Телефон в Ижевске: +7 (3412) 72-11-00
Телефон в Москве: +7 (499) 277-1560
Сайт: www.directum.ru
E-mail: support@directum.ru

Инструкция по использованию КриптоПро CSP в DIRECTUM

Назначение документа

В системе DIRECTUM для работы с электронной подписью и шифрованием можно использовать средства криптографической защиты информации (СКЗИ) КриптоПро CSP 3.0 и выше (в исполнении 1 и 2, соответствующих уровням защиты КС1 и КС2).

Рекомендуется использовать КриптоПро CSP версии 3.6, так как он имеет сертификат соответствия ФСБ, на основании которого может использоваться для обеспечения целостности и подлинности информации, не содержащей сведений, составляющих государственную тайну. Поэтому КриптоПро целесообразно использовать вместо стандартных встроенных в Microsoft Windows СКЗИ при организации юридически значимого документооборота на предприятиях.

Для хранения ключей в КриптоПро используются контейнеры, содержащие закрытый и открытый ключи. Контейнеры можно создавать на различных устройствах, в зависимости от установленных драйверов (TouchMemory, e-token, дискета, реестр Microsoft Windows). Контейнеры могут быть защищены паролем, что обеспечивает двухуровневую аутентификацию и, как следствие, большую достоверность электронной подписи по сравнению с СКЗИ Microsoft Windows.

При использовании СКЗИ КриптоПро CSP, рекомендуется исключить возможность использования отличных от СКЗИ КриптоПро CSP криптопровайдеров посредством удаления соответствующих библиотек модулей расширения. Как правило они находятся по адресу:

- для 32-разрядной системы – %PROGRAMFILES%\NPO Computer\IS-Builder <Номер версии платформы IS-Builder>\Plugins\Encryption\<Имя модуля расширения>;
- для 64-разрядной системы – %PROGRAMFILES(x86)%\NPO Computer\IS-Builder <Номер версии платформы IS-Builder >\Plugins\Encryption\<Имя модуля расширения>.

В противном случае не гарантируется корректность работы СКЗИ КриптоПро CSP совместно с DIRECTUM.

Перед использованием СКЗИ необходимо изучить соответствующую документацию на СКЗИ и выполнить ее требования и рекомендации.

В тексте инструкции указываются названия документов и их разделов, поставляемых с ПО КриптоПро CSP для версии 3.6.

Рассматривается работа с операционными системами Microsoft Windows Server 2008/2008 R2/2012/2012 R2.

Содержание

Перечень терминов и сокращений

Ключ электронной подписи

Уникальная последовательность символов, предназначенная для создания электронной подписи.

Средства электронной подписи

Шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Сертификат ключа проверки электронной подписи (сертификат)

Электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Шаблон сертификата

Образец сертификата с заранее заданными настройками по умолчанию. Используется для создания новых сертификатов.

Установка и настройка КриптоПро в DIRECTUM

Чтобы настроить КриптоПро в DIRECTUM:

- установите и настройте центр сертификации, если он не был установлен ранее. Подробнее см. в документе «DIRECTUM. Инструкция по установке и настройке центра сертификации», входит в комплект поставки;
- при необходимости установите ПО КриптоПро CSP на все компьютеры, где установлена клиентская часть системы DIRECTUM. Подробнее см. раздел «Установка ПО КриптоПро CSP на компьютеры с клиентской частью DIRECTUM»;
- установите ПО КриптоПро CSP на компьютер с центром сертификации. Подробнее см. раздел «Установка ПО КриптоПро CSP на компьютер с Центром Сертификации Microsoft»;
- установите и настройте ПО КриптоПро CSP на компьютерах администратора и пользователей, которые будут подписывать или шифровать документы на основе сертификатов (пользователи СКЗИ). Подробнее см. раздел «Установка и настройка ПО КриптоПРО CSP на компьютеры пользователей СКЗИ»;
- при необходимости создайте и настройте шаблоны сертификатов. Например, если у имеющегося сертификата истек срок действия, создается новый сертификат, которым будут подписываться или зашифровываться документы.

  Для этого последовательно выполните этапы:

  - создание шаблонов сертификатов на Microsoft Windows Server;
  - настройка шаблонов сертификатов на Microsoft Windows Server;
- до начала генерации ключевой пары настройте автоматическое получение сертификатов. Подробнее см. раздел «Автоматическая выдача сертификатов на Microsoft Windows Server»;
- сгенерируйте ключевые пары и создайте контейнеры для администратора и пользователей СКЗИ. Подробнее см. раздел «Генерация ключевой пары»;
- экспортируйте сертификаты с расширением *cer. Подробнее см. раздел «Экспорт открытой части ключа»;
- свяжите полученные части ключевой пары. Подробнее см. раздел «Связывание открытой и закрытой части ключа»;
- установите сертификаты в локальные хранилища сертификатов пользователя и зарегистрируйте их в системе DIRECTUM. Подробнее см. раздел «Импорт сертификатов в локальные хранилища и регистрация в DIRECTUM».

Установка ПО КриптоПро CSP на компьютеры с клиентской частью DIRECTUM

Установка осуществляется при помощи пакета установки из поставки КриптоПро CSP, где CSPrus.msi – русскоязычная версия, CSPeng.msi – англоязычная версия.

Установку можно проводить в скрытом режиме и в режиме с отображением пользовательского интерфейса.

Скрытый режим рекомендуется использовать при автоматической установке через Active Directory. В этом случае командная строка для установки русскоязычной версии CPRus.msi должна иметь формат:

```
msiexec /i CSPrus.msi /qn
```

Режим с отображением пользовательского интерфейса рекомендуется использовать при ручной установке на компьютеры пользователя. В этом случае командная строка для установки русскоязычной версии должна иметь формат:

```
msiexec /i CSPrus.msi /qb
```

Установка ПО КриптоПро CSP на компьютер с Центром Сертификации Microsoft (Microsoft Certification Authority)

Установка ПО КриптоПро CSP на компьютер с центром сертификации осуществляется аналогично установке на компьютеры с клиентской частью системы DIRECTUM.

Установка и настройка ПО КриптоПро CSP на компьютеры пользователей СКЗИ

Установка и настройка ПО КриптоПро CSP производится в соответствии с документом «КриптоПро CSP. Инструкция по использованию», поставляемым с ПО КриптоПро CSP. Необходимо установить ПО и настроить считыватели (устройства), на которых будут храниться контейнеры.

Для всех носителей, определяемых операционной системой Windows как сменные – гибких дисков, flash-дисков, ZIP – предназначен считыватель «дисковод».

Например, пользователь будет хранить контейнер на flash-диске. Операционная система Windows при подключении диска присваивает ему букву F. В этом случае необходимо вставить flash-диск и в контрольной панели КриптоПро CSP добавить новый считыватель – дисковод F. Если пользователь имеет несколько подобных устройств и возможна ситуация, когда при подключении будет присвоена буква, отличная от F, то необходимо добавить новый считыватель на каждую букву.

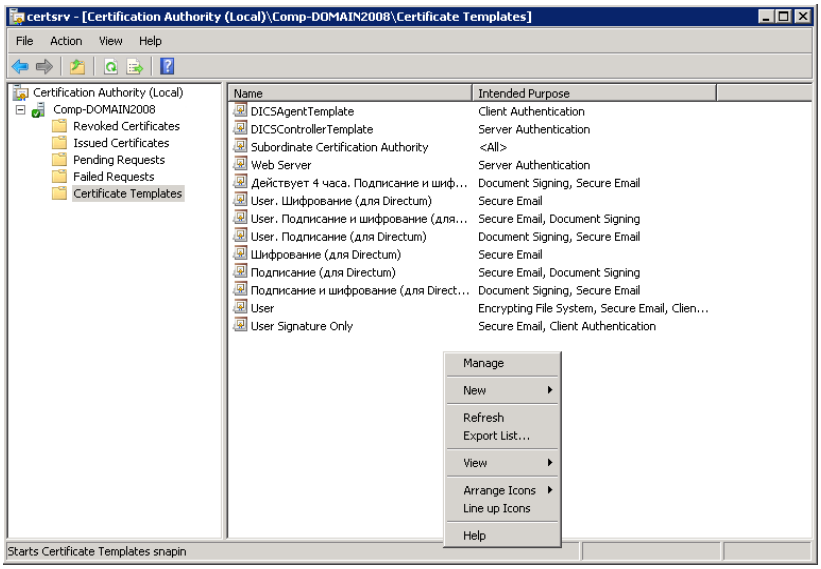
Создание шаблонов сертификатов на Microsoft Windows Server

Если необходимо создать сертификаты, которыми можно будет подписывать и шифровать документы, или если истек срок действия лицензии на предыдущие сертификаты, то создаются новые сертификаты на основе шаблонов.

Шаблоны сертификатов создаются в центре сертификации.

Чтобы создать шаблоны:

1. Войдите в систему под учетной записью администратора.
2. Откройте оснастку **Certification Authority**. Для этого в меню **Пуск** последовательно выберите **Администрирование**, **Центр сертификации**, **Certification Authority**:



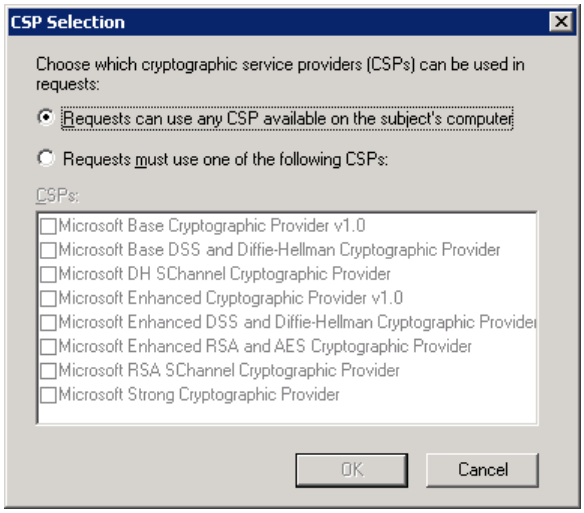
3. Разверните дерево оснастки и выберите папку **Certificate Templates**.
4. В контекстном меню области содержимого папки выберите пункт **Manage**.
5. Откроется окно с образцами готовых шаблонов. Новый шаблон создается путем копирования существующих образцов. Для этого выберите необходимый образец шаблона и в контекстом меню выберите пункт **Duplicate Template**. Откроется окно **Duplicate Template**.
6. Установите переключатель используемой операционной системы и нажмите на кнопку **OK**. Откроется окно свойств шаблона. Рекомендуется установить переключатель в значение **Windows Server 2003 Enterprise**, чтобы корректно выполнить последующие этапы настойки.
7. Перейдите на вкладку **General**. Курсор автоматически встанет в поле **Template display name**, в котором необходимо ввести имя шаблона.
8. Введите имя нового шаблона.
9. Сохраните введенные данные.

Настройка шаблонов сертификатов на Microsoft Windows Server

Чтобы настроить шаблоны:

1. В окне оснастки **Certification Authority** в папке **Certificate Templates** перейдите к списку шаблонов.
2. В списке выберите созданный шаблон центра сертификации. Перейдите в контекстное меню и выберите пункт **Properties**. Откроется окно свойств шаблона «<Название шаблона>Properties».
3. На вкладке **General** оставьте значения по умолчанию. При необходимости можно установить срок использования сертификата и опубликовать его в Active Directory.

4. Перейдите на вкладку **Request Handing** и установите параметры:
   - в выпадающем списке **Purpose** выберите значение **Signature and encryption**;
   - установите флажок **Include symmetric algorithms by the subject**;
   - в выпадающем списке **Minimum key size** задайте значение **512**. Если настраиваются шаблоны сертификатов, имеющих алгоритм RSA, то задайте значение **1024**;
   - установите флажок **Allow private key to be exported** и переключатель **Enroll subject without requiring any user input**.
5. Нажмите на кнопку **CSPs...**. Откроется окно **CSP Selection**:



6. Установите переключатель **Requests can use any CSP available on the subject's computer** и нажмите на кнопку **OK**.
7. Сохраните настройки шаблона. Нажмите на кнопку **OK** в окне «<Название шаблона>Properties».
8. Сделайте шаблоны видимыми. Для этого откройте окно оснастки **Certification Authority**.
9. В контекстном меню области содержимого последовательно выберите пункт **New**, **Certificate Template to Issue**. Откроется окно **Enable Certificate Templates**.
10. В окне выберите созданные новые шаблоны и нажмите на кнопку **OK**.
11. Если настраиваются шаблоны службы взаимодействия систем (DICS), то дополнительно выполняются этапы:
    - Настройка шаблона сертификата с проверкой подлинности клиента
    - Настройка шаблона сертификата с проверкой подлинности сервера

Настройка шаблона сертификата с проверкой подлинности клиента

Раздел используется при наличии лицензии на службу взаимодействия систем (DICS).

Настройка выполняется для шаблона серверной части агента DICS.

Чтобы настроить шаблон сертификата с проверкой подлинности клиента:

1. Перейдите в свойства шаблона. Откроется окно «<Название шаблона>Properties».
2. На вкладке **Extensions** в области **Extensions included in this template** для каждого параметра задайте значение по кнопке **Edit...**:

Параметр	Значение
Application Policies	Client Authentication
Basic Constraints	The subject is end-entity
Certificate Template Information	-
Issuance Polices	Certificate policies are also known as issuance policies
Key Usage	**Signature:** Digital signature; Signature is proof of origin (nonrepudiation). **Encryption:** Allow key exchange only with key encryption; Allow encryption of user data. Флажок Make this extension critical

Настройка шаблона сертификата с проверкой подлинности сервера

Раздел используется при наличии лицензии на службу взаимодействия систем (DICS).

Настройка выполняется для шаблона контроллера DICS.

Чтобы настроить шаблон сертификата с проверкой подлинности сервера, выполните аналогичные действия как при настройке шаблона с проверкой подлинности клиента.

На вкладке **Extensions** в области **Extensions included in this template** для каждого параметра задайте значение по кнопке **Edit...**:

Параметр	Значение
Application Policies	Server Authentication
Basic Constraints	The subject is end-entity
Certificate Template Information	-
Issuance Polices	Certificate policies are also known as issuance policies
Key Usage	**Signature:** Digital signature; Signature is proof of origin (nonrepudiation). **Encryption:** Allow key exchange only with key encryption; Allow encryption of user data. Флажок Make this extension critical

Автоматическая выдача сертификатов на Microsoft Windows Server

Чтобы настроить автоматическую выдачу сертификатов, необходимо выполнить настройки для каждого шаблона:

1. В дереве оснастки **Certification Authority** перейдите к папке **Certificate Templates** и в области содержимого папки выберите необходимый шаблон.
2. В контекстном меню шаблона выберите пункт **Properties**. Откроется окно свойств шаблона «<Название шаблона>Properties».
3. На вкладке **Security** в области **Permissions for Authenticated Users** в столбце **Allow** установите флажки **Read**, **Enroll** и **Autoenroll**.
4. Перейдите обратно к главному окну оснастки **Certification Authority**. В дереве оснастки выберите центр сертификации и в контекстом меню выберите пункт Properties. Откроется окно свойств центра сертификации.
5. Перейдите на вкладку **Policy Module** и нажмите на кнопку **Properties…**. Откроется окно свойств службы сертификатов ЦС.
6. Установите переключатель **Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate** и нажмите на кнопку **OK**.

Примечание

Если автоматическая выдача сертификатов не настроена, то необходимо скопировать из ЦС полученный сертификат на компьютер, на котором он будет использоваться. Рекомендуется настраивать автоматическую выдачу сертификатов, чтобы избежать лишних действий.

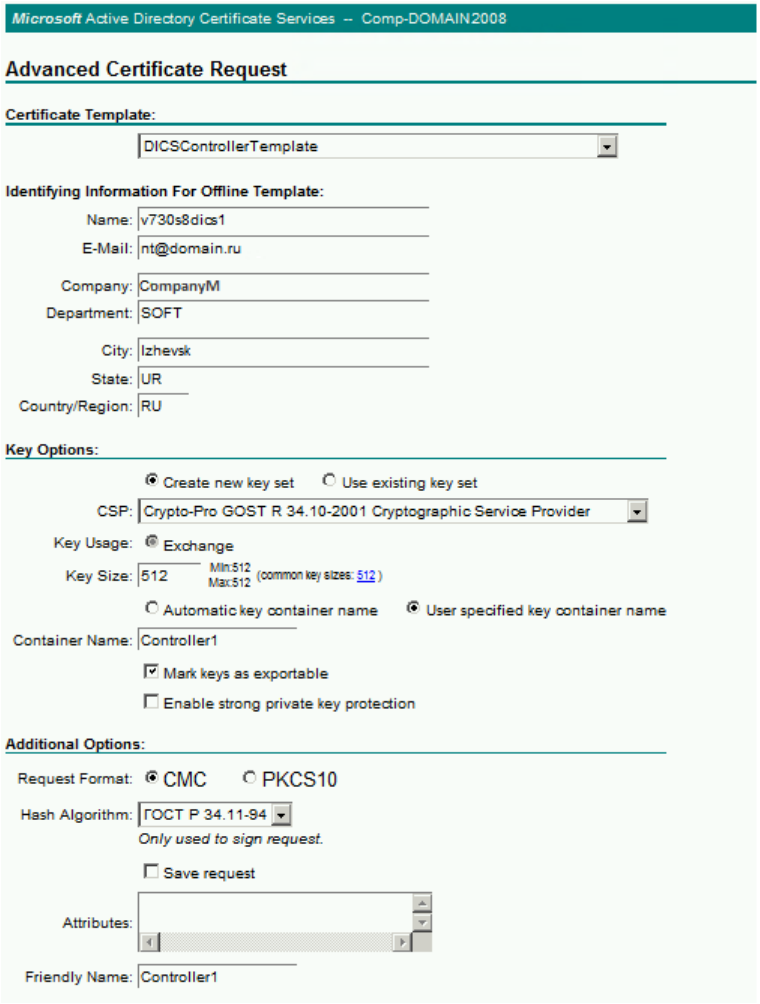
Генерация ключевой пары

На компьютер, где будет осуществляться генерация ключевой пары, необходимо установить ПО КриптоПро CSP. Подробнее см. в документе «КриптоПро CSP. Инструкция по использованию», входит в комплект поставки с ПО КриптоПро CSP.

Чтобы сгенерировать для пользователя закрытый ключ и сертификат:

1. Войдите в операционную систему Windows. Рекомендуется выполнять вход под именем пользователя, обладающего правами администратора.
2. Запустите Internet Explorer и перейдите по адресу http://<Сервер>/CertSrv/, где <Сервер> – это полное имя компьютера, включая имя домена, на котором установлен центр сертификации. Откроется окно регистрации.
3. Введите имя и пароль учетной записи администратора домена и нажмите на кнопку **OK**. Откроется страница приветствия «Welcome».

4. Последовательно перейдите по ссылкам **Request a certificate, Advanced certificate request, Create and submit a request to this CA**. Откроется страница ввода параметров для запроса сертификата **Advanced Certificate Request**:



В используемом браузере для страницы **Advanced Certificate Request** рекомендуется установить подписанные элементы ActiveX, чтобы форма шаблона отображалась корректно. Для этого:

1. В меню браузера Internet Explorer последовательно выберите **Сервис** и пункт **Свойства браузера**. Откроется окно свойств браузера.
2. В окне перейдите на вкладку **Безопасность** и выберите зону для настройки – **Интернет**.
3. Нажмите на кнопку **Другой...**. Отроется окно «Параметры безопасности – зона Интернет».
4. В группе **Элементы ActiveX и модули подключения** для всех параметров установите переключатель **Включить**.
5. Нажмите на кнопку **ОК** для сохранения настроек браузера.

На открывшейся странице:

1. В выпадающем списке **Certificate Template** выберите необходимый шаблон. Страница запроса изменит свой вид. Появится группа полей **Identifying Information for offline template**.
2. В поле **Name** укажите имя компьютера, для которого выполняется генерация сертификата. Остальные параметры заполните произвольно.

3. В выпадающем списке **CSP** выберите значение **Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider**.
4. В поле **Key Size** укажите значение **512**. Если настраиваются генерируются сертификаты, имеющие алгоритм RSA, то укажите значение **1024**. Указанный размер ключа влияет на криптостойкость и производительность.
5. Установите переключатель **User specified key container name** и в поле **Container Name** укажите необходимое имя контейнера.
6. В поле **Friendly Name** укажите имя сертификата. Например **Controller1**, если сертификат создается для контроллера службы взаимодействия систем (DICS). Лицензия на DICS приобретается отдельно.
7. Нажмите на кнопку **Submit**. Появится сообщение о том, что сертификат выдан.

   В случае генерации ключевой пары для службы взаимодействия систем (DICS) откроется окно запроса устройства, на которое необходимо записать закрытую часть ключа – контейнер. В окне «КриптоПро CSP»:

   a) Выберите носитель или реестр и нажмите на кнопку **OK**. Откроется окно запроса пароля и подтверждения пароля.

   b) Введите пароль и нажмите на кнопку **OK**. Пароль можно не указывать.

Примечание

Если контейнер генерируется в реестр, то пользователю, от имени которого запускается контроллер DICS или серверная часть агента, созданные сертификаты должны быть доступны в реестре.

В результате сертификат открытого ключа будет установлен в локальное хранилище пользователя, от имени которого выполнялась генерация сертификата. Закрытая часть ключа будет находиться на том устройстве, куда она была сгенерирована.

Экспорт открытой части ключа

После генерации открытой и закрытой части ключа необходимо экспортировать открытую часть ключа, так как она будет указываться при связывании ключевой пары. Экспорт можно выполнить через браузер Internet Explorer. Для этого:

1. В меню браузера последовательно выберите **Сервис** и пункт **Свойства браузера**. Откроется окно «Свойства браузера».
2. На вкладке «Содержание» нажмите на кнопку **Сертификаты**. Откроется окно «Сертификаты».
3. Выполните экспорт необходимых сертификатов по одноименной кнопке **Экспорт...**.

Связывание открытой и закрытой части ключа

Чтобы связать открытую и закрытую часть ключа выполните шаги, описанные в документе «КриптоПро CSP. Инструкция по использованию», раздел «Установка личного сертификата, хранящегося в файле», входит в комплект поставки с ПО КриптоПро CSP. На шаге, где необходимо нажать на кнопку **Установить личный сертификат**, укажите сертификат открытой части ключа, полученный от центра сертификации.

Импорт сертификатов в локальные хранилища и регистрация в DIRECTUM

Чтобы использовать полученные ключи в системе DIRECTUM, для каждого пользователя, имеющего контейнер:

- импортируйте сертификат из контейнера в локальное хранилище сертификатов компьютера. Подробнее см. в документе «КриптоПро CSP. Инструкция по использованию», раздел «Просмотр и установка личного сертификата, хранящегося в контейнере закрытого ключа», входит в комплект поставки с ПО КриптоПро CSP;
- экспортируйте сертификат с расширением *.cer на диск и зарегистрируйте сертификат в системе DIRECTUM. Подробнее см. в документации системы DIRECTUM, в руководстве администратора, в главе «Инструкции администратора», раздел «Инструкция по работе с сертификатами пользователей в системе DIRECTUM».

Настройка и запуск службы штампов времени

Подключение системы DIRECTUM к службе штампов времени включает в себя:

- создание оператора службы
- создание политики штампов времени
- настройки групповой политики
- запуск службы штампов времени

В результате выполненных настроек обращение к службе штампов времени происходит от имени стандартной учетной записи IIS IUSR.

Чтобы включить аутентификацию по логину и паролю:

1. В свойствах экземпляра службы штампов времени на закладке «Доступ» установите флажок **Обычная проверка**.
2. Заполните поле **Домен по умолчанию**. Если поле останется пустым, то в настройках DIRECTUM и агента необходимо будет указывать пользователя и домен.
3. В оснастке **Групповая политика** установите тип аутентификации **Обычный доступ**.

На клиентской машине должен быть установлен КриптоПро TSP Client. В оснастке **Групповая политика** укажите адрес сервера штампов времени и тип аутентификации. Если данные не будут указаны, то настройки DIRECTUM и агента, касающиеся службы штампов времени, при подписании игнорируются.

Создание оператора службы

1. В дереве оснастки **КриптоПро PKI** выделите созданный ранее экземпляр службы и в контекстом меню узла **Операторы** последовательно выберите **Создать**, **Оператора службы...**. Откроется окно мастера создания оператора службы.
2. Нажмите на кнопку **Далее >**.
3. В окне «Учетная запись оператора службы» в поле **Учетная запись** будет указана запись локального администратора текущего компьютера. При необходимости измените значение.
4. Нажмите на кнопку **Далее >**.

5. В окне «Сертификат оператора» укажите сертификат подписи оператора. Для этого нажмите на кнопку **Выбрать из хранилища...** и выберите из списка сертификат штампа времени.
6. Нажмите на кнопку **Далее >**.
7. В окне завершения работы мастера нажмите на кнопку **Готово**.

Создание политики штампов времени

1. В дереве оснастки **КриптоПро PKI** выделите созданный ранее экземпляр службы и в контекстом меню узла **Политики** последовательно выберите **Создать**, **Политику штампов времени...**. Откроется окно мастера создания политики штампов времени.
2. Нажмите на кнопку **Далее >**.
3. В окне «Идентификация политики»:
   - заполните поля **Объектный идентификатор** и **Название политики**. Если сертификат штампов времени выдан в тестовом центре сертификации КриптоПро, то идентификатор будет иметь значение **1.2.643.2.2.38.4**;
   - нажмите на кнопку **Далее >**.
4. В окне «Допустимые алгоритмы хеширования» выберите нужные алгоритмы и нажмите на кнопку **Далее>**.
5. В окне завершения работы мастера нажмите на кнопку **Готово**.

Настройка групповой политики

1. В дереве оснастки **Групповые политики** в узле **Конфигурация компьютера** последовательно перейдите **Административные шаблоны**, **Классические административные шаблоны**, **КриптоПро**, **КриптоПро TSP Client**.
2. Задайте параметры:
   - **Аутентификация: тип по умолчанию**. Рекомендуется использовать анонимную аутентификацию;
   - **Службы штампов: адрес службы штампов времени по умолчанию**. Соответствует значению, указанному в свойствах узла службы. Можно посмотреть в оснастке **КриптоПро PKI**.

Запуск службы штампов времени

Запуск службы штампов времени осуществляет из контекстного меню экземпляра службы. Для корректного запуска в свойствах службы необходимо выключить проверку цепочки сертификатов службы на отзыв.

Установка электронной подписи и шифрование документа сертификатом из контейнера

Чтобы подписать документ электронной подписью или зашифровать на основе сертификата, необходимо проделать те же действия, что и при использовании обычного сертификата. Подробнее см. документацию системы DIRECTUM, руководство пользователя, разделы «Подписание документов» и «Шифрование документов».

Отличие заключается в дополнительных диалоговых окнах. Так, при попытке подписания документа сертификатом из контейнера, на котором установлен пароль, будет показано окно запроса пароля. В данном окне введите пароль и при необходимости установите флажок **Запомнить пароль**. Это позволяет избежать повторного ввода пароля в течение текущего сеанса пользователя (до выхода пользователя из операционной системы Windows).

Если носитель с контейнером не вставлен, после ввода пароля будет предложено выбрать устройство и вставить носитель.

Устройства, зарегистрированные в КриптоПро CSP, могут быть различны. Если носитель с контейнером вставлен, но операционная система Windows присвоила ему букву диска, которой нет в списке устройств, то необходимо переопределить букву диска средствами оснастки Windows **Управление дисками** или добавить новое устройство с данной буквой диска при помощи контрольной панели КриптоПро CSP. Подробнее см. в документе «КриптоПро CSP. Инструкция по использованию», входит в комплект поставки ПО КриптоПро CSP.

Использование списков отозванных сертификатов

Для обеспечения контроля доверия к сертификату, который используется для подписания и шифрования в системе DIRECTUM, необходимо иметь актуальный список отозванных сертификатов (CRL), установленный на локальный компьютер.

CRL представляет собой список отозванных сертификатов с указанием времени и даты отзыва выданного сертификата. В списке CRL каждый отозванный сертификат опознается по своему серийному номеру. Список формируется центром сертификации на предприятии в строго обозначенный промежуток времени и свободно распространяется через общедоступный ресурс.

При подписании данных в системе DIRECTUM происходит сверка со списком отозванных сертификатов, установленных на локальном компьютере. Если сертификат оказывается в списке отозванных, пользователь при подписании данных получит соответствующую ошибку.

Чтобы реализовать данный механизм:

1. Скачайте на локальный компьютер список отозванных сертификатов с расширением *.crl. Как правило этот список располагается по сетевому пути:

   \\<Имя сервера центра сертификации>\CertEnroll\<Имя списка отозванных сертификатов>.crl
2. Установите список отозванных сертификатов на локальный компьютер. Для этого вызовите контекстное меню на скачанном файле списка отозванных сертификатов и выберите пункт меню **Установить список отзыва (CRL)**.
3. Нажмите на кнопку **Далее >**. Откроется окно «Хранилище сертификатов».
4. Установите переключатель **Поместить все сертификаты в следующее хранилище** и нажмите кнопку **Обзор...**. Установите флажок **Показать физические хранилища**. Выберите хранилище **Доверенные корневые центры сертификации > Локальный компьютер**.
5. Нажмите на кнопку **Далее >**. Откроется окно завершения работы мастера.
6. Нажмите на кнопку **Готово**. В появившемся окне нажмите на кнопку **ОК**. Мастер импорта завершит свою работу.

Важно помнить, что для корректной проверки сертификата на нахождение его в списке отозванных сертификатов необходимо всегда иметь актуальный установленный список с расширением *.crl на локальном компьютере.

Контроль целостности

Для обеспечения контроля целостности установленной системы необходимо руководствоваться рекомендациями, указанными в документации на СКЗИ КриптоПро.

Контролю подлежат папки с файлами системы, указанные администратором в ходе установки системы.

Периодичность контроля целостности определяется в соответствии с политикой безопасности предприятия и настраивается администратором безопасности.