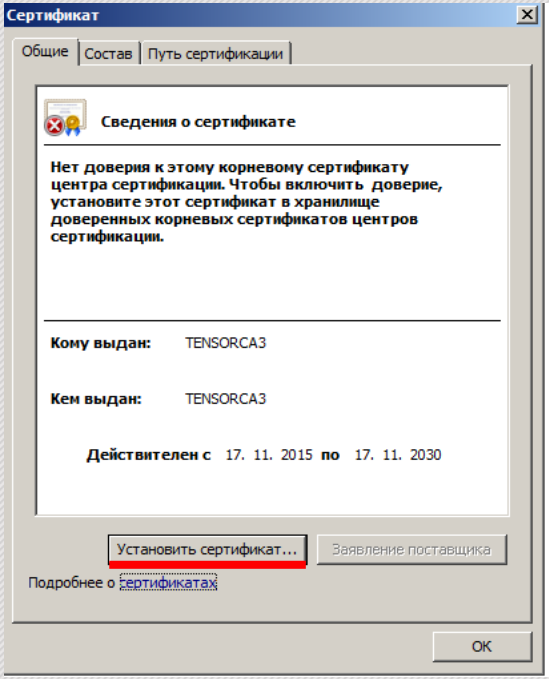


Установка сертификатов с токенов или смарт-карт

11. Для «ручного» построения пути сертификации в **Свойствах** сертификата нажмите **Просмотреть** – **Состав** – **Доступ к информации о центрах сертификации**. Найдите URL корневого сертификата (*.crt), скачайте и установите его.

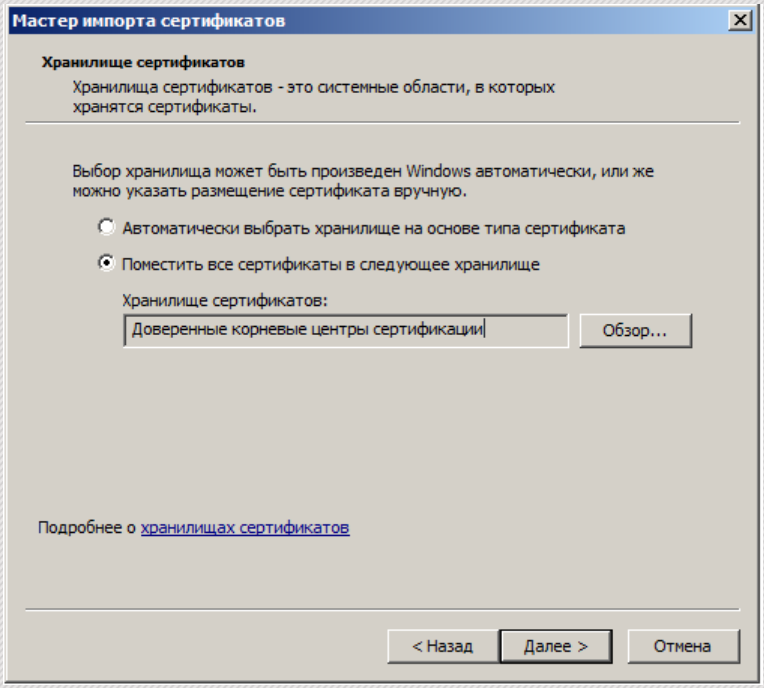






Установка сертификатов с токенов или смарт-карт

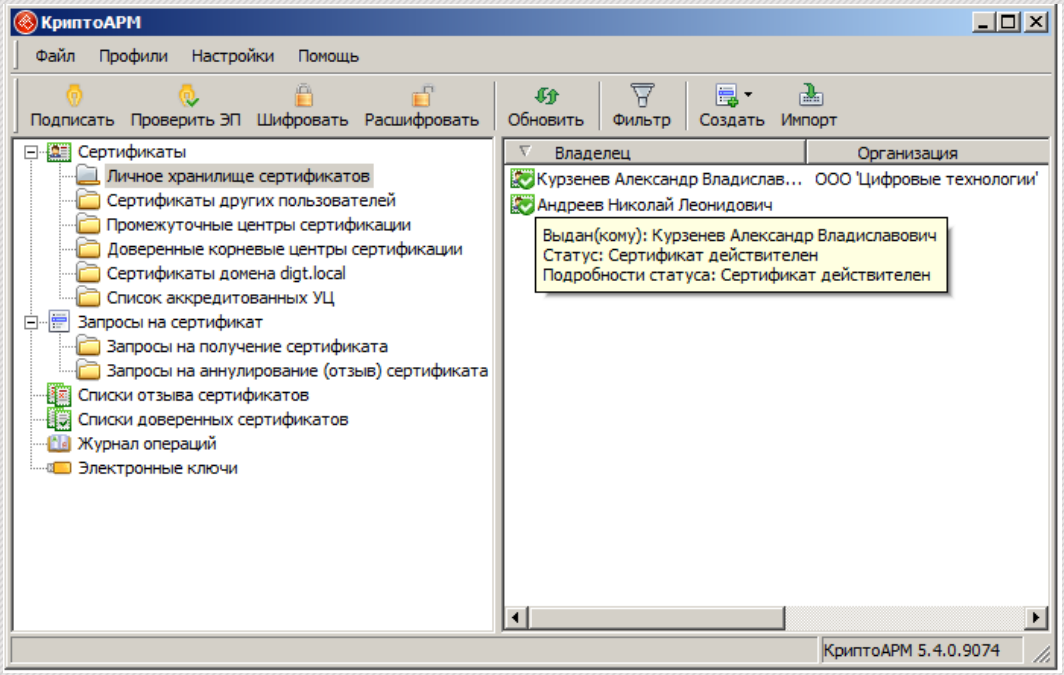
12. При установке корневого сертификата важно поместить его в хранилище **Доверенные корневые центры сертификации**



Примечание:
Важно принудительно выбрать именно данное хранилище. При автоматическом выборе хранилища возможна некорректная установка сертификата.

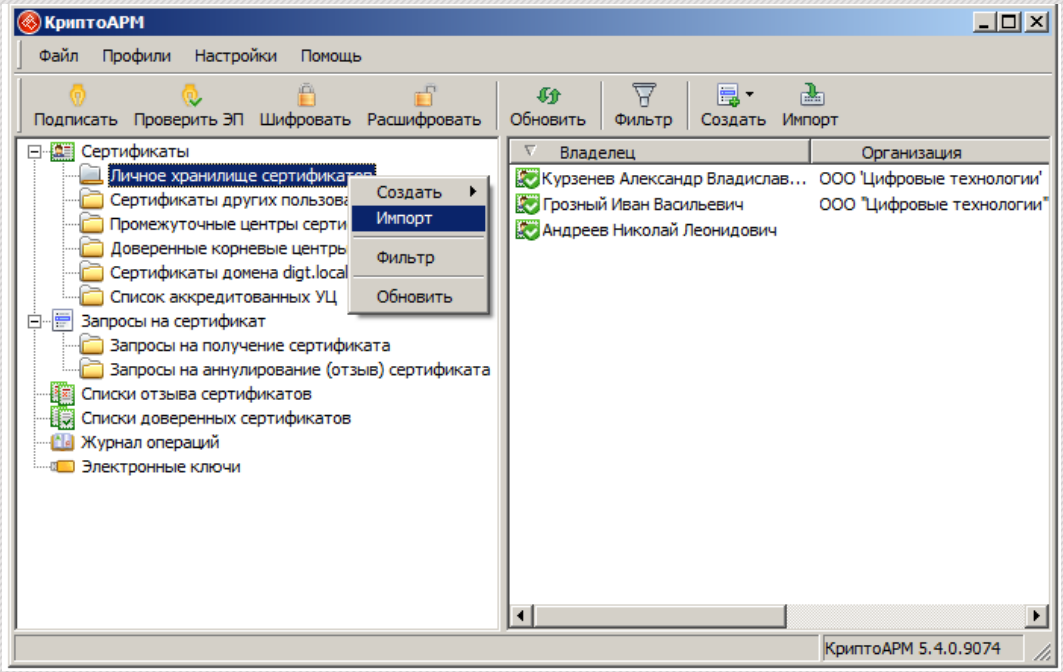
Установка сертификатов с токенов или смарт-карт

13. Поздравляем! Все необходимые сертификаты установлены!



Установка сертификатов с дискеты или флешки

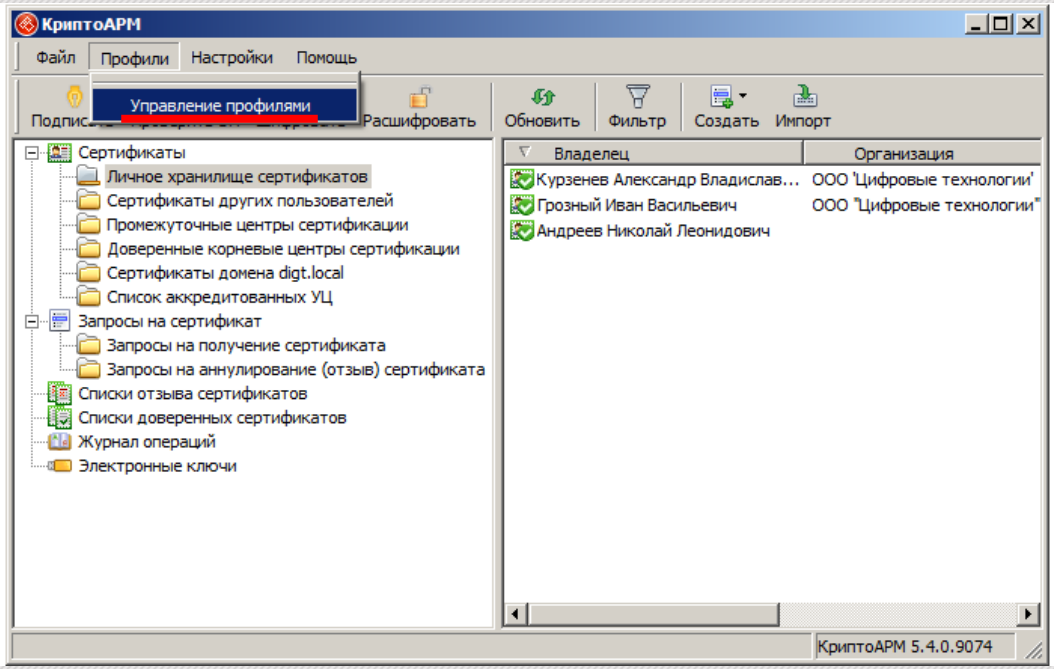
Если ваш сертификат хранится на обычной дискете или флешке, то для установки сертификата необходимо воспользоваться мастером Установки сертификатов, CRL и CTL.



Внимание!
Мы не рекомендуем использовать незащищенные отчуждаемые носители, а также локальное хранилище для хранения закрытого ключа.

Управление профилями

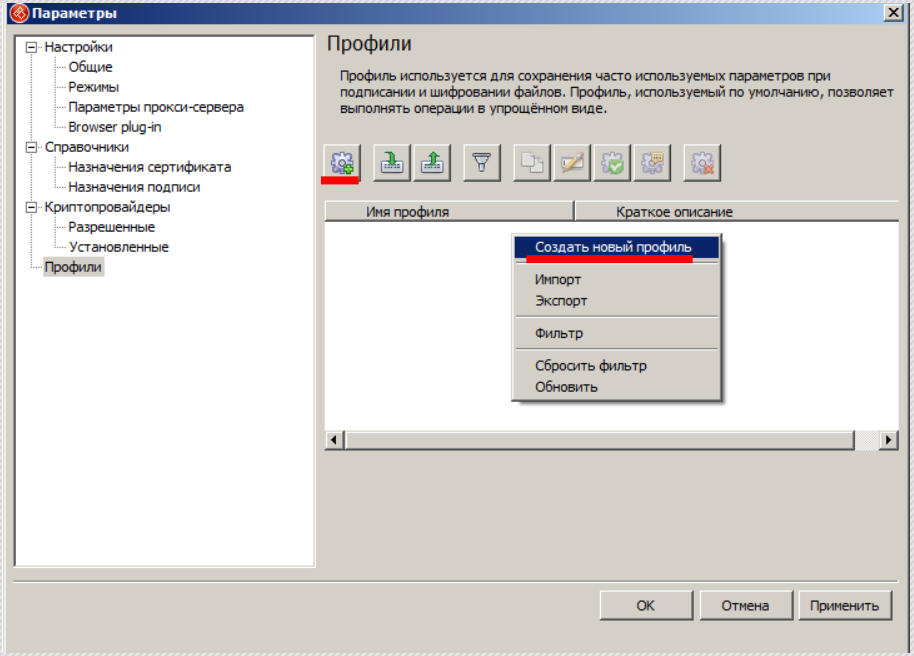
Для упрощения работы с электронной подписью и шифрованием файлов вы можете использовать **Профили**, которые позволят сохранить необходимые настройки заранее.



Для того, чтобы создать свой первый профиль, зайдите в раздел **Управление профилями**.

Управление профилями

Для того, чтобы создать новый профиль нажмите на кнопку **Создать** (левая кнопка на панели) или выберите **Создать новый профиль** в контекстном меню

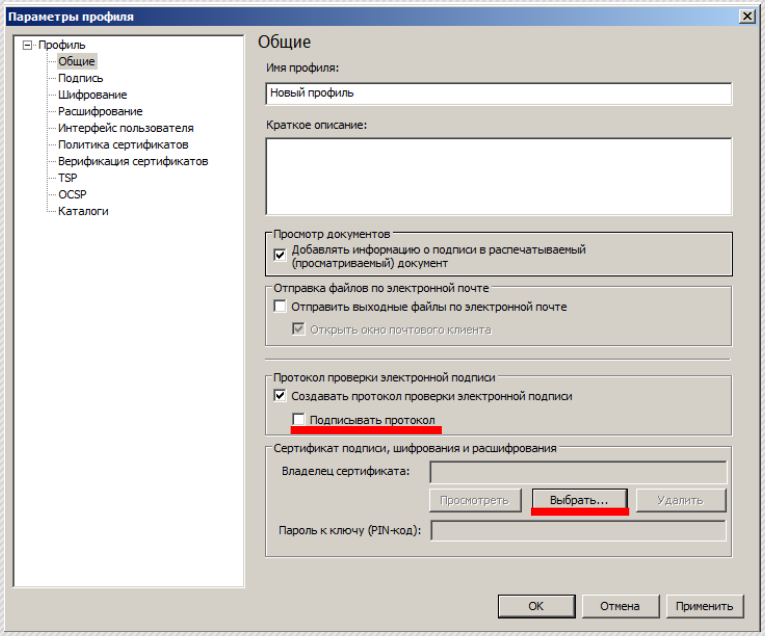


Кнопки на панели:

- Создать
- Импорт
- Экспорт
- Фильтр
- Создать копию
- Переименовать
- По умолчанию
- Свойства
- Удалить

Управление профилями

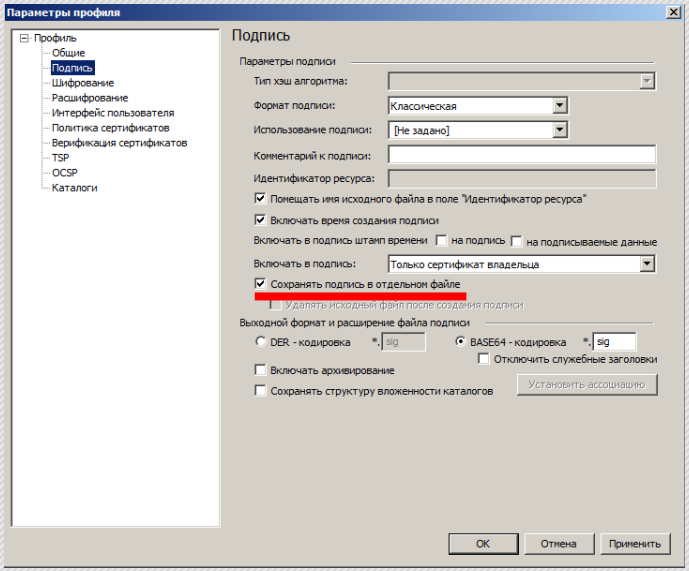
В разделе **Общие** введите имя профиля, а также выберите настройки, исходя из своих требований. Вы также можете **Выбрать сертификат**, который будет использоваться по умолчанию, и сохранить PIN-код.

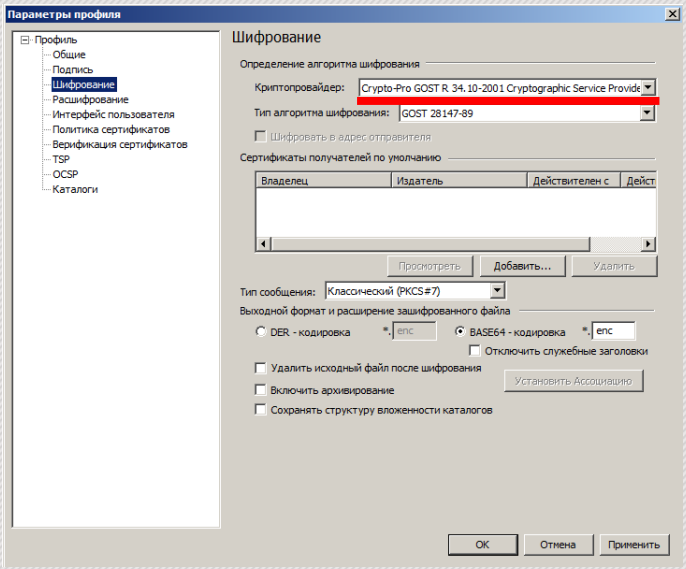


Обратите особое внимание на возможность создания протокола проверки электронной подписи (отдельным документом в формате PDF), а также возможность подписания данного протокола электронной подписью.

Управление профилями

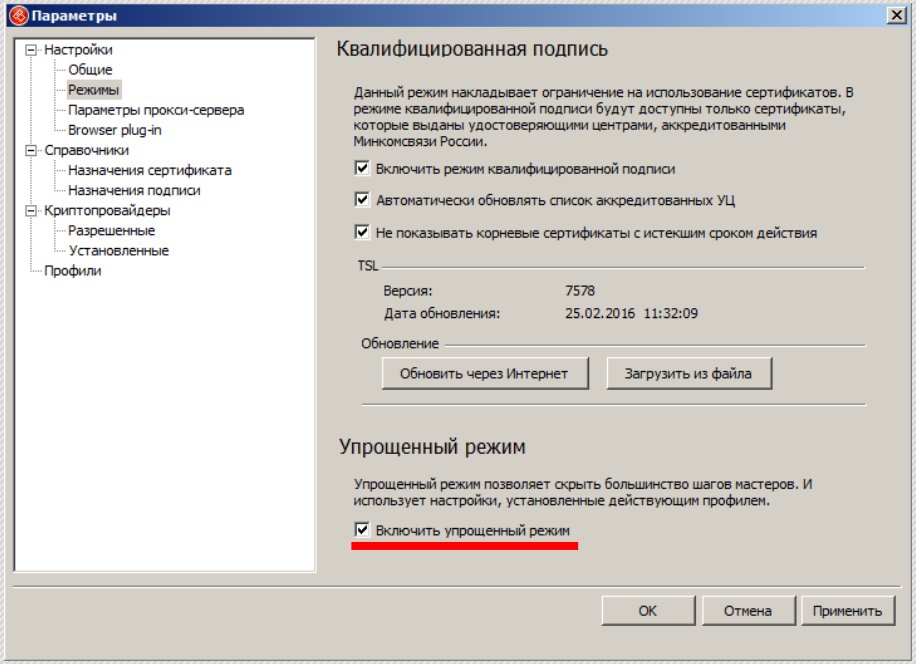
В разделах **Подпись** и **Шифрование** выберите настройки, исходя из своих требований. Обратите внимание на возможность изменения параметров Сохранить подпись в отдельном файле, а также выбора криптопровайдера и типа кодировки, используемых по умолчанию.





Управление профилями

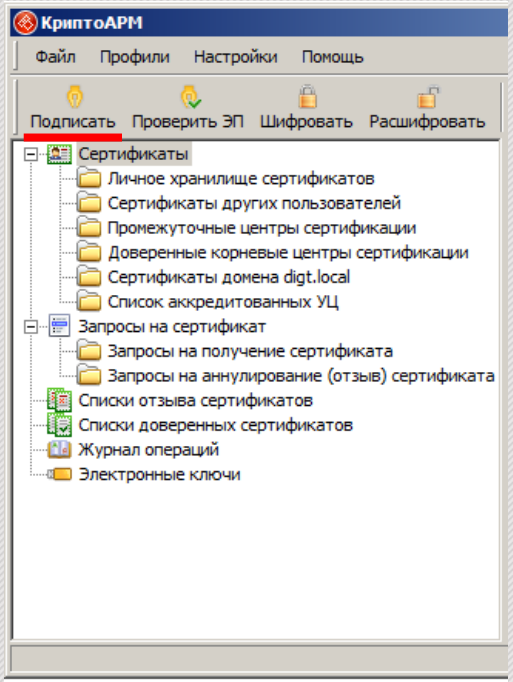
После того, как вы выбрали все необходимые настройки профиля, нажмите **Применить**, а затем во вкладке **Режимы** включите **Упрощенный режим**.

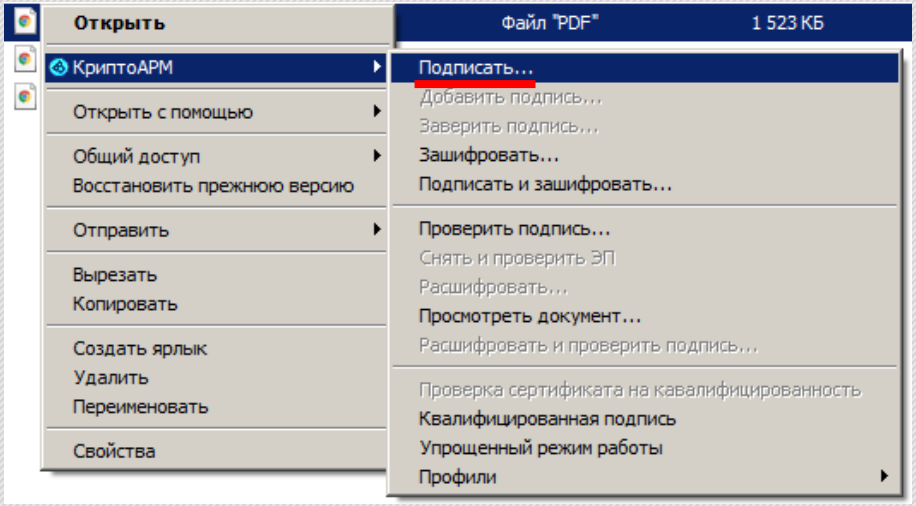


На этом настройка вашего профиля завершена. Далее рассмотрим операции подписания и шифрования уже с учетом включенного **упрощенного режима**.

Как подписать файл

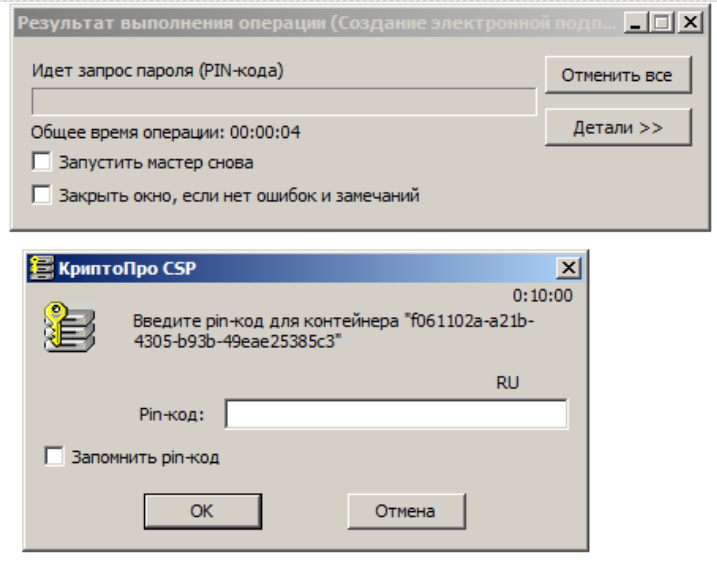
Подписать файлы можно в главном окне программы и через контекстное меню файла. Программа позволяет подписывать несколько файлов любого формата одновременно.



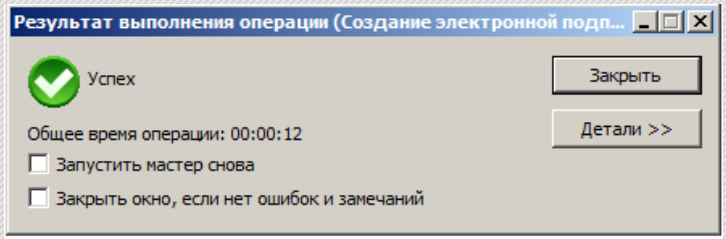


Как подписать файл

В зависимости от размера и количества файлов, а также от конфигурации рабочего места операция может занять от нескольких секунд до нескольких минут.



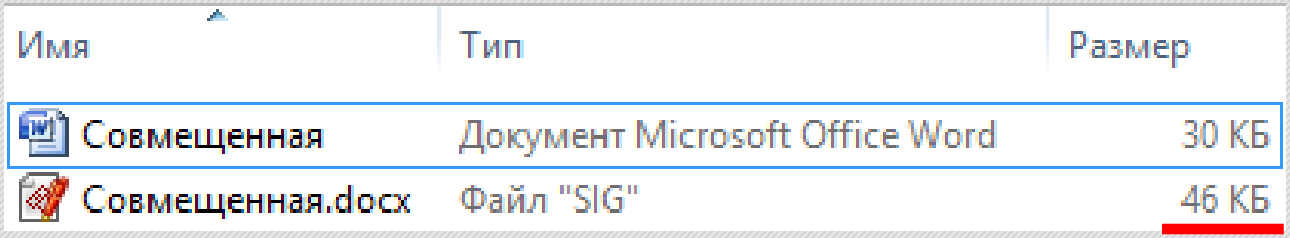
Введите пароль (PIN-код) для контейнера и нажмите ОК. Если все настройки были произведены правильно, то в результатам операции будет «Успех».

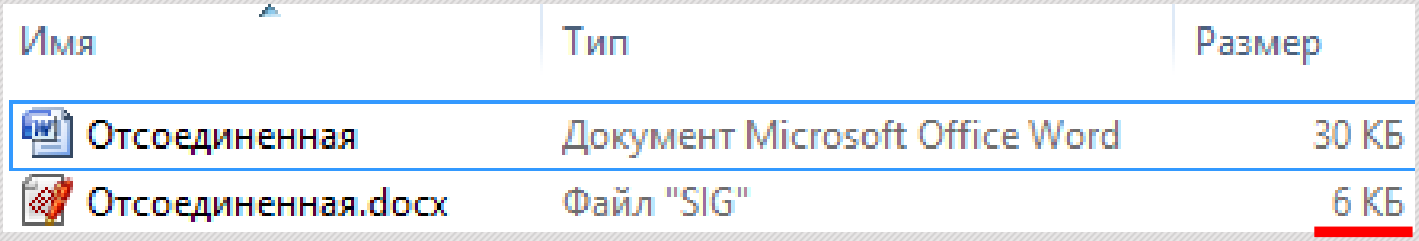


Как подписать файл

В результате операции в той же папке, в которой хранился исходный документ, появится файл с аналогичным названием, но с расширением *.SIG

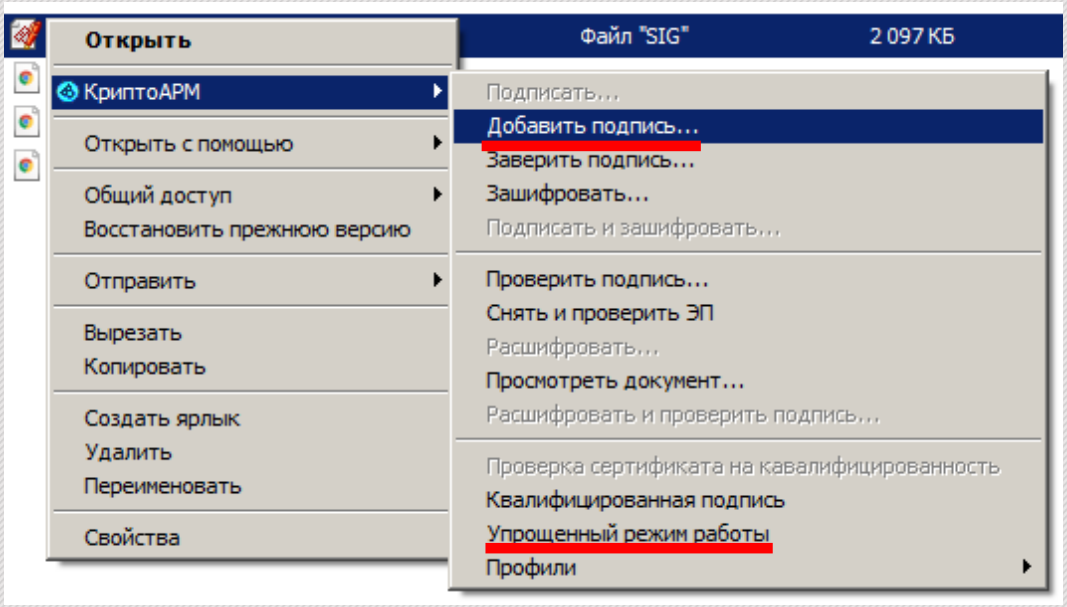
Если в профиле был включен параметр «Сохранять подпись в отдельном файле», то в результате вы получите отсоединенную подпись, которую необходимо отправлять вместе с исходным файлом.





Как добавить подпись

Чтобы к подписанному файлу добавить еще одну подпись, выберите файл с расширением *.SIG, отключите **Упрощенный режим** и выберите операцию **Добавить подпись**.

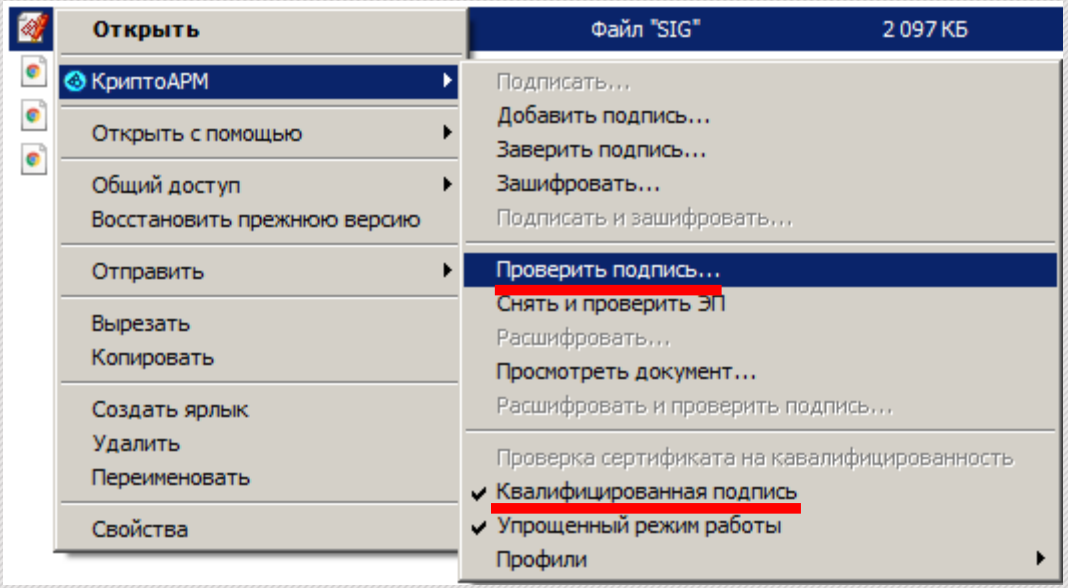


Примечание:
По количеству добавляемых подписей нет никаких ограничений.

Как проверить подпись

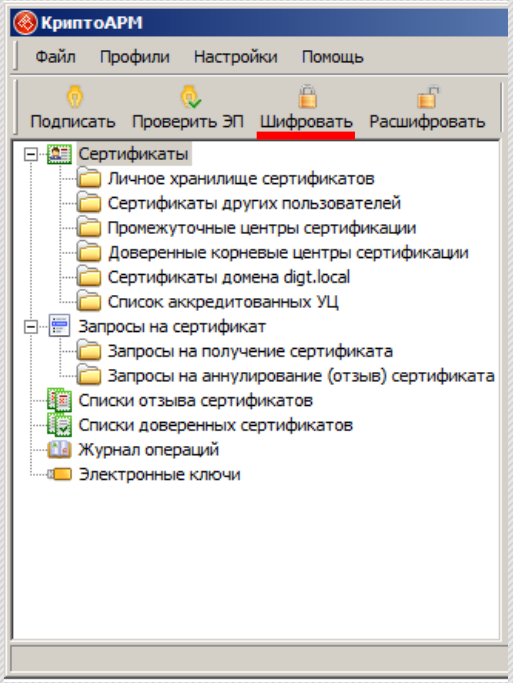
Чтобы проверить корректность электронной подписи, в контекстном меню файла выберите **Проверить подпись**.

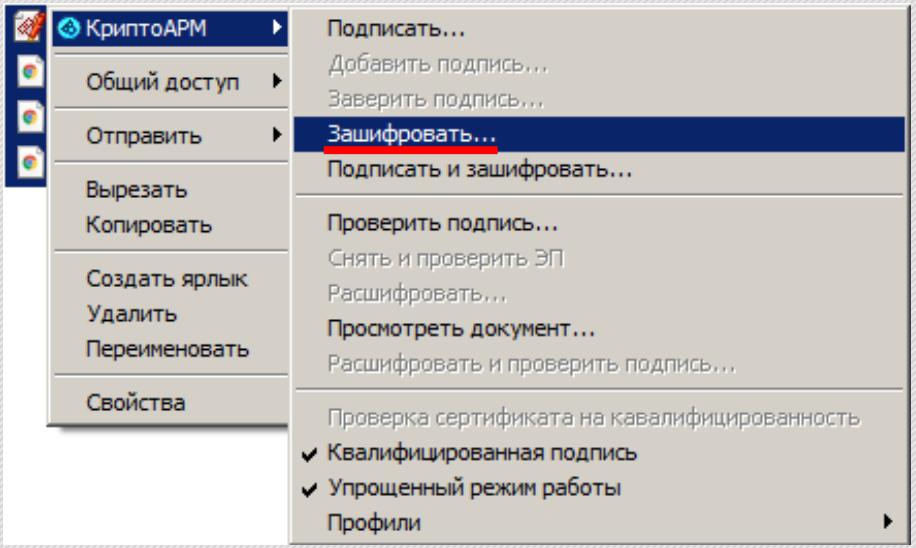
Если для вас важно проверить не только корректность электронной подписью, но и то, является ли она квалифицированной, убедитесь, что **включен** режим **Квалифицированная подпись**.



Как зашифровать файл

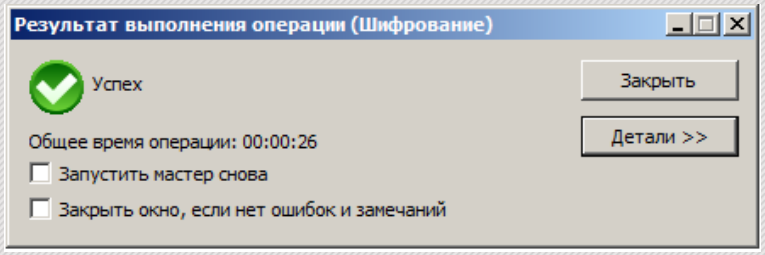
Зашифровать файлы можно в главном окне программы и через контекстное меню файла. Программа позволяет шифровать несколько файлов любого формата одновременно (в т.ч. файлы подписи).





Как зашифровать файл

В зависимости от размера и количества файлов, а также от конфигурации рабочего места операция может занять от нескольких секунд до нескольких минут.



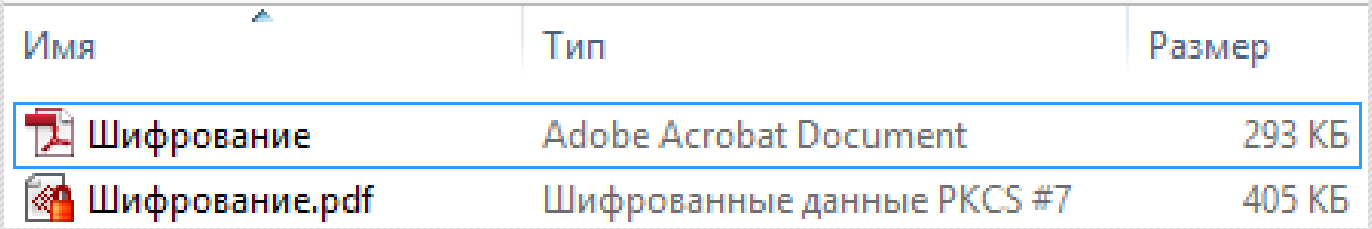
Для того, чтобы просмотреть подробную информацию о зашифрованном файле, нажмите на кнопку «Детали».

Как зашифровать файл

В результате операции в той же папке, в которой хранился исходный документ, появится файл с расширением *.ENC (шифрованные данные PKCS #7).

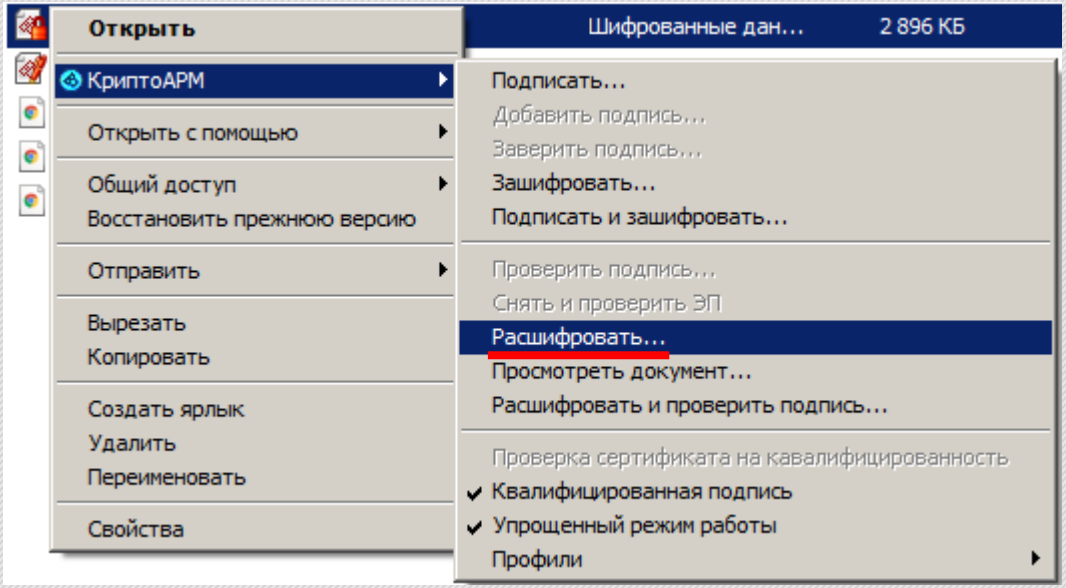
Обратите внимание, что файл, зашифрованный кодировкой «BASE-64», увеличивается в размере примерно на 40%.

При сохранении кодировкой «DER» шифрованный файл будет больше исходного на несколько килобайт (зависит от количества получателей шифрованного файла).



Как расшифровать файл

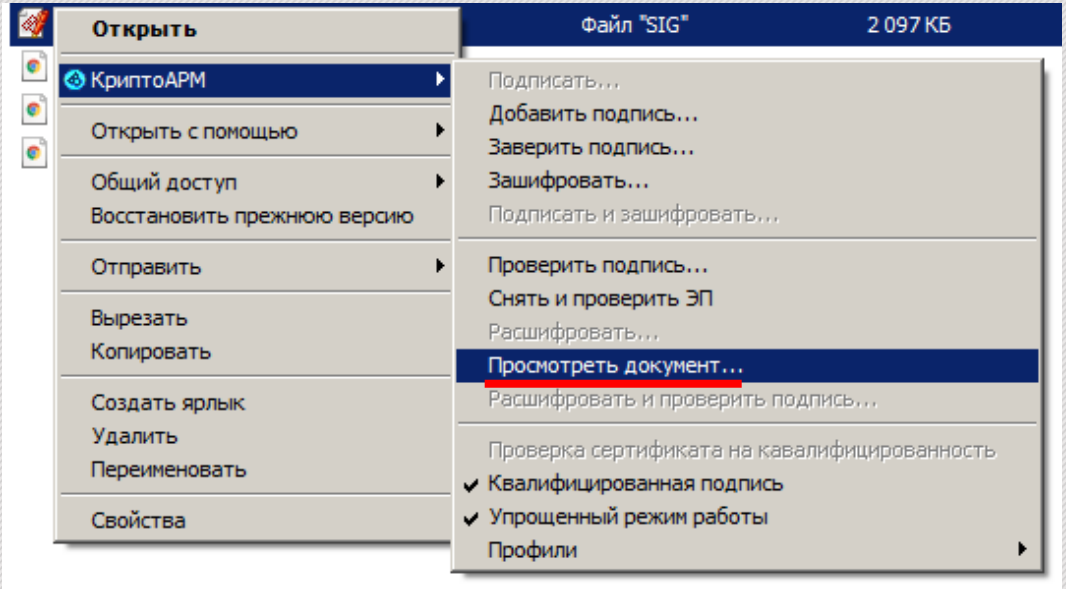
В контекстном меню файла выберите **Расшифровать**, и если ваш сертификат числится в списке получателей, то в текущем каталоге появится исходный (зашифрованный) документ.



Как просмотреть документ

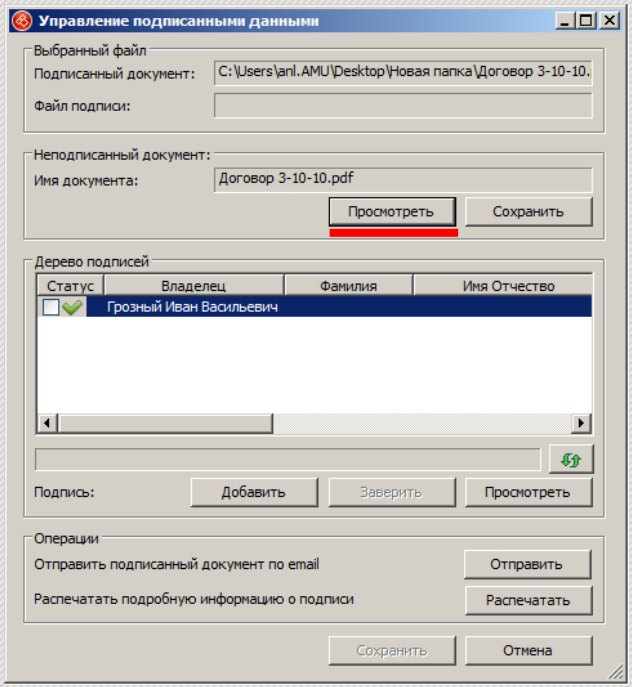
Если документ подписан отсоединенной подписью, то для просмотра документа достаточно открыть исходный файл.

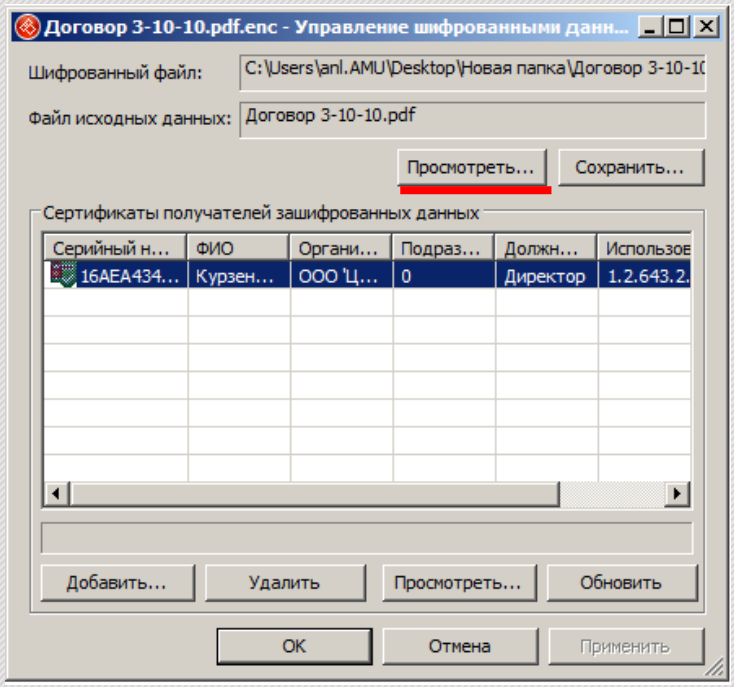
Если документ зашифрован или подписан совмещенной подписью, то просмотреть его можно одном из двух способов: через контекстное меню файла подписи (см. на картинке) или с помощью мастера управления подписанными и шифрованными данными (см. далее).



Как просмотреть документ

Просмотреть исходный документ также можно в окне Управление подписанными данными и Управление шифрованными данными. Для этого нажмите кнопку **Просмотреть**.





Техническая поддержка

Если у вас появились вопросы, и вы не можете найти ответ в данном руководстве , обратитесь в техническую поддержку на нашем сайте: http://www.trusted.ru/support/faq/