

ЗАО «КАЛУГА АСТРАЛ»

**Руководство пользователя  
продукт КриптоАРМ**

Версия редакции: 1.0.0.2.  
Дата редакции 24.08.2018 г.

Калуга, 2018

## СОДЕРЖАНИЕ

АННОТАЦИЯ .....	3
УСЛОВНЫЕ ОБОЗНАЧЕНИЯ .....	4
ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.....	5
1. ОБЩАЯ ИНФОРМАЦИЯ .....	6
2. ПОДПИСАНИЕ И ШИФРОВАНИЕ ФАЙЛОВ .....	6
ЗАКЛЮЧЕНИЕ .....	16

## **Аннотация**

Документ «Руководство пользователя. Продукт КриптоАРМ» содержит описание процесса подписи и шифрования файлов посредством функционала продукта КриптоАРМ на примере документов подготовленных для отправки в Росалкогольрегулирование.

## Условные обозначения

Обозначение	Расшифровка
	Внимание!
	Примечание:
<b>Текст</b>	Обозначение компонентов интерфейса, требующих активного воздействия Пользователя (кнопки, флаги и т.д.)
<i>Текст</i>	Обозначение текста блоков «Внимание!» и «Примечание:»

## Термины и определения

**BASE64** – специальный метод кодирования информации в 64-разрядный код (6 бит), широко используемый в приложениях электронной почты для кодирования бинарных данных. Весь диапазон закодированных символов укладывается в английский алфавит, цифры и ряд специальных символов.

**SIG** – файл, содержащий электронную цифровую подпись.

**КриптоАРМ** – программа, предназначенная для шифрования и расшифрования данных, создания и проверки электронной подписи (ЭП) с использованием сертификатов открытых ключей, для работы с сертификатами и криптопровайдерами.

**Росалкогольрегулирование** – федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции, а также функции по контролю за производством и оборотом этилового спирта, алкогольной и спиртосодержащей продукции, по надзору и оказанию услуг в этой сфере.

## 1. Общая информация

КриптоАРМ – программа, предназначенная для шифрования и расшифрования данных, создания и проверки электронной подписи (ЭП) с использованием сертификатов открытых ключей, для работы с сертификатами и криптопровайдерами. КриптоАРМ наряду со стандартными криптопровайдерами (входящими в поставку Windows) использует реализацию криптоалгоритмов в сертифицированных ФСБ РФ криптопровайдерах компании «КРИПТО-ПРО».

Разработчик: ООО «Цифровые технологии» (Йошкар-Ола).

Используя криптопровайдер, программа «КриптоАРМ» позволяет работать с сертифицированными средствами, создавать электронную цифровую подпись, равнозначную собственноручной.

Функциональные возможности программы:

- шифрование и расшифрование файлов произвольного формата (преобразования файлов функциями СКЗИ);
- создание и проверка корректности одной или нескольких ЭП;
- выполнение операций подписи и шифрования за одно действие;
- управление цифровыми сертификатами и ключами пользователя, списками отозванных и доверенных сертификатов;
- управление криптопровайдерами;
- совместимость с отчуждаемыми ключевыми носителями Рутокен, eToken;
- отправка подписанных и зашифрованных файлов по e-mail.

## 2. Подписание и шифрование файлов

Процесс подписания и шифрования файлов в данном разделе будет рассмотрен на примере документа отправляемого в Росалкогольрегулирование.

Для подписания и шифрования файлов выполните следующие действия.

Откройте в проводнике операционной системы требуемую папку с файлами, которые будут отправляться в Росалкогольрегулирование. Выделите только один файл и нажмите по нему правой кнопкой мыши. В открывшемся контекстном меню выберите **КриптоАРМ – Подписать и зашифровать** (рис. 1.).

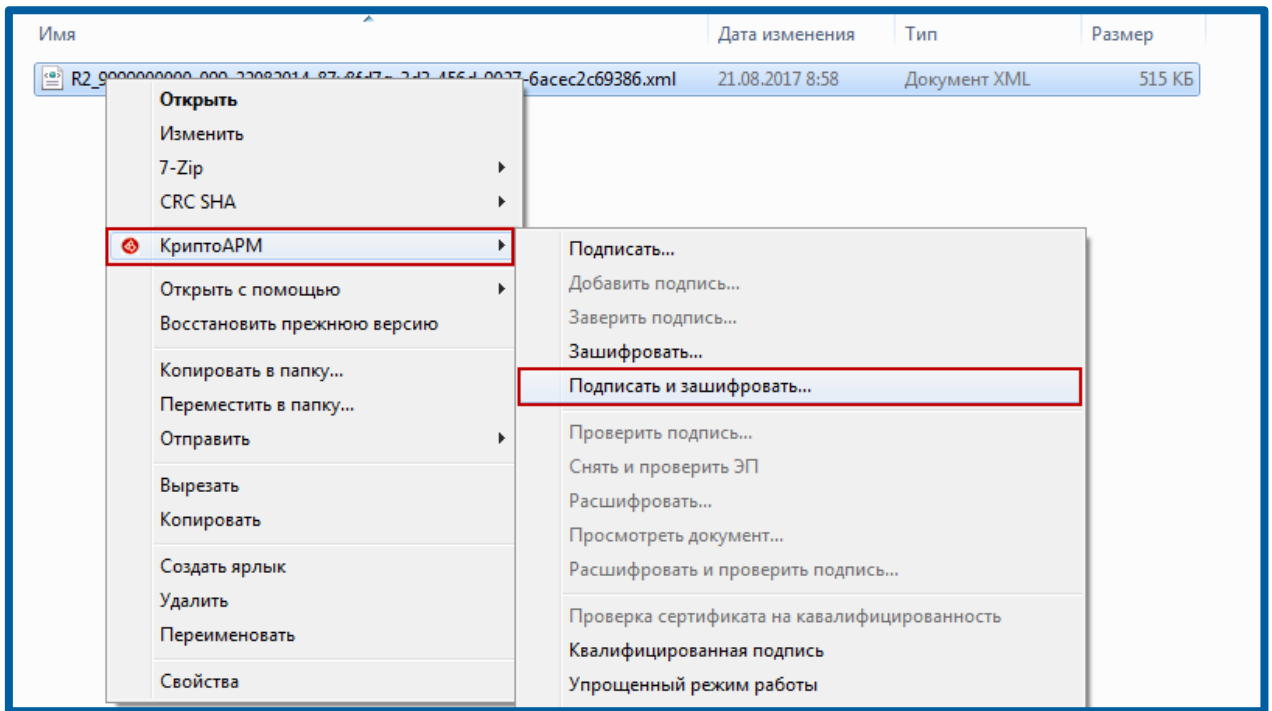


Рис. 1.

Перед Вами откроется окно Мастера создания электронной подписи и шифрования, нажмите кнопку **Далее** (рис. 2).

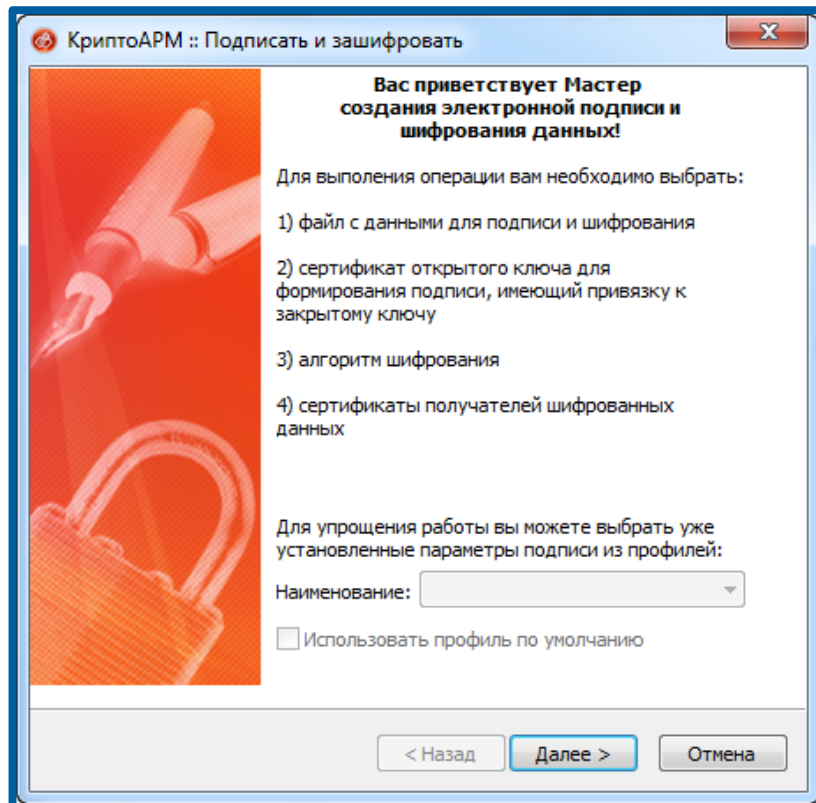


Рис. 2.

В следующем окне отобразится файл, подготовленный для шифрования. Нажмите кнопку **Далее** (рис. 3).

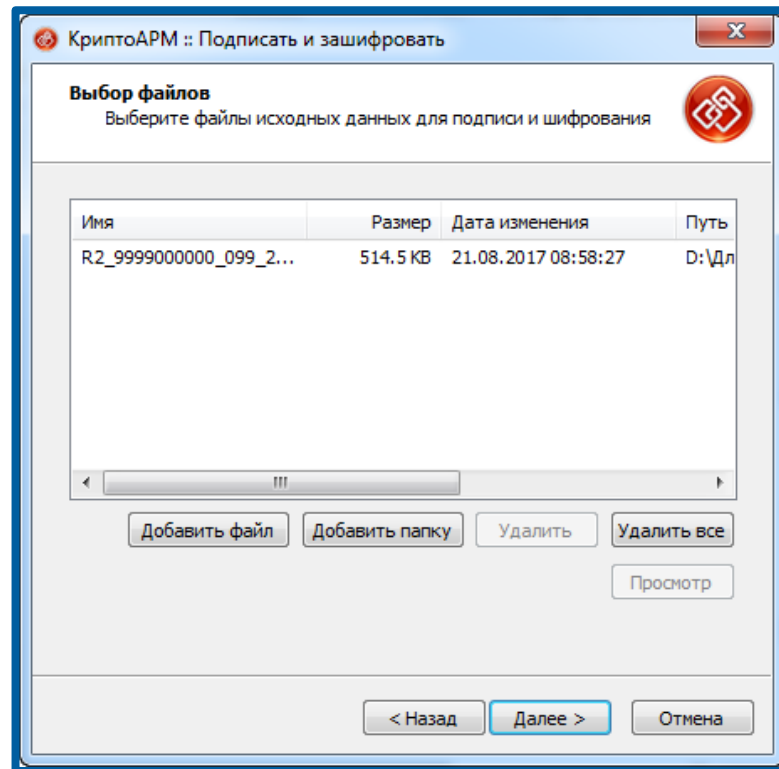


Рис. 3.

В следующем окне выберите кодировку подписи «BASE64» и расширение [\*.\*sig]. Нажмите кнопку **Далее** (рис. 4.).

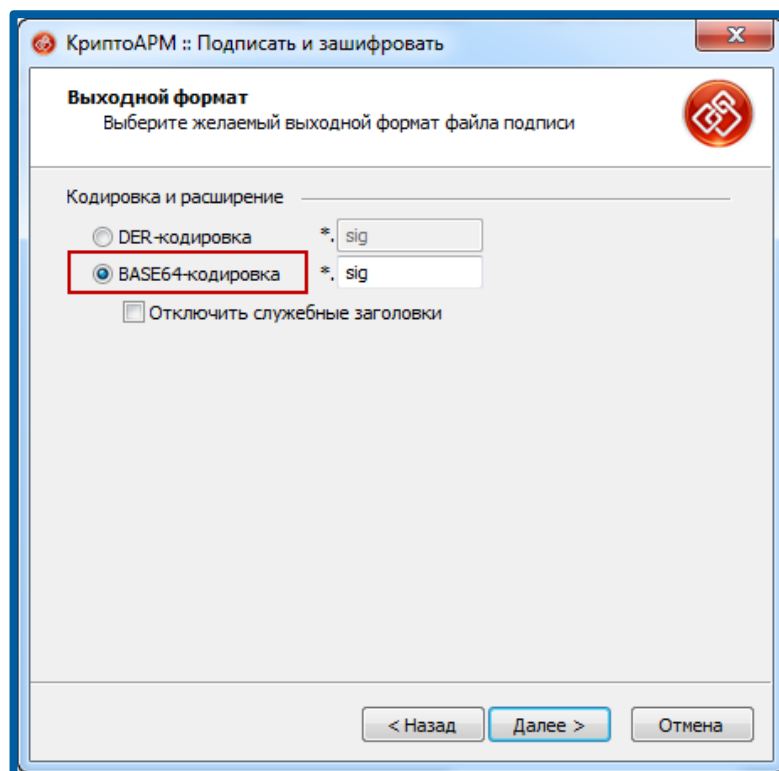


Рис. 4.

В строке «Использование подписи» выберите значение «Утверждено», добавьте комментарий к подписи и нажмите кнопку **Далее** (рис. 5.).



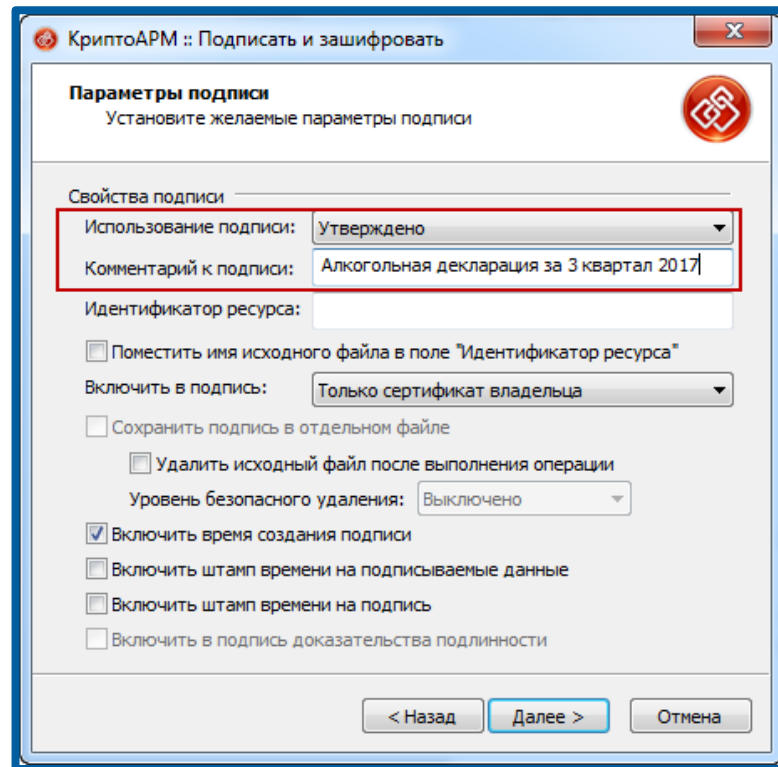


Рис. 5.

Далее требуется указать владельца сертификата. Для этого нажмите кнопку **Выбрать** (рис. 6.).

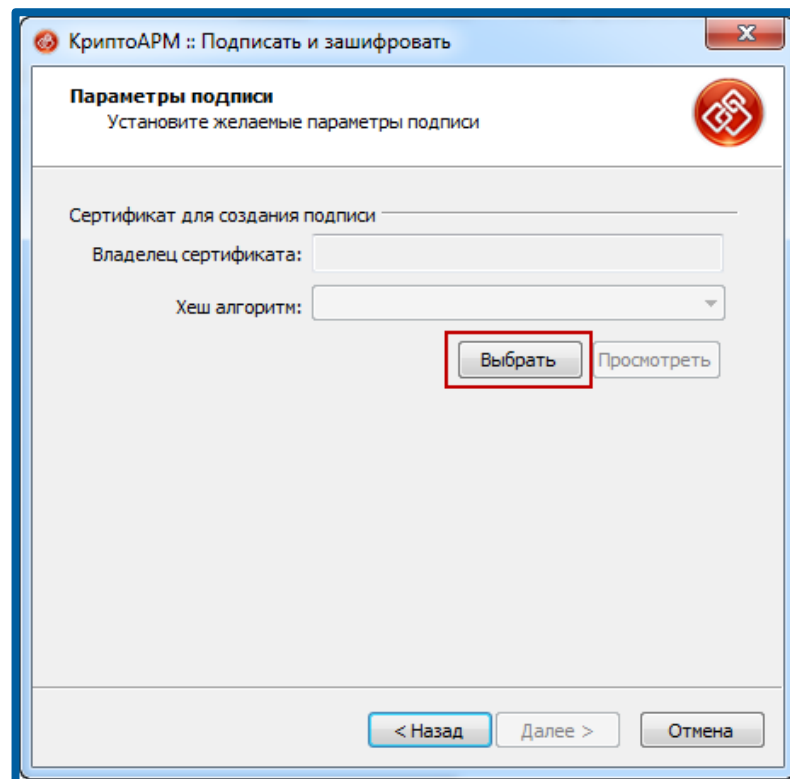


Рис. 6.

В хранилище сертификатов выберите требуемый сертификат и нажмите кнопку **ОК** (рис. 7.).

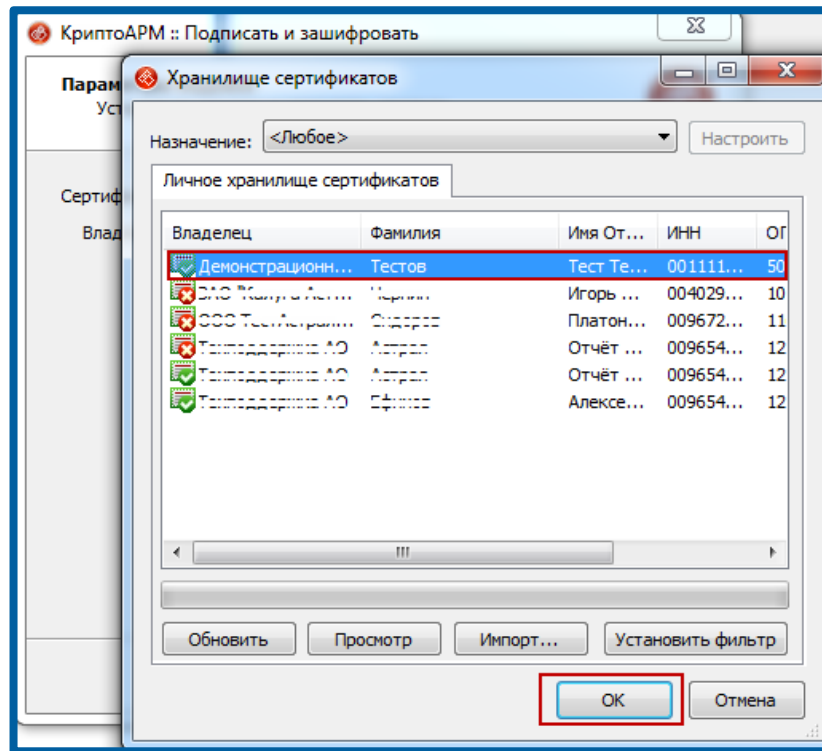


Рис. 7.

Убедитесь, что в поле «Владелец сертификата» указаны требуемые данные, и нажмите кнопку **Далее** (рис. 8).

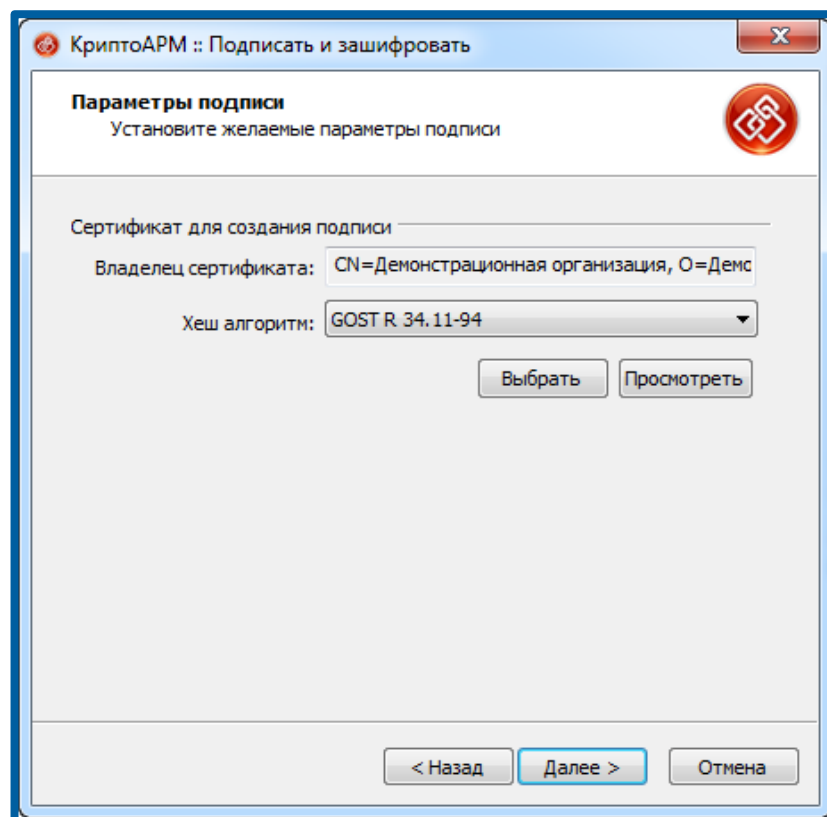


Рис. 8.

Установите переключатель «Кодировка и расширение» на значения **BASE64** и **Архивировать файлы перед шифрованием** (рис. 9.). Нажмите кнопку **Далее**.

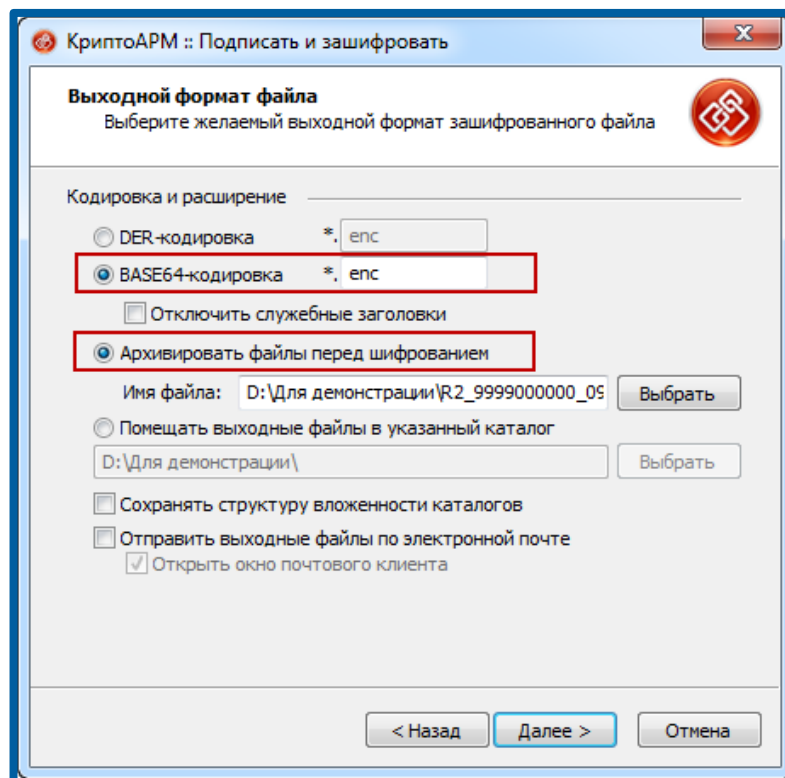


Рис. 9.

В следующем окне нажмите кнопку **Далее** (рис. 10.).

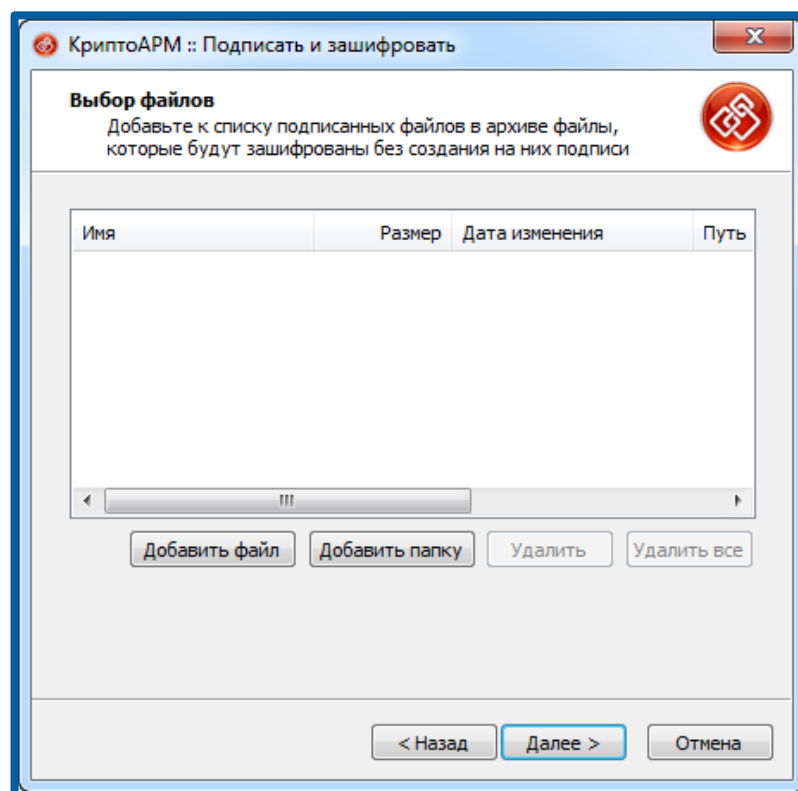


Рис. 10.

Убедитесь, что переключатель установлен на значении «Использовать криптопровайдер», и в строке «Тип криптопровайдера» выберите установленный криптопровайдер (рис. 11.). Нажмите кнопку **Далее**.

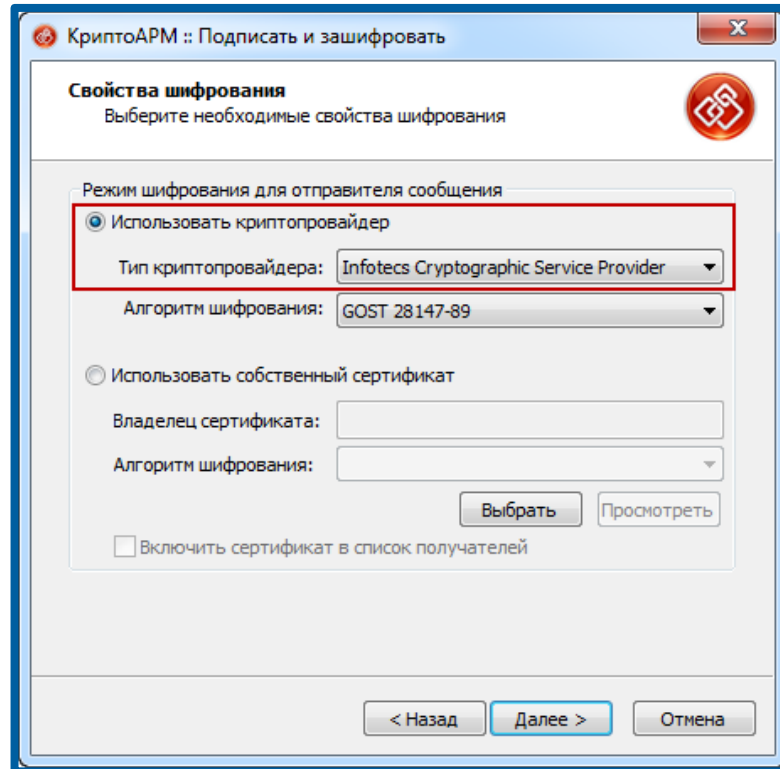


Рис. 11.

Выберите сертификат получателя нажав кнопку **Добавить** (рис. 12.).

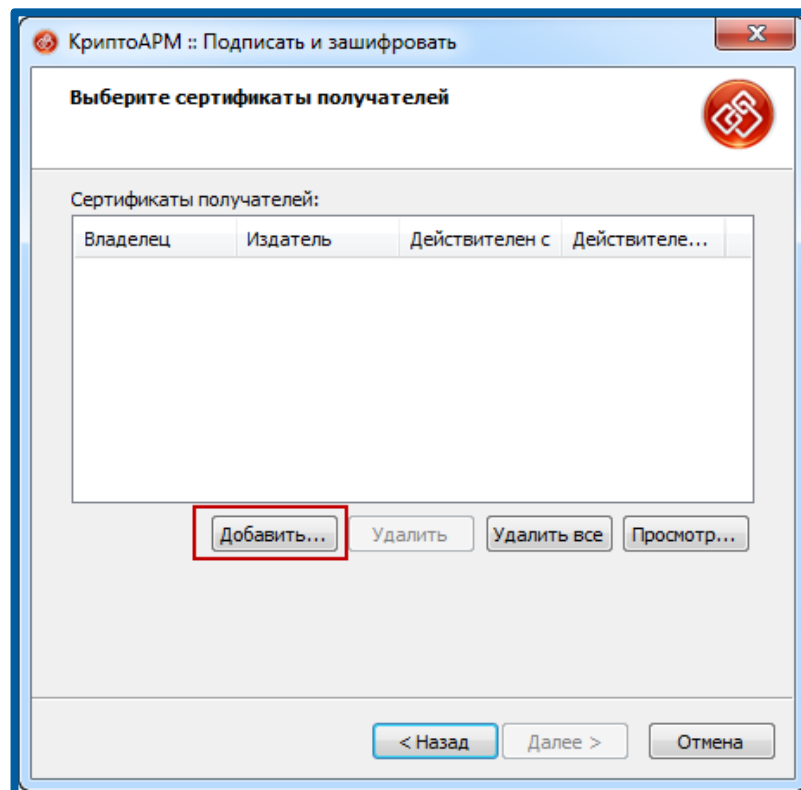


Рис. 12.

Перед Вами откроется окно **Хранилище сертификатов**. Перейдите на закладку **Сертификаты других пользователей**, выберите актуальный сертификат Росалкогольрегулирования и нажмите кнопку **Ок** (рис. 13.).

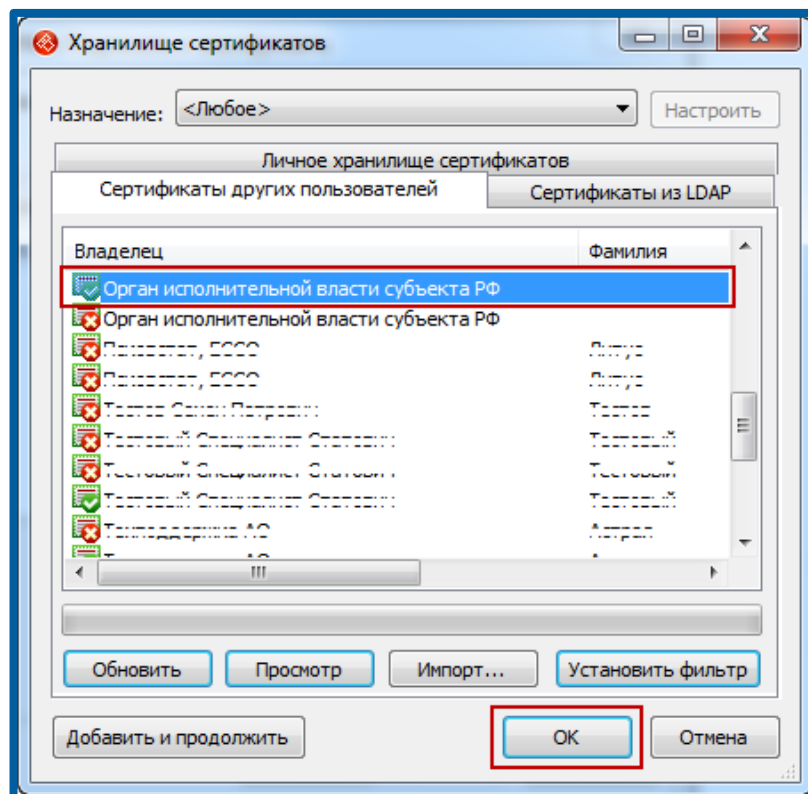


Рис. 13.



В случае отсутствия сертификата в закладке «Сертификаты других пользователей» импортируйте сертификат, нажав кнопку **Импорт** и укажите в Мастере установки сертификатов [сертификаты](http://fsrar.ru/Declaring/poryadok-predstavleniya-deklaracii) загруженные с сайта <http://fsrar.ru/Declaring/poryadok-predstavleniya-deklaracii>.

После отображения сертификата Росалкогольрегулирования в списке получателей нажмите кнопку **Далее** (рис. 14.).

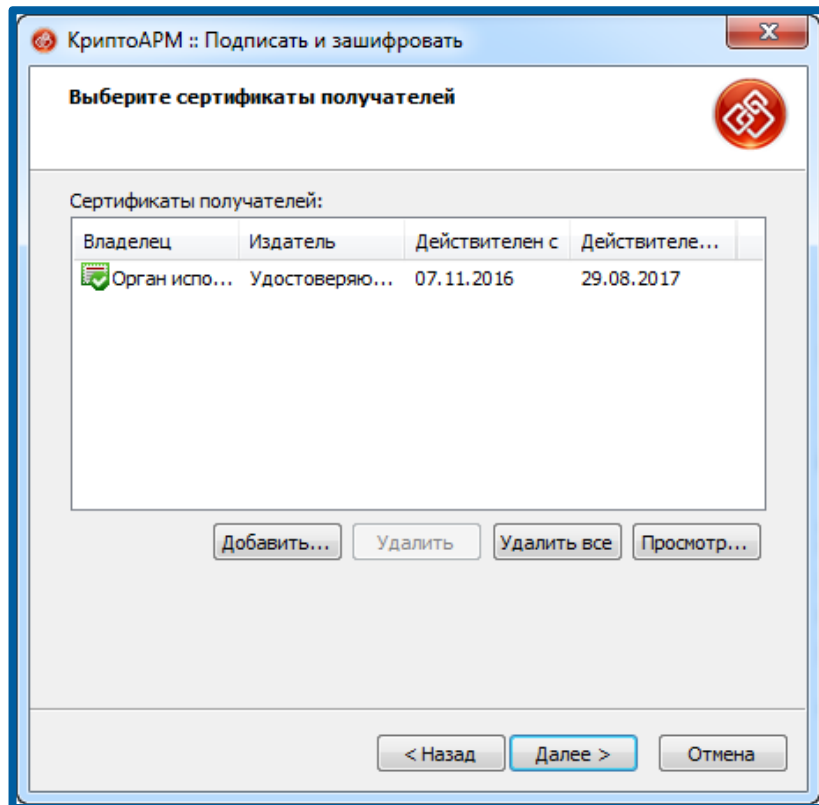


Рис. 14.

Перед Вами появится окно с результатами подготовки файла для подписания и шифрования. Нажмите кнопку **Готово** (рис. 15.).

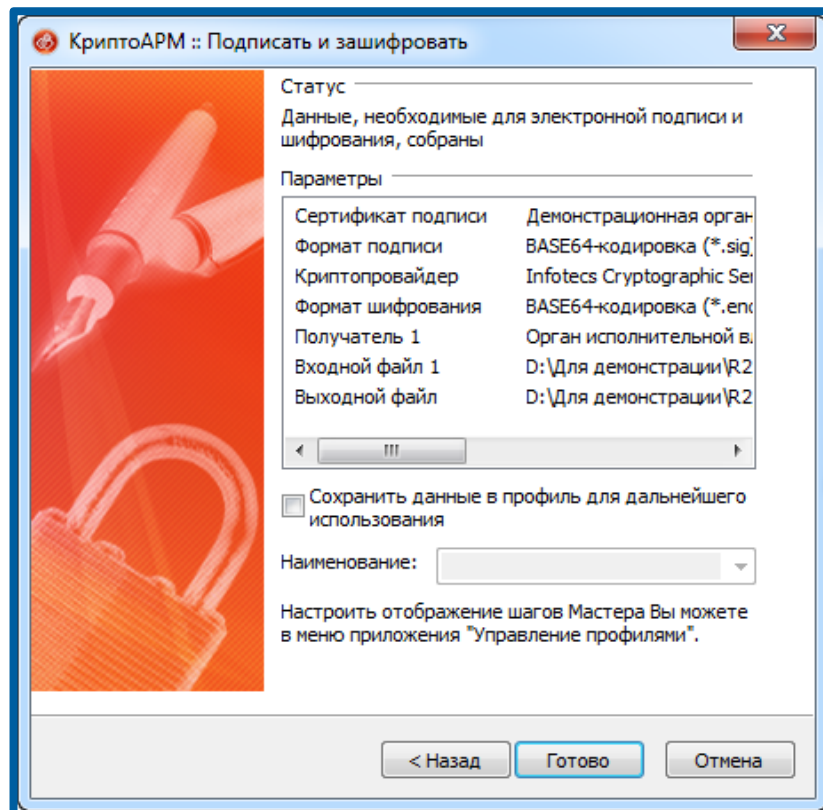


Рис. 15.

Будет ПИН-код ключевого носителя. В случае успешного завершения процесса подписи и шифрования отобразится окно вида (рис. 16.):

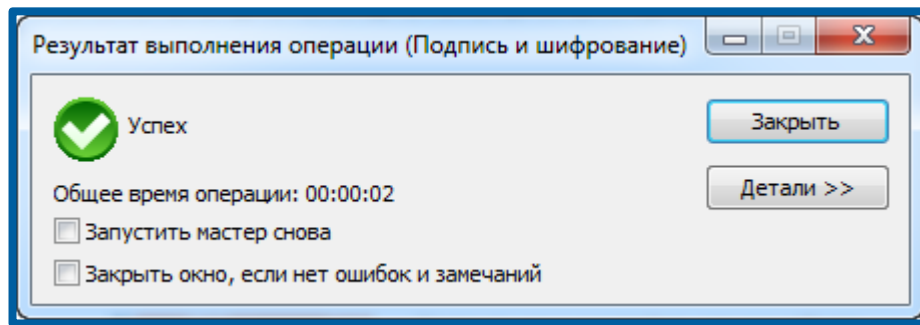


Рис. 16.

В каталоге отобразится новый файл с расширением [\*.xml.sig.zip.enc] (рис. 17.).

Имя	Дата изменения	Тип
R2_9999000000_099_22082014_87v8fd7g-3d3-456d-9027-6асес2с69386.xml	21.08.2017 8:58	Документ XML
R2_9999000000_099_22082014_87v8fd7g-3d3-456d-9027-6асес2с69386.xml.sig.zip.enc	22.08.2017 10:32	Сообщение MIM...

Рис. 17.

При начальном имени файла *R2\_9999000000\_099\_22082014\_87v8fd7g-3d3-456d-9027-6асес2с69386.xml* конечный файл будет иметь вид *R2\_9999000000\_099\_22082014\_87v8fd7g-3d3-456d-9027-6асес2с69386.xml.sig.zip.enc*. Расширение [\*.enc] может не отображаться в проводнике Windows, при этом тип файла всегда будет «Шифрованные данные».

Полученный файл передается в Росалкогольрегулирование через Личный кабинет на сайте <http://fsrar.ru/>.

## **Заключение**

В настоящем документе содержится информация по подписанию и шифрованию файлов для отправки в Росалкогольрегулирование. Подробную информацию по работе КриптоАРМ Вы можете получить на сайте <http://trusted.ru/support/downloads/>.