УТВЕРЖДАЮ
Генеральный директор
ООО «Кейсистемс»
_____ А. А. Матросов
«___» _____ 2018 г.

ПРОГРАММНЫЙ КОМПЛЕКС «БЮДЖЕТ-СМАРТ»

ВЕРСИЯ 18.04

Руководство пользователя

Электронный обмен документами с применением электронно-цифровой подписи

ЛИСТ УТВЕРЖДЕНИЯ

Р.КС. 02120-01 32 02-3-ЛУ

СОГЛАСОВАНО
Заместитель генерального директора
ООО «Кейсистемс»
_____ Е. В. Фёдоров
«___» _____ 2018 г.
Руководитель ДПиРСИБ

_____ Д. В. Галкин
«___» _____ 2018 г.

2018

Литера А

Подп и дата	
Инв.N дубл	
Взам.инв.N	
Подп и дата	
Инв.N подл	

УТВЕРЖДЕНО
Р.КС. 02120-01 32 02-3-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС «БЮДЖЕТ-СМАРТ»

ВЕРСИЯ 18.04

Руководство пользователя

Электронный обмен документами с применением электронно-цифровой подписи

Р.КС. 02120-01 32 02-3-ЛУ

Листов 29

Подп и дата	
Инв.N дубл	
Взам.инв.N	
Подп и дата	
Инв.N подл	

2018

Литера А

АННОТАЦИЯ

Настоящий документ является частью руководства пользователя программного комплекса «Бюджет-СМАРТ» (далее – «программный комплекс») версии 18.04 по автоматизации процесса проектирования, исполнения и анализа бюджетов субъектов Российской Федерации, закрытых автономно-территориальных образований и муниципальных образований.

Документ содержит описание ведения рабочего плана счетов в программном комплексе, формирования бухгалтерских записей и формирования регистров бюджетного учета.

Руководство актуально для указанной версии и для последующих версий вплоть до выпуска обновления руководства.

Порядок выпуска обновлений руководства

Выход новой версии программного комплекса сопровождается обновлением руководства пользователя только в случае наличия в версии значительных изменений режимов, описанных в руководстве, добавления новых режимов или изменения общей схемы работы. Если таких изменений версия не содержит, то остается актуальным руководство пользователя от предыдущей версии с учетом изменений, содержащихся в новой версии.

Перечень изменений версии программного комплекса содержится в сопроводительных документах к версии. Информация об изменениях руководства пользователя публикуется на сайте разработчика в разделе «Документация».

Информация о разработчике ПК «Бюджет-СМАРТ»

ООО «Кейсистемс»
Адрес: 428000, Чебоксары, Главпочтамт, а/я 172
Телефон: (8352) 323-323
Факс: (8352) 571-033
http://www.keysystems.ru
E-mail: info@keysystems.ru

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Настоящий документ является руководством пользователя и содержит описание операций по электронному обмену документами с применением электронно-цифровой подписи.

Электронная (цифровая) подпись (далее ЭЦП) предназначена для идентификации лица, подписавшего электронный документ, и является полноценной заменой собственноручной подписи. Представляет собой реквизит электронного документа, полученный в результате криптографического преобразования (шифрования) информации с использованием закрытого ключа.

Сервис оправдательных документов (ОД) устанавливается на сервере IIS. Применяется для прикрепления к документам сканов и т.п. файлов (так называемых оправдательных документов), а так же для применения режима «**Сохраненные отчеты**».

Обращается (подключается) к сервису ОД клиентское приложение, установленное на компьютере пользователя.

Уровень подготовки пользователя

Для успешного освоения материала, изложенного в руководстве пользователя, и формирования навыков работы в программном комплексе с описанными режимами к пользователю предъявляются следующие требования:

– наличие опыта работы с персональным компьютером на базе операционных систем Windows на уровне квалифицированного пользователя;

– умение свободно осуществлять базовые операции в стандартных приложениях Windows.

Условные обозначения

В документе используются следующие условные обозначения:

Уведомление	_	Важные сведения о влиянии текущих действий пользователя на выполнение других функций, задач программного комплекса.
Предупреждение	_	Важные сведения о возможных негативных последствиях действий пользователя.
Предостережение	_	Критически важные сведения, пренебрежение которыми может привести к ошибкам.
Замечание	_	Полезные дополнительные сведения, советы, общеизвестные факты и выводы.
[Выполнить]	_	Функциональные экранные кнопки.
<F1>	_	Клавиши клавиатуры.
«Чек»	_	Наименования объектов обработки (режимов).
Статус	_	Названия элементов пользовательского интерфейса.
ОКНА => НАВИГАТОР	_	Навигация по пунктам меню и режимам.
п. 2.1.1 *рисунок 5*	_	Ссылки на структурные элементы, рисунки, таблицы текущего документа.
[1]	_	Ссылки на документы из перечня ссылочных документов.

1. ОПИСАНИЕ ОПЕРАЦИЙ

1.1. Сервис оправдательных документов

Сервис оправдательных документов (ОД) устанавливается на сервере IIS. Применяется для прикрепления к документам сканов и т.д. файлов (так называемых оправдательных документов), а также для применения режима «**Сохраненные отчеты**». Режим позволяет хранить на сервисе оправдательных документов (ОД) любые отчеты и произвольные файлы.

К сервису ОД обращается (подключается) клиентское приложение, установленное на компьютере пользователя.

Версию сервиса можно определить:

- в проводнике Windows в свойствах DLL ...\wwwroot\UploadService\Bin\Keysystems.UploadService.dll;
- в браузере, набрав адрес http://<адрес сервиса ОД до каталога >/**uploadservice.ashx**/GetServiceVersion. Если такой адрес не открывается, то, скорее всего, версия сервиса устарела и его следует обновить.

Пример адреса: http://ksws/UploadService/uploadservice.ashx/GetServiceVersion.

После установки сервиса необходимо убедиться в предоставлении полных прав на папку uploads\ для пользователя IIS, от имени которого выполняется пул UploadService. Пользователя по умолчанию можно сменить в web.config в разделе <system.web> , поле <identity userName =...>. Пользователь по умолчанию - IIS_IUSRS, это встроенная группа, используемая службами IIS (с Win7, ранее IIS_WPG).

Если в свойствах пула приложений сервиса ОД (если у него персональный пул приложений) указать учетную запись LocalSystem, то у сервиса ОД будут права на чтение/запись по любому локальному пути (в пределах сети, в которой расположен компьютер IIS).

С версии сервиса 3.2 и выше **настройки конфигурации** сервиса находятся в файле **UploadService.config** *(ранее было в Web.config)*.

Для обновления сервисов предпочтительно использовать утилиту Server Manager . В случае применения нескольких каналов (адресов) подключения к IIS (основной и резервный), рекомендуем применять параметр UseAppServiceHost в файле конфигурации сервиса приложений.

Лог сервиса находится по пути: <IIS_сервер>\wwwroot\UploadService\App_Data\LOGS\, если сервис установлен в папку по умолчанию UploadService\).

1.1.1. Порядок установки сервиса ОД

Для сервиса ОД рекомендуется создать свой отдельный пул приложений (*Рисунок 2*):

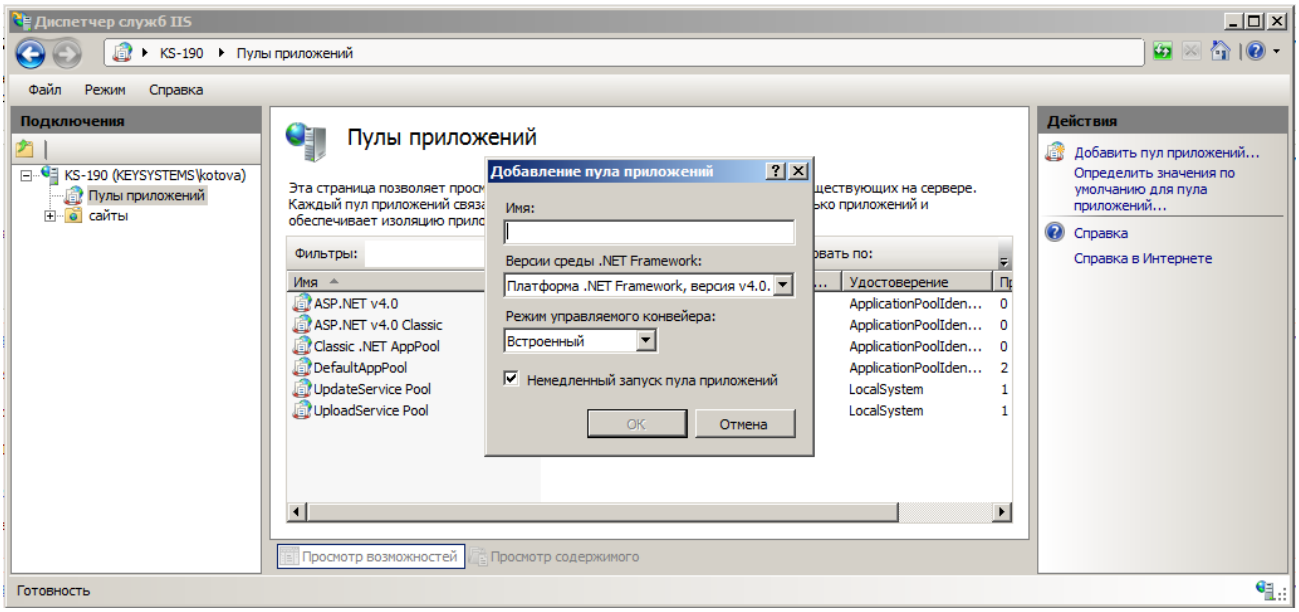

Рисунок 1. Настройка уровней пользователей

– развернуть сервис на IIS (см руководство по установке сервисов в папке manual\ дистрибутива комплекса);

– развернуть сервис на IIS (см. руководство по установке сервисов в папке manual\дистрибутива комплекса);

– выбрать способ хранения файлов оправдательных документов:
  - Хранилище файлов на сервере IIS (WEB сервер);
  - Хранилище файлов в базе данных (SQL сервер);
  - Хранилище файлов на выделенном сервере (файл сервер).

– Настроить применение сервиса. Группа настроек для указания способа и места размещения файлов первичных документов (сканы, текстовые документы и т.п.), а так же отчетов (режим «**Сохраненные отчеты**»). Первичные документы обычно прикрепляются в режиме списка документов по кнопке **Оправдательные документы**, либо принимаются электронно одновременно с платежными поручениями.

Перечень настроек:

– **Хранилище** (на пользователя) – место хранения ОД. Возможные значения:

• Не используется – хранение ОД не применяется, кнопка работы с ОД в списке документов неактивна, режим «**Сохраненные отчеты**» не работает.

• WEB-сервер – хранилище управляется специализированным сервисом первичных/оправдательных документов (сервис ОД), развернутом на сервере IIS. Адрес к сервису задается в настройке «**Адрес сервиса**». При включении настройки «**Проверить ЭЦП на сервисе первичных документов**» проверка ЭЦП как документов, так и ОД осуществляется средствами сервиса ОД, что увеличивает производительность комплекса.

• SQL-сервер – хранилище организовано в отдельной базе данных. Имя базы задается в настройке «**Имя базы данных**».

• Файл сервер – хранилище организовано на сетевом диске в заданной папке. Путь задается в настройке «**Путь к каталогу**». Данное хранилище применимо только для локальных пользователей комплекса.

– **WEB-хранилище**:

- Шаблон пути первичного документа – путь хранения прикрепляемых оправдательных документов хранилища. В результате применения настройки файлы в хранилище первичных документов будут располагаться по пути: {uploads}\{шаблон}\<дата в формате yyyymmdd>\<имя файла ОД>. Где {uploads} – папка uploads\ сервиса ОД; {шаблон} - значение данной настройки. В настройке указывается строка, содержит элементы, разделенные символом '\'. Элемент может быть как обычным именем папки, так и выражением в угловых скобках <> вида:

<database> - имя базы

<user> - имя пользователя

<yyyymmdd> - текущая дата в заданном формате. Содержит в любой комбинации буквы 'y', 'm', 'd' и символ '.' (точка). Здесь формат: yyyy - 4 цифры года, mm - 2 цифры месяца, dd - 2 цифры числа. Другой вариант использования: <dd.mm.yyyy> или <yyyy> и т.д. Так же в качестве разделителя кроме символа "." (точка) можно использовать "-" (тире) и "_" (подчеркивание). Значение настройки по умолчанию: <yyyy>\<user>. Если настройка не задана, то используется имя пользователя <user>.

- Адрес сервиса (на пользователя) – путь к сервису первичных/оправдательных документов (сервис ОД). Требуется установленный сервис оправдательных документов. Настройка на пользователя, например, удаленным пользователям, задается внешний адрес, а пользователям локальной сети – локальный адрес.

В случае применения нескольких каналов (адресов) подключения к IIS (основной и резервный), рекомендуем применять параметр UseAppServiceHost в файле конфигурации сервиса приложений.

Пример значения для внешних пользователей: http://mf.chuv.ru/UploadService/UploadService.svc.

Пример значения для локальных пользователей к тому же сервису ОД: http://serveriis/UploadService/UploadService.svc, где serveriis - имя компьютера, на котором развернут сервис ОД.

- Тип аутентификации – способ проверки подлинности пользователя к сервису ОД (определяется настройками IIS);
- Учетные данные (имя, пароль) – логин и пароль для подключения к сервису ОД (если требуется).

– **SQL-хранилище**:

- Имя базы данных – база данных SQL, в которой будут храниться ОД. Формат значения: <имя_SQL_сервер>.<имя_базы> . Имя SQL сервера может содержать символ "\". База должна иметь определенную структуру, для ее создания применяется специальный скрипт. Пример значения настройки: xandra\2000.fstorage_jpg , где "xandra\2000" - имя SQL сервера, "fstorage_jpg" - имя базы данных.

– **Файловое хранилище**:

- Путь к каталогу – путь к каталогу (обычно сетевой) хранения ОД. Путь не должен содержать символов «пробел». Пример значения настройки \\xenix\bks\jpg_pp\ .SQL-хранилище:

– **Общие:**

- Максимальный размер файла – ограничение на размер файлов ОД, в байтах. Значение «**0**» или пусто означает «**без ограничений**». Пример значения: 10485760 - ограничение в 10 МБ.
- Расширение файлов – перечень, через запятую или точку с запятой, масок разрешенных расширений файлов ОД. Значение «*» или пусто означает «без ограничений» (любое расширение). Для каждого расширения через двоеточие можно указать максимальный размер в байтах. Пример значения: pdf,jp*,bmp:2097152,png - разрешены файлы вида *.pdf, *.jpg, *.jpeg, *.bmp, *.png , причем для bmp установлено ограничение в 2МБ.

1.1.2. Проблемы при установке сервиса ОД

Проблемы, возникающие при установке сервиса ОД:

– Нет связи с сервисом первичных документов: Detail: connect failed in tcp_connect()

Стандартная ошибка подключения по сети. Возникает в случаях:

1. Клиент не может соединиться с сервисом:

– Неправильно прописан адрес в настройке на пользователя;

– Файрволлы прокси, антивирусы запрещают подключение по определенному протоколу;

– Неверно настроена маршрутизация.

2. Сервис не может скачать первичные документы с сетевого диска. Причины аналогичные *пункту 1*, также возможная причина: ОС компьютера, где реально лежат файлы ОД, не серверная и имеет ограничение на 10 одновременных подключений.

– Файлы ОД не открываются на просмотр.

Иногда возникают случаи, когда отдельные первичные файлы успешно прикрепляются к документам, но не могут открыться на просмотр пользователями. Рекомендуется убедиться, что в настройках IIS расширения этих файлов входят в список типов MIME.

1.2. Электронная (цифровая) подпись

Использование ЭЦП позволяет:

– осуществить контроль целостности подписанного документа – при любом случайном или преднамеренном изменении документа ЭЦП станет недействительной. Таким образом, документ защищен от изменений (подделки).

– идентифицировать владельца сертификата ключа подписи (автора подписи) - так как создать корректную подпись можно, лишь зная закрытый ключ, а он есть только у владельца ЭЦП (сертификата).

При наложении ЭЦП (после выбора сертификата) проверяется срок до окончания действия сертификата согласно настройке «**Период напоминания о завершении срока сертификата (дни)**». Если согласно настройке срок подходит к концу, то выводится окно сообщения с предупреждением о скором прекращении действия сертификата. Сообщение не выдается, если в настройке «идентификатор ключа» установлен конкретный серийный номер сертификата (#1234 5678 ...).

Настройка параметров работы с электронно-цифровой подписью выполняется администратором комплекса. Все настройки, связанные с ЭЦП, сгруппированы в отдельный каталог:

КОРНЕВОЙ КАТАЛОГ НАСТРОЕК => НАСТРОЙКИ => ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ

1.2.1. Очередность наложения ЭЦП

Важность ЭП определяется её очередностью, очередность в свою очередь задается для уровней ЭЦП. Для упрощения рекомендуем важность ЭЦП коррелировать с её уровнем, т.е. чем выше должность пользователя, тем более высокий уровень ЭЦП ему присваивается, по умолчанию в комплексе 5 уровней.

Если применяется автомат ЭЦП, то последовательность наложения ЭП задается в нём.

Иначе в порядке возрастания уровня, с учетом настройки (*Рисунок 2*):

НАСТРОЙКИ => НАСТРОЙКИ => ЭЛЕКТРОННАЯ ПОДПИСЬ => НАСТРОЙКА УРОВНЕЙ ПОЛЬЗОВАТЕЛЕЙ

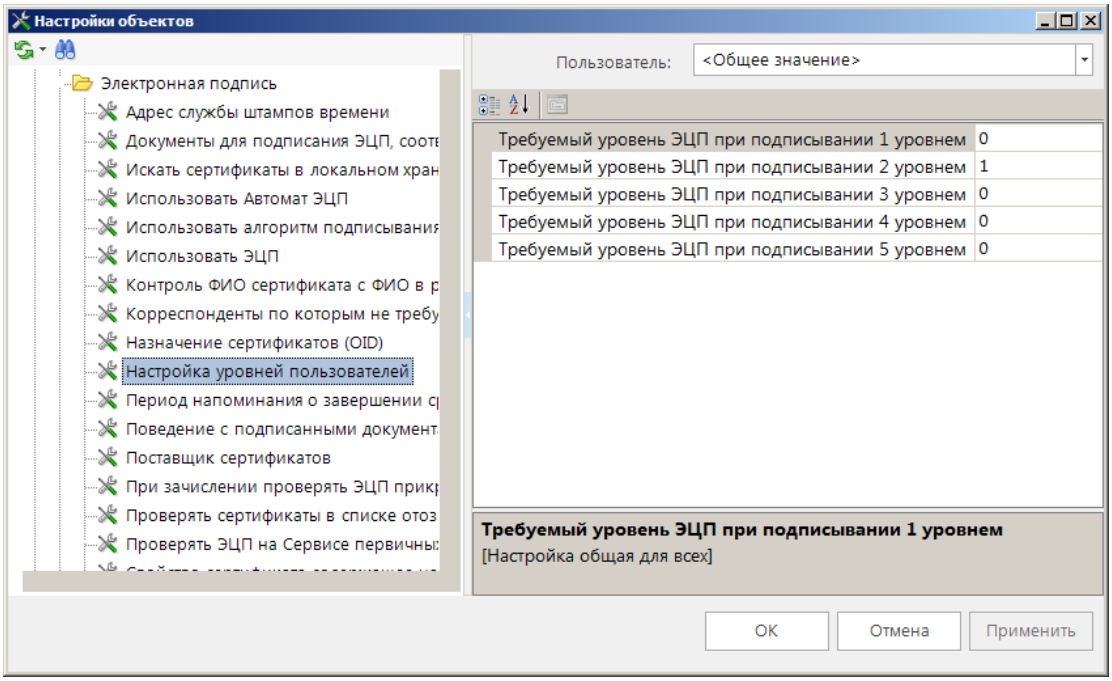

Рисунок 2. Настройка уровней пользователей

И если настройка не задана (нулевые значения), то требуется накладывать ЭЦП в порядке возрастания уровней, начиная с 1. Т.е. невозможно подписать документ пользователю с уровнем 2, пока на документе отсутствует ЭЦП с уровнем 1, и т.д.

1.2.2. Контроль корректности ЭЦП

При наложении ЭЦП проводится комплекс проверок: актуальность (не отозван ли), срок действия, математическая корректность, наличие в локальном хранилище, соответствие OID и т.п.

Наличие в локальном хранилище проверяется по следующим значениям: при значении «**Да**» подписать документы можно будет только сертификатами пользователей, установленными на том же компьютере, что и сервис ОД по проверке ЭЦП, причем в хранилище «локальный компьютер» (реестр windows). Рекомендуемое значение «**Нет**».

Назначение сертификатов (OID): данная настройка применяется в случаях неоднозначного определения сертификата для наложения ЭЦП, например, когда на компьютере клиента установлено несколько сертификатов с одинаковым идентификатором (обычно ФИО пользователя). В этом случае в данной настройке прописывается OID политики нужного сертификата, что позволит ПК «Бюджет-СМАРТ» однозначно идентифицировать сертификат для наложения ЭЦП. Допускается задание нескольких значений, разделенных через запятую.

Политики применения сертификата OID - политики, которые содержат информацию о содержании у субъекта сертификата, который может быть использован для определенных задач. Они (политики) представлены в сертификате OID, который определяет данную политику. Этот OID включается в выпущенный сертификат пользователя. Когда субъект (пользователь) предоставляет сертификат, сертификат может быть рассмотрен на подтверждение политики применения и определения может ли субъект выполнить запрошенные действия.

За счет ограничения политик применения, определенных в шаблоне сертификата, сертификат не может быть использован для неподходящих действий. В сертификате OID представляет собой набор цифр (*Рисунок 3*).

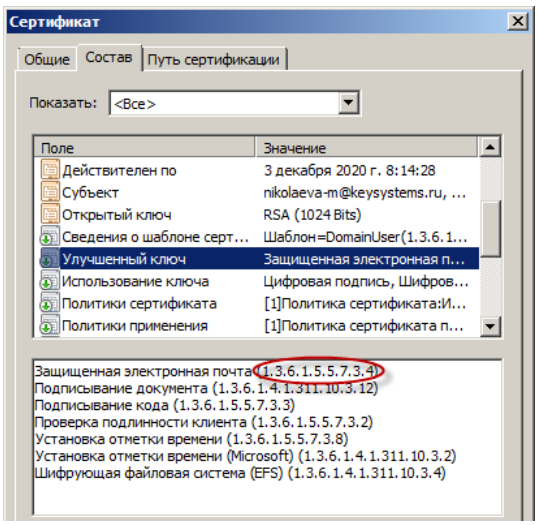

Рисунок 3. Состав сертификата OID

При просмотре (по кнопке **Электронная подпись**) и переводе в беловики наличие сертификата в локальном хранилище не проверяется.

Просмотр ЭЦП осуществляется в списке документов по кнопке **Электронная подпись**, открывается список всех ЭЦП, наложенных на документ с указанием статуса подписи (верна/не верна) с описанием статуса ЭЦП. Также указывается организация - принадлежность подписанта организации. В общем случае это информация из поля «О» сертификата, если в сертификате значение для тега <O> не задано, то берется организация логина по привязке группы, в которую входит логин, к организации согласно дереву групп в меню «**Администратор групп**».

В списке ЭЦП по кнопке **Расширенная информация ЭЦП** открывается отчет в виде протокола с информацией о статусе ЭЦП (математическая достоверность и результат проверки на отзыв), реквизитах сертификата (сроки, кому, организация, издатель и т.п.) (*Рисунок 4*).

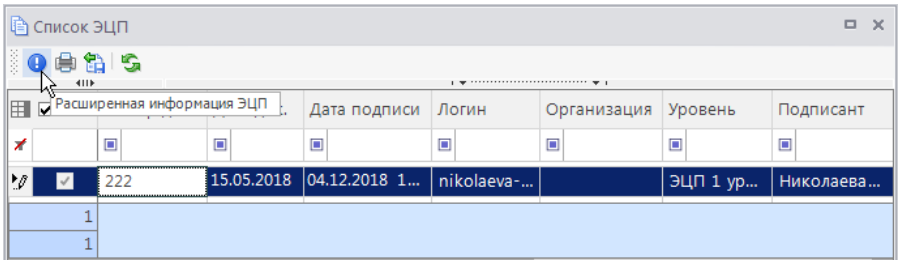

Рисунок 4. Расширенная информация ЭЦП

1.2.3. Выяснение причин неверной ЭЦП

Если при просмотре ЭЦП по кнопке **Электронная подпись** выдается состояние «подпись неверна», то для выяснения причины проделать следующее:

1. В режиме списка ЭЦП по кнопке **Расширенная информация ЭЦП** получить протокол с полной информацией о статусе ЭП и параметрах сертификата (*Рисунок 5*).

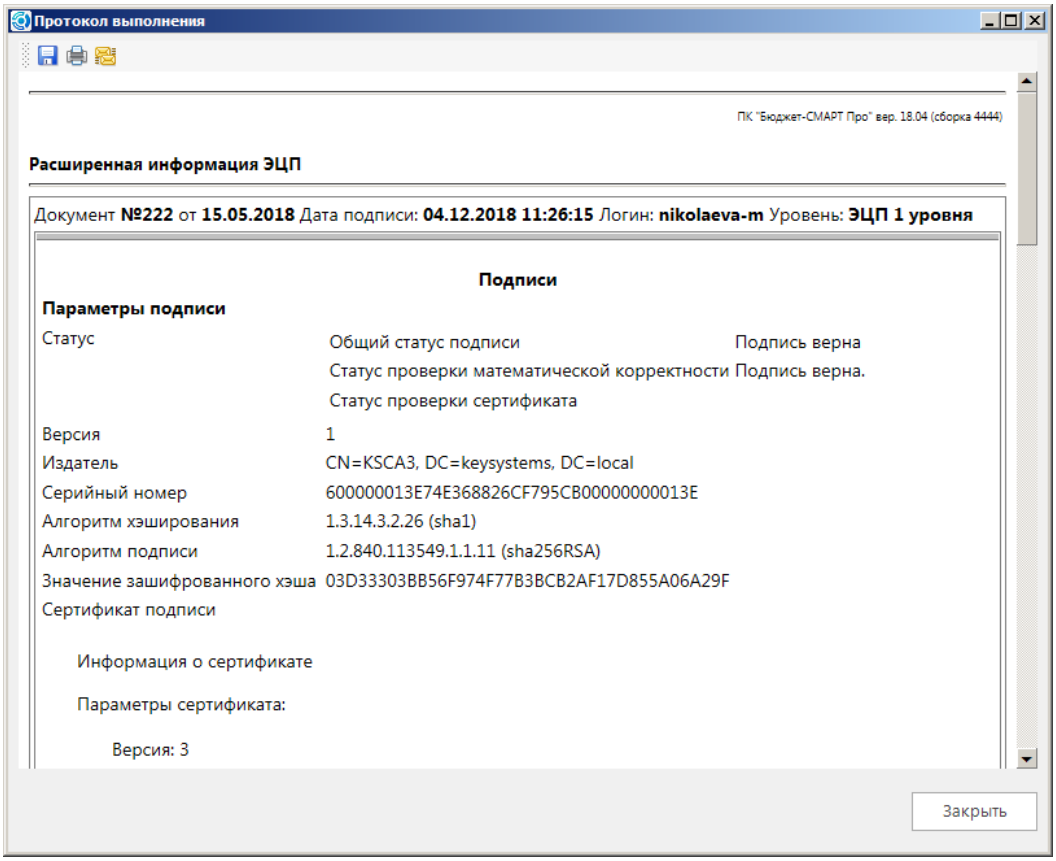

Рисунок 5. Протокол с указанием информации о статусе ЭЦП

Параметры сертификата:

– Статус проверки математической корректности – проверка на внесение изменений в документ после наложения ЭП;

Подпись верна – документ в исходном состоянии;

Подпись не верна – документ изменен и не соответствует состоянию, в котором он был в момент наложения ЭП.

– Статус проверки сертификата – проверка действительности сертификата. Если ничего не указано, то сертификат не отозван.

Общий статус ЭП складывается из этих двух компонентов, и при проблемах с любым из них - математическая корректность и проверка сертификата - статус ЭЦП будет «**Не верна**».

2. Если возникли проблемы с математической корректностью, то для выяснения причины следует получить три файла по кнопке **Передача** (*Рисунок 6*).

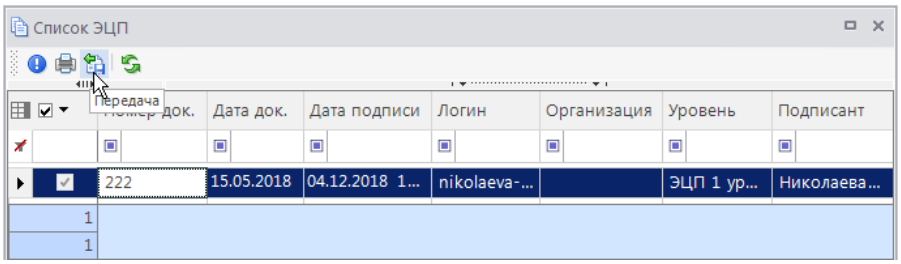

Рисунок 6. Передача файлов

- файл с расширением «.SIG» – подпись, для проверки сторонними приложениями;
- файл с именем «...._подписано.TXT» - текстовое представление реквизитов документа и их значений на момент наложения ЭП;

- Файл с именем «...._формируется.TXT» - текстовое представление реквизитов документа и их значений на текущий момент.

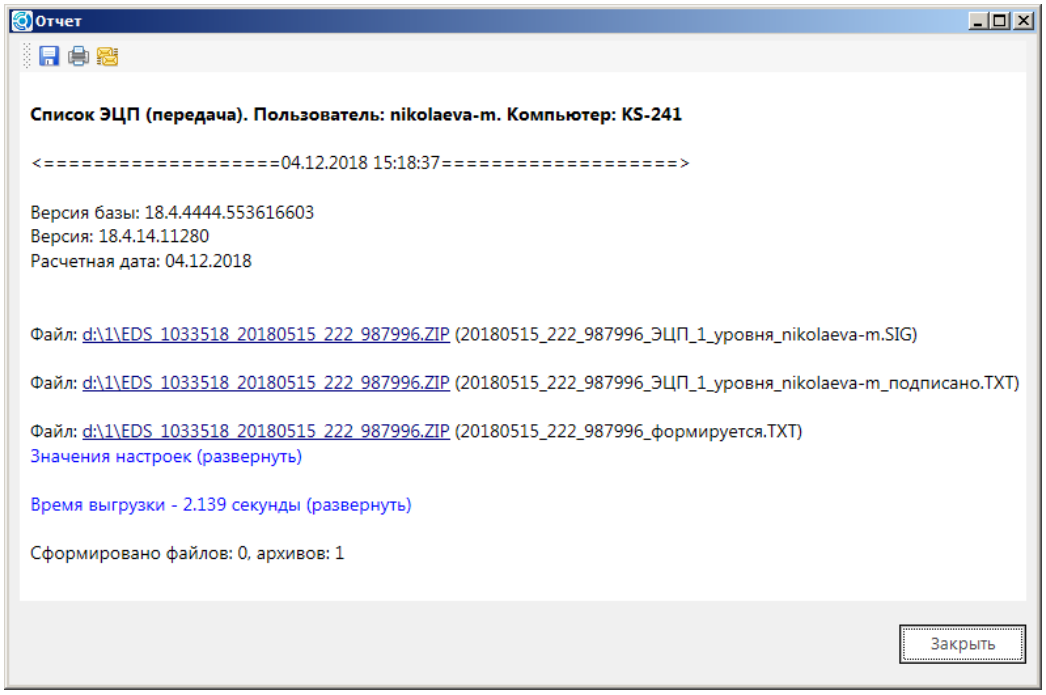

Рисунок 7. Отчет о передаче файлов

Два последних файла следует сравнить между собой и выявить реквизит, измененный с момента подписания.

3. Статус сертификата проверяется при включенной настройке (*Рисунок 8*).

НАСТРОЙКИ => НАСТРОЙКИ => ЭЛЕКТРОННАЯ ПОДПИСЬ => ПРОВЕРЯТЬ СЕРТИФИКАТЫ В СПИСКЕ ОТОЗВАННЫХ СЕРТИФИКАТОВ

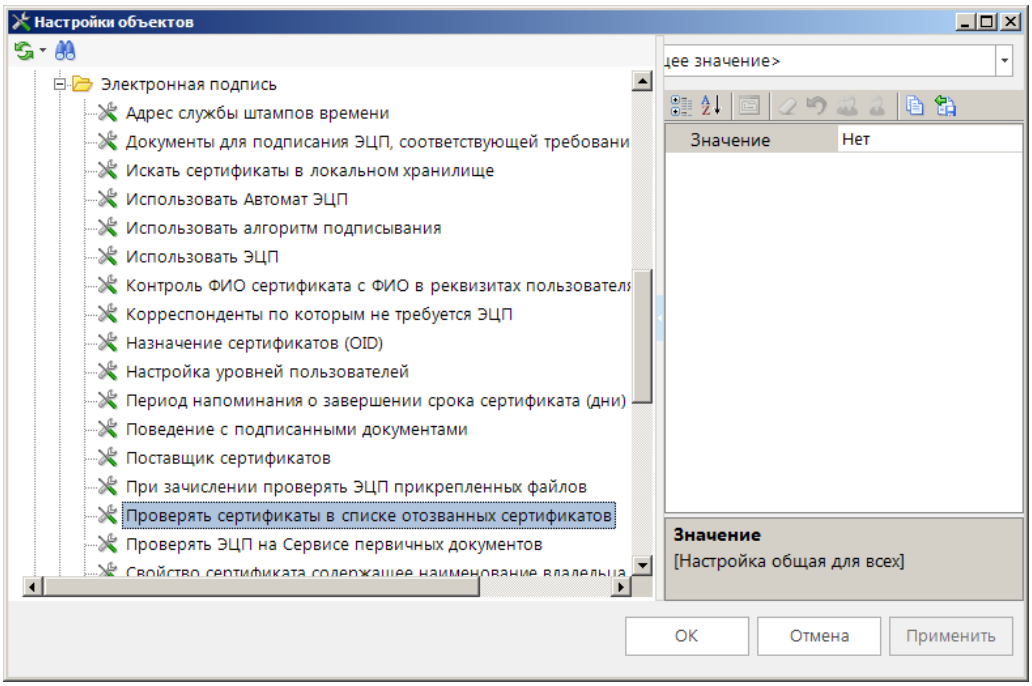

Рисунок 8. Настройка проверки сертификата

Если сертификат был отозван на момент проверки (хотя был действующим на момент наложения ЭЦП), или нет доверия к УЦ и т.д., то общий статус ЭП будет «не верна».

Срок действия сертификата учитывается на дату наложения ЭЦП, т.е. просроченный сертификат не влияет на статус сертификата, если на момент наложения ЭЦП он был действительным по срокам.

1.2.4. Способы наложения ЭЦП в комплексе

В ПК «Бюджет-СМАРТ» предусмотрены следующие способы наложения ЭЦП:

– Обычный – проверяется соответствие идентификатора сертификата и идентификатора логина пользователя, заданного в справочнике «Уровни ЭЦП»;

– С применением автомата ЭЦП – дополнительно проверяется соответствие накладываемой ЭЦП вариантам автомата ЭЦП.

Кнопка панели инструментов режима списка документов «***Просмотр/Установка ЭЦП***» отображается, если включена настройка (*Рисунок 9*).

НАСТРОЙКИ => НАСТРОЙКИ => ЭЛЕКТРОННАЯ ПОДПИСЬ => ИСПОЛЬЗОВАТЬ ЭЦП

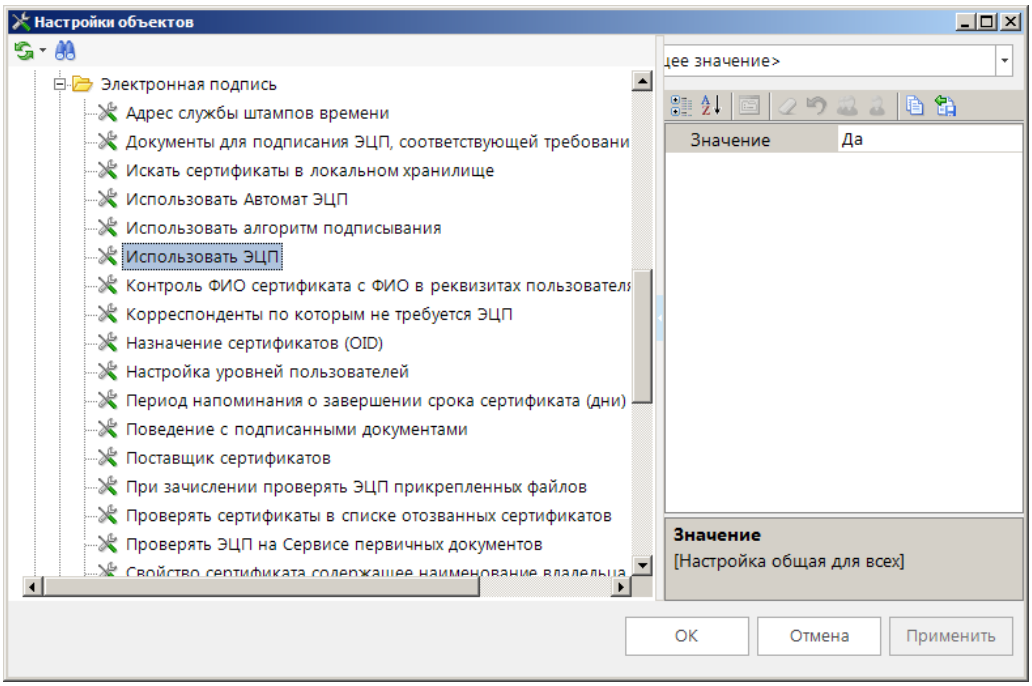

Рисунок 9. Настройка использования ЭЦП

1.2.5. Использование автомата ЭЦП

Настройка определяет, какой алгоритм наложения ЭЦП будет использоваться: по автомату ЭЦП либо по настройкам уровней.

Если включено использование автомата ЭЦП, но при наложении ЭЦП не будет найден вариант автомата для данного документа, то будет выведен протокол отказа с сообщением «Документ не удовлетворяет условиям схем работы с ЭП.».

Если какой-либо документ обрабатывается без применения ЭЦП, то для таких документов надо создать пустой вариант (без галочек на уровнях ЭЦП).

При применении автомата ЭЦП теряют значение (не анализируются) следующие настройки:

- Дерево настроек - НАСТРОЙКИ - Электронная подпись - Настройка уровней пользователей;
- Дерево настроек - НАСТРОЙКИ - Электронная подпись - Требовать необходимые уровни на своих документах при подписании;
- Черновик-<документ> - настройка - Требуемый уровень ЭЦП для зачисления документов;
- Дерево настроек - НАСТРОЙКИ \ Электронная подпись \ Типы счетов, по которым не требуется ЭЦП;
- Дерево настроек - НАСТРОЙКИ \ Электронная подпись \ Корреспонденты, по которым не требуется ЭЦП;
- Меню Настройки: НАСТРОЙКИ \ Электронная подпись \ При зачислении проверять ЭЦП прикрепленных файлов.

Вместо них используются параметры автомата ЭЦП, соответственно:

- Порядок расположения отмеченных галочками уровней ЭЦП в варианте;
- Настройка считается установленной в значении «Да»;
- При зачислении проверяется обязательность наличия ЭЦП всех уровней, отмеченных галочками в сработавшем варианте автомата ЭЦП;
- Условия к варианту автомата ЭЦП: «***Тип счета***», «***Тип организации***»
- Условие к варианту автомата ЭЦП «Подписываемый объект = Первичные документы». Если ОД не подписываются, то создать пустой вариант (без галочек на уровнях ЭЦП) с таким условием.

1.2.6. Требования к ЭЦП при зачислении

Если автомат ЭЦП не используется, то используются следующие настройки для уровней ЭЦП. Требуемый уровень ЭЦП для зачисления документов – настройка документов-черновиков, при зачислении (переводе в беловики) проверяется ЭЦП документа:

- Минус 1 – ЭЦП не обязательно, но при наличии обязано быть корректным. То есть, зачислены будут документы либо без ЭЦП, либо с корректными ЭЦП любых уровней;
- 0 – наличие корректного ЭЦП любого уровня обязательно;
- Больше нуля – обязательно наличие ЭЦП заданного уровня и его корректность.

Требуемый уровень ЭЦП первичных файлов для зачисления документов – настройка документов-черновиков, определяет обязательность ЭЦП на ОД и обязательность наличия самих ОД. Возможные значения:

- Минус 1 – ЭЦП на ОД не важна, но при наличии обязано быть корректным. ОД также необязательно;
- 0 – наличие корректного ЭЦП на ОД заданного уровня и его корректность. Наличие хотя бы одного ОД обязательно.

Эта настройка учитывается, если включена настройка при включении настройки

НАСТРОЙКИ => НАСТРОЙКИ => ЭЛЕКТРОННАЯ ПОДПИСЬ => ПРИ ЗАЧИСЛЕНИИ ПРОВЕРЯТЬ ЭЦП ПРИКРЕПЛЕННЫХ ФАЙЛОВ

Если пользователь включен в несколько уровней ЭЦП, то при использовании «**Автомата ЭЦП**» пользователь может подписать документ несколько раз (по количеству уровней) и все подписи будут разного уровня.

Перечень типовых ошибок, возникающих при наложении ЭЦП:

- Неизвестный криптографический алгоритм (800910002) – на компьютере не установлено приложение от криптовайдера, указанного в сертификате, которым осуществляется попытка наложения ЭЦП либо которым подписан документ (при проверке ЭЦП), см. свойство сертификата «**Алгоритм подписи**». Например, ПО от Крипто Про, если ключевая пара (открытый и закрытый) созданы по ГОСТ.
- Не удается найти указанный файл (00000002), возможные причины:
  - Сертификат установлен без закрытого ключа;
  - Рутокен (носитель с сертификатом) поврежден/неисправен;
  - Применяется (вставлен в компьютер) не тот рутокен (носитель) – не от выбираемого сертификата. Например, в период смены сертификатов используется прежний еще действующий сертификат, а носитель применяют от нового сертификата.
- Неизвестная ошибка (C000000D) – проблема в совместимости ПО «Крипто Про» и «Континент АП», способы решения см. на форумах соответствующих ПО. См. также обсуждение на форуме «Бюджет-СМАРТ» https://keysystems.ru/forum/index.php?showtopic=19187&p=157205.
- Статус аннулирование сертификатов не выявлен, не удалось загрузить список отозванных сертификатов – состояние (статус) ЭЦП.
- Не удается построить цепочку сертификатов для доверенного корневого центра (сообщение при наложении ЭЦП):
  - Корневой сертификат УЦ не соответствует сертификатам пользователей;
  - Корневой сертификат УЦ отсутствует на сервисе ОД/сервере ключей;
  - Корневой сертификат УЦ установлен неверно (местоположение не «локальный компьютер»/ реестр, см. описание «***Сервис проверки ЭЦП***»).

Корневой сертификат УЦ обычно обновляется ежегодно, на сервисе ОД должен быть установлен(-ы) корневой сертификат УЦ, под которым выдавались ключи пользователям.

Примеры ситуаций, приводящие к вышеприведенной ошибке: часть пользователей имеет ключи 2011 года, часть – 2012 года, установлен корневой сертификат 2012 года – пользователи с сертификатом 2011 года не смогут подписать документы с применением ЭЦП (либо их подпись станет неверна)

- Один из сертификатов в цепочке не является доверенным – причина в том, что корневой сертификат УЦ не установлен в список «***Доверенные корневые центры сертификации***» на компьютере, где проверяется ЭЦП (*Рисунок 10*):

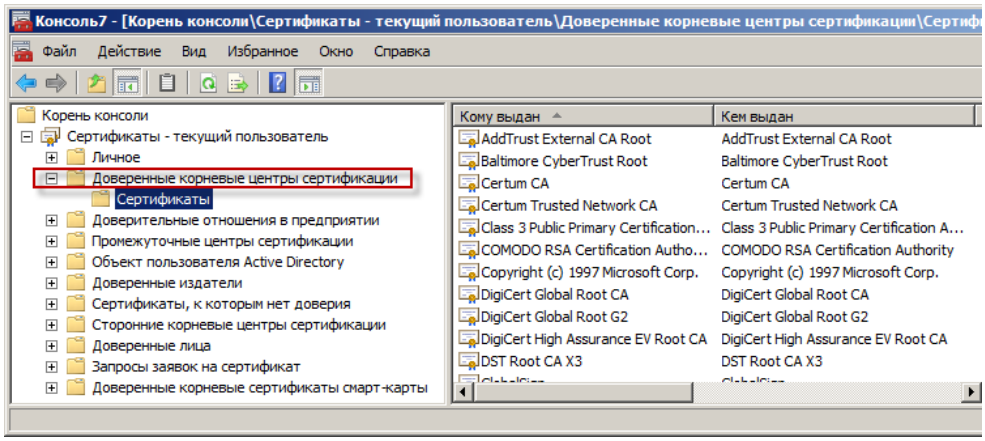

Рисунок 10. Доверенные корневые центры сертификации

– Документ не удовлетворяет условиям схем работы с ЭП – отсутствует подходящий вариант в автомате ЭЦП для данного документа. Если автомат не настраивался, то не следует включать настройку «**Использовать автомат ЭЦП**».

– Невозможно создать файл, так как он уже существует B7: CryptMsgUpdate – при установке сертификата на компьютер пользователя средствами Крипто Про был выбран неверный криптопровайдер в поле «**Выберите CSP для поиска ключевых контейнеров**».

– Возникла ошибка при соединении с сервисом проверки ЭЦП – настройка указана неверно (несуществующий адрес) либо SQL-сервер не может подключиться к сервису ОД из указанной настройки (ограничения сетевых экранов, антивирусы и т.п.)

НАСТРОЙКИ => НАСТРОЙКИ => ЭЛЕКТРОННАЯ ПОДПИСЬ => СЕРВИС ПРОВЕРКИ ЭЦП

– Cannot connect или Cannot resolve IP address или Error get version - при применении сервера ключей (устарело): данные сообщения означают, что не удалось обратиться к серверу ключей, неверно указана настройка сервера ключей, либо за сервера ключей не запущена программа проверки ЭЦП (CertServer.exe), либо не удалось соединиться с сервером ключей (антивирус, брандмауер и т.д.)

1.2.7. Проверка ЭЦП на сервисе первичных документов

Определение способа проверки ЭЦП:

– Нет – ЭЦП проверяется сервером ключей, это устаревший вариант, заморожен по состоянию на 2016 год.

– Да – ЭЦП любого объекта комплекса (документ, прикрепленный скан, сохраненный отчет) проверяется сервисом ОД, и сервер ключей не используется. Адрес сервиса первичных документов по проверке ЭЦП указывается в настройке «Сервис проверки ЭЦП».

Только при значении настройки «Да» возможен вывод в отчетных формах штампа ЭЦП.

Данная настройка временная и существует на период перехода к применению сервиса ОД версии 3.2 и выше. Рекомендуемое значение «**Да**» - увеличивает производительность комплекса ввиду отсутствия лишней пересылки ОД от сервиса ОД к серверу ключей: документы проверяются до 4 раз быстрее, ОД до 10 раз быстрее.

Для проверки ЭЦП сервисом оправдательных документов (ОД) требуется задать две настройки:

– Значение «Да»

НАСТРОЙКИ => НАСТРОЙКИ => ЭЛЕКТРОННАЯ ПОДПИСЬ => ПРОВЕРЯТЬ ЭЦП НА СЕРВИСЕ ПЕРВИЧНЫХ ДОКУМЕНТОВ

– Указание адреса сервиса ОД (*Рисунок 11*):

НАСТРОЙКИ => НАСТРОЙКИ => ПЕРВИЧНЫЕ ДОКУМЕНТЫ => ХРАНИЛИЩЕ ПЕРВИЧНЫХ ДОКУМЕНТОВ

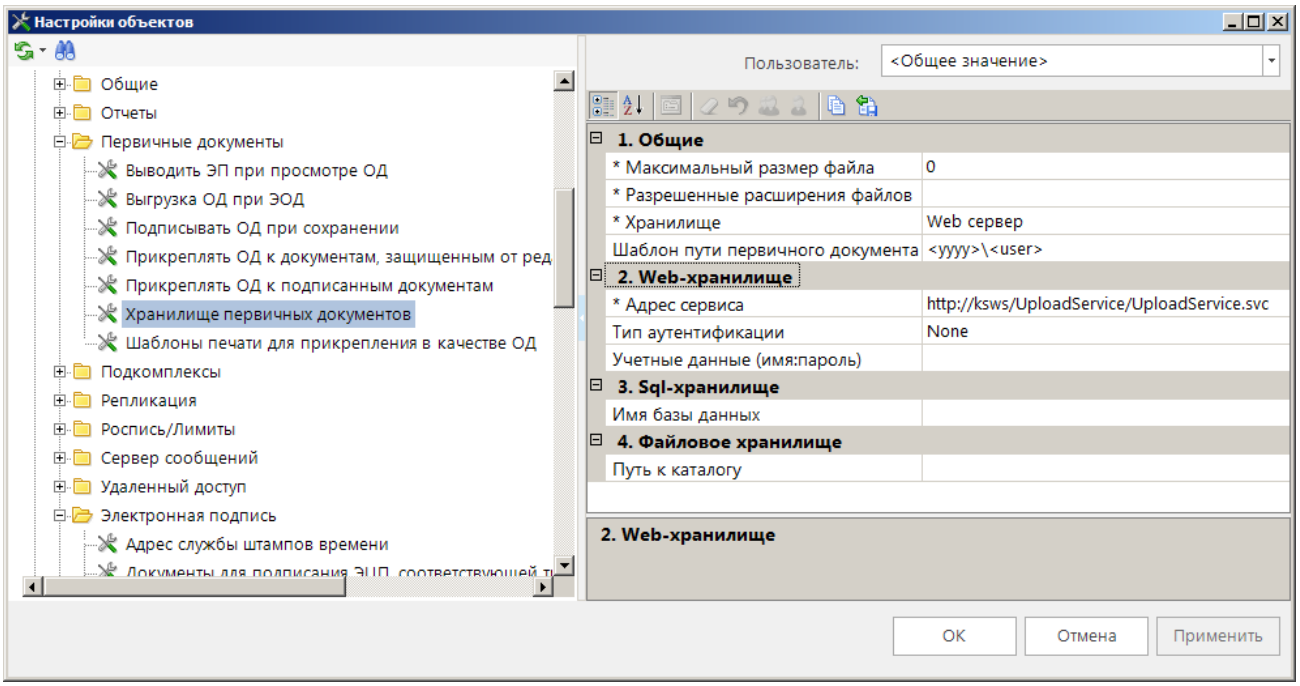

Рисунок 11. Адрес сервиса хранилища первичных документов

При нажатии кнопки **Электронная подпись** на документе (или прикрепленном оправдательном документе), имеющем электронную подпись, SQL сервер обращается к сервису ОД, который проверяет корректность ЭЦП документа (или оправдательного) в соответствии с установленным на сервисе ОД сертификатом открытого ключа (удостоверяющего центра или пользователей) и возвращает результат проверки SQL серверу.

Если настройка сервиса ОД указана неверно (несуществующий адрес), либо SQL сервер не может подключиться к сервису (ограничения сетевых экранов и т.п.), то при нажатии кнопки **Электронная подпись)** будет выдано сообщение «Возникла ошибка при соединении с сервисом проверки ЭЦП: ...» .

1.3. Установка ПО «Крипто-Про» и сертификата ключей

1.3.1. Установка ПО «Крипто-Про»

Дистрибутив программного обеспечения СКЗИ «КриптоПро CSP» представляет собой файл с расширением *.exe. Сохраните файл в локальную папку и разархивируйте его. Запустите файл CSPrus.msi

Дистрибутив программного обеспечения СКЗИ «КриптоПро CSP» представляет собой файл с расширением *.exe. Сохраните файл в локальную папку и разархивируйте его. Запустите файл CSPrus.msi (*Рисунок 12*):

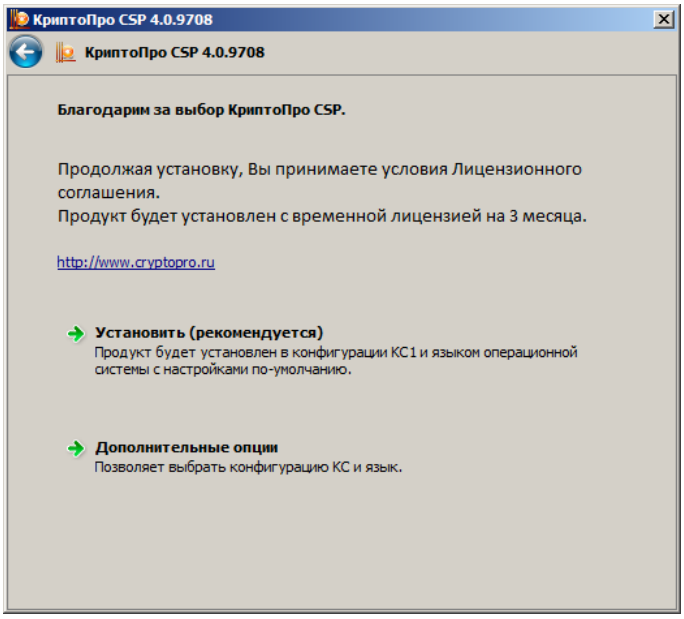

Рисунок 12. Начало установки СКЗИ «КриптоПро CSP»

Выберите тип «Установить (рекомендуется)». Нажмите кнопку **[Установить]**.

1.3.2. Лицензия и регистрация

При установке программного обеспечения КриптоПро CSP без ввода лицензии пользователю предоставляется лицензия с ограниченным сроком действия. Для использования КриптоПро CSP после окончания этого срока пользователь должен ввести серийный номер с бланка Лицензии (поставляется отдельно на бумажном носителе формата А4).

Для ввода лицензии откройте панель управления компьютером, используя кнопку **Пуск**. В открывшемся окне (*Рисунок 13*) выберите значок **КриптоПро CSP**.

ПУСК => НАСТРОЙКА => ПАНЕЛЬ УПРАВЛЕНИЯ

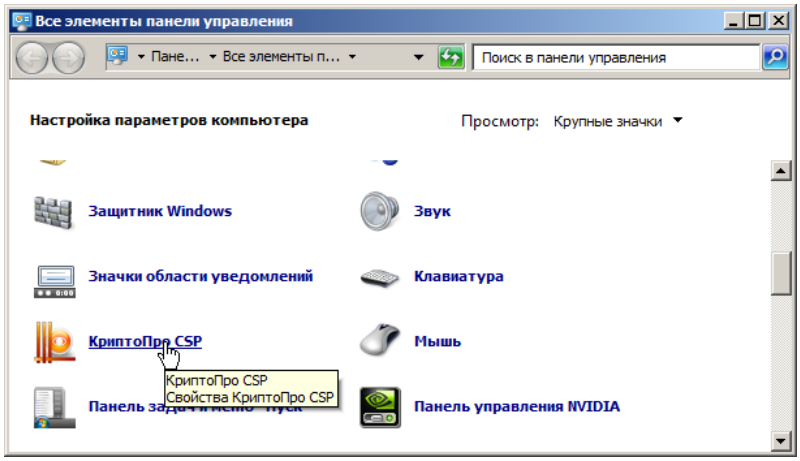

Рисунок 13. Панель управления

На панели настройки СКЗИ КриптоПро CSP выберите вкладку Общие и нажмите кнопку **[Ввод лицензии]** (*Рисунок 14*). Введите серийный номер лицензии.

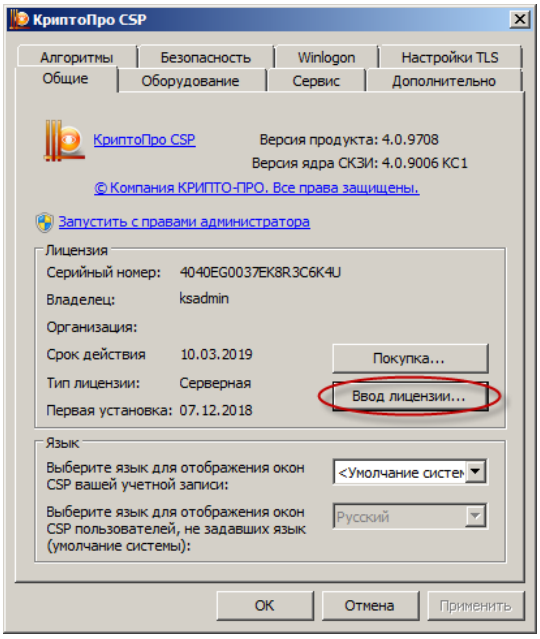

Рисунок 14. Переход к окну ввода информации о лицензии

1.3.3. Установка сертификата Удостоверяющего центра

Для удаленного взаимодействия с удостоверяющим центром ООО «Кейсистемс» необходимо установить сертификат с официального сайта http://keysystems.ru/files/CA/DISTR/.

Для установки сертификата УЦ откройте файл установки сертификата и нажмите кнопку **Установить сертификат** (*Рисунок 15*):

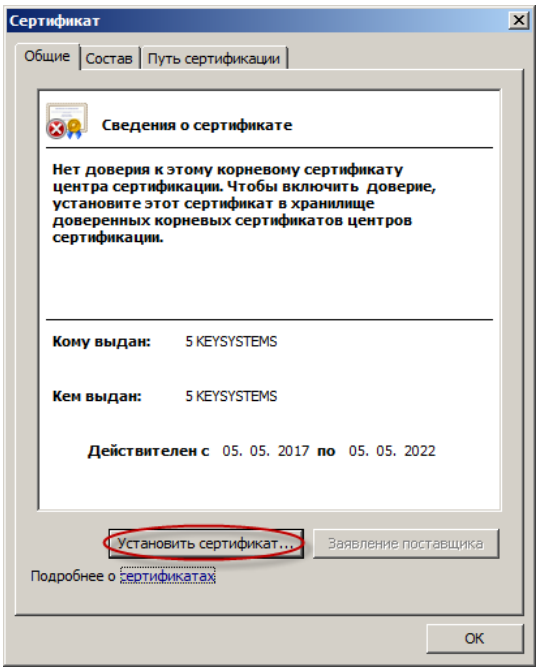

Рисунок 15. Установка сертификата УЦ ООО «Кейсистемс»

Запустится мастер импорта сертификатов (*Рисунок 16*):

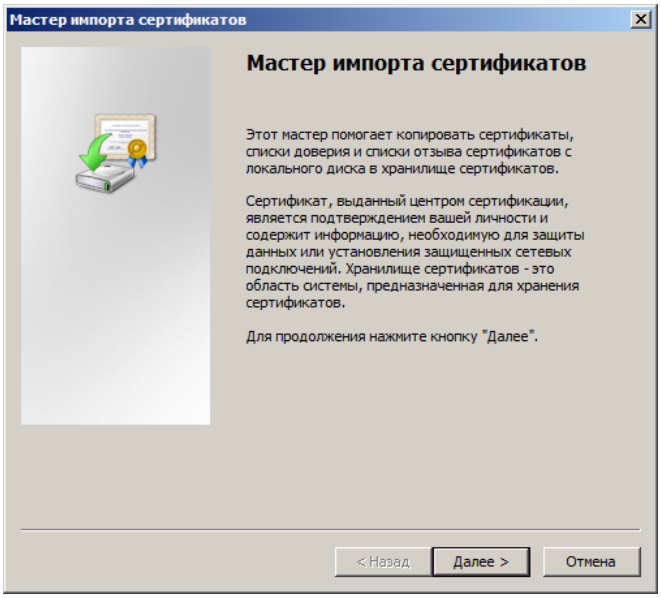

Рисунок 16. Начальное окно импорта сертификатов УЦ

При установке выберите опцию «Поместить все сертификаты в следующее хранилище». Нажмите кнопку **[Обзор]**.

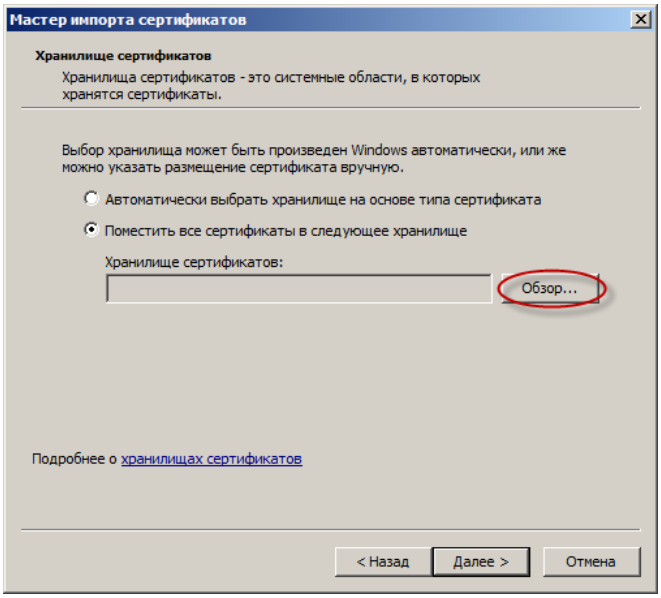

Рисунок 17. Настройка выбора хранилища сертификатов

Выберите хранилище сертификатов **Доверенные корневые центры сертификации** (*Рисунок 18*).

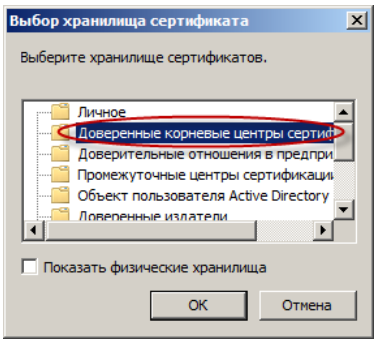

Рисунок 18. Выбор хранилища сертификатов

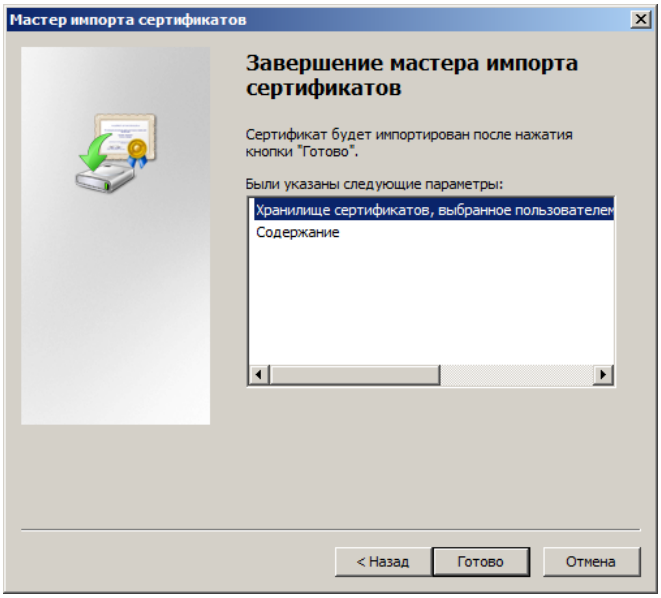

Рисунок 19. Завершение мастера импорта сертификатов

1.3.4. Установка ключевого носителя RuToken

Rutoken - персональное средство аутентификации пользователя при наложении ЭЦП, выполненное в формате USB-брелока. Используется в качестве носителя ключевой информации (открытого и закрытого сертификатов ЭЦП пользователя).

Рисунок 20. Персональное средство аутентификации пользователя «Rutoken»

Для использования Rutoken необходимо установить драйвер и модуль поддержки RuToken для этого скачайте архив rt4CryptoPro.rar, разархивируйте и запустите файл.

1. Нельзя подключать Rutoken к USB-порту до установки драйвера. В случае, если Rutoken был подключен до установки драйвера и появилось окно Поиск нового оборудования/Found New Hardware и Мастер обнаружения нового оборудования/Found New Hardware Wizard, выберите команду **[Отмена]** и отключите Rutoken.
2. Установку на операционную систему Windows 2000/XP/ 2003 производить с правами администратора.
3. На время установки драйверов все приложения должны быть закрыты во избежание ошибки разделения файлов.

Следуйте указаниям мастера установки.

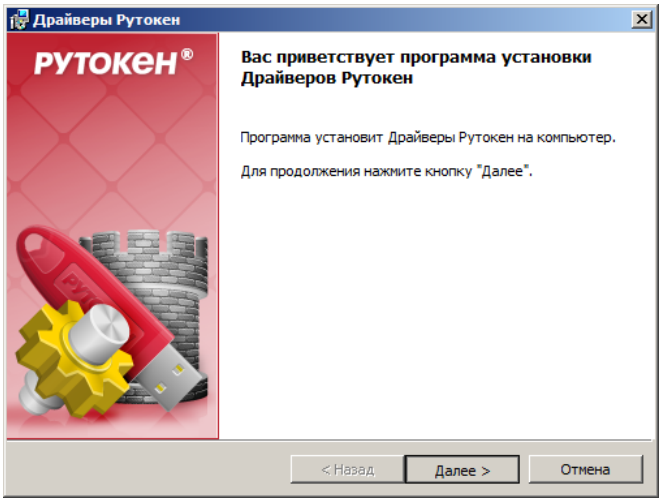

Рисунок 21. Установка персонального средства аутентификации пользователя «Rutoken»

1.3.5. Настройка считывателей в КриптоПро

После установки драйверов Rutoken и модуля поддержки следует настроить считыватели для работы с RuToken. Для добавления считывателя перейдите по пути, указанному ниже.

Кнопка Пуск => Настройки => Панель управления => КриптоПро CSP

В окне «Свойства => КриптоПро CSP» нажмите кнопку **[Настроить считыватели]** на вкладке **Оборудование**.

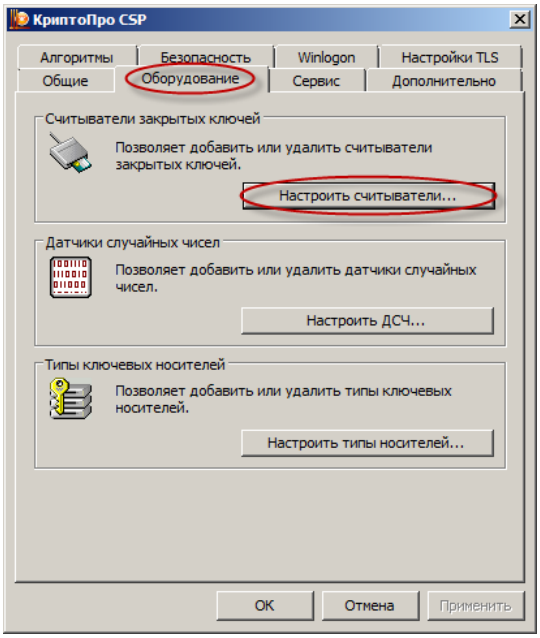

Рисунок 22. Настройка считывателей

В окне «Управление считывателями» нажмите кнопку **[Добавить]**.

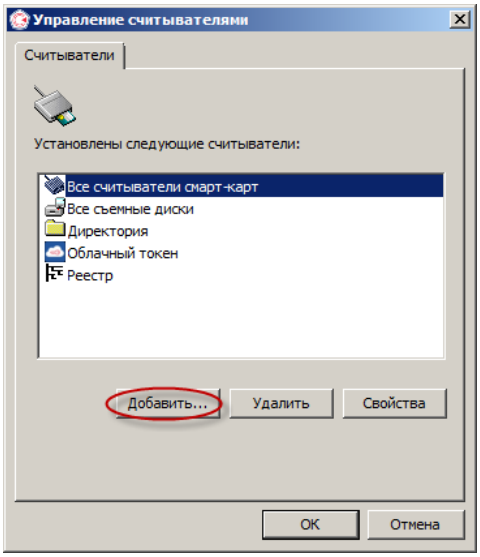

Рисунок 23. Управление считывателями

Откроется окно мастера установки считывателя (*Рисунок 24*).

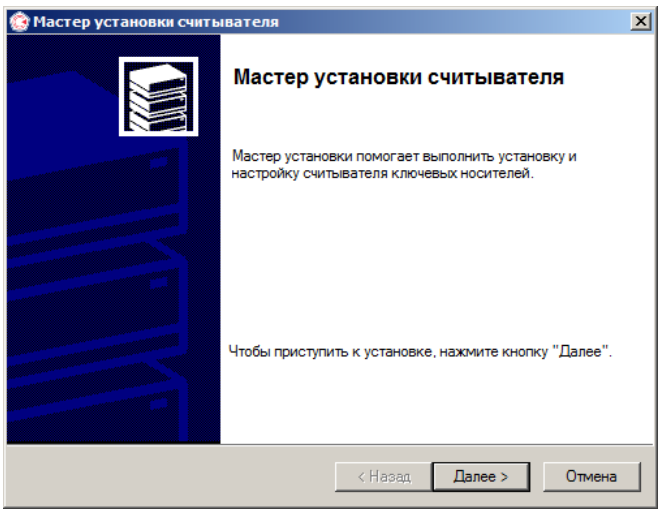

Рисунок 24. Мастер установки считывателя

В открывшемся окне нажмите кнопку **[Далее]**.

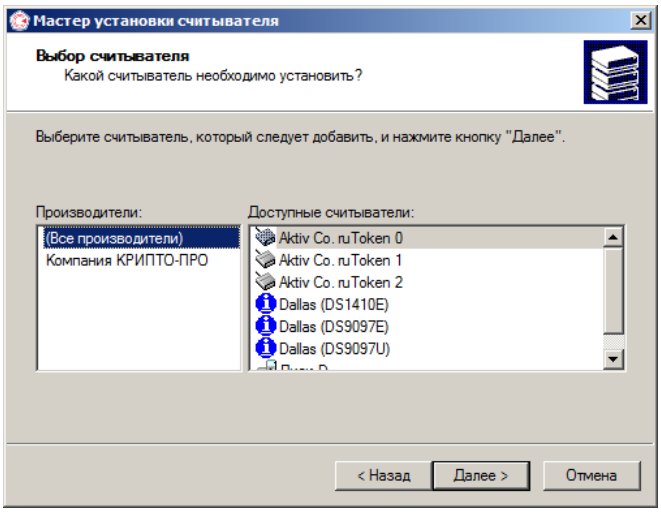

Рисунок 25. Выбор считывателя

По окончании установки нажмите кнопку **[Готово]**.

После установки ридера PC/SC в системе будет доступно три логических считывателя Rutoken:

– Aktiv Co. ruToken 0;
– Aktiv Co. ruToken 1;
– Aktiv Co. ruToken 2.

Считыватель «Aktiv Co. ruToken 0» устанавливается автоматически.

После завершения установки рекомендуется перезагрузить систему.

1.3.6. Установка личного сертификата с RuToken

Для установки сертификата открытого ключа с RuToken перейдите по пути, указанному ниже.

Кнопка Пуск => Настройки => Панель управления => КриптоПро CSP

В окне «Свойства: КриптоПро CSP» нажмите кнопку [**Просмотреть сертификат в контейнере]** на вкладке **Сервис**.

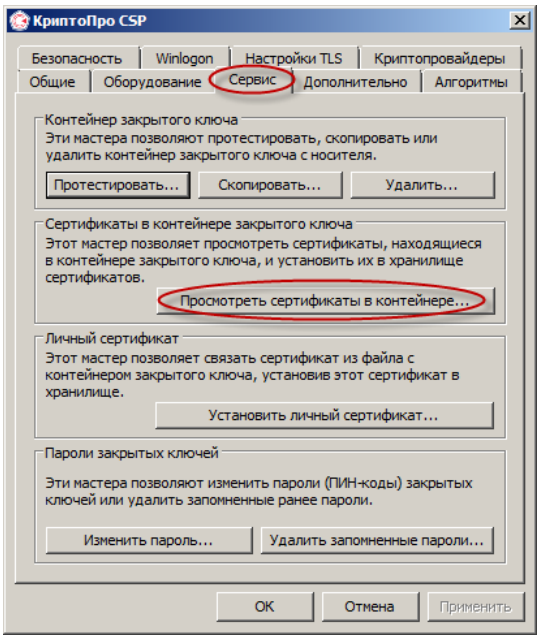

Рисунок 26. Переход к просмотру сертификата

В окне выбора ключевого контейнера выберите считыватель «Aktiv Co. Rutoken 0», нажмите кнопку **[ОК]**. Нажмите кнопку **[Далее]**.

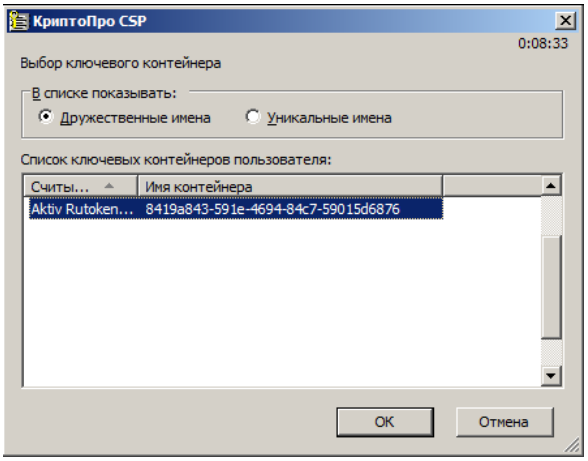

Рисунок 27. Выбор ключевого контейнера

В окне просмотра сертификата нажмите **[Обзор]**

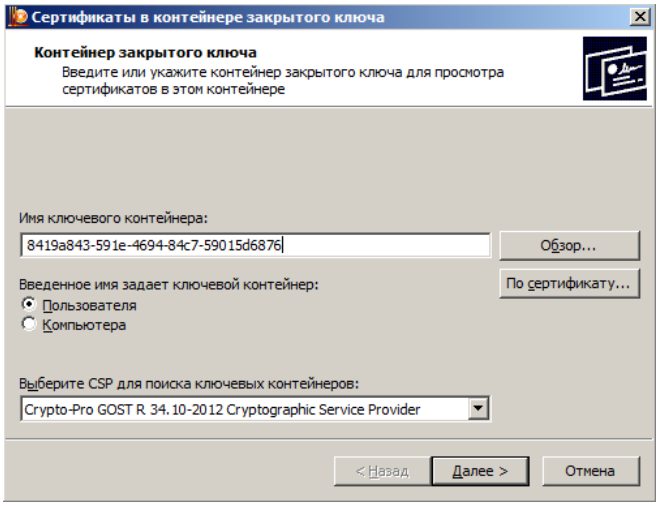

Рисунок 28. Просмотр и выбор сертификата в контейнере закрытого ключа

Выберите хранилище «Личные» и нажмите кнопку **[ОК]**, затем нажмите кнопку **[Далее]**.

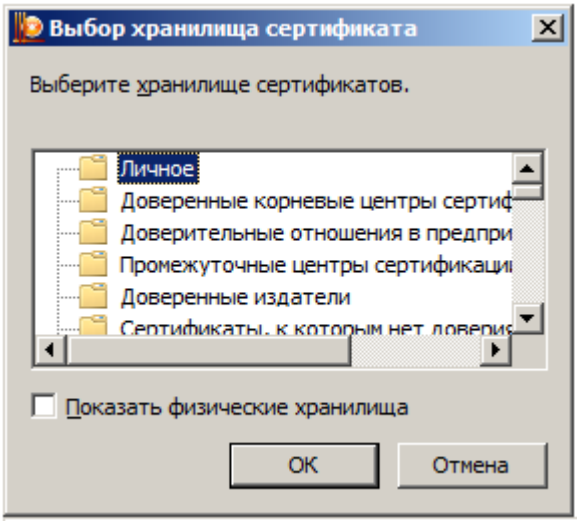

Рисунок 29. Окно выбора хранилища сертификата

В окне завершения работы мастера импорта нажмите кнопку **[Готово]**. Ваш ключ готов к работе.

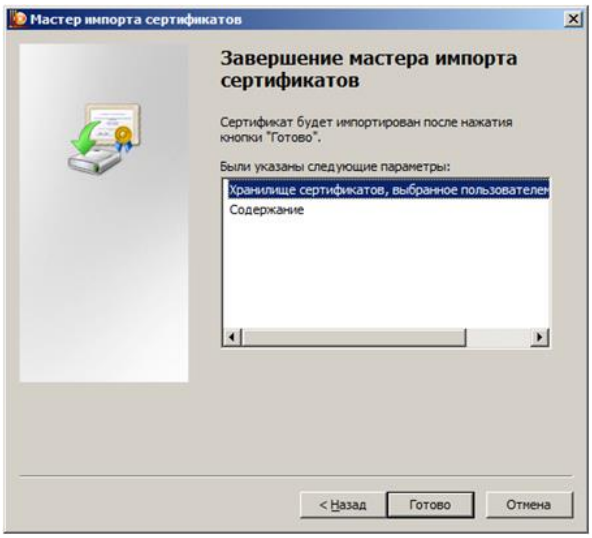

Рисунок 30. Завершение мастера импорта сертификатов

2. РЕКОМЕНДАЦИИ ПО ОСВОЕНИЮ

Корневой сертификат УЦ на сервере ключей следует размещать в «локальном компьютере» (*т.е. для компьютера, а не пользователя*), если служба сервера ключей работает под системной учетной записью. Симптомы неверного размещения сертификатов: при проверке ЭЦП сообщение «Подпись верна. Сертификат не найден в хранилище» либо «Один из сертификатов цепочки - не удалось определить достоверность».

Способ установки корневого сертификата, гарантирующие корректность его размещения: при установке с рутокена средствами ПО «Крипто Про» выбрать пункт «**Поместить все сертификаты в следующее хранилище**», далее, по кнопке «Обзор», в следующем окне включить опцию «***Показать физические хранилища***» и выбрать в качестве места размещения сертификата «**Реестр**».

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Термин
1	2
ДПиРСИБ	Департамент проектирования и разработки систем исполнения бюджета
ОД	Оправдательные документы
ПК	Программный комплекс
ПО	Программное обеспечение
УЦ	Удостоверяющий центр
ЭЦП	Электронно-цифровая подпись

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер версии	Примечание	Дата	ФИО исполнителя
01	Начальная версия	10.03.2011	Семенов О.С.
02	Обновлено до версии 18.04.	12.12.2018	Николаева М.Ю.