**Описание сервиса Росреестра**

**прямого доступа из сети Internet**

Версия 1.0

Содержание

[1. Оказываемые услуги 3](#_Toc324861044)

[2. Описание методов 3](#_Toc324861045)

[2.1 Метод createRequest 3](#_Toc324861046)

[2.1.1 Пример вызова метода 4](#_Toc324861047)

[2.1.2 Примеры формирования файла заявления 5](#_Toc324861048)

[2.2 Метод getEvents 5](#_Toc324861049)

[2.2.1 Пример вызова метода 7](#_Toc324861050)

[2.3 Метод loadEventDetails 7](#_Toc324861051)

[2.3.1 Пример вызова метода 7](#_Toc324861052)

[3. Основные технические решения 8](#_Toc324861053)

[3.1 Схема взаимодействия 8](#_Toc324861054)

[3.2 Обеспечение двусторонней аутентификации 9](#_Toc324861055)

[3.3 Требования к zip-архиву 9](#_Toc324861056)

[3.4 Требования к включению ЭЦП файлов в zip-архив 10](#_Toc324861057)

[3.5 Требования к формированию ЭЦП файла 10](#_Toc324861058)

[Приложение 1 11](#_Toc324861059)

[Приложение 2 12](#_Toc324861060)

[Приложение 3 18](#_Toc324861061)

[Приложение 4 19](#_Toc324861062)

# Оказываемые услуги

Веб-сервис прямого взаимодействия обеспечивает полный цикл оказания государственных услуг Росреестра в электронном виде (от подачи запроса и информирования заявителя о ходе исполнения услуги до предоставления результата оказания услуги в виде электронного документа). Поддерживаются следующие типы заявлений:

В части Государственного Кадастра Недвижимости (ГКН):

* Предоставление сведений государственного кадастра недвижимости о земельном участке в виде кадастрового паспорта объекта недвижимости;
* Предоставление сведений государственного кадастра недвижимости о земельном участке в виде кадастровой выписки;
* Предоставление сведений государственного кадастра недвижимости о территории в пределах кадастрового квартала в виде кадастрового плана территории;
* Постановка на государственный кадастровый учет земельного участка;
* Постановка на государственный кадастровый учет объекта капитального строительства.

В части Единого Государственного Реестра Прав на объекты недвижимого имущества и сделок с ним:

* Предоставление выписки из ЕГРП о правах отдельного лица;
* Предоставление выписки из ЕГРП о зарегистрированных правах на объект недвижимого имущества (земельные участки и объекты капитального строительства).

Описание методов, реализующих функции приема заявления, информирования заявителя о ходе исполнения услуги, предоставления результата оказания услуги приведено в последующих разделах настоящего документа.

# Описание методов

Веб-сервис предоставляет следующие методы:

* CreateRequest – создание заявления;
* GetEvent – предоставление информации о статусе заявления;
* LoadEventDetails – получение информации о результатах выполнения услуги;

Для проведения интеграционных работ следует использовать тестовую площадку: <https://stage-ext.fccland.ru:4433/cxf/External?wsdl>.

Сервис, находящийся в промышленной эксплуатации находится по адресу: <https://portal.rosreestr.ru:4433/cxf/External?wsdl>.

Для доступа к площадкам необходимо иметь установленный контейнер с ключевой парой, с помощью которой устанавливается SSL соединение с сервером.

## Метод createRequest

Метод предназначен для регистрации заявления (запроса) в информационной системе поставщика Росреестра (таблица 1).

|  |  |  |
| --- | --- | --- |
| **Параметр** | **Тип** | **Описание** |
| region | IN | Регион, в который необходимо отправить заявление |
| okato | IN | ОКАТО |
| oktmo | IN | ОКТМО, не обязательный |
| requestData | IN | Пакет заявления. Шифрованный zip-файл |
| requestType | IN | Тип запроса. См. справочник dRequestType.xsd |
| requestNumber | OUT | Номер запроса |
| status | OUT | Статус операции. Тип OperationStatus |

Таблица 1

IN – входной параметр

OUT – выходной параметр

Описание типа OperationStatus приведено в таблице 2:

|  |  |  |
| --- | --- | --- |
| **Параметр** | **Тип** | **Описание** |
| result | boolean | Результат выполнения |
| message | string | Необязательный. Описание, в случае если result==false |

Таблица 2

### Пример вызова метода

|  |  |
| --- | --- |
| **Наименование услуги** | **Примеры запросов/ответов** |
| Предоставление сведений, содержащихся в Государственном Кадастре Недвижимости |  |
| Предоставление сведений, содержащихся в Едином Государственном Реестре прав на недвижимое имущество и сделок с ним |  |

*Примечание: архив* ***sources.zip*** *содержит исходные файлы документов, по которым сформирован пример запроса.*

### Примеры формирования файла заявления

|  |  |
| --- | --- |
| **Наименование услуги** | **Примеры заявлений** |
| Пример формирования запроса в ЕГРП о правах отдельного лица. |  |
| Пример формирования запроса в ЕГРП о правах на объект недвижимости. |  |
| Предоставление сведений государственного кадастра недвижимости о земельном участке в виде кадастрового паспорта объекта недвижимости. |  |
| Предоставление сведений государственного кадастра недвижимости о земельном участке в виде кадастровой выписки. |  |
| Предоставление сведений государственного кадастра недвижимости о территории в пределах кадастрового квартала в виде кадастрового плана территории. |  |
| Постановка на государственный кадастровый учет земельного участка |  |
| Постановка на государственный кадастровый учет объекта капитального строительства |  |

## Метод getEvents

Получение статуса обработки заявления по запросу реализуется методом getEvents.

Описание метода приведено в таблице 3:

|  |  |  |
| --- | --- | --- |
| **Параметр** | **Тип** | **Описание** |
| lastEventID | IN | уникальный идентификатор последнего события, от которого вернется список. либо если необходимо получить все события   * пустая строка * null |
| events | OUT | коллекция структуры EventStruct |
| status | OUT | Статус операции. Типа OperationStatus |

Таблица 3

Описание структуры OperationStatus приведено в таблице 2.

Описание структуры EventStruct приведено в таблице 4:

|  |  |  |
| --- | --- | --- |
| **параметр** | **тип** | **описание** |
| eventID | string | уникальный идентификатор события |
| eventType | string | тип события   * STATUS * OUTDOC * RECEIPT |
| eventDate | dateTime | время записи события |
| requestNumber | string | номер заявки, к которой относится событие |

Таблица 4

Разработанные компоненты предусматривают возможности:

* получения единичного статуса по заявлению (актуального на определенный момент времени);
* получения истории смены всех статусов с момента создания заявления.

В случае присвоения параметру lastEventID значения «null» или пустого значения, возвращается весь список событий (статусов) по заявлению. В противном случае возвращаются данные по последнему статусу.

### Пример вызова метода

|  |  |
| --- | --- |
| **Наименование запроса** | **Примеры запросов/ответов** |
| Получить статус события по заявлению (актуального на определенный момент времени) |  |
| Получить историю смены статусов по всем событиям |  |

## Метод loadEventDetails

Предоставление результатов исполнения услуги осуществляется вызовом метода loadEventDetails.

Описание метода приведено в таблице 5:

|  |  |  |
| --- | --- | --- |
| **Параметр** | **Тип** | **Описание** |
| eventID | IN | уникальный идентификатор события |
| detailsXML | OUT | Детальное описание события   * Status.xsd * Receipt.xsd * Outdoc.xsd |
| binary | OUT | В случае событий   * RECEIPT * OUTDOC  Бинарный файл в base64.  В случае события * STATUS  будет null |
| status | OUT | Статус операции. Типа OperationStatus |

Таблица 5

### Пример вызова метода

|  |  |
| --- | --- |
| **Наименование события** | **Примеры запросов/ответов** |
| Событие STATUS |  |

# Основные технические решения

## Схема взаимодействия

Разработанные программные средства соответствуют общей архитектуре решения по взаимодействию с внешними информационными системами. Логическая схема взаимодействия компонент представлена на Рисунке 1.

Рисунок 1

1. Клиент обращается для формирования выписки из Единого государственного реестра прав, Государственного кадастра недвижимости или постановки земельного участка на Государственный кадастровый учет. Происходит двусторонняя аутентификация.
2. Формируется запрос при помощи метода CreateRequest.
3. Каждому заявлению присваивается идентификационный номер, который сообщается клиенту (в xml запросе соответствует строка <Number>).

В случае сбоя, в ответ на вызов метода поступит сообщение об ошибке.

1. Запрос клиента проходит форматно-логический контроль (ФЛК).

Если форматно-логический контроль не пройден, система формирует сообщение об ошибке, с указанием причины ее возникновения. Результат прохождения ФЛК клиент может узнать вызвав метод getEvents, либо loadEventDetails.

1. Если клиент имеет право на безвозмездное получение услуги, то заявление переходит в статус «В работе», минуя шаг оплаты.
2. В случае, если клиент получает услугу на платной основе, то заявление переходит в статус «Ожидает оплаты». Формируется уникальный код платежа. Данный код содержится в текстовом комментарии к статусу «Ожидает оплаты» и может быть получен вызовом методов getEvents, либо loadEventDetails.

Платеж должен быть совершен через платежные организации, принявшие условия публичной оферты Росреестра. Список таких организаций расположен по адресу: http://portal.rosreestr.ru/wps/portal/cc\_ib\_oferta?param\_infoblock\_document\_path=infoblock-root/cc\_ib\_oferta/perechen.htm

Информация о совершении платежа поступает в Росреестр автоматически. После получения подтверждения платежа (обычно на следующий рабочий день после платежа) заявление переходит в статус «В работе».

1. Заявление обрабатывается в региональной Учетной Системе (в соответствии с установленными нормативной документацией сроками, для большинства услуг – 5 дней).
2. Сформированный ответ на заявление клиент может получить при помощи метода предоставления результатов услуг (метод LoadEventDetails).

## Обеспечение двусторонней аутентификации

При взаимодействии ИС Росреестра с внешними ИС посредством веб-сервисов применяется двусторонняя аутентификация на основе сертификатов, соответствующих ГОСТ. Тестовые ключи представлены в Приложении 1. Для получения ключей предназначенных для взаимодействия в продуктивной среде необходимо обратиться в один из доверенных удостоверяющих центров Росреестра, с перечнем доверенных УЦ можно ознакомиться на портале Росреестра по ссылке - <http://portal.rosreestr.ru/wps/portal/cc_ib_UC>.

Для реализации данного функционала применяется системное ПО Trusted TLS.  Trusted TLS позволяет использовать российские стандарты криптографической защиты информации. Trusted TLS предназначен для построения систем, использующих сертифицированные ФСБ (ФАПСИ) СКЗИ, в прикладной системе, где есть необходимость в создании защищенного соединения между клиентом и сервером.

Для реализации двусторонней аутентификации на базе сертификатов, соответствующих ГОСТ в системе предусмотрен следующий алгоритм:

1. Клиент запрашивает доступ к защищенному ресурсу, в ответ сервис отправляет клиенту свой сертификат;
2. Клиент проверяет полученный сертификат по следующим параметрам:
   1. Текущая дата находится между датами начала и окончания действия сертификата;
   2. Издатель сертификата находится в списке доверенных удостоверяющих центров клиента;
   3. Сертификат отсутствует в списках отозванных сертификатов.
3. При положительном результате выполнения проверок описанных в шаге 2, клиент пересылает сервису свой сертификат, который проходит аналогичную проверку на стороне поставщика;
4. При негативном результате проверки клиентского сертификата, доступ к сервису будет запрещен. В случае успешной проверки, устанавливается защищенное соединение. Данные между клиентом и сервисом передаются в зашифрованном виде (данные от клиента шифруются приватным ключом клиента и открытым ключом сервиса, от сервиса – наоборот).

## Требования к zip-архиву

Имя файла: req\_<GUID\_пакета>.zip

GUID\_пакета имеет вид xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

Состав:

* xml-файл с данными заявления (req\_<GUID\_заявления>.xml), расположенный в корне архива;
* файл подписи заявления (req\_<GUID\_заявления>.xml.sig);
* также может содержать файлы электронных документов (межевые планы, технические паспорта, сканы документов) и образы приложенных документов, которые могут находиться на любом уровне вложенности в архиве, в таком случае пути должны быть прописаны в xml-файле заявления (req\_<GUID\_заявления>.xml). Если к заявлению добавляются дополнительные файлы, их можно шифровать. Такая процедура необязательна и применяется в случае необходимости. Более подробно процедура ручного шифрования файлов описана в [Приложении 2](#_Приложение_2._Инструкция) (Инструкция по шифрование файла запроса).
* Для формирования корректного пакета заявления следует руководствоваться соответствующей типу запрашиваемой услуги XSD схемой. XSD схемы для различных типов услуг приведены в таблице ниже:

| **Наименование услуги** | **Описание XSD схемы** |
| --- | --- |
| Предоставление сведений, содержащихся в Государственном Кадастре Недвижимости |  |
| Предоставление сведений, содержащихся в Едином Государственном Реестре прав на недвижимое имущество и сделок с ним |  |

## Требования к включению ЭЦП файлов в zip-архив

Все файлы, входящие в zip-архив, подписываются ЭЦП.

ЭЦП файла формируется по правилам, указанным в п. 5.

ЭЦП включаются в zip-архив в виде отдельных файлов, каждый из которых располагается в том же каталоге/подкаталоге, что и подписываемый файл, причем имя файла подписи получается из имени подписываемого файла с расширением добавлением расширения .sig

## Требования к формированию ЭЦП файла

ЭЦП передаются при помощи контейнера PKCS #7 (RFC 2315, <http://www.ietf.org/rfc/rfc2315.txt>).

Для сохранения в файл используется DER-кодировка.   
ЭЦП передаются в виде структуры ContentInfo со структурой SignedData в качестве содержимого. ЭЦП должна включать в себя сертификат и не должна включать подписанное содержимое.

Контейнер PKCS #7 должен быть совместим с контейнером, формируемым криптопровайдером КриптоПро CSP версии 3.6 (<http://www.cryptopro.ru/CryptoPro/documentation>).

# Приложение 1

**Тестовые сертификаты**

Сертификат, обеспечивающий двустороннюю аутентификацию и подписание заявления.

Данные сертификата:

Паспорт:

Серия: 1111

Номер: 111111

Дата выдачи: 11.11.2011



Сертификат, предназначенный для подписания технического плана помещения



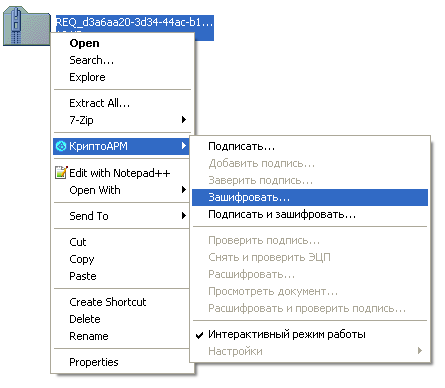
# Приложение 2

**Инструкция по ручному шифрованию файла запроса.**

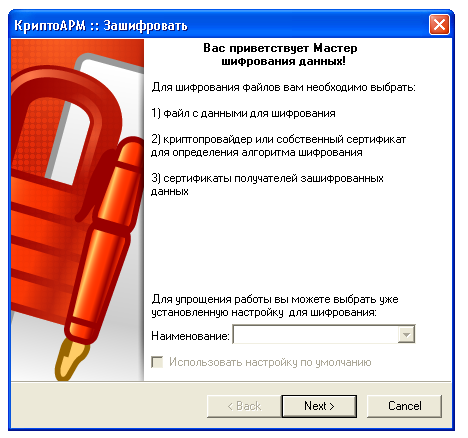
После того как получен zip архив для отправки, его необходимо зашифровать.

Далее будет представлен пример шифрования файла *REQ\_d3a6aa20-3d34-44ac-b119-3c5514980907.zip*, который можно посмотреть в п. [2.1.1](#_Пример_вызова_метода) .

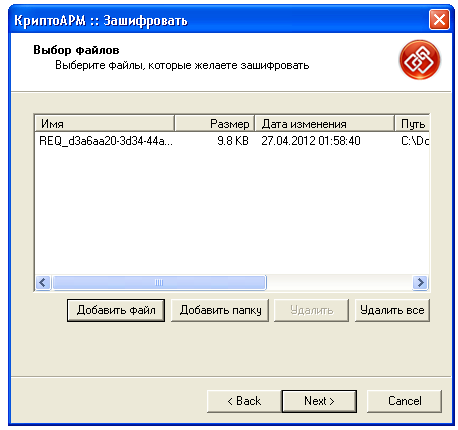
1. Вызываем выпадающее меню на файле, который необходимо зашифровать:



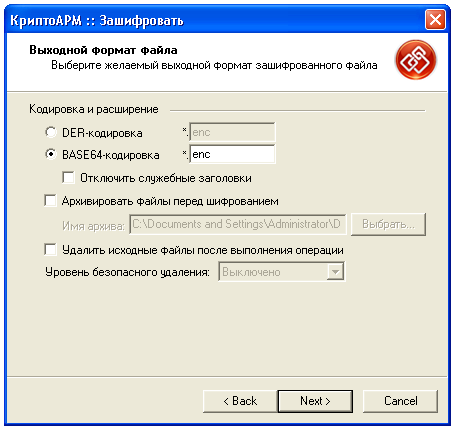
1. Появляется приветственное окно, нажимаем Next



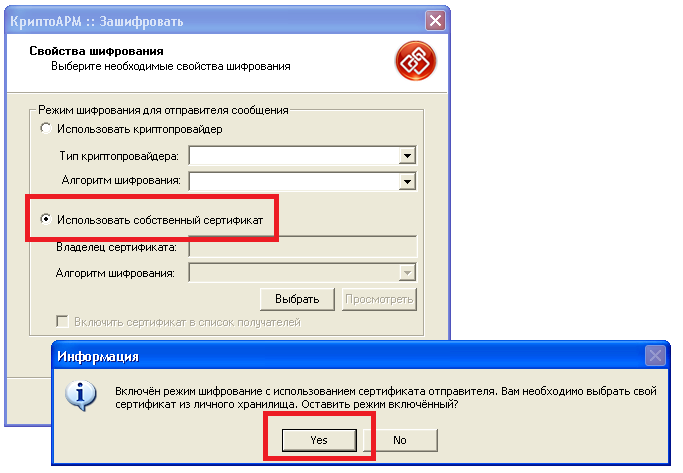
1. Нажимаем Next

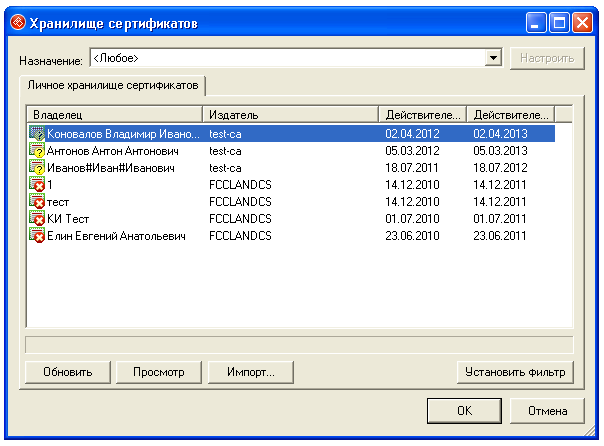


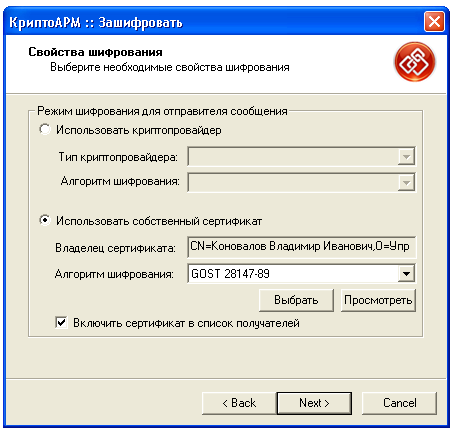
1. Нажимаем Next



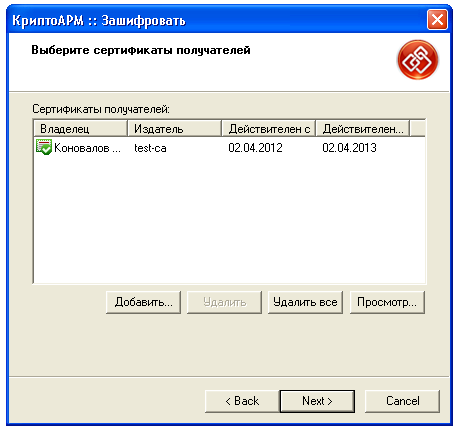
1. Выбираем «Использовать собственный сертификат».  
   Важно: сертификат должен быть заранее добавлен в хранилище сертификатов.



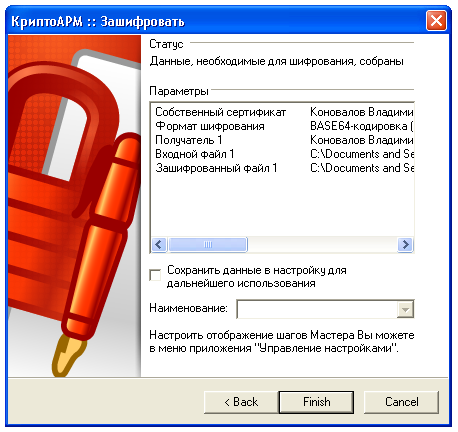
1. Выбираем сертификат, с помощью которого необходимо зашифровать файл
2. Нажимаем Next



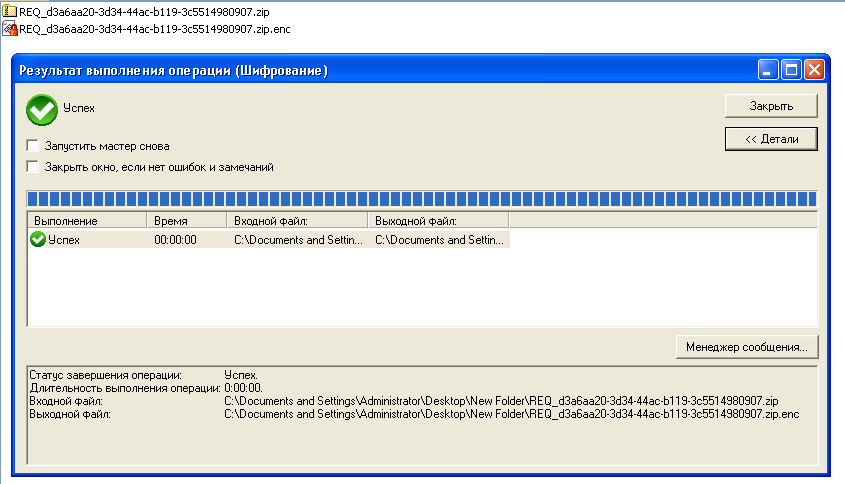
1. Нажимаем Next



1. Нажимаем Finish



1. Рядом появляется ваш зашифрованный файл с расширением .enc



# Приложение 3

**Получение сертификата из приватных ключей.**

1. Запускаем КриптоПро CSP
2. Выбираем закладку "Сервис" и далее "Посмотреть сертификат в контейнере"
3. На появившейся форме кликаем "Обзор"
4. Выбираем контейнер на съемном носителе и жмем "Ок". Далее "Next"
5. В появившейся форме жмем "Свойства" и нам открывается содержимое сертификата
6. Инсталлируем сертификат. Жмем "Install Certificate..."
7. В форме "Certificate Import Wizard" жмем на первом шаге "Next". Далее оставляем автоматическое определение и жмем "Next". Потом "Finish". Закрываем все окна кроме криптопровайдера.
8. Открываем реестр сертификатов. Можно с помощью меню. Программы -> КриптоПро -> Сертификаты
9. Открываем список персональных сертификатов в дереве консоли. Корень консоли -> Сертификаты - текущий пользователь -> Personal -> Registry -> Certificates
10. Выбираем только что установленный сертификат, правой кнопкой мыши вызываем на нем контекстное меню, далее All Tasks -> Export...
11. В визарде "Certificate Export Wizard" жмем "Next", оставляем пункт "не экспортировать ключи", жмем "Next", оставляем кодировку DER, жмем "Next". Указываем путь куда сохраняем и имя файла, например C:\cert.cer и жмем "Next", а потом "Finish".
12. Удаляем сертификат из реестра. Для этого выделяем его в консоли, правой кнопкой мыши вызываем на нем контекстное меню и далее пункт "Delete"

# Приложение 4

**Создание тестовых наборов.**

Для формирования тестовых наборов данных необходим стартовый набор, который впоследствии можно будет клонировать по определенным правилам:

1. Пример стартового набора состоит из трёх фалов:  
   GKUZU\_17e4efc4-ff95-42cb-8141-3c4d18c0aff1.xml - межевой план  
   RFile1.tif - образ межевого плана  
   RFile1.tif.sig - подпись к образу межевого плана
2. В названии файла GKUZU\_17e4efc4-ff95-42cb-8141-3c4d18c0aff1.xml, меняем три последних символа на любое значение, например **001**:

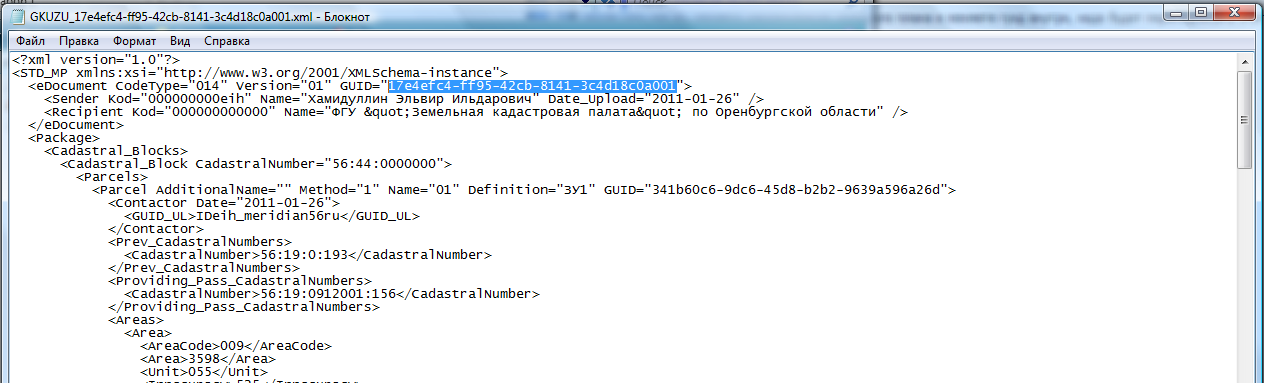
* исходное наименование: GKUZU\_17e4efc4-ff95-42cb-8141-3c4d18c0a**ff1**.xml
* новое наименование: GKUZU\_17e4efc4-ff95-42cb-8141-3c4d18c0a**001**.xml

все последующие наборы можно именовать - 002, 003 и т.п.).

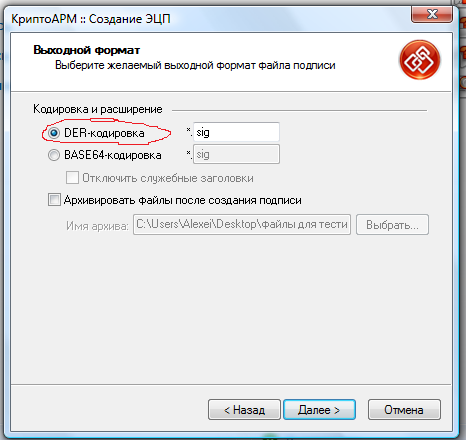
Получаем имя:

GKUZU\_17e4efc4-ff95-42cb-8141-3c4d18c0a**001**.xml

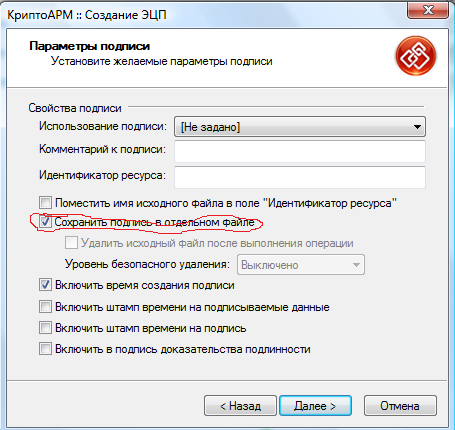
1. Изменяем атрибут GUID в файле GKUZU\_17e4efc4-ff95-42cb-8141-3c4d18c0a001.xml на значение соответствующее новому наименованию файла.

****Значение внутри xml и наименование файла обязательно должны совпадать

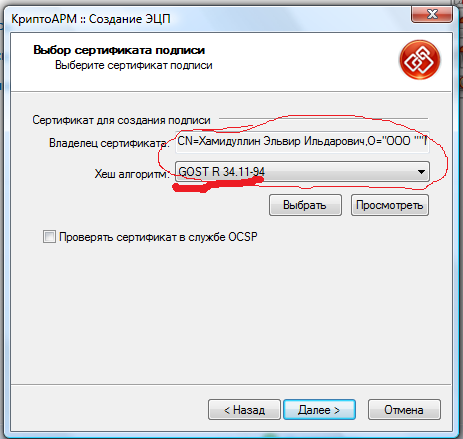
1. Файлы RFile1.tif RFile1.tif.sig можно оставить без изменений, их можно использовать сколь угодно много раз.
2. Необходимо создать файл подписи для вновь сформированного файла межевого плана GKUZU\_17e4efc4-ff95-42cb-8141-3c4d18c0a001.xml. Для этого запускаем КриптоАрм, выбираем опцию «Подпись», далее «Подписать» и следуем пошаговым инструкциям. При этом важно указать выходной формат подписи – DER



1. Указать необходимость использования отдельного файла подписи.



1. Выбрать сертификат кадастрового инженера и проверить что выбран хеш алгоритм – GOST.



1. Получится новый тестовый набор, который состоит из четырёх файлов:  
   ***GKUZU\_17e4efc4-ff95-42cb-8141-3c4d18c0a001.xml.sig – подписанный межевой план, полученный на предыдущем шаге.*** *GKUZU\_17e4efc4-ff95-42cb-8141-3c4d18c0a001.xml - межевой план  
   RFile1.tif - образ межевого плана  
   RFile1.tif.sig - подпись к образу межевого плана*

Таким образом, можно формировать неограниченное количество наборов, выполняя описанные выше шаги.