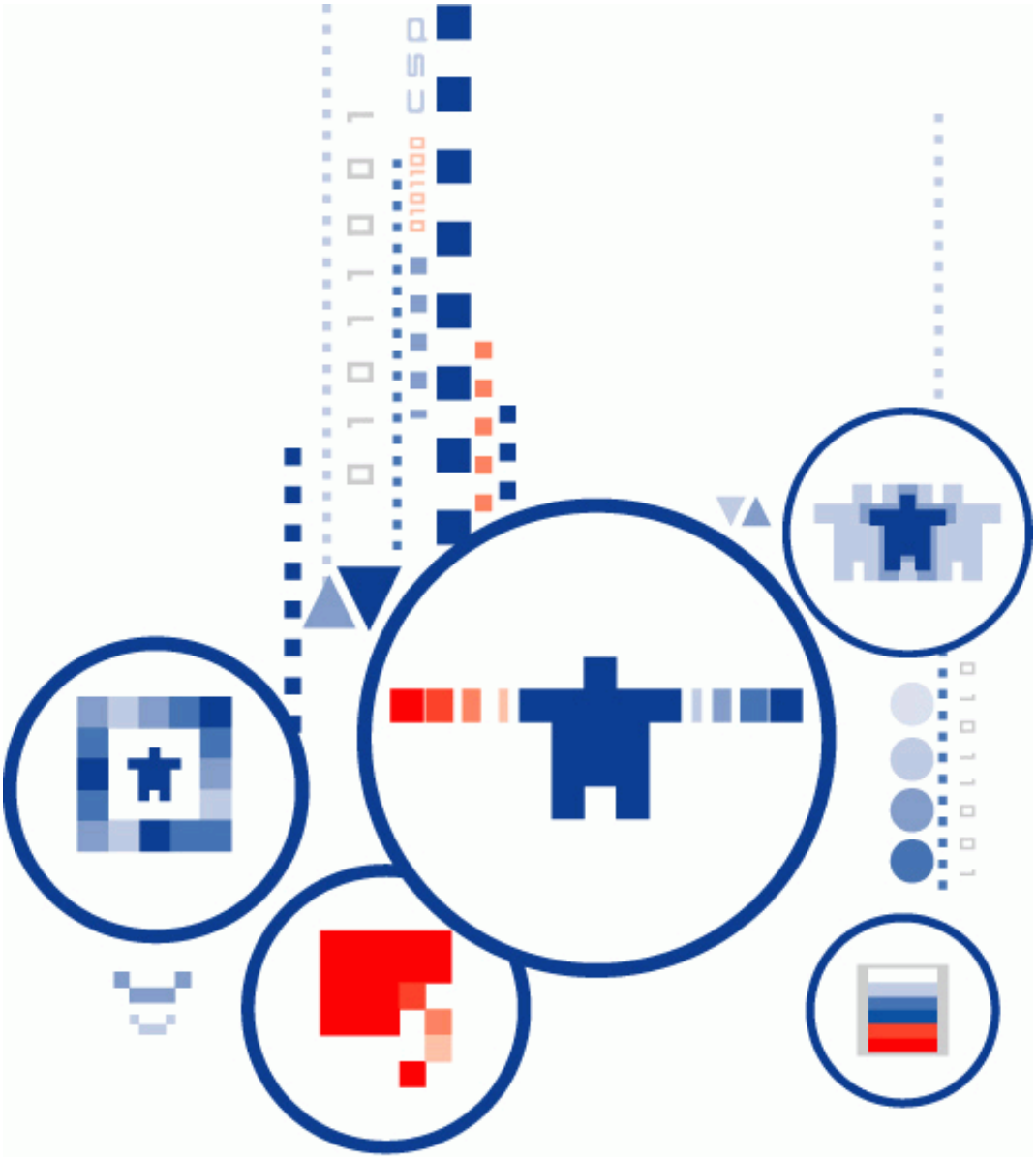

Сервер Электронной Подписи «КриптоПро DSS»

КОМПОНЕНТ ПАКМ «КРИПТОПРО HSM»

Руководство Администратора

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

CAdES	—	Расширенная версия стандарта электронной подписи CMS (CMS Advanced Electronic Signatures)
CMIS	—	Сервисы взаимодействия при управлении контентом (Content Management Interoperability Services)
CRL	—	Список отзыва сертификатов (Certificate Revocation List)
CSP	—	Криптопровайдер (Cryptographic Service Provider)
HSM	—	Аппаратный модуль системы безопасности (Hardware security module)
HOTP	—	алгоритм защищенной аутентификации с использованием одноразового пароля. (HMAC-Based One-Time Password Algorithm)
IIS	—	Набор серверов от компании Microsoft (Internet Information Services)
OATH	—	Набор алгоритмов аутентификации с использованием одноразовых паролей
OAuth	—	Открытый протокол авторизации, который позволяет предоставить третьей стороне ограниченный доступ к защищённым ресурсам Пользователя без необходимости передавать ей (третьей стороне) логин и пароль (Open Authorization)
OCSP	—	Протокол получения статуса сертификата в реальном времени (Online Certificate Status Protocol)
OTP	—	Пароль, действительный только для одного сеанса аутентификации (One-Time Password)
REST	—	Архитектурный стиль построения распределенного приложения (Representational State Transfer)
RFC	—	Рекомендация Internet Engineering Task Force (Request for Comments)
SAML	—	Язык разметки декларации безопасности, язык разметки, основанный на языке XML (Security Assertion Markup Language)
SOAP	—	Простой протокол доступа к объектам (Simple Object Access Protocol)
SSL	—	Протокол защиты сокетов (Secure Sockets Layer)

TLS	—	Протокол защиты транспортного уровня (Transport Layer Security)
TOTP	—	OATH-алгоритм создания одноразовых паролей для защищенной аутентификации, генерирующий пароль на основе времени. (Time-based One Time Password Algorithm)
URL	—	Единый указатель ресурсов (Uniform Resource Locator)
WCF	—	Программный фреймворк, используемый для обмена данными между приложениями, входящий в состав .NET Framework. (Windows Communication Foundation)
МЭ	—	Межсетевой экран
АРМ	—	Автоматизированное рабочее место
БД	—	База данных
ИС	—	Информационная система
СУБД	—	Система управления базой данных
ОС	—	Операционная система
ПО	—	Программное обеспечение
СКЗИ	—	Средство криптографической защиты информации
СЭП	—	Сервер электронной подписи
ЭП	—	Электронная подпись
ПАК	—	Программно-аппаратный комплекс
ПАКМ	—	Программно-аппаратный криптографический модуль
УЦ	—	Удостоверяющий Центр

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Электронная подпись	—	информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.
Сертификат открытого ключа	—	электронный или бумажный документ, содержащий открытый ключ, информацию о владельце ключа, области применения ключа, подписанный выдавшим его Удостоверяющим центром и подтверждающий принадлежность открытого ключа владельцу.
Квалифицированный сертификат открытого ключа (квалифицированный сертификат)	—	сертификат открытого ключа, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.
Владелец сертификата открытого ключа	—	лицо, которому в установленном Федеральным законом (№63-ФЗ от 06.04.2011 г. «Об электронной подписи») порядке выдан сертификат открытого ключа.
Закрытый ключ	—	уникальная последовательность символов, предназначенная для шифрования.
Ключ электронной подписи	—	уникальная последовательность символов, предназначенная для создания электронной подписи
Ключ проверки электронной подписи	—	уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.
Удостоверяющий центр	—	юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов открытых ключей, а также иные функции, предусмотренные Федеральным законом №63-ФЗ от 06.04.2011 г. «Об электронной подписи».
Средства электронной подписи	—	шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание закрытого и открытого ключей.

СОДЕРЖАНИЕ

1. Аннотация

Настоящий документ содержит Руководство Администратора Сервера Электронной Подписи «КриптоПро DSS». СЭП «КриптоПро DSS» используется для создания электронной подписи, шифрования документов, а также для централизованного защищенного хранения закрытых ключей Пользователей. Для хранения в СЭП сертификатов и закрытых ключей Пользователей в зашифрованном виде, а также для реализации криптографических операций используется ПАКМ «КриптоПро HSM».

Документ предназначен для системных администраторов и Администраторов СЭП как руководство по установке и конфигурированию СЭП «КриптоПро DSS».

Данный документ, включая подбор и расположение иллюстраций и материалов в нём, является объектом авторских прав и охраняется в соответствии с законодательством Российской Федерации. Обладателем исключительных авторских и имущественных прав является ООО «КРИПТО-ПРО» Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ. Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены компанией ООО «КРИПТО-ПРО» без предварительного уведомления. Все указанные данные о характеристиках продуктов основаны на международных или российских стандартах и результатах тестирования, полученных в независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе компания ООО «КРИПТО-ПРО» не предоставляет никаких ни явных, ни подразумеваемых гарантий. Владельцем товарных знаков КриптоПро, КРИПТО-ПРО, логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является ООО «КРИПТО-ПРО». Названия прочих технологий, продуктов, компаний, упоминающихся в данном документе, могут являться товарными знаками своих законных владельцев. Сведения, приведённые в данном документе, актуальны на дату его публикации. При перепечатке и использовании данных материалов либо любой их части ссылки на ООО «КРИПТО-ПРО» обязательны.

© 2000-2017, ООО «КРИПТО-ПРО» Все права защищены.

2. Системные требования

2.1. Требования к аппаратному обеспечению

Аппаратные требования к техническим средствам, на которых размещаются программные компоненты СЭП «КриптоПро DSS», зависят от количества зарегистрированных Пользователей и требований по производительности всего комплекса.

В Таблица 1 приведены рекомендуемые минимальные требования к техническим средствам, которые обеспечивают установку и работу компонентов при 1000 Пользователях:

Таблица 1. Требования к аппаратному обеспечению

Оборудование	Минимальные требования
Центральный процессор	64-разрядный двухъядерный процессор с тактовой частотой 1,86 ГГц.
Оперативная память	4 ГБ ОЗУ.
Жесткий диск	4 ГБ свободного места.
Сетевые адаптеры	Один сетевой адаптер, совместимый с операционной системой компьютера, для взаимодействия с внутренней сетью.

2.2. Требования к программному обеспечению

В Таблица 2 указаны предъявляемые к программному обеспечению требования. На пересечениях строк с ПО и столбцов с указанием компонента КриптоПро DSS стоит знак «+» в случае необходимости установки ПО, и «-» в противном случае.

При тестировании КриптоПро DSS можно использовать СУБД MS SQL Express, однако при эксплуатации необходимо использовать СУБД Microsoft SQL Server 2008 R2 и выше. В комплект поставки СЭП «КриптоПро DSS» входит только дистрибутив Microsoft SQL Server Express 2008 R2.

Таблица 2. Требования к программному обеспечению

Название	Сервис Подписи	Центр Идентификации	Веб-интерфейс Пользователя	Сервис Аудита	myDSS
Windows Server 2008 R2/2012/2012R2 (x64)/2016	+	+	+	+	+, кроме Windows Server 2008 R2
Microsoft SQL Server 2008 R2/2012/2014/2016/2017	+	+	–	+	+
КриптоПро HSM Client	+	–	–	-	+ (Internal Interaction Server)

2.3. Требования к компонентам ОС, установленной на веб-сервере

Для функционирования всех компонентов СЭП «КриптоПро DSS» необходима установка Microsoft Internet Information Services (IIS). Для различных ОС необходима установка и настройка различных компонентов:

Microsoft Windows Server 2008 R2

Для настройки работы веб-сервера необходимо установить **Microsoft Internet Information Services 7.5.** В Мастере добавления ролей и компонентов необходимо добавить следующие роли веб-сервера IIS:

- ASP.NET;
- Расширяемость .NET (.NET Extensibility 4.5);
- Расширения ISAPI (ISAPI Extensions);
- Фильтры ISAPI (ISAPI Filters);
- Статическое содержимое (Static content);
- Фильтрация запросов (Request Filtering);
- Консоль управления IIS (IIS Management Console).

Microsoft Windows Server 2012 и 2012 R2

Для настройки работы веб-сервера необходимо установить **Microsoft Internet Information Services 8.** В Мастере добавления ролей и компонентов необходимо добавить следующие роли веб-сервера IIS:

- ASP.NET 4.5;
- Расширяемость .NET (.NET Extensibility 4.5);
- Расширения ISAPI (ISAPI Extensions);
- Фильтры ISAPI (ISAPI Filters);
- Статическое содержимое (Static content);
- Фильтрация запросов (Request Filtering);
- Консоль управления IIS (IIS Management Console);
- Дополнительные службы .NET Framework 4.5;
- Активация по HTTP (HTTP Activation).

3. Развертывание КриптоПро DSS

В данном разделе описывается развертывание СЭП «КриптоПро DSS». Для выполнения развертывания СЭП «с нуля» необходимо выполнить следующие шаги:

1. Развертывание веб-сервера.
2. Установка КриптоПро DSS и дополнительного ПО (включая автоматическую установку с диска Microsoft .NET Framework версии 4.6.1 и PowerShell версии 3.0).
3. Установка ПАКМ «КриптоПро HSM».
4. Развертывание ЦИ.
5. Развертывание Сервиса Подписи.
6. Развертывание Веб-интерфейса Пользователя (при необходимости).
7. Развертывание Сервиса Аудита (при необходимости).
8. Развертывание myDSS (при необходимости).
9. Развертывание баз данных служб (при использовании для СЭП нескольких серверов).

3.1. Развертывание веб-сервера

В данном разделе описывается настройка компонентов и ролей Internet Information Services для ОС Microsoft Windows Server 2008 R2, 2012, 2012 R2.

3.1.1. Развертывание веб-сервера на ОС Microsoft Windows Server 2008 R2

Для настройки работы веб-сервера необходимо установить **Microsoft Internet Information Services 7.5.** В Мастере добавления ролей и компонентов необходимо добавить следующие роли веб-сервера IIS:

- ASP.NET;
- Расширяемость .NET (.NET Extensibility 4.5);
- Расширения ISAPI (ISAPI Extensions);
- Фильтры ISAPI (ISAPI Filters);
- Статическое содержимое (Static content);
- Фильтрация запросов (Request Filtering);
- Консоль управления IIS (IIS Management Console).

Если установка Microsoft .NET Framework 4.5.1 происходила **до** установки роли IIS, то после добавления данной роли необходимо в командной строке выполнить команду (в одну строку):

```
%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -iru
```

3.1.2. Развертывание веб-сервера на ОС Microsoft Windows Server 2012

Для настройки работы веб-сервера необходимо установить **Microsoft Internet Information Services 8.** В Мастере добавления ролей и компонентов необходимо добавить следующее:

Компоненты.

- Служба активации процессов Windows:
  - Модель процесса;
  - API конфигурации;
- Функции .NET Framework 4.6:
  - .NET Framework 4.6
  - ASP.NET 4.6
- Службы WCF:
  - Активация по HTTP
- Платформа .NET 3.5.

Службы ролей.

- Фильтрация запросов;
- Ведение журнала;
- Статическое содержимое;
- Расширяемость .NET (.NET Extensibility 4.5);
- Расширения ISAPI (ISAPI Extensions);
- Фильтры ISAPI (ISAPI Filters);
- Статическое содержимое (Static content);
- Фильтрация запросов (Request Filtering);
- Консоль управления IIS (IIS Management Console).

3.1.3. Развертывание веб-сервера на ОС Microsoft Windows Server 2012 R2

Для функционирования всех компонентов СЭП «КриптоПро DSS» необходима установка Microsoft Internet Information Services (IIS) 8. В Мастере добавления ролей и компонентов необходимо добавить следующие роли веб-сервера IIS:

- ASP.NET 4.5;
- Расширяемость .NET (.NET Extensibility 4.5);
- Расширения ISAPI (ISAPI Extensions);
- Фильтры ISAPI (ISAPI Filters);

Указанные роли находятся в разделе *«Веб-сервер (IIS) – Веб-сервер – Разработка приложений»* (см. Рис. 1).

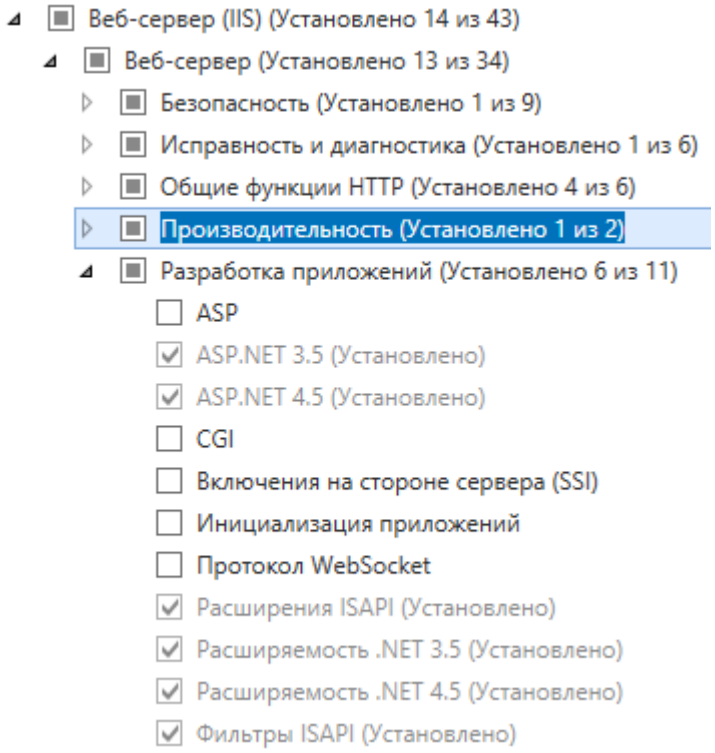

Рис. 1 – Настройка ролей веб-сервера IIS (1)

- Статическое содержимое (Static content);

Указанная роль находится в разделе *«Веб-сервер (IIS) – Веб-сервер – Общие функции HTTP»* (см. Рис. 2).

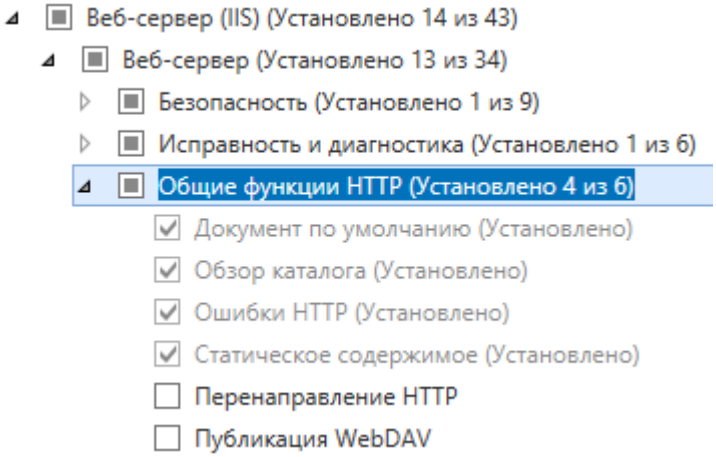

Рис. 2 – Настройка ролей веб-сервера IIS (2)

- Фильтрация запросов (Request Filtering);

Указанная роль находится в разделе *«Веб-сервер (IIS) – Веб-сервер – Безопасность»* (см. Рис. 3).

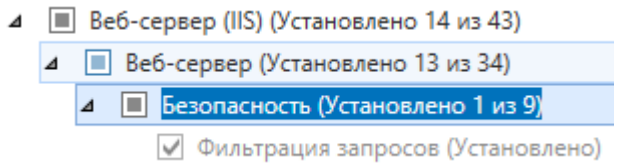

Рис. 3 – Настройка ролей веб-сервера IIS (3)

- Консоль управления службами IIS (IIS Management Console).

Указанная роль находится в разделе *«Веб-сервер (IIS) – Средства управления – Консоль управления службами IIS»* (см. Рис. 4).

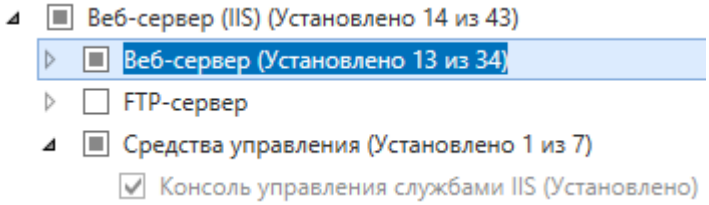

Рис. 4 – Настройка ролей веб-сервера IIS (4)

Также необходимо выбрать и установить следующие компоненты IIS: Дополнительные службы .NET Framework 4.5:

- Активация по HTTP (HTTP Activation).

Указанный компонент находится в разделе *«Компоненты – Функции .NET Framework 4.5 – Службы WCF – Активация по HTTP»* (см. Рис. 5).

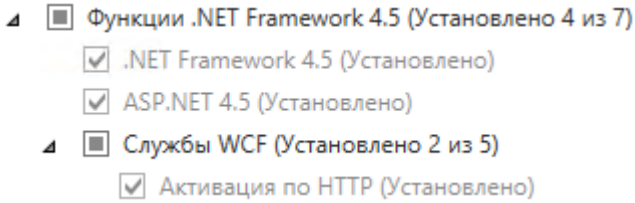

Рис. 5 – Настройка компонентов веб-сервера IIS

Установить необходимые компоненты можно как через Диспетчер Сервера, так и с помощью командной строки. Для установки указанных выше компонент сервера выполните следующую команду:

```
dism.exe /Online /Enable-Feature /FeatureName:IIS-WebServerRole
/FeatureName:IIS-WebServer /FeatureName:IIS-ASPNET45 /FeatureName:IIS-
NetFxExtensibility45 /FeatureName:IIS-ISAPIExtensions /FeatureName:IIS-
ISAPIFilter /FeatureName:IIS-StaticContent /FeatureName:IIS-ManagementConsole
/FeatureName:IIS-RequestFiltering /FeatureName:WAS-WindowsActivationService
/FeatureName:WCF-HTTP-Activation45 /FeatureName:NetFx3 /FeatureName:IIS-
NetFxExtensibility45 /FeatureName:NetFx4Extended-ASPNET45 /FeatureName:WAS-
ConfigurationAPI
```

3.2. Установка КриптоПро DSS

3.2.1. Установка

Для установки компонентов сервера электронной подписи «КриптоПро DSS» запустите установку пакета DSSInstall.exe, расположенного на компакт-диске. Установка КриптоПро DSS должна осуществляться от имени пользователя с правами администратора. После коротких подготовительных процедур на экране появится окно Мастера установки (см. Рис. 6).

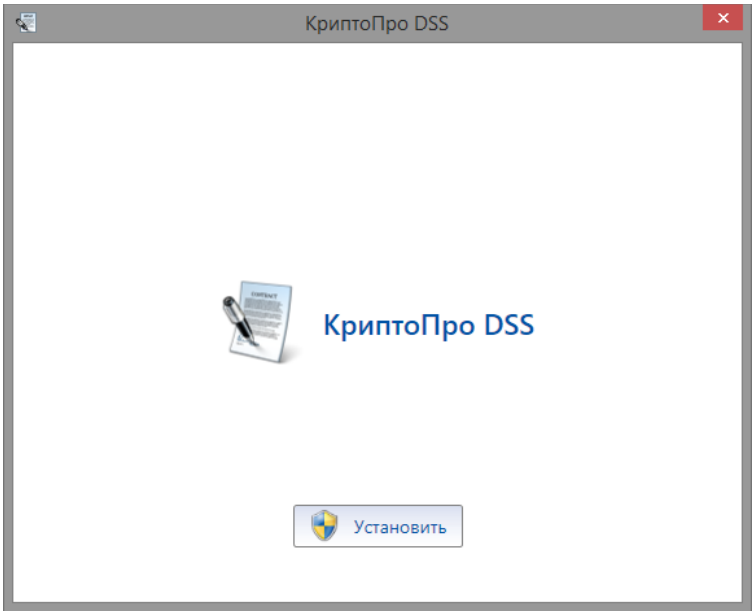

Рис. 6 – Начало установки КриптоПро DSS

После нажатия кнопки «Установить» будет предложено установить Microsoft .NET Framework, если он отсутствует (Рис. 7). Для его установки также потребуются права администратора. Установка проходит в автоматическом режиме.

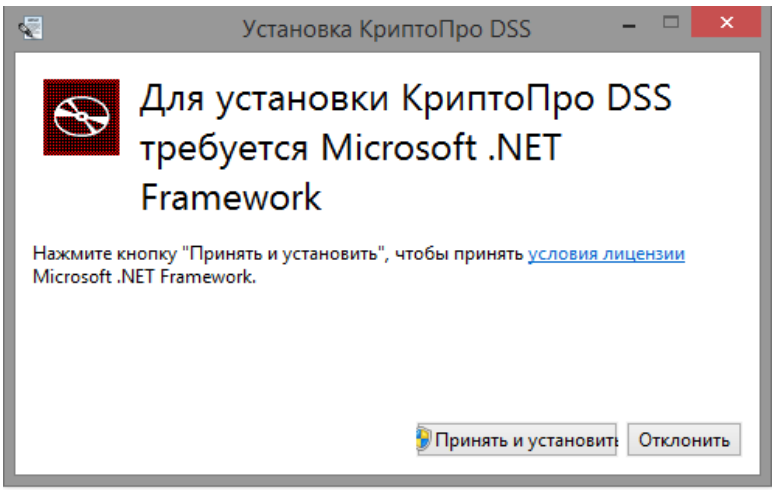

Рис. 7 – Установка Microsoft .NET Framework

После установки дополнительного ПО предлагается ознакомиться и принять условия лицензионного соглашения на использование ПО (Рис. 8). Если Вы согласны со всеми пунктами соглашения, выделите пункт «Я принимаю условия этого соглашения», и нажмите «Далее».

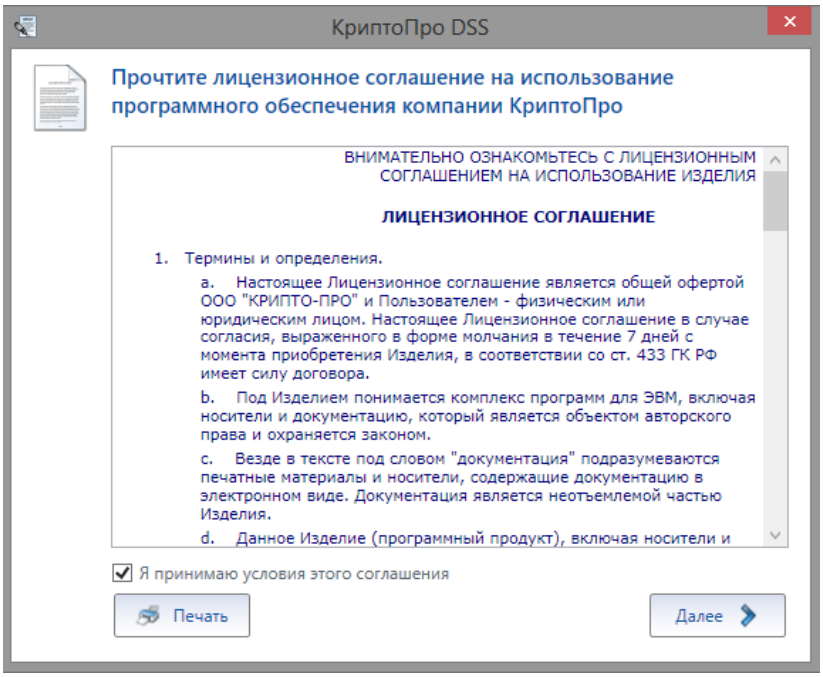

Рис. 8 – Условия лицензионного соглашения

На следующем этапе необходимо выбрать компоненты СЭП «КриптоПро DSS», которые будут установлены (Рис. 9).

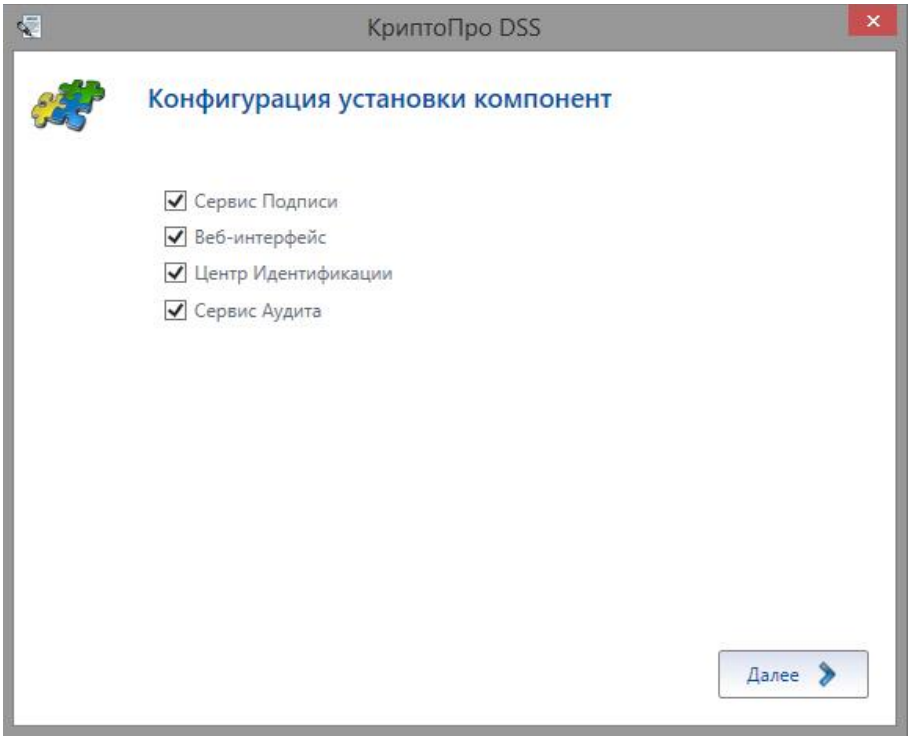

Рис. 9 – Выбор компонентов для установки

На следующем шаге необходимо выбрать директорию, куда будет установлен КриптоПро DSS (Рис. 10).

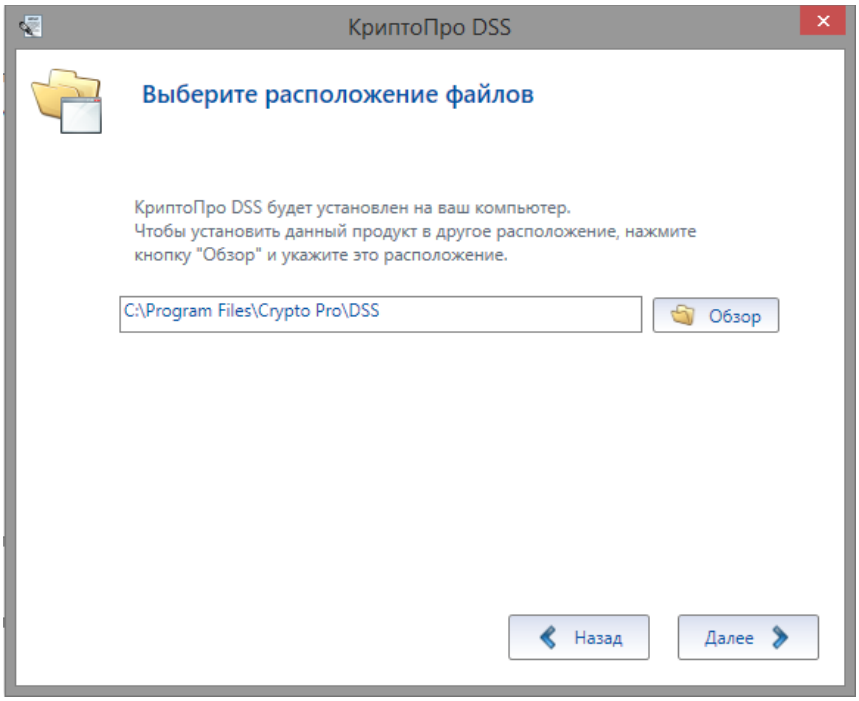

Рис. 10 – Выбор директории установки

Следующее окно (Рис. 11) носит информационный характер, сообщая, какие компоненты будут установлены в выбранную директорию. Нажатие кнопки «Установить» запускает процесс установки.

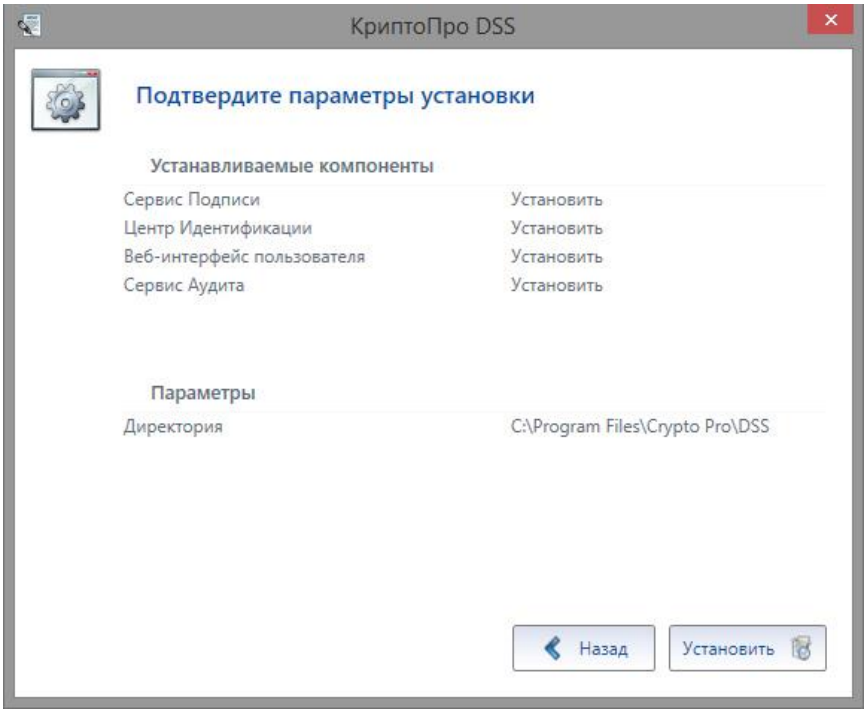

Рис. 11 – Подтверждение параметров установки

После завершения установки КриптоПро DSS (Рис. 12) необходимо нажать кнопку «Готово» и перезагрузить рабочую станцию.

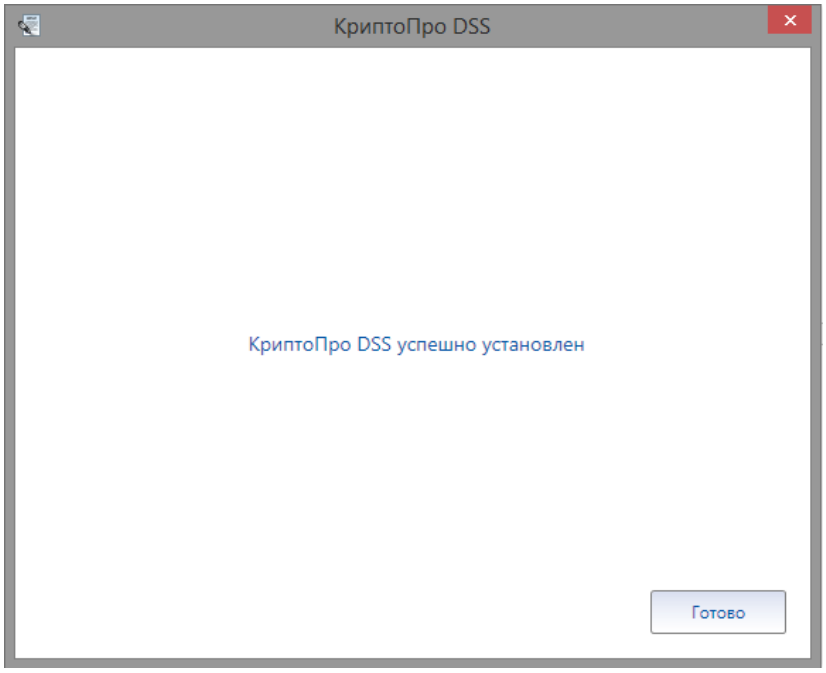

Рис. 12 – Завершение установки

3.2.2. Добавление/удаление компонентов

Для добавления или удаления компонентов сервера электронной подписи «КриптоПро DSS» запустите установку пакета DSSInstall.exe, расположенного на компакт-диске и нажмите «Установить» (см. Рис. 6). Изменение установки КриптоПро DSS должно осуществляться от имени пользователя с правами администратора.

На следующей странице мастера установки необходимо выбрать «Добавить/удалить компоненты» и нажать кнопку «Далее» (Рис. 13).

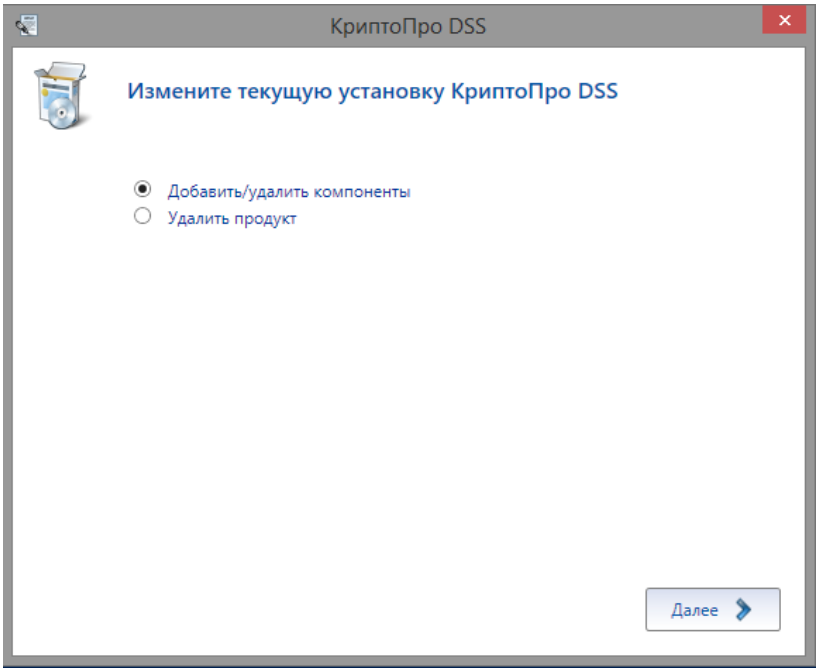

Рис. 13 – Выбор изменения установки

На следующей странице мастера необходимо выбрать конфигурацию установки КриптоПро DSS (см. Рис. 14). В списке компонентов отмечены уже установленные компоненты. Если требуется установить компонент – отметьте его в списке. Если требуется удалить установленный компонент – снимите выделение нужного компонента. Для продолжения установки нажмите кнопку «Далее».

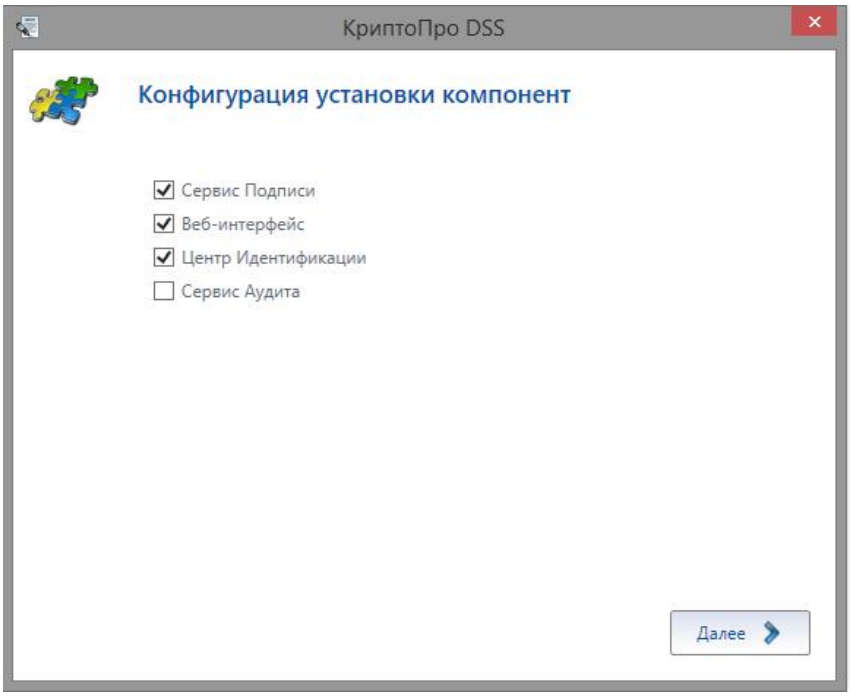

Рис. 14 – Выбор компонентов для изменения

На следующей странице подтвердите параметры изменения и нажмите кнопку «Далее» (см. Рис. 15). Если один или несколько компонентов КриптоПро DSS были выбраны для удаления, напротив них в списке появится слово «Удалить». Если один или несколько компонентов КриптоПро DSS были выбраны для установки, напротив них в списке появится слово «Установить». Напротив компонента, который изменения не затрагивают, в списке появится слово «Не изменять».

При желании изменить конфигурацию компонентов, подлежащих установке/удалению, нажмите кнопку «Назад».

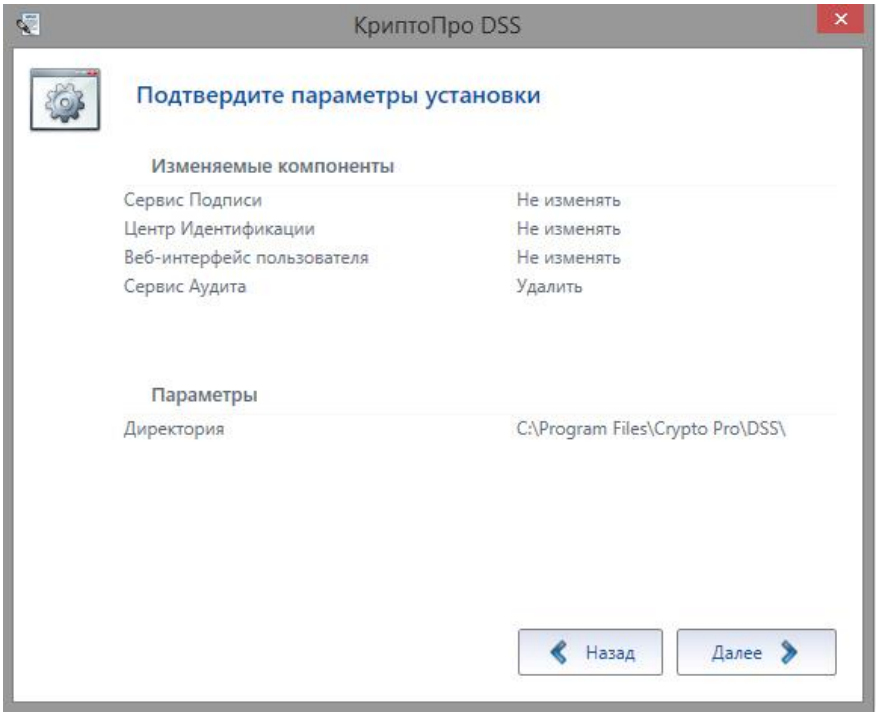

Рис. 15 – Информация об изменении конфигурации компонентов

На следующей странице (Рис. 16) отображаются созданные ранее экземпляры служб, которые затрагивает изменение установки. При удалении компонента уничтожаются все созданные экземпляры служб. При желании изменить конфигурацию компонентов, подлежащих установке/удалению, нажмите кнопку «Назад», в противном случае – кнопку «Далее».

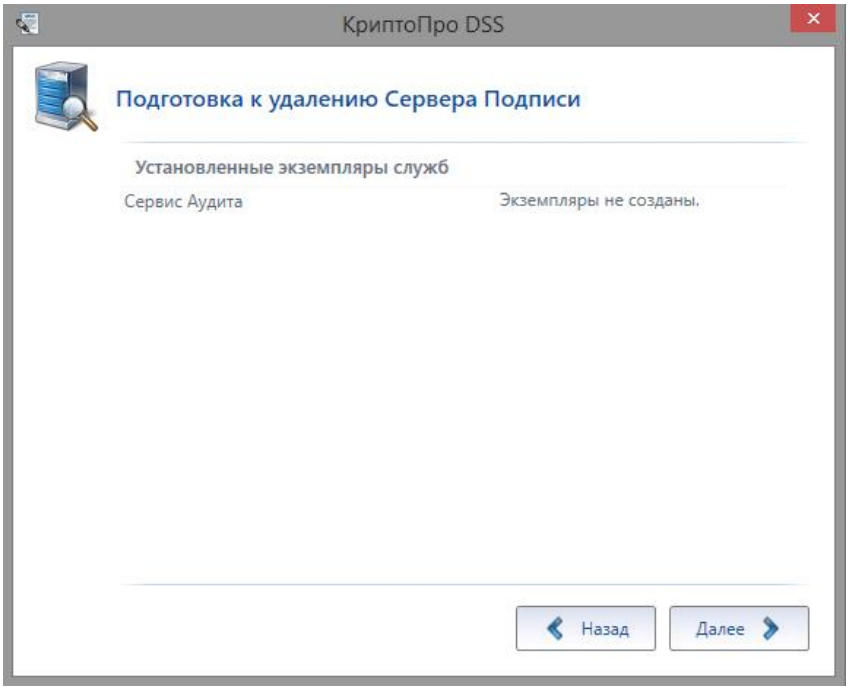

Рис. 16 – Информация о затрагиваемых изменением установки экземплярах служб

После выполнения всех описанных шагов мастер изменит установку КриптоПро DSS, сопровождая действия комментариями. По окончании изменения мастер покажет окно с подтверждением успешного изменения (Рис. 17), в котором необходимо нажать кнопку «Готово». После завершения установки требуется перезагрузить рабочую станцию.

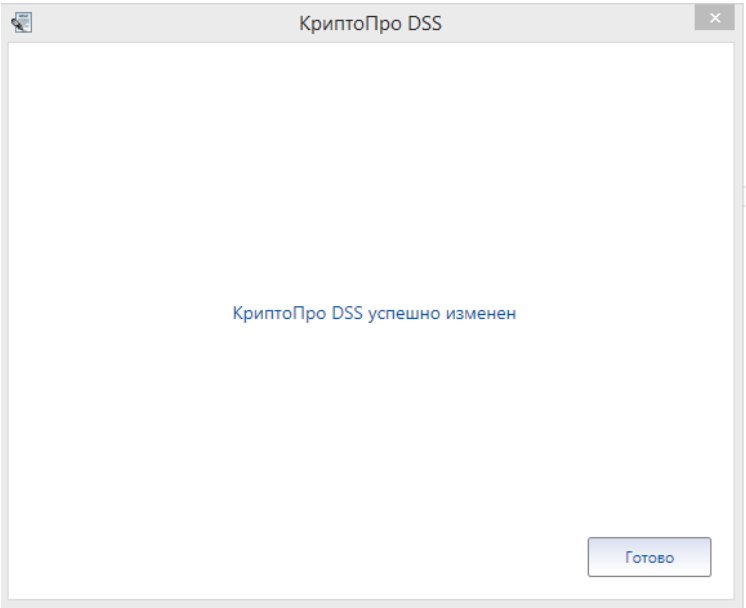

Рис. 17 – Завершение изменения компонентов КриптоПро DSS

3.2.3. Обновление

Для обновления КриптоПро DSS запустите установку пакета **DSSInstall.exe**, расположенного на компакт-диске (Рис. 6). После подготовительных процедур отобразится страница с информацией об обновлении (см. Рис. 18). Для продолжения нажмите кнопку «Далее».

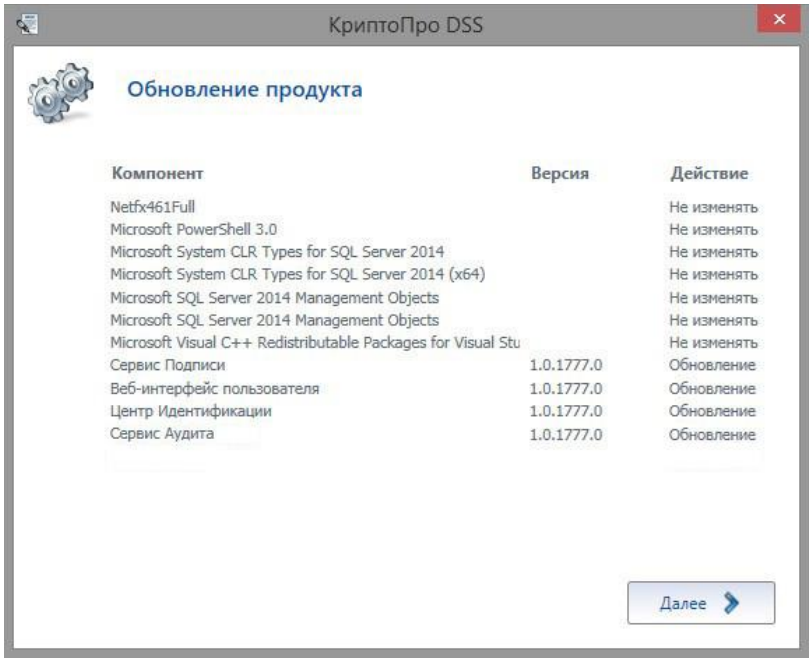

Рис. 18 – Компоненты КриптоПро DSS, подлежащие обновлению

На странице подготовки к обновлению (Рис. 19) отображаются необходимые проверки, которые будут проведены перед установкой обновления. Здесь же можно получить сведения о них, выбрав иконку с буквой «i». Чтобы выполнить обновление КриптоПро DSS, нажмите кнопку «Выполнить».

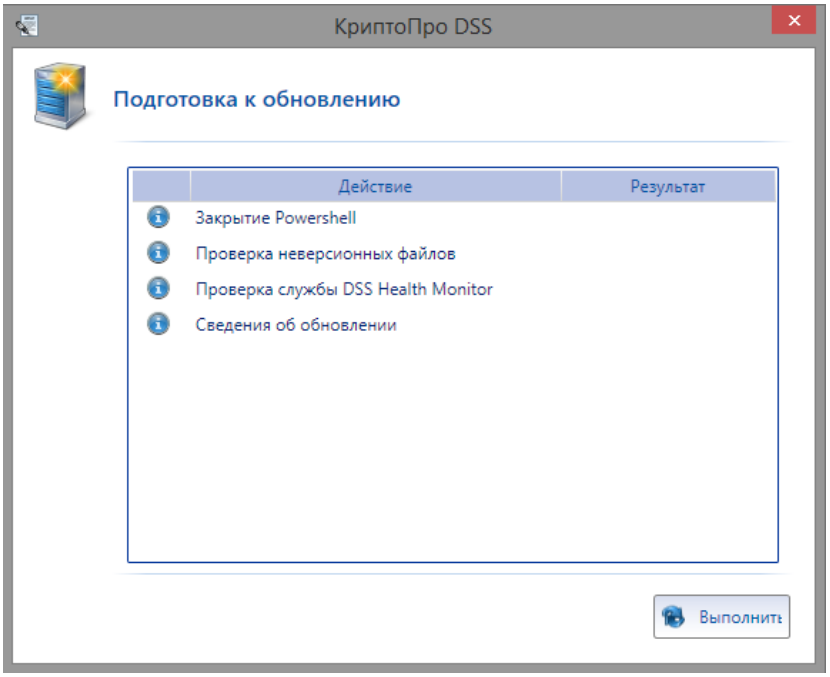

Рис. 19 – Подготовка к обновлению (1)

На следующей странице подготовки к обновлению (Рис. 20) отображаются результаты проведенных проверок, где также можно получить сведения об этих результатах, выбрав иконку с буквой «i». Чтобы продолжить обновление КриптоПро DSS, нажмите кнопку «Далее».

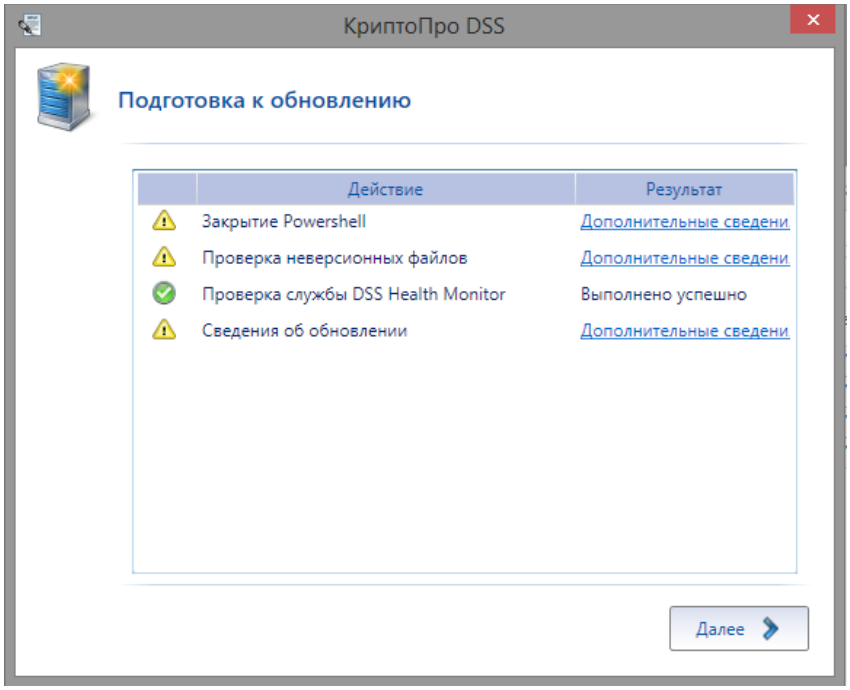

Рис. 20 – Подготовка к обновлению (2)

После обновления файлов отобразится страница с обновлением развёрнутых экземпляров компонентов КриптоПро DSS (Рис. 21). Для продолжения нажмите кнопку «Далее».

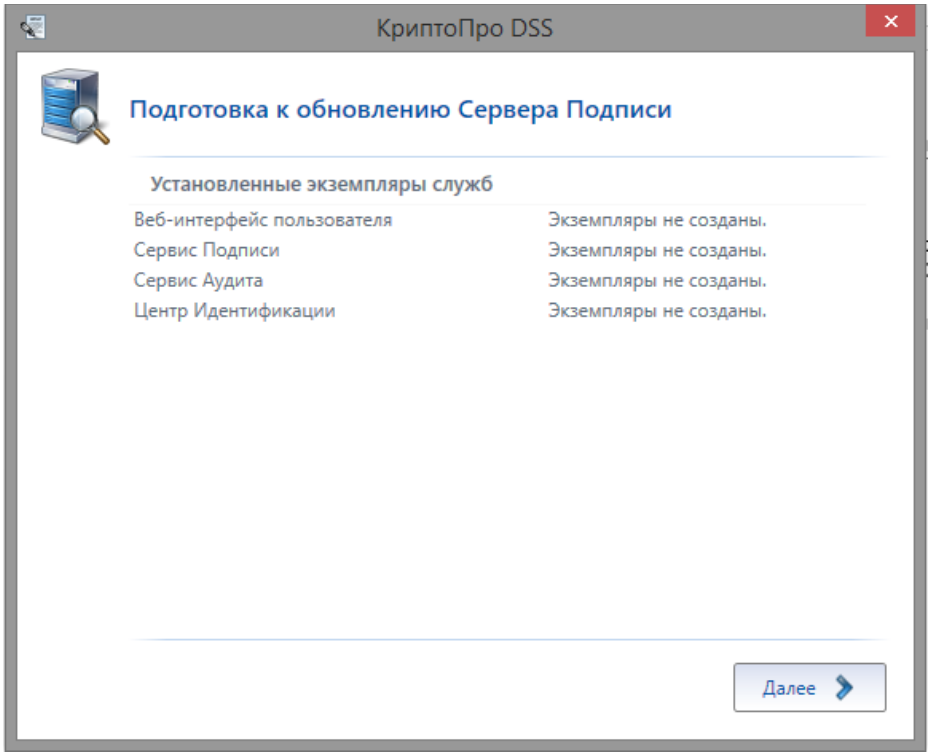

Рис. 21 – Сведения об имеющихся экземплярах КриптоПро DSS

Обновление КриптоПро DSS продолжится в автоматическом режиме. По его завершении отобразится окно с надписью «КриптоПро DSS успешно обновлен» (Рис. 22). Для завершения обновления и выхода из программы установки нажмите «Готово».

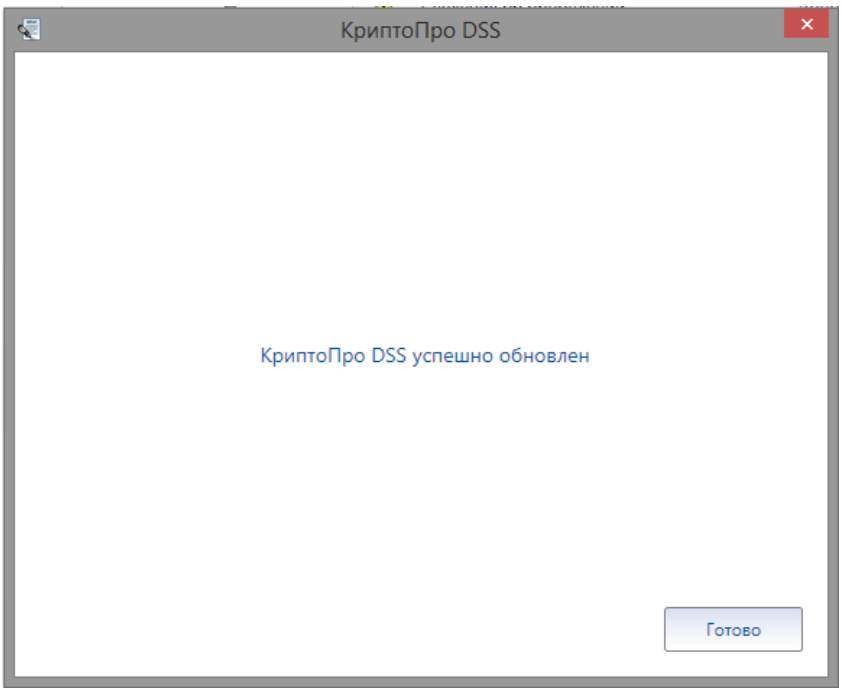

Рис. 22 – Завершение обновления КриптоПро DSS

3.2.4. Удаление

Для удаления сервера электронной подписи «КриптоПро DSS» запустите установку пакета **DSSInstall.exe**, расположенного на компакт-диске, или запустите установщик на удаление из раздела Программы и Компоненты на Панели управления. Удаление «КриптоПро DSS» должно осуществляться от имени пользователя с правами администратора.

При удалении компонентов «Сервис Подписи», «Центр Идентификации», «Сервис Аудита», будут удалены БД соответствующих экземпляров служб.

Если установщик «КриптоПро DSS» запускается с компакт-диска, на первой странице Мастера установки необходимо выбрать необходимое действие: удаление продукта. Для продолжения нажмите кнопку «Далее» (Рис. 23).

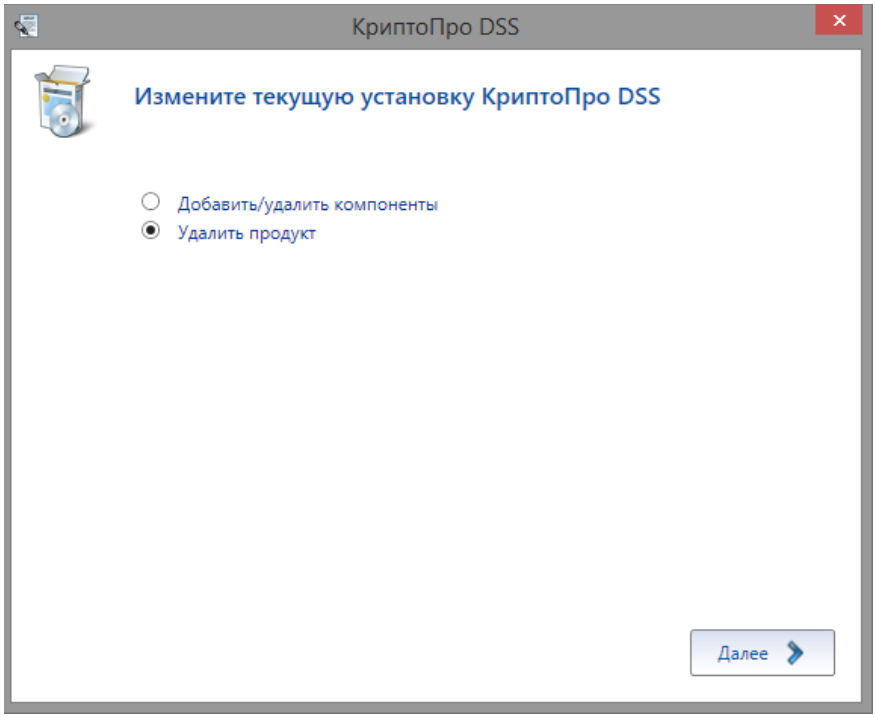

Рис. 23 – Выбор удаления КриптоПро DSS

На следующей странице Мастера (Рис. 24) отображаются развернутые экземпляры служб, которые будут затронуты при удалении КриптоПро DSS. Для продолжения нажмите кнопку «Далее».

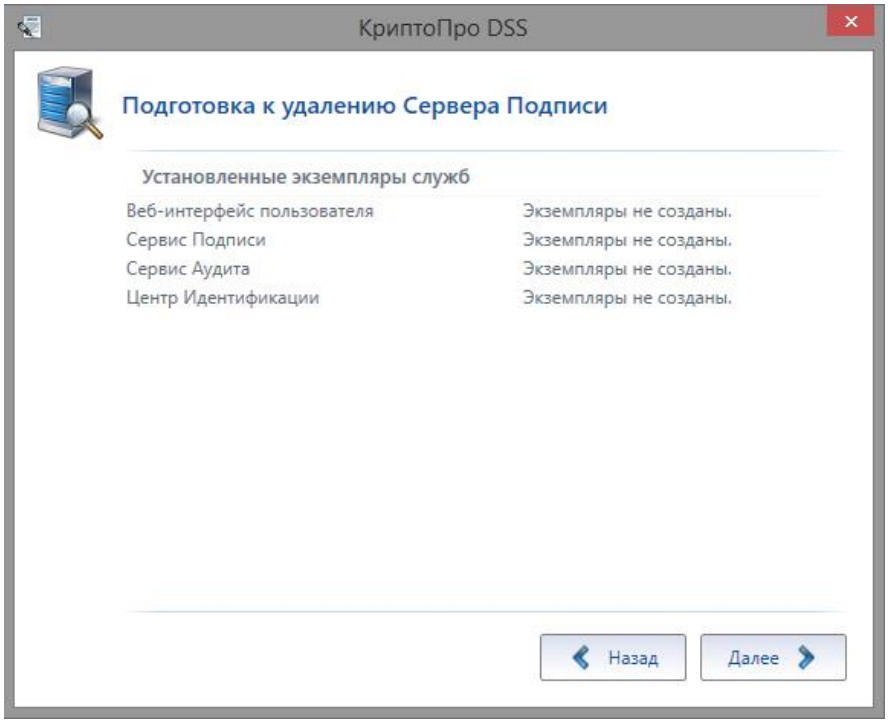

Рис. 24 – Подготовка к удалению КриптоПро DSS

После выполнения всех описанных шагов, мастер установки удалит КриптоПро DSS, сопровождая действия комментариями. По окончании удаления мастер покажет

окно с подтверждением успешного удаления (Рис. 25), в котором необходимо нажать кнопку «Готово», чтобы выйти из программы установки.

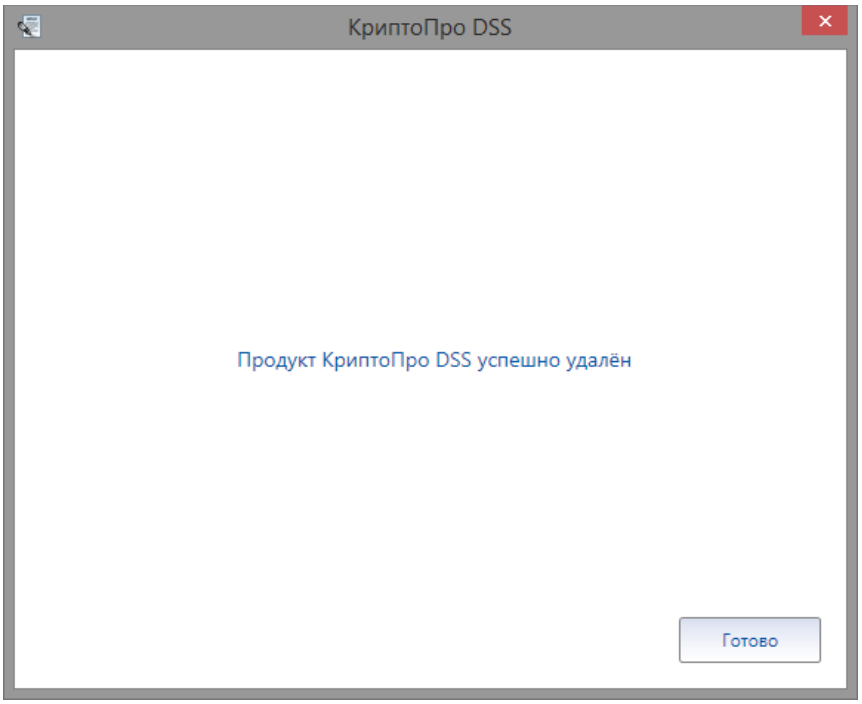

Рис. 25 – Завершение удаления КриптоПро DSS

3.3. Установка ПАКМ «КриптоПро HSM»

Программно-аппаратный криптографический модуль (ПАКМ) «КриптоПро HSM» является необходимым элементом архитектуры комплексного решения на базе СЭП «КриптоПро DSS» и должен устанавливаться в соответствии с процедурой, описанной в документе «ЖТЯИ.00096-02 95 01 КриптоПро HSM. Правила пользования», входящем в комплект поставки ПАКМ «КриптоПро HSM».

После того, как ПАКМ «КриптоПро HSM» установлен, на рабочую станцию, на которой развертывается компонент Сервис Подписи, следует установить КриптоПро HSM Client. Подробная инструкция по установке приведена в документе «ЖТЯИ.00096-02 93 01 КриптоПро HSM. Руководство Пользователя», входящем в комплект поставки ПАКМ «КриптоПро HSM».

Сервис Подписи может работать только с криптопровайдером «Crypto-Pro HSM Svc CSP» (тип 75). Для регистрации криптопровайдера на Сервисе Подписи используйте командлет Add-DssCryptoProvider.

Для взаимодействия сервиса электронной подписи с ПАКМ «КриптоПро HSM» необходимо добавить учетную запись, под которой работает Сервис Электронной подписи (по умолчанию – **IIS AppPool\CryptoProDSS-1-SignServer)**, в группу «**Привилегированные пользователи КриптоПро HSM**» (пользователи, которые имеют право подключения к «КриптоПро HSM»). Если такой группы нет, то ее необходимо создать.

3.5. Развертывание ЦИ

Развёртывание Центра Идентификации КриптоПро DSS осуществляется в следующем порядке:

1. Установка веб-сервера Microsoft IIS с необходимыми компонентами (см. раздел 3.1).
2. Установка экземпляра СУБД Microsoft SQL Server версии 2008 R2/2012/2014/2016/2017. В качестве метода аутентификации необходимо выбрать «Режим проверки подлинности Windows».
3. Установка «КриптоПро CSP».
4. Установка Центра Идентификации КриптоПро DSS (см. раздел 3.2.1).
5. Настройка Центра Идентификации КриптоПро DSS (см. раздел 4.5).

3.6. Развертывание Сервиса Подписи

Развёртывание Сервиса Подписи осуществляется в следующем порядке:

1. Развертывание веб-сервера Microsoft IIS с необходимыми компонентами (см. пункт 4.1).
2. Установка экземпляра СУБД Microsoft SQL Server версии 2008 R2/2012/2014/2016/2017. В качестве метода аутентификации необходимо выбрать Windows проверка подлинности.
3. Установка «КриптоПро CSP».
4. Установка КриптоПро HSM Client (см. раздел 3.3).
5. Установка «КриптоПро .NET».
6. Установка Сервиса Подписи (см. раздел 3.2.1).
7. Настройка Сервиса Подписи (см. раздел 4.5.8).

Для поддержки форматов подписи (XMLDSig, PDF, MS Office) необходимо установить продукт «КриптоПро .NET» и ввести действующую лицензию.

Для поддержки формата подписи CAdES-X Long Type 1 требуется ввести действующие лицензии на продукты «КриптоПро TSP Client» и «КриптоПро OCSP Client». Данные продукты входят в состав дистрибутива СЭП «КриптоПро DSS».

Для корректной работы СЭП потребуется наличие на сервере продукта «КриптоПро CSP» (входит в комплект поставки ПАКМ «КриптоПро HSM»).

3.7. Развертывание Веб-интерфейса Пользователя

Развёртывание Веб-интерфейса Пользователя КриптоПро DSS осуществляется в следующем порядке:

1. Установка веб-сервера Microsoft IIS с необходимыми компонентами (см. пункт 4.1).

2. Установка Веб-интерфейса Пользователя КриптоПро DSS (см. раздел 3.1.1).
3. Настройка Веб-интерфейса Пользователя КриптоПро DSS (см. раздел 5.4).

3.8. Развертывание Сервиса Аудита

Развертывание Сервиса Аудита КриптоПро DSS осуществляется в следующем порядке:

1. Установка веб-сервера Microsoft IIS с необходимыми компонентами (см. пункт 4.1).
2. Установка экземпляра СУБД Microsoft SQL Server версии 2008 R2/2012/2014/2016/2017. В качестве метода аутентификации необходимо выбрать Windows проверка подлинности.
3. Установка Сервиса Аудита (см. раздел 3.1.1).
4. Настройка Сервиса Аудита (см. раздел 4.7.4).

3.9. Развертывание myDSS

Развёртывание компонента myDSS осуществляется в следующем порядке:

1. Установка веб-сервера Microsoft IIS с необходимыми компонентами (см. раздел 3.1).
2. Установка экземпляра СУБД Microsoft SQL Server версии 2008 R2/2012/2014/2016/2017. В качестве метода аутентификации необходимо выбрать «Режим проверки подлинности Windows».
3. Установка «КриптоПро CSP».
4. Установка компонента myDSS (см. раздел 3.2.1).
5. Настройка компонента myDSS (см. раздел 4.11).

3.10. Развертывание баз данных служб

Сервис Подписи, Центр Идентификации, Сервис Аудита и myDSS для своей работы требуют подключения к базам данных на SQL-сервере. Базы данных служб создаются при разворачивании экземпляров Сервиса Подписи, Центра Идентификации, Сервиса Аудита и myDSS с помощью командлетов New-DssSignServerInstance, New-DssStsInstance, New-DSSCmisInstance, New-MyDssServerExternalInstance, New-MyDssServerInternalInstance.

В простейшем случае, когда SQL-сервер развёрнут на одном сервере с экземпляром службы DSS, требуется задать только имя SQL-сервера и имя базы данных. Подключение Пользователя (Администратора DSS) и службы DSS будет осуществелено под соответствующими учётными записями Windows.

Если SQL-сервер развёрнут на отдельном хосте, то при разворачивании экземпляров службы требуется использовать параметр **ConnectionInfo** типа **CryptoPro.DSS.Common.Utils.SqlConnectionInfo.**

В Таблица 3 приведено описание структуры **SqlConnectionInfo:**

Таблица 3. Описание структуры SqlConnectionInfo

Параметр	Тип	Описание
ServerName	string	Адрес экземпляра SQL-сервера, на котором следует развернуть базу данных. Формат: <SQL-сервер host>\<имя экземпляра>
DatabaseName	string	Имя базы данных.
AsUser	string	Имя Пользователя SQL-сервера, под которым будет установлено соединение.
AsUserPassword	string	Пароль Пользователя SQL-сервера, под которым будет установлено соединение.
AccountType	ServiceAccountType	Тип учетной записи службы.
ServiceAccountName	string	Имя учётной записи службы для подключения к SQL-серверу.
ServiceAccountPassword	string	Пароль учётной записи службы для подключения к SQL-серверу.
SkipValidation	bool	Пропустить проверки подключения к SQL-серверу.
UseExistingDB	bool	Подключиться к существующей базе данных.

Если хост SQL-сервера и хост экземпляра службы DSS находятся в домене Windows, то по умолчанию будет использована Windows-аутентификация Пользователя и службы DSS при подключении к SQL-серверу. В этом случае требуется задать имя и пароль учётной записи службы DSS (параметры **ServiceAccountName** и **ServiceAccountPassword**). Учётная запись службы должна быть предварительно создана в домене. Под данной учётной записью будет работать пул приложений службы на IIS. Учётная запись службы DSS будет зарегистрирована на SQL-сервере при разворачивании экземпляра. Ниже приведён пример скрипта для разворачивания экземпляра Сервиса Подписи с базой данных на удалённом SQL-сервере.

```
Import-Module CryptoPro.DSS.PowerShell.SignServer
$connInfo = New-Object -Type CryptoPro.Dss.Common.Utils.SqlConnectionInfo
$connInfo.DatabaseName = “SignatureServerDB”
$connInfo.ServerName = “alwaysOn”
$connInfo.ServiceAccountName = “test\dssservice”
$connInfo.ServiceAccountPassword = “P@s$w0rd”
New-DssSignServerInstance -DisplayName SignServer -SiteName “Default Web
Site” -ConnectionInfo $connInfo
```

Если один или оба хоста не включены в домен Windows, то для подключения к SQL-серверу будет использована SQL-аутентификация. В этом случае требуется задать учётные данные пользователя, который разворачивает экземпляр службы (параметры **AsUser** и **AsUserPassword**), и учётные данные службы DSS (параметры **ServiceAccountName** и **ServiceAccountPassword**). Учётная запись пользователя должна быть предварительно зарегистрирована на SQL-сервере и иметь достаточный набор прав для создания базы данных. Учётная запись службы DSS будет зарегистрирована на SQL-сервере при разворачивании экземпляра.

Пользователь может самостоятельно решить, с какими учётными данными будет подключаться служба к SQL-серверу и пользователь для создания базы данных. Для этого требуется установить параметр **SkipValidation** в значение $true. Если не заданы параметры **AsUser** и **AsUserPassword,** то пользователь будет подключаться к SQL-серверу с помощью Windows-аутентификации. В противном случае - с помощью SQL-аутентификации с заданными учётными данными. Для службы требуется явно указать тип учётной записи через параметр **AccountType.** Параметр может принимать следующие значения:

- CryptoPro.Dss.Common.Utils.SqlConnectionInfo.ServiceAccountType.Windows;
- CryptoPro.Dss.Common.Utils.SqlConnectionInfo.ServiceAccountType.SqlAccount.

В обоих случаях требуется задать имя и пароль учётной записи службы DSS через параметры **ServiceAccountName** и **ServiceAccountPassword**.

Если разворачивается дополнительный экземпляр службы Сервиса Подписи или Центра Идентификации, то требуется указать имя существующей базы данных основного экземпляра и выставить параметр **UseExistingDB** в значение **$true.**

4. Настройка КриптоПро DSS

4.1. Общие сведения об администрировании компонентов КриптоПро DSS

Администрирование осуществляется через консоль PowerShell с помощью командлетов, входящих в состав PowerShell-модуля каждого из компонентов. В общем случае объекты администрирования поддерживают следующий набор действий:

- Создать объект (Add-*, New-*);
- Изменить параметры объекта (Set-*, Update-*);
- Получить параметры объекта (Get-*);
- Удалить объект (Remove-*).

Часть объектов поддерживают дополнительные действия, такие как: включить/отключить (Enable-*, Disable-*), копировать (Copy-*), протестировать (Test-*). Имена командлетов имеют следующую структуру: <Verb>-<Name>, где

- <Verb> – имя действия, выполняемого над объектом администрирования. Например: Add, Get, Update и т.д.
- <Name> – имя объекта администрирования

Список командлетов, входящих в состав PowerShell-модуля каждого из компонентов КриптоПро DSS, можно получить, выполнив команду:

```
Get-Command -Module CryptoPro.DSS.PowerShell.<Компонент> -CommandType Cmdlet
```

PowerShell-модули компонентов КриптоПро DSS приведены в Таблица 4.

Таблица 4. Модули компонентов КриптоПро DSS

Компонент	Имя модуля
Центр Идентификации	CryptoPro.DSS.PowerShell.STS
Сервис Подписи	CryptoPro.DSS.PowerShell.SignServer
Веб-интерфейс Пользователя	CryptoPro.DSS.PowerShell.Frontend
Сервис Аудита	CryptoPro.DSS.PowerShell.Analytics
Модуль аутентификации myDSS	CryptoPro.DSS.PowerShell.MyDSSInternal CryptoPro.DSS.PowerShell.MyDSSExternal

Для получения справки по каждому из командлетов выполните команду

```
Get-help <имя_командлета>
```

Например:

```
Get-Help Set-DSSStsProperties
```

или

```
Get-Help Set-DSSStsProperties -Full
```

4.1.1. Конвейер

Командлеты, входящие в состав Powershell-модулей DSS, поддерживают работу через конвейер (pipeline). Все командлеты Get- возвращают объекты. Полученные объекты могут быть через конвейер направлены в командлеты select, where, foreach, format-list, format-table и т.д.

Ниже приведены примеры работы с командлетами DSS через конвейер.

- Проверка доступности криптопровайдеров

```
Get-DssCryptoProvider | Test-DssCryptoProvider
```

- Добавление идентификатора проверяющей стороны

```
$identities = (Get-DssRelyingPartyTrust -Id 2).Identities
$identities.Add("https://newhostname/frontend")
Set-DssRelyingPartyTrust -Id 2 -Identities $identities
```

- Добавление новой службы TSP

```
$newTSP = New-Object -TypeName CryptoPro.DSS.Common.Service.TspService
$newTSP.Name = "New TSP Service Name"
$newTSP.Title = "New TSP Service Title"
$newTSP.Url = "http://hostname/tspNew/tsp.srf"
$tspList = (Get-DssProperties).TSPList
$tspList.Add($newTSP)
Set-DssProperties -TSPList $tspList
```

- Просмотр отдельных свойств объектов
  - Просмотр свойств криптопровайдеров

```
Get-DssCryptoProvider | select -ExpandProperty Settings
```

  - Просмотр свойств модуля оповещения

```
Get-DssStsNotifier -NotifierID 1 | select -ExpandProperty TransportPlugin
```

- Форматирование вывода в виде списка

```
Get-DssFeWSFederationSettings | format-list
```

- Форматирование вывода в виде таблицы

```
Get-DssFeWSFederationSettings | format-table
```

- Получение свойств (получение имени Мастер-ключа у объекта криптопровайдера)

```
 (Get-DssCryptoProvider -ID <prov_ID>) .Settings[
[CryptoPro.DSS.Common.Cryptography.Enums.CryptoProviderParam]::MasterKeyName]
```

- Изменение сертификата Оператора

```
$cert = Get-Item Cert:\LocalMachine\TrustedPeople\0A5193D4C … CA4437063
Set-DssIdentityOperator -IssuerName realsts -Login adminGost -Certificate
$cert
```

- Поиск модуля оповещения заданного типа

```
Get-DssStsNotifier | where { $_.Type -eq "Audit" }
```

- Выбор шаблонов сообщений заданного типа

```
Get-DssStsFormatterTemplate | where { $_.Destination -eq "MyDssAuth" }
```

- Получение кодов событий

```
(Get-DssSignServerEvent) | foreach { Write-host $_.EventType  "
("([int]$_.EventType)") - " $_.Id  }
```

- Вывод информации об ошибке

```
$error[0].Exception
$error[0].Exception.InnerException
```

4.2. Настройка лицензии в КриптоПро DSS

4.2.1. Лицензия на Сервис Подписи

Для использования Сервиса Подписи требуется ввести лицензию. Есть следующие типы лицензии на Сервис Подписи:

- **Демонстрационная.** Рассчитана на 10 Пользователей и не ограничена по сроку действия. Задается при помощи командлета Командлет Add-DssLicense. Лицензия закрепляется за каждым новым Пользователем, создавшим запрос на сертификат. После ввода Базовой лицензии Демонстрационная уничтожается.
- **Базовая.** Лицензия выдается на ограниченное количество Пользователей и позволяет им создать запрос на сертификат. Не ограничена по времени. Для одного экземпляра Сервиса Подписи может быть введена только одна Базовая лицензия. При вводе новой Базовой лицензии, старая уничтожается.
- **На расширение Базовой лицензии.** Лицензия выдается на ограниченное количество Пользователей и назначается Пользователю только после исчерпания лимита Пользователей в Базовой лицензии. Лицензий на расширение может быть сколько угодно.
- **Ограниченная по сроку действия.** В лицензии прописан явно срок окончания действия, а также может быть ограничено количество Пользователей. Данная лицензия заменяет Демонстрационную, не требует обязательного наличия Базовой и/или лицензии На расширение, но может их дополнять. Ограниченная по сроку действия лицензия может быть введена только одна. Ввод новой Ограниченной по сроку лицензии заменяет старую.
- **На дополнительный сервер.** Используется для создания сервера репликации.

Ввод лицензии осуществляется при помощи командлетов PowerShell. Команды управления общей лицензией на Сервис Подписи включены в модуль **CryptoPro.DSS.PowerShell.SignServer.** Список команд приведен в Таблица 5.

Таблица 5. Список командлетов для управления лицензией на Сервис Подписи

Командлет	Описание
Add-DssLicense	Задание лицензии на Сервис Подписи.
Remove-DssLicense	Удаление лицензии на Сервис Подписи.
Get-DssLicense	Вывод на консоль сведений о лицензии на Сервис Подписи.

4.2.1.1. Командлет Add-DssLicense

Командлет позволяет задать лицензию на Сервис Подписи. К основным параметрам относятся:

- Серийный номер;
- Наименование организации (если выданная лицензия предусматривает обязательный ввод имени организации).

Ввод командлета без параметров активирует Демонстрационную лицензию на Сервис Подписи (см. Раздел 4.2.1).

Синтаксис:

```
Add-DssLicense [-SerialNumber <string>] [-CompanyName <string>] [-DisplayName
<string>] [-Force]
```

Таблица 6. Параметры командлета Add-DssLicense

Параметр	Тип	Описание
SerialNumber	string	Серийный номер.
CompanyName	string	Наименование организации.
DisplayName	string	Отображаемое имя экземпляра Сервиса Подписи.
Force	switch	Параметр позволяет без подтверждения открепить Пользователей от предыдущей лицензии и привязать к новой.

4.2.1.1. Командлет Get-DssLicense

Командлет позволяет вывести на консоль информацию о лицензии на Сервис Подписи.

Синтаксис:

```
Get-DssLicense -DisplayName <string> -AssignedUsersInfo
```

Таблица 7. Параметры командлета Get-DssLicense

Параметр	Тип	Описание
AssignedUsersInfo	string	При наличии данного параметра выводится информации о текущем количестве Пользователей, подключенных к данной лицензии.
DisplayName	string	Отображаемое имя экземпляра Сервиса Подписи.

4.2.1.1. Командлет Remove-DssLicense

Командлет позволяет удалить лицензию на Сервис Подписи. К параметрам относятся:

Синтаксис:

```
Remove-DssLicense [-DisplayName <string>] -SerialNumber <string> [Force]
```

Таблица 8. Параметры командлета Remove-DssLicense

Параметр	Тип	Описание
SerialNumber	string	Серийный номер.
DisplayName	string	Отображаемое имя экземпляра Сервиса Подписи
Force	switch	Параметр позволяет без подтверждения открепить Пользователей от предыдущей лицензии и привязать к новой.

4.2.2. Лицензия на компоненты ЦИ

Для каждого из следующих компонентов ЦИ, отвечающих за аутентификацию, требуется лицензия:

- **На средство аутентификации myDSS** (аутентификация пользователей с помощью мобильного приложения myDSS);
- **На средство аутентификации SimAuth** (аутентификация Пользователей с помощью апплета на SIM-карте);
- **На модуль доступа Cloud CSP** (облачный крипропровайдер Cloud CSP).

Для каждого из этих компонентов существуют следующие типы лицензии:

- **Демонстрационная.** Активируется автоматически при создании экземпляра ЦИ, рассчитана на 10 Пользователей и не ограничена по сроку действия. После ввода Базовой или Ограниченной по сроку действия лицензии Демонстрационная уничтожается.
- **Базовая.** Лицензия выдается на ограниченное количество Пользователей и не ограничена по времени. Для одного экземпляра ЦИ может быть введена только одна Базовая лицензия. При вводе новой Базовой лицензии, старая уничтожается, а

переназначение лицензии Пользователям происходит автоматически при попытке подтверждения операции или вручную при назначении метода аутентификации.

- **На расширение Базовой лицензии.** Лицензия дополняет Базовую (не может быть введена без нее) и выдается на ограниченное количество Пользователей. Лицензий На расширение может быть сколько угодно.
- **Ограниченная по сроку действия.** В лицензии прописан явно срок окончания действия, а также может быть ограничено количество Пользователей. Данная лицензия заменяет Демонстрационную, не требует обязательного наличия Базовой и/или лицензии На расширение, но может их дополнять. Ограниченная по сроку действия лицензия может быть введена только одна. Ввод новой Ограниченной по сроку лицензии заменяет старую.

При наличии введенной лицензии на тот или иной компонент ЦИ из перечисленных выше, лицензии закрепляются за Пользователями автоматически при назначении метода аутентификации или при попытке подтверждения операции. При отключении у Пользователя какого-либо из методов аутентификации или модуля доступа Cloud CSP, лицензия освобождается и может быть занята другим Пользователем.

Команды управления лицензий на компоненты ЦИ включены в модуль **CryptoPro.DSS.PowerShell.Sts.** Список команд приведен в Таблица 9.

Таблица 9. Список командлетов для управления лицензией на средства аутентификации

Командлет	Описание
Add-DssStsLicense	Задание лицензии на компоненты ЦИ.
Get-DssStsLicense	Вывод на консоль сведений о лицензии на компоненты ЦИ.
Remove-DssStsLicense	Удаление лицензии на компоненты ЦИ.

4.2.2.1. Командлет Add-DssStsLicense

Командлет позволяет задать лицензию на компоненты ЦИ. К основным параметрам относятся:

- Серийный номер;
- Наименование организации (если выданная лицензия предусматривает обязательный ввод имени организации).

Синтаксис:

```
Add-DssStsLicense -SerialNumber <string> [-CompanyName <string>] [-
DisplayName <string>] [-Force]
```

Таблица 10. Параметры командлета Add-DssStsLicense

Параметр	Тип	Описание
SerialNumber	string	Серийный номер.
CompanyName	string	Наименование организации.

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра ЦИ.
Force	bool	Параметр позволяет без подтверждения открепить Пользователей от предыдущей лицензии и привязать к новой.

4.2.2.2. Командлет Get-DssStsLicense

Командлет позволяет вывести на консоль информацию о лицензии на компоненты ЦИ Пользователя.

Синтаксис:

```
Get-DssStsLicense -IdentityMethodType <string>[-DisplayName] <string>
```

Таблица 11. Параметры командлета Get-DssStsLicense

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра ЦИ.
IdentityMethodType	string Возможные значения: myDSS, SimAuth CloudCSP	Метод аутентификации, информацию о лицензии на который нужно получить.

4.2.2.3. Командлет Remove-DssStsLicense

Командлет позволяет удалить лицензию на компоненты ЦИ.

Синтаксис:

```
Remove-DssStsLicense -SerialNumber <string> [-DisplayName] <string> [-Force]
```

Таблица 12. Параметры командлета Remove-DssStsLicense

Параметр	Тип	Описание
SerialNumber	string	Серийный номер.
DisplayName	string	Отображаемое имя экземпляра ЦИ.
Force	switch	Параметр позволяет без подтверждения открепить Пользователей от предыдущей лицензии и привязать к новой.

4.3. Настройка учетных записей

Управление учетными записями в КриптоПро DSS осуществляется на основе ролевой модели. Выделяется 4 типа ролей, относящихся непосредственно к СЭП «КриптоПро DSS»(см. Рис. 26):

- Пользователь;
- Оператор;
- Оператор Аудита;
- Администратор.

Поскольку роль Администратора логически не зависит от групп и создается на каждом экземпляре компонента КриптоПро DSS, имеющем БД, только для получения прав на выполнение управляющих командлетов (см. раздел 4.3.4), на данной схеме она не отображается.

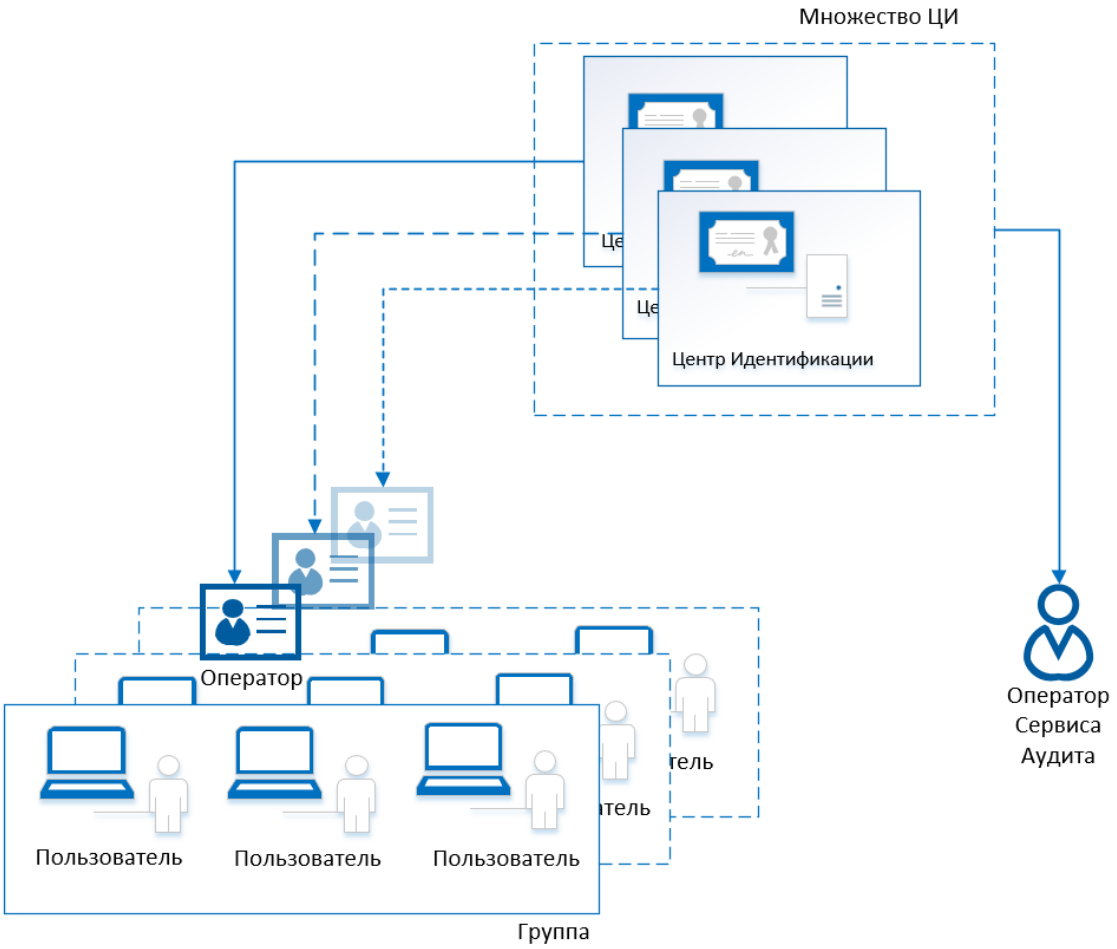

Рис. 26 – Логическая структура ролей СЭП

Соответственно перечисленным ролям, в КриптоПро DSS можно создавать учетные записи. Кроме этого, учетная запись может принадлежать к конкретному экземпляру (экземплярам) ЦИ, на котором была создана, а также к группе.

Далее дано подробное описание настройки учетных записей для каждой из перечисленных ролей.

4.3.1. Настройка учетных записей Пользователей

Пользователь СЭП «КриптоПро DSS» - любой пользователь, получивший учетные данные для входа от Оператора. Ему доступен основной функционал СЭП и личный кабинет, где он может просмотреть свой профиль и настроенные для него виды аутентификации. Редактирование личных данных и способов аутентификации осуществляется в основном Оператором, однако в системе есть возможность выдачи Пользователю прав на такие действия. Пользователю может быть назначена только одна группа.

Управление учетными записями Пользователей в СЭП «КриптоПро DSS» может осуществляться только через веб-интерфейс (Оператором и частично самим Пользователем).

Пользователи, прошедшие процедуру аутентификации, объединены вокруг своего экземпляра Центра Идентификации. Для них могут быть включены общие настройки первичной и вторичной аутентификации, а также политика компонент имени, в которой указывается, какие компоненты имени обязательно должны присутствовать при регистрации Пользователя.

Пользователи, относящиеся к одному экземпляру ЦИ, могут быть разделены на группы под управлением Операторов. Группа Пользователей характеризуется различными политиками, настроенной для всех входящих в нее Пользователей и Операторов. Это могут быть правила входа, вторичной аутентификации (подтверждение входа и подтверждение операций и др., см. раздел 4.5). Если на Центре Идентификации разрешена самостоятельная регистрация (в тестовом режиме), то при создании Пользователем своей учётной записи он будет включен в группу по умолчанию.

Для каждого Пользователя индивидуально могут быть заданы способы аутентификации и подтверждения входа и операций. Однако изменение этих настроек должно соответствовать настройкам экземпляра ЦИ, в котором Пользователь создан.

4.3.2. Настройка учетных записей Операторов

Оператор СЭП «КриптоПро DSS» – привилегированный пользователь, имеющий право на создание, редактирование и удаление учётных записей Пользователей, а также на управление сертификатами Пользователей DSS. Оператор может управлять учётными записями и сертификатами Пользователей только в рамках своего Центра Идентификации и своей группы. Оператор может быть включен в одну и более групп. При создании учётной записи Оператора ему назначается группа по умолчанию Default. В дальнейшем можно изменить набор групп, в которые включен Оператор.

Оператор СЭП «КриптоПро DSS» обеспечивает выполнение следующих задач:

- Регистрация Пользователей СЭП «КриптоПро DSS»;
- Управление (редактирование, удаление) учетными записями зарегистрированных Пользователей СЭП «КриптоПро DSS»;
- Настройка аутентификации Пользователей;
- Прием заявлений на регистрацию средств аутентификации Пользователей;
- Просмотр средств аутентификации, зарегистрированных в ЦИ КриптоПро DSS;

- Создание запросов на сертификаты Пользователей СЭП «КриптоПро DSS»;
- Выдача сертификатов Пользователям;
- Просмотр и печать событий аудита назначенных Оператору групп.

В целях обеспечения безопасности Центр Идентификации не имеет предустановленной встроенной учетной записи Оператора. Поэтому создание учетной записи Оператора возможно только локально на сервере, где установлен Центр Идентификации КриптоПро DSS. Роль Оператора назначается Администратором путем выдачи Оператору сертификата с расширенными правами и клиентской аутентификацией. Сертификат должен храниться в хранилище «Личные» текущего пользователя.

КриптоПро DSS поддерживает выделенное хранилище издателей сертификатов аутентификации. Имя хранилища можно посмотреть в выводе параметра **ClientAuthenticationIssuersStoreName** командлета **Get-DssStsProperties** (по умолчанию – STS Client Authentication Issuers). Использование данного хранилища регулируется параметром **IsClientAuthenticationIssuersStoreEnabled** (см. раздел 4.5.7.2).

Создание самой учётной записи Оператора осуществляется с помощью командлета Add-DssIdentityOperator, входящего в состав модуля **CryptoPro.DSS.PowerShell.STS**. Полный список командлетов по настройке учетных записей Операторов КриптоПро DSS находится в разделе 4.5.7.10.

4.3.3. Настройка учетных записей Операторов Аудита

Роль **Оператора Аудита** СЭП «КриптоПро DSS» существует для мониторинга событий, поступающих с компонентов СЭП от всех Пользователей. Поскольку Оператор Аудита прикрепляется только к экземпляру ЦИ, а не к группе, на веб-интерфейсе Сервиса Аудита ему доступны все события всех Пользователей данного экземпляра ЦИ, в отличие от других ролей (Пользователя и Оператора), которым события доступны только в фильтрованном по группе/пользователю виде. Оператор Аудита существует только в пределах Сервиса Аудита и не имеет доступа к другим компонентам и функциям КриптоПро DSS.

Основной функцией Оператора Аудита является создание отчетов. Для этого требуются плагины формирования отчетности. В КриптоПро DSS существуют предопределенные типы отчетов, но для добавления возможности выпуска таких отчетов необходимо сначала настроить соответствующие плагины. Описание их настройки находится в разделе 4.8.1.4.

В целях обеспечения безопасности Центр Идентификации не имеет предустановленной встроенной учетной записи Оператора Аудита. Поэтому создание учетной записи Оператора Аудита возможно только локально на сервере, где установлен Центр Идентификации КриптоПро DSS. Роль Оператора Аудита назначается Администратором путем выдачи Оператору Аудита сертификата с клиентской аутентификацией. Сертификат должен храниться в хранилище «Личные» текущего пользователя.

КриптоПро DSS поддерживает выделенное хранилище издателей сертификатов аутентификации. Имя хранилища можно посмотреть в выводе параметра **ClientAuthenticationIssuersStoreName** командлета **Get-DssStsProperties** (по умолчанию – STS Client Authentication Issuers). Использование данного хранилища регулируется параметром **IsClientAuthenticationIssuersStoreEnabled** (см. раздел 4.5.7.2).

Создание самой учётной записи Оператора Аудита осуществляется с помощью командлета Add-DssIdentityOperator, с **обязательным** флагом **–audit,** входящего в состав модуля **CryptoPro.DSS.PowerShell.STS**. Полный список командлетов по настройке учетных записей Операторов КриптоПро DSS находится в разделе 4.5.7.10.

Одна и та же учетная запись не может выполнять роль Оператора и Оператора Аудита одновременно.

4.3.4. Настройка учетных записей Администраторов

4.3.4.1. Общие сведения об Администраторах

Администратор СЭП «КриптоПро DSS» занимается администрированием непосредственно СЭП «КриптоПро DSS». Его задачами являются:

- Администрирование специального программного обеспечения;
- настройка экземпляров компонентов СЭП «КриптоПро DSS»;
- управление (создание, редактирование, удаление) учетными записями Операторов СЭП;
- управление лицензиями КриптоПро DSS.

Для доступа Администратора к БД экземпляра компонента СЭП «КриптоПро DSS» ему необходима учетная запись в БД каждого из экземпляров. Только в этом случае он сможет выполнять командлеты в PowerShell, принадлежащие пространству командлетов того или иного модуля. При этом учетная запись Администратора в ЦИ КриптоПро DSS не создается.

Создание учетных записей Администраторов требуется для следующих компонентов КриптоПро DSS:

Таблица 13. Командлеты для создания учетных записей Администраторов

Компонент	Командлет	Описание
Центр Идентификации	Add-DssStsAdministrator	Добавляет Администратора для экземпляра ЦИ.
	Get-DssStsAdministrator	Выводит сведения об Администраторах экземпляра ЦИ.
	Remove-DssStsAdministrator	Удаляет Администратора с экземпляра ЦИ.

Компонент	Командлет	Описание
Сервис Подписи	Add-DssSignServerAdministrator	Добавляет Администратора для экземпляра Сервиса Подписи.
	Get-DssSignServerAdministrator	Выводит сведения об Администраторах экземпляра Сервиса Подписи.
	Remove-DssSignServerAdministrator	Удаляет Администратора с экземпляра Сервиса Подписи.
Сервис Аудита	Add-DssAnalyticsServiceAdministrator	Добавляет Администратора для экземпляра Сервиса Аудита.
	Get-DssAnalyticsServiceAdministrator	Выводит сведения об Администраторах экземпляра Сервиса Аудита.
	Remove-DssAnalyticsServiceAdministrator	Удаляет Администратора с экземпляра Сервиса Аудита.
Сервер взаимодействия с ЦИ myDSS	Add-MyDssInternalAdministrator	Добавляет Администратора для экземпляра Сервиса взаимодействия с ЦИ myDSS.
	Get-MyDssInternalAdministrator	Выводит сведения об Администраторах экземпляра Сервиса взаимодействия с ЦИ myDSS.
	Remove-MyDssInternalAdministrator	Удаляет Администратора с экземпляра Сервиса взаимодействия с ЦИ myDSS.
Сервис взаимодействия с мобильным приложением myDSS	Add-MyDssExternalAdministrator	Добавляет Администратора для экземпляра Сервиса взаимодействия с мобильным приложением myDSS.
	Get-MyDssExternalAdministrator	Выводит сведения об Администраторах экземпляра Сервиса взаимодействия с мобильным приложением myDSS
	Remove-MyDssExternalAdministrator	Удаляет Администратора с экземпляра Сервиса взаимодействия с мобильным приложением myDSS

4.3.4.1. Администрирование учетных записей Администраторов

Администрирование учетных записей Администраторов КриптоПро DSS осуществляется с помощью командлетов, входящих в состав следующих модулей:

- **CryptoPro.DSS.PowerShell.SignServer;**
- **CryptoPro.DSS.PowerShell.STS;**
- **CryptoPro.DSS.PowerShell.Analytics;**
- **CryptoPro.DSS.PowerShell.MyDssServerExternal;**
- **CryptoPro.DSS.PowerShell.MyDssServerInternal**

в зависимости от компонента для которого выполняется настройка. Все модули содержат однотипный набор команд для настройки учетных записей Администраторов. Список команд приведён в Таблица 13.

Командлет Add-DssStsAdministrator

Добавляет Администратора для экземпляра ЦИ.

Синтаксис:

```
Add-DssStsAdministrator [-Password <string>] -UserName <string> -DisplayName
<string>
```

Таблица 14. Параметры командлета Add-DssStsAdministrator

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации.
Password	string	Пароль учетной записи Администратора.
UserName	string	Имя учетной записи Администратора.

Командлет Get-DssStsAdministrator

Выводит сведения об Администраторах указанного экземпляра ЦИ.

Синтаксис:

```
Get-DssStsAdministrator -DisplayName <string>
```

Командлет Remove-DssStsAdministrator

Удаляет Администратора с указанного экземпляра ЦИ.

Синтаксис:

```
Remove-DssStsAdministrator [-DisplayName <string>] -UserName <string>
```

Таблица 15. Параметры командлета Remove-DssStsAdministrator

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации.
UserName	string	Имя учетной записи Администратора.

4.3.5. Управление группами на Центре Идентификации

Центр Идентификации КриптоПро DSS позволяет разделить Пользователей на группы. Разделение на группы введено для удобства администрирования учётных записей Пользователей Операторами. То есть управление учётными записями Пользователей можно разделить между несколькими Операторами, таким образом каждый Оператор будет управлять только своим набором Пользователей.

Для управления группами используются командлеты New-DssIdentityGroup, Get-DssIdentityGroup, Remove-DssIdentityGroup, Set-DssIdentityGroup. Для каждого зарегистрированного экземпляра Центра Идентификации всегда создаётся группа по умолчанию с предопределённым именем Default.

Пользователю может быть назначена только одна группа. По умолчанию при создании учётной записи Пользователь будет включен в группу по умолчанию Default.

Оператор может быть включен в одну и более групп. При создании учётной записи Оператора ему назначается группа по умолчанию Default. В дальнейшем можно изменить набор групп, в которые включен Оператор, с помощью командлета Set-DssIdentityOperator. Если Оператор создаёт учётную запись Пользователя, то он может назначить группу Пользователя из списка групп, в которые он включён.

4.4. Настройка ограничений размера документов

В КриптоПро DSS существует возможность настроить максимальный размер документа, с которым совершается операция шифрования, расшифрования или подписи. По умолчанию максимальный размер такого документа составляет 5 Мбайт. Если требуется изменить данное ограничение, эта настройка должна быть выполнена на Сервисе Подписи, на Веб-интерфейсе Пользователя, а также на Центре Идентификации. При необходимости подтверждения операций с использованием мобильного приложения myDSS аналогичную настройку нужно выполнить на экземпляре Сервиса взаимодействия с мобильным приложением myDSS и экземпляре Сервиса взаимодействия с ЦИ myDSS.

Список командлетов, при помощи которых настраивается ограничение максимального размера передаваемого документа, приведен в Таблица 16.

Таблица 16. Командлеты для настройки ограничений размера документа

Компонент	Командлет
Сервис Подписи	Set-DssEndpointGlobalSettings с параметром **MaxMessageSize.**
Центр Идентификации	Set-DssStsEndpointGlobalSettings с параметром **MaxMessageSize.**
Веб-интерфейс Пользователя	Set-DssFeProperties с параметром **MaxIISContentLength.**

Компонент	Командлет
myDSS External Interaction Server	Set-MyDssServerInteractionPushServiceEndpointGlobalSettings И Set-MyDssServerInteractionServiceEndpointGlobalSettings с параметром **MaxMessageSize.**
myDSS Internal Interaction Server	Set-EndpointGlobalSettings с параметром **MaxMessageSize.**

Если допускается передача больших документов (к примеру, размером более 50 Мбайт), может потребоваться настройка таймаута на передачу данных. Данные настройки осуществляются на компонентах Сервис Подписи, Центр Идентификации, Сервис взаимодействия с мобильным приложением myDSS myDSS и Сервис взаимодействия с ЦИ при помощи тех же командлетов, что и в Таблица 16, но с параметрами **MaxRecieveTimeOut и MaxSendTimeOut.** Эти параметры позволяют настроить время получения и отправки сообщения сервером.

В целях исключения деградации производительности КриптоПро DSS, рекомендуется не устанавливать ограничение на максимальный размер документа выше 50 Мбайт.

Пример настройки ограничений передаваемого документа:

```
# Настройка ограничения на ЦИ
Set-DssStsEndpointGlobalSettings -MaxMessageSize 5242880 -DisplayName STS

# Настройка ограничения на Сервисе Подписи
Set-DssEndpointGlobalSettings -MaxMessageSize 5242880 -DisplayName SignServer

# Настройка ограничения на Веб-интерфейсе Пользователя
Set-DssFeProperties -MaxIISContentLength 5242880 -DisplayName Frontend
```

4.5. Настройка ЦИ

Центр Идентификации представляет собой приложение ASP.NET, которое предназначено для регистрации и аутентификации Пользователей, а также подтверждения волеизъявления Пользователя на операции с его ключами. В случае успешной аутентификации выдаётся электронный идентификатор, который затем может быть использован для доступа к Сервису Подписи или для управления Центром Идентификации. Взаимодействие с Центром Идентификации может осуществляться по протоколу SOAP, а также с использованием архитектурного стиля REST.

4.5.1. Последовательность шагов по настройке компонента Центр Идентификации

Данный раздел Руководства Администратора определяет последовательность и порядок действий по разворачиванию и настройке экземпляра Сервиса Подписи в режиме «с нуля».

Предварительные условия:

- Установленный SQL-Server;
- Установленная роль Сервер приложений (IIS);
- Настроенная привязка https на Сервере приложений (IIS);
- Выпущенный и установленный сервисный сертификат Центра Идентификации (см. Раздел 6).

Базовая последовательность шагов по настройке (обязательные):

1. Создание экземпляра службы Центра Идентификации (см. раздел 4.5.7.1).

На данном шаге будет создано веб-приложение на Сервере приложений IIS, развёрнуты базы данных, зарегистрированы журналы Windows.

2. Настройка сервисного сертификата Центра Идентификации.

На данном шаге экземпляру Центра Идентификации назначается сервисный сертификат, который используется для аутентификации при межсервисном взаимодействии (см. раздел 6).

Учетной записи, под которой работает пул приложения Центра Идентификации, необходимо выдать права на доступ к закрытому ключу сервисного сертификата (см. раздел 6.3).

3. Настройка Службы маркеров безопасности.

При необходимости можно задать собственный сертификат подписи службы маркеров безопасности (см. Руководство по интеграции с ЦИ). По умолчанию сервисный сертификат ЦИ и сертификат подписи службы маркеров безопасности совпадают, а сама служба создается автоматически при создании экземпляра ЦИ.

Дополнительные действия по настройке (опциональные):

- Настройка отношений доверия (см. раздел 4.5.3).

- Параметры первичной аутентификации локальных Пользователей.

Администратор может задать требования к паролю Пользователя, такие как длина и сложность паролей, максимальное количество попыток неверного ввода пароля (см. раздел 5).

Администратор может включить следующие методы первичной аутентификации:

- Вход по логину/паролю (включен по умолчанию);
- Вход по сертификату (включен по умолчанию);

Администратор может разрешить или запретить Пользователям изменять настройки первичной аутентификации. Данная настройка имеет значение, только если включено несколько методов первичной аутентификации, но назначать Пользователю тот или иной метод входа должен только Оператор. Данная настройка не запрещает Пользователю менять данные аутентификации - например, сменить пароль или назначить другой сертификат для входа.

- Параметры профиля Пользователя (см. раздел 4.5.4).

Администратор может задать требования к компонентам профиля Пользователя:

- Состав компонентов (имя, фамилия, должность, адрес, организация, ИНН и т.д.);
- Установить, какие компоненты являются обязательными и опциональными для заполнения;
- Установить значения по умолчанию для компонентов (для организации, страны и т.п.)

Администратор может изменить параметры компонентов имени, зарегистрированных по умолчанию, удалить или добавить новые компоненты (см. раздел 4.5.4).

Также Администратор может разрешить или запретить Пользователям редактирование своего профиля. По умолчанию Пользователям разрешено редактировать профиль.

- Требования к уникальности данных (см. раздел 4.5.7.5, 4.5.7.15).

Администратор может включить или отключить требование уникальности следующих данных в профиле Пользователя:

- Номер телефона;
- Адрес электронной почты;
- Различительное имя Пользователя (совокупность всех компонент в профиле Пользователя: имя, фамилия, должность, адрес, организация, ИНН и т.д.).

Требование уникальности номера телефона и/или адреса электронной почты является обязательным, если они используются для идентификации Пользователей. То есть, если Администратор разрешил использование номера телефона и/или адреса электронной почты в качестве идентификатора (логина) Пользователя.

- Оператор DSS (см. раздел 4.5.7.10).

Администратор может зарегистрировать учётные данные Операторов DSS. Оператор DSS является привилегированной учётной записью на Центре Идентификации, которой разрешено создавать, редактировать, удалять учётные записи Пользователей; так же Оператор DSS может управлять сертификатами Пользователей: создавать, одобрять, отклонять запросы на сертификаты Пользователей.

- Настройка оповещения Пользователей.

Администратор DSS может настроить SMS- или Email-оповещение Пользователей о действиях, выполненных на Центре Идентификации (см. Раздел 4.9).

Оповещение Пользователей требует подключения ЦИ к SMS-шлюзу оператора сотовой связи или к почтовому серверу в соответствии со схемой размещения компонентов (см документ ЖТЯИ.00046-03 90 02 КриптоПро DSS. Общее описание). и в соответствии с требованиями к подключению к сетям общего пользования, описанными в Разделе 10 ЖТЯИ.00046-03 05 01. Правила пользования.

- Настройка аудита.

Администратор DSS может подключить Центр Идентификации к Сервису Аудита для ведения журнала событий (см. Раздел 4.8.2).

- Кастомизация (см. раздел 4.5.7.13).

Администратор DSS может кастомизировать Веб-интерфейс Центра Идентификации: изменить цвета фона, текста, логотипы, тексты заголовков и т.п.

4.5.2. Объекты администрирования

На Рис. 27 приведена схема объектов, доступных для администрирования на Центре Идентификации.

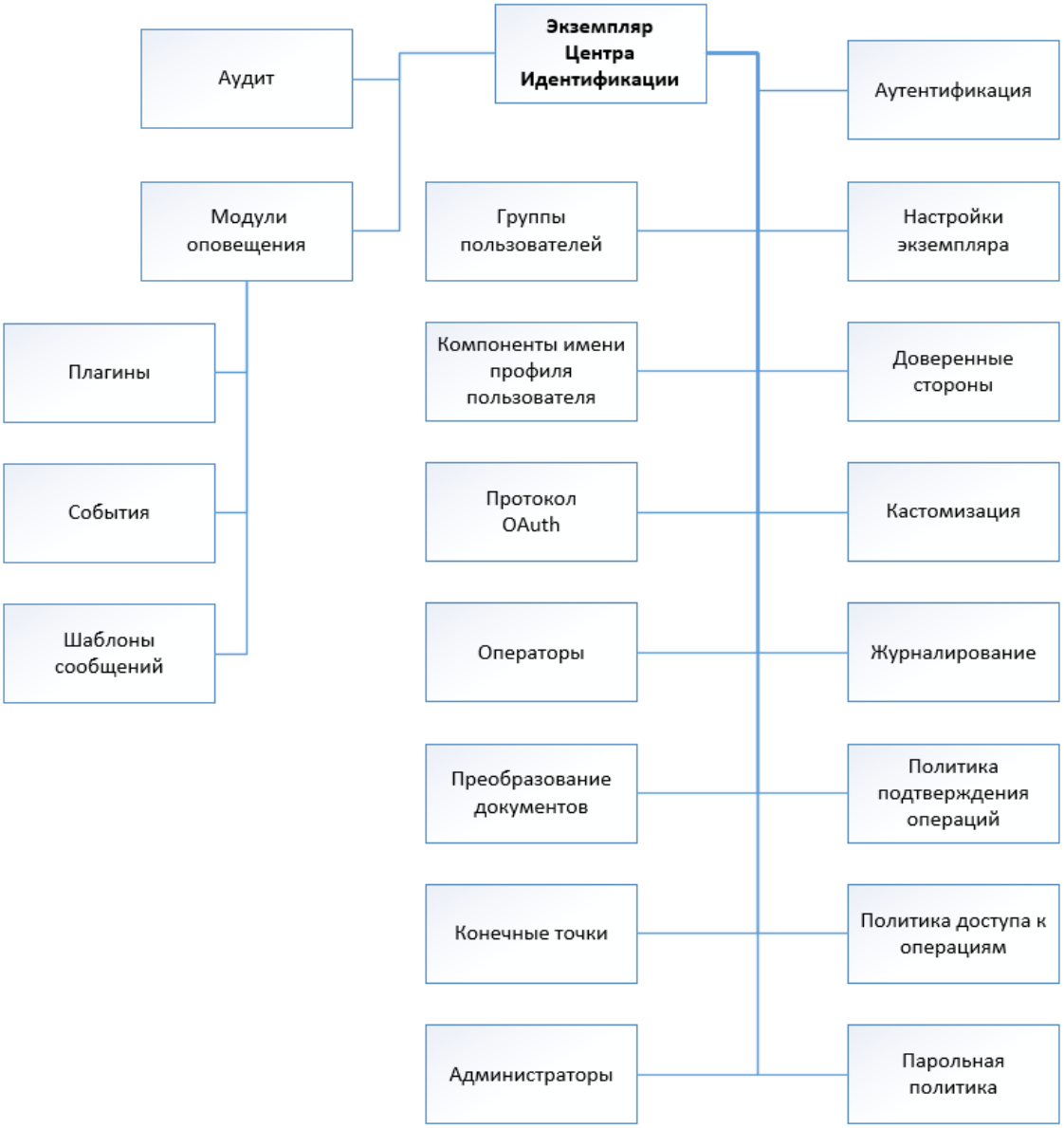

Рис. 27 – Объекты администрирования Центра Идентификации

Таблица 17. Список командлетов компонента «Центр Идентификации»

Объект администрирования	Командлет	Описание
Настройки экземпляра	Командлет Remove-DssStsInstance	Объект отвечает за управление экземплярами ЦИ.
	Командлет Remove-DssStsInstance	
	Командлет Get-DssStsInstance	
	Update-DssStsInstance	
Общие настройки	Командлет Set-DssStsProperties	Объект отвечает за настройку экземпляра ЦИ и

Объект администрирования	Командлет	Описание
	Командлет Get-DssStsProperties	строки подключения к базе данных.
	Get-DSSStsRegistryProperties	
	Set-DSSStsRegistryProperties	
Конечные точки	Get-DssStsEndpointGlobalSettings	Объект отвечает за общие настройки параметров взаимодействия ЦИ с интегрируемыми системами.
	Set-DssStsEndpointGlobalSettings	
Политика доступа к операциям	Get-DssAccessPolicy	Объект отвечает за настройку разрешенных операций.
	Set-DssAccessPolicy	
Настройки создания учетных записей	Get-DssAccountPolicy	Объект отвечает за общие настройки создания учетных записей .
	Set-DssAccountPolicy	
Парольные политики	Get-DssPasswordPolicy	Объект отвечает за настройку парольных политик ЦИ.
	Set-DssPasswordPolicy	
Доверенные стороны	Командлет Add-DssRelyingPartyTrust	Объект отвечает за настройку доверенных сторон ЦИ КриптоПро DSS.
	Командлет Remove-DssRelyingPartyTrust	
	Командлет Get-DssRelyingPartyTrust	
	Командлет Set-DssRelyingPartyTrust	
	Командлет Enable-DssRelyingPartyTrust	
	Командлет Disable-DssRelyingPartyTrust	
Протокол OAuth	Add-DssClient	Объект отвечает за настройку аутентификации по протоколу OAuth.
	Disable-DssClient	
	Enable-DssClient	
	Get-DssClient	
	Remove-DssClient	
	Set-DssClient	

Объект администрирования	Командлет	Описание
Группы Пользователей	Командлет New-DssIdentityGroup	Объект отвечает за настройку групп Пользователей КриптоПро DSS.
	Командлет Get-DssIdentityGroup	
	Командлет Set-DssIdentityGroup	
	Командлет Remove-DssIdentityGroup	
Операторы	Командлет Add-DssIdentityOperator	Объект отвечает за настройку Операторов КриптоПро DSS.
	Командлет Get-DssIdentityOperator	
	Командлет Set-DssIdentityOperator	
	Командлет Remove-DssIdentityOperator	
Преобразование документов	Командлет Get-DssStsConverterPlugin	Объект отвечает за настройки плагина для преобразования документов.
	Командлет Add-DssStsConverterPlugin	
	Командлет Remove-DssStsConverterPlugin	
Аутентификация	Командлет Get-DssAuthenticationMethod	Объект отвечает за настройку методов аутентификации ЦИ.
	Командлет Enable-DssAuthenticationMethod	
	Командлет Disable-DssAuthenticationMethod	
	Import-DssStsOtpTokenData	
Кастомизация	Командлет Get-DssStsCustomization	Объект отвечает за настройку отображения веб-интерфейса ЦИ.
	Командлет Set-DssStsCustomization	
	Командлет Reset-DssStsCustomization	
Компоненты имени Пользователя	Командлет Add-DssRDN	Объект отвечает за настройку компонентов различительных имен Пользователей.
	Командлет Set-DssRDN	
	Командлет Get-DssRDN	
	Командлет Remove-DssRDN	
	Add-DssRdnPolicy	Объект отвечает за настройку политик

Объект администрирования	Командлет	Описание
Политики компонентов имени Пользователя	Get-DssRdnPolicy	компонентов различительных имен Пользователей.
	Set-DssRdnPolicy	
	Remove-DssRdnPolicy	
Политики подтверждения операций	Get-DssConfirmationPolicy	Объект отвечает за настройку политики подтверждения операций.
	Set-DssConfirmationPolicy	
Журналирование	Get-DssStsTracing	Объект отвечает за журналирование сетевых взаимодействий (см. раздел 7.3).
	Set-DssStsTracing	
	Enable-DssStsTracing	
	Disable-DssStsTracing	
	Get-DssUmsTracing	
	Set-DssUmsTracing	
	Enable-DssUmsTracing	
	Disable-DssUmsTracing	
Модули оповещения	Add-DSSStsNotifier	Объект отвечает за рассылку уведомлений Пользователям и Операторам КриптоПро DSS (см. раздел 4.9.5).
	Get-DSSStsNotifier	
	Set-DSSStsNotifier	
	Remove-DSSStsNotifier	
	Enable-DSSStsNotifier	
	Disable-DSSStsNotifier	
Плагины	Add-DSSStsPlugin	Объект является частью модуля оповещения и отвечает за формирование сообщений, отправляемых Пользователям и Операторам, а также за отправку сообщений по каналу связи (SMS, Email и т.д.) (см. раздел 4.9.5).
	Get-DSSStsPlugin	
	Set-DSSStsPlugin	
	Remove-DSSStsPlugin	

Объект администрирования	Командлет	Описание
События	Get-DSSStsEvent	Объект «События» позволяет настроить список событий, о которых будут оповещаться Пользователи и Операторы, а также задать каналы отправки сообщений (SMS, Email, и т.п.) (см. раздел 4.9.5).
	Set-DSSStsEvent	
Шаблоны сообщений	Get-DSSStsFormatterTemplate	Объект позволяет настроить шаблоны сообщений, отправляемых ЦИ.
	Set-DSSStsFormatterTemplate	
Аудит	New-DSSStsAudit	Объект отвечает за взаимодействие с Сервисом Аудита и запись событий ЦИ в журнал Аудита (см. раздел 4.8.2).
	Remove-DSSStsAudit	

4.5.3. Доверенные стороны

Приложение, которое в своей работе опирается на утверждения (claims), называется приложением доверенной стороны (relying party, RP). Доверенной стороной может быть, как веб-приложение, так и веб-служба. Приложение доверенной стороны принимает маркеры, выданные службой маркеров безопасности (Security Token Service, STS), и извлекает из них утверждения, чтобы использовать их в задачах, связанных с аутентификацией.

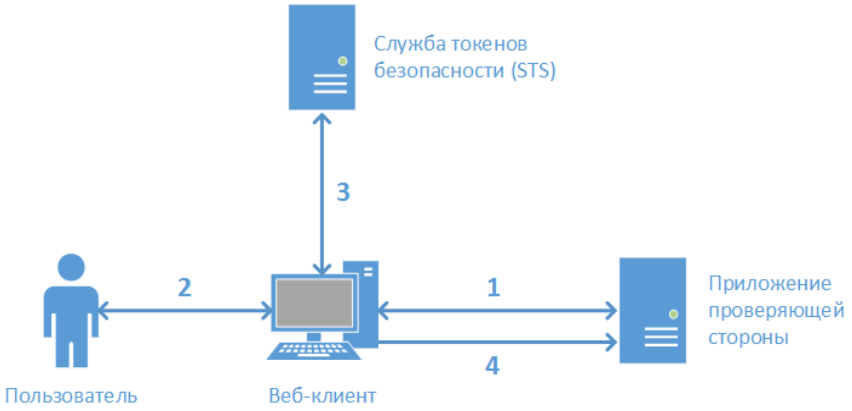

Рис. 28 – Сценарий аутентификации на основе утверждений

На данной схеме (Рис. 28) представлен веб-сайт (приложение доверенной стороны) и веб-клиент (веб-браузер), желающий использовать данный сайт.

1. Пользователь, прошедший проверку подлинности, запрашивает веб-страницу; приложение доверенной стороны перенаправляет его на поставщика удостоверений (STS).

2. Пользователь предоставляет поставщику удостоверений свои учетные данные, например, имя Пользователя и пароль, билет Kerberos и т.д.

3. Поставщик удостоверений создает токен и отправляет его клиенту.

4. Клиент отправляет доверенной стороне запрос вместе с полученным токеном, и доверенная сторона решает, соответствует ли токен условиям доступа и стоит ли удовлетворять запрос клиента.

В КриптоПро DSS поставщиком удостоверений является Центр Идентификации, а доверенными сторонами являются Сервис Подписи и Веб-интерфейс Пользователя.

Регистрация доверенных сторон и управление зарегистрированными доверенными сторонами осуществляется с помощью командлетов Add-DssRelyingPartyTrust, Set-DssRelyingPartyTrust, Enable-DssRelyingPartyTrust, Disable-DssRelyingPartyTrust, Remove-DssRelyingPartyTrust.

4.5.3.1. Регистрация доверенной стороны

Регистрация доверенной стороны в Центре Идентификации решает следующие задачи:

- Ограничение сервисов и приложений в сторону, которых ЦИ может выпускать маркеры безопасности.
- Шифрование маркеров безопасности.
- Отображение понятного имени доверенной стороны в веб-интерфейсе ЦИ при аутентификации Пользователя.
- Задание адреса Веб-интерфейса для управления Пользователем.

Доверенными сторонами в КриптоПро DSS являются:

- Сервис Подписи;
- Веб-интерфейс Пользователя;
- Сервис Аудита.

Регистрация доверенных сторон осуществляется через загрузку метаданных, которые публикует каждый из компонентов DSS по протоколу WS Federation Metadata.

Адреса публикации метаданных следующие:

Сервис Подписи

```
http://<HostName>/<SignServer>/FederationMetadata/2007-06/FederationMetadata.xml
```

Загрузка возможна как по http, так и по https.

Веб-интерфейс Пользователя

```
https://<HostName>/<Frontend>/FederationMetadata/2007-06/FederationMetadata.xml
```

Загрузка возможна только по https.

Сервис Аудита

```
https://<HostName>/<Analytics>/FederationMetadata/2007-06/FederationMetadata.xml
```

Загрузка возможна как по http, так и по https.

Доверенная сторона определяется идентификатором, который имеет вид:

```
urn:cryptopro:dss:<apptype>:<appname> ,
```

где **apptype** – компонент DSS, **appname –** имя экземпляра компонента.

Данные идентификаторы используются в том числе при интеграции с КриптоПро DSS через API:

SOAP API:

Идентификатор Сервиса Подписи передается в поле **AppliesTo** запроса на выпуск маркера безопасности. По умолчанию идентификатор имеет вид:

```
urn:cryptopro:dss:signserver:<SignServer>
```

REST API:

Идентификатор Сервиса Подписи передается в поле **Resource** в запросе на выпуск JWT-токена. По умолчанию идентификатор имеет вид:

```
http://<hostname>/<SignServer>/rest/api
```

4.5.3.2. Регистрация Веб-интерфейса Пользователя

Для работы Пользователей через Веб-интерфейс Пользователя его необходимо зарегистрировать в качестве доверенной стороны на Центре Идентификации.

Веб-интерфейс поддерживает публикацию метаданных по протоколу WS Federation Metadata, которые могут использоваться для настройки доверенной стороны на Центре Идентификации.

```
Add-DssRelyingPartyTrust -Name "Frontend" -MetadataUri
https://<HostName>/<Frontend>/FederationMetadata/2007-
06/FederationMetadata.xml
```

Также можно настроить понятное имя, которое будет отображаться в процессе аутентификации в веб-интерфейсе ЦИ.

```
Set-DssRelyingPartyTrust -Id 2 -Name 'СКО ООО "Рога и копыта"'
```

При добавлении Веб-интерфейса Пользователя в качестве доверенной стороны регистрируется специфический для него параметр – адрес личного кабинета Оператора DSS (**-AdministrativeUrl**). Если сервер, на котором развернут Веб-интерфейс Пользователя, имеет несколько имен (к примеру, внутреннее и внешнее), значение по умолчанию может потребоваться изменить. Данная операция выполняется при помощи следующей команды:

```
Set-DssRelyingPartyTrust -Id <FrontendId> -ForOperator
$true -AdministrativeUrl https://<hostname>/<Frontend>/Admins/
```

4.5.3.3. Регистрация Сервиса Подписи

Для работы Пользователей через SOAP-интерфейс веб-сервис Сервиса Подписи необходимо зарегистрировать в качестве доверенной стороны на Центре Идентификации.

Сервис Подписи поддерживает публикацию метаданных по протоколу WS Federation Metadata, которые могут использоваться для настройки доверенной стороны на Центре Идентификации.

```
Add-DssRelyingPartyTrust -Name "SignServer" -MetadataUri
http://<HostName>/SignServer/FederationMetadata/2007-
06/FederationMetadata.xml
```

При добавлении Сервиса Подписи в качестве доверенной стороны регистрируется специфический для него параметр – адрес взаимодействия с Сервисом Подписи (**-BackChannelUrl)**. Данный параметр применяется только при использовании вторичной аутентификации. Если сервер, на котором развернут Веб-интерфейс Пользователя, имеет несколько имен (к примеру, внутреннее и внешнее), значение по умолчанию может потребоваться изменить. Данная операция выполняется при помощи следующей команды:

```
Set-DssRelyingPartyTrust -Id <SignServerId> -BackChannelUrl
https://<hostname>/<SignServer>/SignService.svc/transactiontokens -
SupportsBackChannel
```

Если в качестве сервисного сертификата используется сертификат с алгоритмом открытого ключа ГОСТ Р 34.10–2001 или ГОСТ Р 34.10–2012, то в параметрах доверенной стороны Сервиса Подписи **обязательно** требуется указать сертификат шифрования (сервисный сертификат Сервиса Подписи). Данный сертификат регистрируется автоматически при настройке доверенной стороны через загрузку метаданных. Изменить сервисный сертификат можно с помощью следующей команды:

```
Set-DssRelyingPartyTrust -Id <SignServerid> -EncryptionCertificate
C:\fakepath\enccert.cer -DisableTokenEncryption $false
```

4.5.3.4. Регистрация Сервиса Аудита

Для того, чтобы пользователь мог просматривать свои операции через Сервис Аудита, сервис необходимо зарегистрировать в качестве доверенной стороны на Центре Идентификации.

Сервис Аудита поддерживает публикацию метаданных по протоколу WS Federation Metadata, которые могут использоваться для настройки доверенной стороны на Центре Идентификации.

```
Add-DssRelyingPartyTrust -Name "AnalyticsService" -MetadataUri
https://<HostName>/AnalyticsService/FederationMetadata/2007-
06/FederationMetadata.xml
```

Также можно настроить понятное имя, которое будет отображаться в процессе аутентификации в веб-интерфейсе ЦИ.

```
Set-DssRelyingPartyTrust -Id 2 -Name 'СКО ООО "Рога и копыта"'
```

4.5.4. Настройка компонентов имени Пользователя

4.5.4.1. Общие сведения о компонентах имени Пользователя в КриптоПро DSS

При формировании запроса на сертификат поля формы заполняются из данных, которые могут передаваться в утверждении **X500DistinguishedName** (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/x500distinguishedname) от

Центра Идентификации. Данное утверждение должно содержать различительное имя Пользователя в виде:

«CN=Иванов Иван, E=ivanov@ivanov.ru,C=RU,O=КРИПТО-ПРО».

Центр Идентификации КриптоПро DSS позволяет формировать такое утверждение на основе данных имени Пользователя. Настройка компонентов имени Пользователя осуществляется с помощью командлетов Set-DssRDN, Add-DssRDN, Get-DssRDN, Remove-DssRDN.

Различительное имя Пользователя состоит из отдельных компонентов, называемых относительными различительными именами (RDN - Relative Distinguished Name). Для каждого такого компонента возможно настроить параметры, описанные в Таблица 18.

Таблица 18. Настраиваемые параметры для компонента имени Пользователя

Параметр	Тип	Описание
Id	String	Идентификатор компонента имени в БД ЦИ
Oid	String	Идентификатор в общем каталоге объектов
StringIdentifier	String	Идентификатор строки, содержащей компонент имени Пользователя
FriendlyName	String	Отображаемое имя компонента имени Пользователя
MaxLength	int	Максимальная длина компонента имени Пользователя
MinLength	int	Минимальная длина компонента имени Пользователя
ValueType	string	Тип значения компонента имени Пользователя. Может принимать значения Numeric или String.
ClaimType	string	Тип утверждения (сведений о Пользователе), содержащего данный компонент
Description	String	Описание компонента имени Пользователя

По умолчанию в экземпляре ЦИ КриптоПро DSS зарегистрировано 16 RDN. Они приведены в Таблица 19.

Таблица 19. Компоненты имени Пользователя по умолчанию

Компонент (Отображаемое имя)	Идентификатор Строки	Max длина	Min длина	Тип значения	OID
ОГРН	OGRN	13	13	Numeric	1.2.643.100.1
ОГРНИП	OGRNIP	15	15	Numeric	1.2.643.100.5
СНИЛС	SNILS	11	11	Numeric	1.2.643.100.3

Компонент (Отображаемое имя)	Идентификатор Строки	Max длина	Min длина	Тип значения	OID
ИНН	INN	12	12	Numeric	1.2.643.3.131.1.1
Электронная почта	E	128	0	String	1.2.840.113549.1.9.1
Страна	C	2	0	String	2.5.4.6
Область	S	128	0	String	2.5.4.8
Город	L	128	0	String	2.5.4.7
Организация	O	64	0	String	2.5.4.10
Подразделение	OU	64	0	String	2.5.4.11
Общее имя	CN	128	0	String	2.5.4.3
Адрес	Street	30	0	String	2.5.4.9
Должность	T	64	0	String	2.5.4.12
Инициалы	I	5	0	String	2.5.4.43
Имя	G	16	0	String	2.5.4.42
Фамилия	SN	40	0	String	2.5.4.4

4.5.4.2. Политики компонентов имени Пользователя

КриптоПро DSS позволяет настроить компоненты имени Пользователя на двух уровнях: глобальном (уровень настройки ЦИ, см раздел 4.5.4.1) и уровне группы (см. раздел 4.3.5). Для каждого из указанных уровней существует собственная политика RDN. Политика RDN представляет собой набор идентификаторов глобально зарегистрированных RDN и соответствующих каждому из них параметров **Required** и **DefaultValues**.

Настройка политики RDN уровня ЦИ (глобального) и уровня группы КриптоПро DSS осуществляется при помощи командлетов Add-DssRdnPolicy, Get-DssRdnPolicy, Set-DssRdnPolicy, Remove-DssRdnPolicy.

Политики RDN обладают следующими особенностями:

- Для Пользователя могут быть заполнены только те компоненты имени, которые зарегистрированы в политике группы, в которой находится Пользователь.
- Нельзя удалить RDN из глобальной политики ЦИ, если в политике группы зарегистрирован этот RDN.

- Нельзя удалить RDN из политики группы, если в этой группе существуют Пользователи, у которых заполнен данный компонент имени.
- Для редактирования политики определенной группы необходимо указать параметр **GroupId**. В случае, если параметр **GroupId** не указан, будет производиться редактирование глобальной политики ЦИ КриптоПро DSS.
- После создания экземпляра ЦИ КриптоПро DSS глобальная политика ЦИ и группа по умолчанию (Default) автоматически заполняются глобально зарегистрированными RDN. Каждый такой RDN является необязательным и может принимать любые значения.
- При добавлении новой группы в определенный ЦИ для нее создается политика, в которую по умолчанию копируются настройки из глобальной политики ЦИ КриптоПро DSS.

Изменение настроек политики компонентов имени Пользователя не распространяется на уже созданных с использованием данной политики Пользователей. Это изменение будет распространяться только на вновь созданных Пользователей.

4.5.5. Политика подтверждений операций

При создании экземпляра ЦИ КриптоПро DSS для него автоматически создается политика подтверждения операций. Политика подтверждения операций является многоуровневой, в которой нижние уровни наследуют по умолчанию настройки от верхних уровней политики. В настоящий момент возможно произвести редактирование политики подтверждения операций на трех уровнях: уровне ЦИ КриптоПро DSS, уровне группы Пользователей и уровне Пользователя. При добавлении новой группы в ЦИ для нее создается политика, в которую копируются настройки из политики ЦИ. При создании нового Пользователя внутри группы, в его индивидуальные настройки подтверждения операций копируется список операций для подтверждения из политики группы.

Настройка политики подтверждения операций осуществляется при помощи командлетов Get-DssConfirmationPolicy, Set-DssConfirmationPolicy.

Политика подтверждения операций представляет собой набор следующих настроек:

Таблица 20. Настраиваемые параметры политики подтверждения операций

Параметр	Тип	Описание
Операции для подтверждения	DssActions ИЛИ NoneOpcActions ИЛИ AllOpcActions	Набор операций, для которых необходимо подтверждение.
AllowChangeByOperator	bool	Определяет, может ли Оператор изменять список операций для подтверждения.
AllowChangeByUser	bool	Определяет, может ли Пользователь изменять список операций для подтверждения.

Параметр	Тип	Описание
AllowOverride	bool	Определяет, может ли политика быть переопределена на более низком уровне иерархии.

После создания экземпляра ЦИ глобальная политика ЦИ и политика группы группы по умолчанию (Default) автоматически заполняются следующим образом:

- Список операций = NoneOpcActions
- AllowChangeByUser = true
- AllowChangeByOperator = true
- AllowOverride = true

Если в иерархии политик есть политика с **AllowOverride** = false, применяются настройки политики, которая стоит уровнем выше. Если такой политики нет, параметры **AllowChangeByUser** и **AllowChangeByOperator** используются из политики группы, а настройка **OpcActions** применяется индивидуально для каждого Пользователя.

Для применения глобального требования подтверждать все операции необходимо выполнить следующую PowerShell-команду:

```
Set-DssConfirmationPolicy -AllOpcActions -AllowOverride 0
```

Для применения глобального требования не подтверждать никакие операции необходимо выполнить следующую PowerShell-команду:

```
Set-DssConfirmationPolicy -NoneOpcActions -AllowOverride 0
```

4.5.6. Политика доступа к операциям

При создании экземпляра ЦИ КриптоПро DSS, для него автоматически создается политика доступа к операциям. Политика доступа к операциям является многоуровневой, в которой нижние уровни наследуют по умолчанию настройки от верхних уровней политики. В настоящий момент возможно произвести редактирование политики доступа к операциям на трех уровнях: уровне ЦИ КриптоПро DSS, уровне группы Пользователей и уровне Пользователя. При добавлении новой группы в ЦИ для нее создается политика, в которую копируются настройки из политики ЦИ. При создании нового Пользователя внутри группы, в его индивидуальные настройки доступа к операциям копируется список операций, к которым разрешен доступ, из политики группы.

Настройка политики доступа к операциям осуществляется при помощи командлетов Get-DssAccessPolicy, Set-DssAccessPolicy.

Политика доступа к операциям представляет собой набор следующих настроек:

Таблица 21. Настраиваемые параметры политики доступа к операциям

Параметр	Тип	Описание
Доступ к операциям	AllActionsAllowed ИЛИ AllActionsDisallowed ИЛИ DisallowedActions	Набор операций, к которым настраивается доступ.

Параметр	Тип	Описание
AllowChangeByOperator	bool	Определяет, может ли Оператор изменять политику доступа к операциям.
AllowChangeByUser	bool	Определяет, может ли Пользователь изменять политику доступа к операциям.
AllowOverride	bool	Определяет, может ли политика быть переопределена на более низком уровне иерархии.

После создания экземпляра ЦИ глобальная политика ЦИ и политика группы группы по умолчанию (Default) автоматически заполняются следующим образом:

- Доступ к операциям = AllActionsAllowed
- AllowChangeByUser = true
- AllowChangeByOperator = true
- AllowOverride = true

Если в иерархии политик есть политика с **AllowOverride** = false, применяются настройки политики, которая стоит уровнем выше. Если такой политики нет, параметры **AllowChangeByUser** и **AllowChangeByOperator** используются из политики группы, а настройка самого доступа к операциям применяется индивидуально для каждого Пользователя.

Для применения глобального требования подтверждать все операции необходимо выполнить следующую PowerShell-команду:

```
Set-DssAccessPolicy [-AllActionsAllowed] [-AllowChangeByUser <bool>] [-
AllowChangeByOperator <bool>] [-AllowOverride <bool>] [-GroupId <int>] [-
DisplayName <string>]
```

Для применения глобального требования не подтверждать никакие операции необходимо выполнить следующую PowerShell-команду:

```
Set-DssAccessPolicy [-AllActionsDisallowed] [-AllowChangeByUser <bool>] [-
AllowChangeByOperator <bool>] [-AllowOverride <bool>] [-GroupId <int>] [-
DisplayName <string>]
```

4.5.7. Администрирование компонента Центр Идентификации

Настройка компонента «Центр Идентификации» осуществляется с помощью Windows PowerShell. Команды администрирования включены в модуль **CryptoPro.DSS.PowerShell.STS** . Для поиска необходимого командлета перейдите в Объекты администрирования (см. Раздел 4.5.2) и выберите объект, чьи параметры необходимо настроить.

4.5.7.1. Настройки экземпляра

Командлет New-DssStsInstance

Создаёт экземпляр компонента Центр Идентификации.

К основным параметрам относятся:

- название веб-сайта IIS, на котором следует развернуть веб-приложение Центра Идентификации;
- адрес SQL-сервера, на котором следует развернуть БД Центра Идентификации;
- отображаемое имя экземпляра Центра Идентификации.

Синтаксис:

```
New-DssStsInstance -SiteName <string> [-ApplicationName <string>] -
SQLServerName <string> -DisplayName <string>
```

Таблица 22. Параметры командлета New-DssStsInstance

Параметр	Тип	Описание
SiteName	string	Название веб-сайта, на котором следует развернуть веб-приложение.
ApplicationName	string	Название веб-приложения Центра Идентификации. Если параметр не задан, используется значение STS.
SQLServerName	string	Адрес экземпляра SQL-сервера, на котором следует развернуть экземпляр БД Центра Идентификации. Формат: <SQL-сервер host>\<имя экземпляра>
DBname	string	Имя базы данных Цента Идентификации. По умолчанию IdentityServiceDB.
DisplayName	String	Отображаемое имя экземпляра компонента Центр Идентификации.
ConnectionInfo	SqlConnectionInfo	Расширенные данные для подключения к SQL-серверу (см. раздел 3.10).

Командлет Remove-DssStsInstance

Удаляет экземпляр компонента Центра Идентификации.

К основным параметрам относятся:

- флаг, определяющий, требуется ли удалять БД Центра Идентификации.

Синтаксис:

```
Remove-DssStsInstance [-DisplayName <string>] -DeleteDB <bool>
```

Таблица 23. Параметры командлета Remove-DssStsInstance

Параметр	Тип	Описание
DisplayName	String	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
DeleteDB	bool	Флаг, определяющий, требуется ли удалять БД Центра Идентификации

Параметр	Тип	Описание
ConnectionInfo	SqlConnectionInfo	Расширенные данные для подключения к SQL-серверу (см. раздел 3.10).

Командлет Get-DssStsInstance

Выводит на консоль список экземпляров Центра Идентификации.

Синтаксис:

```
Get-DssStsInstance
```

Командлет Update-DssStsInstance

Обновляет экземпляр компонента Центр Идентификации после установки новых библиотек.

Синтаксис:

```
Update-DssStsInstance [-DisplayName <string>]
```

4.5.7.2. Общие настройки

Командлет Set-DssStsProperties

Командлет **Set-DssStsProperties** позволяет задать основные параметры компонента «Центр идентификации». К основным параметрам относят:

- отпечаток сертификата ключа подписи электронного идентификатора;
- использование подтверждения телефона;
- использование подтверждения входа;
- настройки одноразовых паролей;
- общие настройки доверенных сторон.

Синтаксис:

```
Set-DssStsProperties [-ServiceCertificate <string>] [-AllowUserRegistration
<bool>] [-AllowUserPrimaryAuthChange <bool>] [-PhoneConfirmation <bool>] [-
DefaultTokenLifetime <int>] [-MaximumTokenLifetime <int>] [-
TransactionTimeOut <int>] [-OtpConfirmationTimeOut <int>] [-
MinOtpConfirmationTimeOut <int>] [-PasswordLength <int>] [-PasswordComplexity
<string> {Trivial | Weak | Fair | Strong}] [-OtpLength <int>] [-OtpComplexity
<string> {Trivial | Weak | Fair | Strong}] [-InvalidPasswordAttempts <int>]
[-InvalidOtpAttempts <int>] [-MaxDocumentInfoSize <int>] [-RequireUniqueEmail
<bool>] [-RequireUniquePhone <bool>] [-RequireUniqueDn <bool>] [-
AppliesToValidationRequired <bool>] [-SslAuthHostName <string>] [-SslAuthPort
<int>] [-AvailableIdentitifers <string[]> {Login | PhoneNumber | Email}] [-
EmailConfirmation <bool>] [-AnalyticsServiceAddress <string>] [-UserCabTitle
<string>] [-UserCabDescription <string>] [-AdminCabTitle <string>] [-
AdminCabDescription <string>] [-RequireMutualHttps <bool>] [-
AllowUserProfileChange <bool>] [-DisplayName <string>] [-
PasswordDisplayFormatList <string[]> {Phone | Screen | Email | Print}]
```

Таблица 24. Параметры командлета Set-DssStsProperties

Параметр	Тип	Значение по умолчанию	Описание
AllowUserPrimaryAuthChange	bool	False	Разрешено ли Пользователю менять настройки первичной аутентификации.
AllowUserSecondaryAuthChange	bool	True	Разрешено ли Пользователю менять настройки вторичной аутентификации.
AllowUserProfileChange	bool	False	Разрешить самостоятельное изменение профиля Пользователем.
AllowUserRegistration	bool	True	Разрешить самостоятельную регистрацию пользователей.
DisplayName	string	STS	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
IsClientAuthenticationIssuersStoreEnabled	bool	True	Использовать собственное хранилище доверенных издателей сертификатов аутентификации. Имя хранилища не изменяется.
EmailConfirmation	bool	False	Подтверждение электронной почты при задании.
PhoneConfirmation	bool	False	Подтверждение телефона после регистрации. По умолчанию выключено.
ServiceCertificate	string	-	Отпечаток сертификата ключа подписи маркера безопасности.
DefaultTokenLifeTime	In t	600	Время жизни маркера безопасности по умолчанию (в секундах)
LockUserAfterRegistration	bool	False	Блокируются ли зарегистрировавшиеся пользователи.
MaximumTokenLifeTime	int	1800	Максимальное время жизни маркера безопасности (в секундах).
PasswordDisplayFormatList	String[] Возможные значения: {Phone, Email, Screen, Print, Frame}	{Phone, Email, Screen, Print, Frame}	Список разрешенных идентификаторов.
SslAuthHostName	int	-	Имя хоста для SSL-аутентификации.
SslAuthPort	int	-	Номер порта для SSL-аутентификации.
TransactionTimeOut	int	44	Максимальное время (в секундах), которое предоставляется Пользователю для выполнения операции, подтверждённой одноразовым паролем. Подробнее про данный параметр см. раздел 5.5.1.

Параметр	Тип	Значение по умолчанию	Описание
MaxTransactionLifeTime	Int	0	Максимальное время (в секундах), которое предоставляется Пользователю для подтверждения произвольной операции.
OtpConfirmationTimeOut	int	300	Время подтверждения одноразового пароля (в секундах). Подробнее про данный параметр см. раздел 5.5.1.
MinOtpConfirmationTimeOut	int	300	Минимальное время (в секундах), в течение которого Пользователь не может запрашивать повторную отправку одноразового пароля. Подробнее про данный параметр см. раздел 5.5.1.
RequireMutualHttps	bool	False	Требовать двусторонний TLS для доступа к Веб-интерфейсу Пользователя.
TransactionMonitorInterval	int	10	Интервал проверки истёкших транзакций (в секундах).
MaxDocumentInfoSize	int	256	Максимальный размер (в символах) поля с информацией о документе, передаваемой в SAML-токене Пользователя.
AppliesToValidationRequired	bool	True	Осуществлять ли проверку идентификаторов зарегистрированных доверенных сторон.
AvailableIdentifierTypes	string[] {Login | PhoneNumber| Email}	{Login}	Список идентификаторов Пользователя, доступных для использования на ЦИ. Login – использовать логин Пользователя в качестве идентификатора. PhoneNumber – использовать номер мобильного телефона в качестве идентификатора. Email – использовать адрес электронной почты в качестве идентификатора Пользователя.
AnalyticsServiceAddress	string	http://<hostname>/<analyticsAppName>/AnalyticsService.svc	Адрес компонента Сервис Аудита.

Командлет Get-DssStsProperties

Командлет **Get-DssStsProperties** позволяет вывести на консоль значение основных параметров компонента «Центр Идентификации».

Синтаксис:

```
Get-DssSTSProperties [-DisplayName <string>]
```

Командлет Get-DssStsRegistryProperties

Используется для отображения строки подключения к базе данных Сервиса Подписи.

Синтаксис:

```
Get-DSSStsRegistryProperties
```

Командлет Set-DSSStsRegistryProperties

Используется для изменения строки подключения к базе данных Сервиса Подписи.

Синтаксис:

```
Set-DSSStsRegistryProperties [-DisplayName <string>] [-DBConnection <string>]
```

Таблица 25. Параметры командлета Set-DSSStsRegistryProperties

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
DBConnection	string	Строка подключения к базе данных Сервиса Подписи.

4.5.7.3. Общие настройки конечных точек

Командлет Get-DssStsEndpointGlobalSettings

Используется для вывода на консоль общих настроек конечных точек Центра Идентификации.

Синтаксис:

```
Get-DssStsEndpointGlobalSettings [-DisplayName <string>]
```

Командлет Set-DssStsEndpointGlobalSettings

Используется для изменения общих настроек конечных точек Центра Идентификации. Список параметров команды указан в Таблица 26.

Синтаксис:

```
Set-DssStsEndpointGlobalSettings [-MaxRecieveTimeOut <int>] [-MaxSendTimeOut
<int>] [-MaxMessageSize <int>] [-DisplayName <string>]
```

Таблица 26. Параметры командлета Set-DssStsEndpointGlobalSettings

Параметр	Тип	Описание
MaxRecieveTimeOut	int	Максимальное время получения сообщения в секундах. По умолчанию равен 30 секунд.
MaxSendTimeOut	int	Максимальное время отправки сообщения в секундах. По умолчанию равен 30 секунд.
MaxMessageSize	int	Максимальный размер сообщения в байтах. По умолчанию равен 5 Мбайт.
DisplayName	string	Имя экземпляра Центра Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.

4.5.7.4. Политика доступа к операциям

Командлет Get-DssAccessPolicy

Командлет позволяет вывести на консоль текущие настройки политики доступа к операциям.

Синтаксис:

```
Get-DssAccessPolicy [-GroupId <int>] [-DisplayName <string>]
```

Таблица 27. Параметры командлета Get-DssAccessPolicy

Параметр	Тип	Описание
GroupId	int	Идентификатор группы, для которой необходимо вывести сведения о политике доступа к операциям.
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.

Командлет Set-DssAccessPolicy

Используется для изменения настроек доступа к операциям. Помимо настроек доступа к операциям, настраиваются права пользователя/оператора изменять настройки доступа к операциям самостоятельно.

Синтаксис:

Запрещенные операции не настраиваются

```
Set-DssAccessPolicy [-AllowChangeByUser <bool>] [-AllowChangeByOperator
<bool>] [-AllowOverride <bool>] [-GroupId <int>] [-DisplayName <string>]
```

Все операции разрешены

```
Set-DssAccessPolicy -AllActionsAllowed [-AllowChangeByUser <bool>] [-
AllowChangeByOperator <bool>] [-AllowOverride <bool>] [-GroupId <int>] [-
DisplayName <string>]
```

Все операции запрещены

```
Set-DssAccessPolicy -AllActionsDisallowed [-AllowChangeByUser <bool>] [-
AllowChangeByOperator <bool>] [-AllowOverride <bool>] [-GroupId <int>] [-
DisplayName <string>]
```

Запрещены указанные операции

```
Set-DssAccessPolicy -DisallowedActions <string[]> {SignDocument |
DecryptDocument | CreateRequest | DeleteCertificate | RenewCertificate |
RevokeCertificate | HoldCertificate | UnholdCertificate | ChangePin} [-
AllowChangeByUser<bool>] [-AllowChangeByOperator <bool>] [-AllowOverride
<bool>] [-GroupId <int>] [-DisplayName <string>]
```

Таблица 28. Параметры командлета Set-DssAccessPolicy

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.

Параметр	Тип	Описание
DisallowedActions	String[] Возможные значения: {SignDocument; DecryptDocument; CreateRequest; DeleteCertificate; RenewCertificate; RevokeCertificate; HoldCertificate; UnholdCertificate; ChangePin}	Строка подключения к базе данных Сервиса Подписи.
AllActionsAllowed	-	Указание данного параметра разрешает все операции.
AllActionsDisallowed	-	Указание данного параметра запрещает все операции.
AllowChangeByOperator	bool	Определяет, может ли Оператор изменять доступ к операциям.
AllowChangeByUser	bool	Определяет, может ли Пользователь изменять доступ к операциям.
AllowOverride	bool	Определяет, может ли политика быть переопределена на более низком уровне иерархии.
GroupId	int	Идентификатор группы, для которой необходимо настроить политику доступа к операциям.

4.5.7.5. Настройки создания учетных записей

Командлет Get-DssAccountPolicy

Командлет позволяет вывести на консоль текущие настройки создания учетных записей

Синтаксис:

```
Get-DssAccountPolicy [-DisplayName <string>]
```

Командлет Set-DssAccountPolicy

Командлет позволяет настроить политики создания учетных записей

Синтаксис:

```
Set-DssAccountPolicy [-RequireUniqueEmail <bool>] [-RequireUniquePhone
<bool>] [-RequireUniqueDn <bool>] [-DisplayName <string>]
```

Таблица 29. Параметры командлета Set-DssAccountPolicy

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра ЦИ. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.

Параметр	Тип	Описание
RequireUniqueDn	bool	Требовать уникальность различительного имени Пользователя.
RequireUniqueEmail	bool	Требовать уникальность адреса электронной почты.
RequireUniquePhone	bool	Требовать уникальность номера телефона.

4.5.7.6. Парольные политики

Командлет Get-DssPasswordPolicy

Позволяет получить информацию об используемой парольной политике.

Синтаксис:

```
Get-DssPasswordPolicy [-DisplayName <string>]
```

Командлет Set-DssPasswordPolicy

Позволяет настроить парольную политику как долговременных, так и одноразовых паролей.

Синтаксис:

```
Set-DssPasswordPolicy [-PasswordLength <int>] [-PasswordComplexity
<ComplexityEnum> {Trivial | Weak | Fair | Strong}] [-OtpLength <int>] [-
OtpComplexity <ComplexityEnum> {Trivial | Weak | Fair | Strong}] [-
InvalidPasswordAttempts<int>] [-InvalidOtpAttempts <int>] [-PasswordSource
<PasswordSources> {ClientAndServer | ClientOnly | ServerOnly}] [-PasswordType
<PasswordType> {Symbolic | Phrase}] [-PasswordPhraseComplexity
<PasswordPhraseComplexityEnum> {Common | Strong}] [-PasswordLifetime <int>]
[-ChangePasswordAfterReset <bool>] [-DisplayName <string>]
```

Таблица 30. Параметры командлета Set-DssPasswordPolicy

Параметр	Тип	Значение по умолчанию	Описание
PasswordSource	PasswordSources Возможные значения: **ClientOnly**; **ServerOnly**; **ClientAndServer**.	ClientAndServer	Кто создает пароль: Клиент и сервер дает выбрать, кто генерирует пароль.
PasswordType	PasswordType Возможные значения **Phrase**; **Symbolic.**	Symbolic	Задает тип пароля – символьный или фраза.

Параметр	Тип	Значение по умолчанию	Описание
PasswordComplexity	ComplexityEnum Возможные значения: **Trivial** – только цифры; **Weak** – цифры и латинские буквы **Fair** – цифры и латинские буквы различных регистров **Strong** – цифры, латинские буквы различных регистров, спецсимволы.	3	Сложность долговременных паролей.
PasswordLifetime	int	0	Срок действия пароля (в днях).
PasswordLength	Int	8	Длина долговременных паролей.
InvalidPasswordAttempts	int	5	Количество неверных попыток ввода долговременного пароля.
ChangePasswordAfterReset	bool	False	Получает или задает значение, показывающее, требуется ли от пользователя смена долговременного пароля после сброса этого пароля Оператором.
OTPLength	Int	5	Длина одноразовых паролей.
OTPComplexity	ComplexityEnum Возможные значения: **Trivial** – только цифры; **Weak** – цифры и латинские буквы **Fair** – цифры и латинские буквы различных регистров **Strong** – цифры, латинские буквы различных регистров, спецсимволы.	1	Сложность одноразовых паролей.
InvalidOtpAttempts	int	3	Количество неверных попыток ввода одноразового пароля. Подробнее про данный параметр см. раздел 5.5.1
PasswordPhraseComplexity	PasswordPhraseComplexityEnum Возможные значения: **Common** – 3 слова; **Strong** – 4 слова.	Common	Сложность парольной фразы.

Параметр	Тип	Значение по умолчанию	Описание
DisplayName	string		Имя экземпляра ЦИ. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.

4.5.7.7. Доверенные стороны

Командлет Add-DssRelyingPartyTrust

Командлет Add-DssRelyingPartyTrust позволяет зарегистрировать потребителя маркеров безопасности – проверяющую сторону.

Синтаксис:

```
Add-DssRelyingPartyTrust -Name <string> -Identities <List[string]> [-
Description <string>] [-EncryptionCertificate <X509Certificate2>] [-
AdministrativeUrl <string>] [-DisplayName <string>] [-
AuthenticationCertificate <X509Certificate2>]
```

Таблица 31. Параметры командлета Add-DssRelyingPartyTrust

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Name	string	Отображаемое имя доверенной стороны.
Description	string	Краткое описание доверенной стороны.
MetadataUri	string	URI-адрес файла метаданных доверенной стороны.
EncryptionCertificate	X509Certificate2	Сертификат шифрования маркера безопасности. В качестве значения данного параметра можно указать объект PowerShell X509Certificate2 или путь к файлу с сертификатом.
Identities	List<string>	Список идентификаторов доверенной стороны.
AdministrativeUrl	string	URL-адрес раздела администрирования пользователей (часть веб-интерфейса, доступная Оператору).
AuthenticationCertificate	X509Certificate2	Сертификат аутентификации доверенной стороны. В качестве значения данного параметра можно указать объект PowerShell X509Certificate2 или путь к файлу с сертификатом.

Параметр	Тип	Описание
BackChannelUrl	string	URL-адрес канала для получения токенов операции.

Командлет Set-DssRelyingPartyTrust

Командлет **Set-DssRelyingPartyTrust** позволяет изменить параметры зарегистрированной доверенной стороны.

Синтаксис:

```
Set-DssRelyingPartyTrust [-Name <string>] [-Description <string>] [-
EncryptionCertificate <X509Certificate2>] [-Identities <List[string]>] [-
DisableTokenEncryption <bool>] [-ForOperator <bool>] [-AdministrativeUrl
<string>] [-AuthenticationCertificate <X509Certificate2>] [-DisableActAs
<bool>] [-DisplayName <string>]

Set-DssRelyingPartyTrust -Id <int> [-Name <string>] [-Description <string>]
[-EncryptionCertificate <X509Certificate2>] [-Identities <List[string]>] [-
DisableTokenEncryption <bool>] [-ForOperator <bool>] [-AdministrativeUrl
<string>] [-AuthenticationCertificate <X509Certificate2>] [-DisableActAs
<bool>] [-DisplayName <string>]
```

Таблица 32. Параметры командлета Set-DssRelyingPartyTrust

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Id	int	Поиск по уникальному идентификатору доверенной стороны.
Name	string	Отображаемое имя доверенной стороны.
Description	String	Краткое описание доверенной стороны.
EncryptionCertificate	X509Certificate2	Сертификат шифрования маркера безопасности для доверенной стороны. В качестве значения данного параметра можно указать объект PowerShell X509Certificate2 или путь к файлу с сертификатом.
Identities	List<string>	Список идентификаторов доверенной стороны.
ForOperator	bool	Возможно ли управление Пользователями в данной доверенной стороне.
AdministrativeUrl	string	URL адрес раздела администрирования Пользователей.
DisableTokenEncryption	bool	Отключено ли шифрование маркеров безопасности для доверенной стороны.

Параметр	Тип	Описание
AuthenticationCertificate	X509Certificate2	Сертификат аутентификации доверенной стороны. В качестве значения данного параметра можно указать объект PowerShell X509Certificate2 или путь к файлу с сертификатом.
DisableActAs	bool	Отключена ли возможность запросов маркеров делегирования для доверенной стороны.

Командлет Enable-DssRelyingPartyTrust

Командлет **Enable-DssRelyingPatryTrust** делает активной проверяющую сторону, зарегистрированную в КриптоПро DSS.

Синтаксис:

```
Enable-DssRelyingPartyTrust [-DisplayName <string>] -Id <int>
```

Таблица 33. Параметры командлета Enable-DssRelyingPartyTrust

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Id	int	Поиск по уникальному идентификатору доверенной стороны.

Командлет Disable-DssRelyingPartyTrust

Командлет **Disable-DssRelyingPatryTrust** делает неактивной проверяющую сторону, зарегистрированную в КриптоПро DSS.

Синтаксис:

```
Disable-DssRelyingPartyTrust [-DisplayName <string>] -Id <int>
```

Таблица 34. Параметры командлета Enable-DssRelyingPartyTrust

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Id	int	Поиск по уникальному идентификатору доверенной стороны.

Командлет Get-DssRelyingPartyTrust

Командлет **Get-DssRelyingPatryTrust** позволяет отобразить список всех зарегистрированных доверенных сторон или подробную информацию об одной из зарегистрированных доверенных сторон.

Синтаксис:

```
Get-DssRelyingPartyTrust [-DisplayName <string>] [-Id <int>]
```

Таблица 35. Параметры командлета Enable-DssRelyingPartyTrust

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Id	int	Поиск по уникальному идентификатору доверенной стороны.

Командлет Remove-DssRelyingPartyTrust

Командлет **Remove-DssRelyingPatryTrust** позволяет удалить проверяющую сторону.

Синтаксис:

```
Remove-DssRelyingPartyTrust [-DisplayName <string>] -Id <int>
```

Таблица 36. Параметры командлета Remove-DssRelyingPartyTrust

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Id	int	Поиск по уникальному идентификатору доверенной стороны.

4.5.7.8. Протокол OAuth

Командлет Add-DssClient

Командлет используется для регистрации нового клиента, использующегося для аутентификации приложения в системе с использованием протоколов OAuth и стандарта OpenID. Основные параметры командлета указаны в Таблица 37. Полное описание протокола OAuth содержится в соответствующем RFC 6749. Информацию об OpenID можно получить на странице проекта.

Таблица 37. Параметры командлета Add-DssClient

Параметр	Тип	Описание
Identifier	string	Идентификатор клиента
Name	string	Имя добавляемого клиента
Description	string	Описание приложения-клиента

Параметр	Тип	Описание
AllowedFlow	Flows [] Сценарии взаимодействия: AuthorizationCode Implicit ResourceOwner Другие возможные сценарии согласно стандарту зарезервированы для будущего использования и в текущей версии КриптоПро DSS недоступны: Hybrid ClientCredentials Custom AuthorizationCodeWithProofKey HybridWithProofKey	Определение допустимых для клиента сценариев использования, совместимых с OpenID.
RedirectUri	string	OAuth-параметр, содержит адрес, куда будет перенаправлен полученный код авторизации, либо Маркер доступа.
AuthorizationCodeLifetime	int	Время жизни кода авторизации в секундах.
AccessTokenLifetime	int	Маркер доступа (сведения о приложении-клиенте).
IdentityTokenLifetime	int	OpenID-параметр, содержит Маркер учетных данных пользователя.
GenerateSecret		Делает приложение публичным или конфиденциальным в рамках протокола OAuth. Сгенерирует ключ, который аутентифицирует клиента. Включается в запрос клиента к ЦИ на Маркер доступа.
PassThru	switch	Позволяет передать объект, над которым совершается действие, в следующий командлет.
DisplayName	string	Отображаемое имя клиента.

Синтаксис:

```
Add-DssClient [-Identifier <string>] [-Name <string>] [-Description <string>]
[-AllowedFlow <Flows[]> {AuthorizationCode | Implicit | Hybrid |
ClientCredentials | ResourceOwner | Custom | AuthorizationCodeWithProofKey |
HybridWithProofKey}] [-RedirectUri <string[]>] [-AuthorizationCodeLifetime
<int>] [-AccessTokenLifetime <int>] [-IdentityTokenLifetime <int>] [-
GenerateSecret] [-PassThru] [-DisplayName <string>]
```

Командлет Get-DssClient

Командлет позволяет получить вывод на консоль информации о зарегистрированных клиентах.

Синтаксис:

```
Get-DssClient [-ClientId <string>] [-DisplayName <string>]
```

Командлет Set-DssClient

Командлет позволяет настроить свойства клиента непосредственно по его идентификатору, либо передать с помощью конвейера объект из предыдущего командлета, используя скрытый параметр –TargetClient.

Синтаксис:

```
Set-DssClient -ClientId <string> [-Name <string>] [-Description <string>] [-
AllowedFlow <Flows[]> {AuthorizationCode | Implicit | Hybrid |
ClientCredentials | ResourceOwner | Custom | AuthorizationCodeWithProofKey |
HybridWithProofKey}] [-RedirectUri <string[]>] [-AuthorizationCodeLifetime
<int>] [-AccessTokenLifetime <int>] [-IdentityTokenLifetime <int>] [-
PassThru] [-DisplayName <string>]
```

ИЛИ

```
Set-DssClient -TargetClient <Client> [-Name <string>] [-Description <string>]
[-AllowedFlow <Flows[]> {AuthorizationCode | Implicit | Hybrid |
ClientCredentials | ResourceOwner | Custom | AuthorizationCodeWithProofKey |
HybridWithProofKey}] [-RedirectUri <string[]>] [-AuthorizationCodeLifetime
<int>] [-AccessTokenLifetime <int>] [-IdentityTokenLifetime <int>] [-
PassThru] [-DisplayName <string>]
```

Командлет Enable-DssClient

Командлет используется для включения аутентификации клиента по протоколу OAuth непосредственно по идентификатору клиента, либо с помощью конвейера объект из предыдущего командлета, используя скрытый параметр –TargetClient.

Синтаксис:

```
Enable-DssClient -ClientId <string> [-PassThru] [-DisplayName <string>]
```

ИЛИ

```
Enable-DssClient -TargetClient <Client> [-PassThru] [-DisplayName <string>]
```

Командлет Disable-DssClient

Командлет используется для отключения аутентификации клиента по протоколу OAuth непосредственно по его идентификатору, либо с помощью конвейера объект из предыдущего командлета, используя скрытый параметр –TargetClient.

Синтаксис:

```
Disable-DssClient -ClientId <string> [-PassThru] [-DisplayName <string>]
```

ИЛИ

```
Disable-DssClient -TargetClient <Client> [-PassThru] [-DisplayName <string>]
```

Командлет Remove-DssClient

Командлет используется для удаления существующего клиента непосредственно по его идентификатору, либо с помощью конвейера объект из предыдущего командлета, используя скрытый параметр –TargetClient.

Синтаксис:

```
Remove-DssClient -ClientId <string> [-DisplayName <string>]
```

ИЛИ

```
Remove-DssClient -TargetClient <Client> [-DisplayName <string>]
```

4.5.7.9. Группы Пользователей

Командлет New-DssIdentityGroup

Командлет создаёт новую группу Пользователей в рамках указанного доверенного издателя.

Синтаксис:

```
New-DSSIdentityGroup -Name <string> -Title <string> [-IdentityProviderID
<int>] [-IssuerName <string>] [-Description <string>] [-DisplayName <string>]
```

Таблица 38. Параметры командлета New-DssIdentityGroup

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Name	string	Имя группы Пользователей.
Title	string	Отображаемое имя группы Пользователей.
IdentityProviderID	int	Идентификатор доверенного издателя.
IssuerName	string	Строковый идентификатор издателя.
Description	string	Описание группы Пользователей.

Параметры **IdentityProviderID** и **IssuerName** являются взаимоисключающими.

Командлет Set-DssIdentityGroup

Командлет изменяет настройки группы Пользователей.

Синтаксис:

```
Set-DSSIdentityGroup -GroupId <int> [-Name <string>] [-Title <string>] [-
Description <string>] [-DisplayName <string>]
```

Таблица 39. Параметры командлета Set-DssIdentityGroup

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
GroupId	int	Идентификатор редактируемой группы.

Параметр	Тип	Описание
Name	string	Имя группы Пользователей.
Title	string	Отображаемое имя группы Пользователей.
Description	string	Описание группы Пользователей.

Командлет Get-DssIdentityGroup

Командлет выводит на консоль информацию о группах Пользователей.

Синтаксис:

```
Get-DSSIdentityGroup [-GroupId <int>] [-DisplayName <string>]
```

Таблица 40. Параметры командлета Get-DssIdentityGroup

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
GroupId	int	Идентификатор отображаемой группы. Если значение не указано, будет выведен список всех групп данного экземпляра.

Командлет Remove-DssIdentityGroup

Командлет удаляет группу Пользователей Центра Идентификации.

Синтаксис:

```
Remove-DSSIdentityGroup -GroupId <int> [-DisplayName <string>]
```

Таблица 41. Параметры командлета Remove-DssIdentityGroup

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
GroupId	int	Идентификатор удаляемой группы.

4.5.7.10. Операторы

Командлет Add-DssIdentityOperator

Командлет создаёт учётную запись Оператора Центра Идентификации.

Синтаксис:

```
Add-DSSIdentityOperator -Login <string> -Name <string> -IssuerName <string>
[-Audit <bool>] [-Certificate <string> ИЛИ <X509Certificate2>] [-DisplayName
<string>]
```

Таблица 42. Параметры командлета Add-DssIdentityOperator

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Login	string	Логин Оператора, представляющий собой уникальный идентификатор в БД Центра Идентификации.
Name	string	ФИО Оператора.
Audit	bool	Значение, указывающее, добавлять ли Оператора в качестве Оператора Аудита.
Certificate	string ИЛИ X509Certificate2	Путь к файлу сертификата Оператора ИЛИ в качестве значения данного параметра можно указать объект PowerShell X509Certificate2.
IssuerName	string	Строковый идентификатор доверенного издателя, к которому относится добавляемый Оператор. Фиксированное имя – **realsts.**

Командлет Get-DssIdentityOperator

Командлет выводит на консоль информацию об Операторах Центра Идентификации.

Синтаксис:

```
Get-DssIdentityOperator [-Groups] [-Login <string>] [-DisplayName <string>] -
IssuerName <string>]
```

Таблица 43. Параметры командлета Get-DssIdentityOperator

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Login	string	Логин Оператора, информацию о котором требуется получить.
Groups	SwitchParameter	Данный параметр используется для получения информации о членстве Операторов в группах.
IssuerName	string	Строковый идентификатор доверенного издателя, к которому относится Оператор, информацию о котором требуется получить.

Параметры **IssuerName, Groups** и **Login** являются взаимоисключающими.

Командлет Set-DssIdentityOperator

Командлет изменяет учётную запись Оператора Центра Идентификации.

Синтаксис:

```
Set-DSSIdentityOperator -Login <string> [-NewName <string>] [-GroupList
<string[]>] [-DisplayName <string>] [-Certificate <string> или
<X509Certificate2>] [-IssuerName <string>]
```

Таблица 44. Параметры командлета Set-DssIdentityOperator

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Login	string	Логин Оператора, учетная запись которого будет изменяться.
NewName	string	Новые ФИО Администратора.
Certificate	string ИЛИ X509Certificate2	Путь к файлу .cer с новым сертификатом Оператора ИЛИ в качестве значения данного параметра можно указать объект PowerShell X509Certificate2.
GroupList	string[]	Список групп, в которые следует поместить данного Оператора.
IssuerName	string	Строковый идентификатор доверенного издателя, к которому будет отнесен Оператор.

Параметр **GroupList** используется в случаях, когда необходимо изменить членство Оператора в группах. Является взаимоисключающим с **Certificate.**

КриптоПро DSS поддерживает выделенное хранилище издателей сертификатов аутентификации. Имя хранилища можно посмотреть в выводе параметра **ClientAuthenticationIssuersStoreName** командлета **Get-DssStsProperties** (по умолчанию – STS Client Authentication Issuers). Использование данного хранилища регулируется параметром **IsClientAuthenticationIssuersStoreEnabled** (см. раздел 4.5.7.2).

Командлет Remove-DssIdentityOperator

Командлет удаляет учетную запись Оператора Центра Идентификации.

Синтаксис:

```
Remove-DssIdentityOperator [-DisplayName <string>] -Login <string> [-
IssuerName <string>]
```

Таблица 45. Параметры командлета Set-DssIdentityOperator

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Login	string	Логин Оператора, представляющий собой уникальный идентификатор в БД Центра Идентификации.
IssuerName	string	Строковый идентификатор доверенного издателя, Оператор которого будет удален.

Параметры **IssuerName** и **Login** являются взаимоисключающими.

4.5.7.11. Преобразование документов

Командлет Get-DssStsConverterPlugin

Командлет используется для вывода на консоль всех зарегистрированных плагинов для преобразования документов.

Синтаксис:

```
Get-DssStsConverterPlugin [-DisplayName <string>]
```

Командлет Add-DssStsConverterPlugin

Добавление нового плагина для преобразования документов в конфигурационный файл.

Синтаксис:

```
Add-DssStsConverterPlugin [-DisplayName <string>] -FileExtension
<string> -Assembly <string> [-Classname <string>] [-Priority <int>] [-
Parameters <Hashtable>]
```

Таблица 46. Параметры командлета Add-DssStsConverterPlugin

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
FileExtension	string	Расширение документа.
Assembly	string	Полный путь до файла сборки плагина. В качестве значения данного параметра можно указать только имя dll файла сборки, в этом случае полный путь будет отсчитываться относительно директории: <Путь установки>\DSS\Plugins\Converters\<Тип плагина>.
Classname	string	Имя класса, реализующего интерфейс IDSSDocumentConverter.
Priority	int	Приоритет плагина относительно остальных зарегистрированных для данного расширения плагинов.
Parameters	Hashtable	Дополнительные параметры плагина.

В PowerShell для задания параметра типа **Hashtable** можно применить следующую конструкцию:

```
@{paramName1=paramValue1; paramName2=paramValue2;…;paramNameN=paramValueN}
```

где **paramName**$_i$, **paramValue**$_i$ – название и значение параметра соответственно.

Командлет Remove-DssStsConverterPlugin

Удаление зарегистрированного плагина для преобразования документов из конфигурационного файла.

Синтаксис:

```
Remove-DssStsConverterPlugin [-DisplayName <string>] -FileExtension <string> -Assembly <string> -Classname <string>
```

Таблица 47. Параметры командлета Remove-DssStsConverterPlugin

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
FileExtension	string	Расширение документа.
Assembly	string	Полный путь до файла сборки плагина. В качестве значения данного параметра можно указать только имя dll файла сборки, в этом случае полный путь будет отсчитываться относительно директории: <Путь установки>\DSS\Plugins\Converters\<Тип плагина>.
Classname	string	Имя класса, реализующего интерфейс IDSSDocumentConverter.

4.5.7.12. Аутентификация

Командлет Get-DssAuthenticationMethod

Выводит на консоль список зарегистрированных методов двухфакторной аутентификации.

Синтаксис:

```
Get-DssAuthenticationMethod [-DisplayName <string>] -Id <int> -Uri <string>
```

Таблица 48. Параметры командлета Get-DssAuthenticationMethod

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Id	int	Идентификатор метода аутентификации.
Uri	string	Уникальный идентификатор ресурса для метода аутентификации.

Командлет Enable-DssAuthenticationMethod

Выводит на консоль список зарегистрированных методов двухфакторной аутентификации.

Синтаксис:

```
Enable-DssAuthenticationMethod -Id <int> [-DisplayName <string>]
```

Таблица 49. Параметры командлета Enable-DssAuthenticationMethod

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Id	int	Идентификатор метода аутентификации.

Командлет Disable-DssAuthenticationMethod

Выводит на консоль список зарегистрированных методов двухфакторной аутентификации.

Синтаксис:

```
Disable-DssAuthenticationMethod -Id <int> [-DisplayName <string>]
```

Таблица 50. Параметры командлета Disable-DssAuthenticationMethod

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Id	int	Идентификатор метода аутентификации.

Командлет Import-DssStsOtpTokenData

Импортирует параметры OATH-токенов из файла инициализации.

Синтаксис:

```
Import-DssStsOtpTokenData -FilePath <string> [-DisplayName <string>]
```

Таблица 51. Параметры командлета Import-DssStsOtpTokenData

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.

Параметр	Тип	Описание
FilePath	string	Путь к файлу инициализации.

КриптоПро DSS поддерживает работу с OATH-токенами “**eTokenPass**” и файлами инициализации в формате “dat”.

4.5.7.13. Кастомизация

Командлет Get-DssStsCustomization

Данный командлет используется для вывода на консоль всех настроек отображения экземпляра Веб-интерфейса ЦИ.

Синтаксис:

```
Get-DssStsCustomization [-DisplayName <string>]
```

Командлет Set-DssStsCustomization

Данный командлет используется для изменения настроек отображения экземпляра Веб-интерфейса ЦИ.

Синтаксис:

```
Set-DssStsCustomization [-DisplayName <string>] [-Title <string>] [-Copyright
<string>] [-LogotypeFile <string>] [-HelpFile <string>] [-MainColor <string>]
[-AdditionalColor <string>] [-FontColor <string>] [-Font <string>]
[-StsLinksColor <string>] [-FavIconFile <string>]
```

Таблица 52. Параметры командлета Set-DssStsCustomization

Параметр	Тип	Описание
Title	string	Заголовок веб-приложения.
Copyright	string	Копирайт.
LogotypeFile	string	Полный путь до файла с логотипом. Размер логотипа – максимум 80 pix в высоту и 220 pix в ширину.
HelpFile	string	Полный путь до файла со справкой. Файл справки представляет собой HTML-документ.
MainColor	string	Основной цвет интерфейса веб-приложения (меню, выделенные кнопки). Цвет задается в формате HEX.
AdditionalColor	string	Дополнительный цвет интерфейса веб-приложения (выделенный элемент меню, выпадающий список под учетной записью). Цвет задается в формате HEX.
FontColor	string	Цвет шрифта заголовка, пунктов меню. Цвет задается в формате HEX.
Font	string	Тип шрифта.

Параметр	Тип	Описание
StsLinksColor	string	Цвет ссылок на стартовой странице. Цвет задается в формате HEX.
FavIconFile	string	Полный путь до файла с favicon. Допустимое расширение для файла – ico.

Ниже приведён пример скрипта для кастомизации веб-интерфейса Центра Идентификации

```
Set-DSSSTSCustomization -AdditionalColor f37c20 -MainColor 02458d -
StsLinksColor f37c20
Set-DSSSTSCustomization -FontColor f37c20 -Font Calibri
Set-DSSSTSCustomization -FavIconFile E:\Temp\favicon.ico -LogotypeFile
E:\Temp\logo.jpg -HelpFile E:\Temp\Help.html
Set-DSSSTSCustomization -Title "Центр идентификации Тест" -Copyright "Тест"
```

Командлет Reset-DssStsCustomization

Командлет используется для восстановления настроек по умолчанию отображения экземпляра Веб-интерфейса.

Синтаксис:

```
Reset-DssStsCustomization [-DisplayName <string>]
```

4.5.7.14. Компоненты имени Пользователя

Командлет Add-DssRDN

Командлет позволяет добавить компонент различительного имени Пользователя.

Синтаксис:

```
Add-DssRdn -Oid <string> -StringIdentifier <string> -FriendlyName <string> [-
DisplayName <string>]
```

Таблица 53. Параметры командлета Add-DssRDN

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Oid	string	Идентификатор добавляемого компонента в общем каталоге.
StringIdentifier	string	Строковый идентификатор добавляемого компонента (например, O, OU, C и т.д.)
FriendlyName	string	Отображаемое имя компонента различительного имени Пользователя.

Командлет Set-DssRDN

Командлет позволяет настроить компонент различительного имени Пользователя.

Синтаксис:

```
Set-DssRdn -Identifier <int> [-MaxLength <int>] [-MinLength <int>] [-Required
<bool>] [-ValueType <string> {Numeric | String}] [-DefaultValue <string>] [-
ClaimType <string>] [-Description <string>] [-DisplayName <string>]
```

Таблица 54. Параметры командлета Set-DssRDN

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Identifier	int	Идентификатор компонента различительного имени Пользователя в БД Центра Идентификации.
MaxLength	int	Максимальная длина значения компонента имени.
MinLength	int	Минимальная длина значения компонента имени.
ValueType	string	Тип значения компонента. Может принимать значения Numeric или String.
ClaimType	string	Тип утверждения (сведений о Пользователе), содержащего данный компонент.
Description	string	Описание компонента имени.

Командлет Get-DssRDN

Выводит на консоль список компонентов различительного имени Пользователя.

Синтаксис:

```
Get-DssRdn [-DisplayName <string>]
```

Командлет Remove-DssRDN

Данный командлет позволяет настроить компонентов различительного имени Пользователя.

Синтаксис:

```
Remove-DssRdn -Identifier <int> [-DisplayName <string>]
```

Таблица 55. Параметры командлета Remove-DssRDN

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Identifier	int	Идентификатор компонента различительного имени Пользователя в БД Центра Идентификации.

4.5.7.15. Политики компонентов имени Пользователя

Командлет Add-DssRdnPolicy

Данный командлет позволяет создать новую политику компонента различительного имени Пользователя.

Синтаксис:

```
Add-DSSRdnPolicy -Identifier <int> -Required <bool> -DefaultValues
<List[string]> -DisplayName <string> [-GroupId <int>]
```

Таблица 56. Параметры командлета Add-DssRdnPolicy

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Identifier	int	Идентификатор компонента различительного имени Пользователя в БД Центра Идентификации.
Required	bool	Значение, показывающее, является ли данный компонент обязательным.
DefaultValues	List[string]	Список значений по умолчанию для компонента
GroupId	int	Идентификатор группы, для которой производится редактирование политики.

Командлет Get-DssRdnPolicy

Данный командлет позволяет получить список настроенных политик компонентов различительных имен Пользователей. Командлет можно вызвать и без дополнительных параметров.

Синтаксис:

```
Get-DSSRdnPolicy [-Identifier <int> -DisplayName <string>]
```

Таблица 57. Параметры командлета Get-DssRdnPolicy

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Identifier	int	Идентификатор компонента различительного имени Пользователя в БД Центра Идентификации.

Командлет Set-DssRdnPolicy

Данный командлет позволяет настроить политику компонентов различительного имени Пользователя.

Синтаксис:

```
Set-DSSRdnPolicy -Identifier <int> -Required <bool> -DefaultValues
<List[string]> -DisplayName <string> [-GroupId <int>]
```

Таблица 58. Параметры командлета Set-DssRdnPolicy

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Identifier	int	Идентификатор компонента различительного имени Пользователя в БД Центра Идентификации.
Required	bool	Значение, показывающее, является ли данный компонент обязательным.
DefaultValues	List[string]	Список значений по умолчанию для компонента
GroupId	int	Идентификатор группы, для которой производится редактирование политики.

Командлет Remove-DssRdnPolicy

Данный командлет позволяет удалить политику компонентов различительного имени Пользователя.

Синтаксис:

```
Remove-DSSRdnPolicy -Identifier <int> [-DisplayName <string> -GroupId <int>]
```

Таблица 59. Параметры командлета Remove-DssRdnPolicy

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Identifier	int	Идентификатор компонента различительного имени Пользователя в БД Центра Идентификации.
GroupId	int	Идентификатор группы, для которой производится удаление политики.

4.5.7.16. Политики подтверждения операций

Командлет Get-DssConfirmationPolicy

Данный командлет позволяет получить список настроенных политик подтверждения операций.

Синтаксис:

```
Get-DssConfirmationPolicy [-DisplayName <string> -GroupId <int>]
```

Таблица 60. Параметры командлета Get-DssConfirmationPolicy

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
GroupId	int	Идентификатор группы, для которой необходимо вывести сведения о политике подтверждения операций.

Командлет Set-DssConfirmationPolicy

Данный командлет позволяет настроить политику подтверждения операций.

Синтаксис:

```
Set-DssConfirmationPolicy -NoneOpcActions [-AllowChangeByOperator -
DisplayName <string> -GroupId <int> -AllowChangeByUser -AllowOverride]

ИЛИ

Set-DssConfirmationPolicy -AllOpcActions [-DisplayName <string> -GroupId
<int> -AllowChangeByOperator -AllowChangeByUser -AllowOverride]

ИЛИ

Set-DssConfirmationPolicy -OpcActions <DssActions[]> [-DisplayName <string> -
GroupId <int> -AllowChangeByOperator -AllowChangeByUser -AllowOverride]
```

Таблица 61. Параметры командлета Set-DssConfirmationPolicy

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Центр Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
OpcActions	DssActions[] Может принимать значения: ➢ Issue, ➢ SignDocument, ➢ SignDocuments, ➢ DecryptDocument, ➢ CreateRequest, ➢ ChangePin, ➢ RenewCertificate, ➢ RevokeCertificate, ➢ HoldCertificate, ➢ UnholdCertificate, ➢ DeleteCertificate, ➢ PrivateKeyAccess.	Определяет набор действий на ЦИ, для которых требуется подтверждение операций.

Параметр	Тип	Описание
NoneOpcActions	-	Применяет требование не подтверждать никакие операции.
AllOpcActions	-	Применяет требование подтверждать все операции.
AllowChangeByOperator	bool	Определяет, может ли Оператор изменять список операций для подтверждения.
AllowChangeByUser	bool	Определяет, может ли Пользователь изменять список операций для подтверждения.
AllowOverride	bool	Определяет, может ли политика быть переопределена на более низком уровне иерархии.
GroupId	int	Идентификатор группы, для которой необходимо настроить политику подтверждения операций.

4.5.8. Пример PowerShell-сценария для настройки компонента «Центр Идентификации».

Данный сценарий выполняет минимально необходимую настройку экземпляра компонента «Центр Идентификации».

```
#Обязательные настройки:

# Создание экземпляра ЦИ
New-DssStsInstance -SiteName "Default Web Site" -DisplayName STS -
SQLServerName ".\SQLESXPRESS"

# Добавление отпечатка сервисного сертификата Центра Идентификации
Set-DssStsProperties –ServiceCertificate <Отпечаток сертификата компонента>
```

```
#Опциональные настройки:

# Добавление локального Оператора DSS

# Получаем объект сертификата Оператора из хранилища Личное текущего
Пользователя
$cert = Get-Item cert:\CurrentUser\My\<отпечаток сертификата Оператора>

Add-DssIdentityOperator -Login Admin -Name "Иванов Иван Иванович" –IssuerName
realsts –Certificate $cert
```

Пример добавления доверенной стороны:

```
# Регистрация Веб-интерфейса Пользователя в качестве доверенной стороны
Add-DssRelyingPartyTrust -Name "Frontend" -MetadataUri
https://$HostName/Frontend /FederationMetadata/2007-06/FederationMetadata.xml

# Регистрация Сервиса Подписи в качестве доверенной стороны
Add-DssRelyingPartyTrust -Name "SignServer" -MetadataUri
http://$HostName/SignServer /FederationMetadata/2007-
06/FederationMetadata.xml

# Включаем валидацию доверенных сторон
Set-DssStsProperties -AppliesToValidationRequired 1
```

4.6. Настройка Сервиса Подписи

Компонент КриптоПро DSS Сервис Подписи предназначен для выполнения операций по шифрованию документов, созданию электронной подписи и ее проверки.

4.6.1. Последовательность шагов по настройке экземпляра Сервиса Подписи

Данный раздел Руководства определяет последовательность и порядок действий по разворачиванию и настройке экземпляра Сервиса Подписи в режиме «с нуля».

Предварительные условия:

- Установленный SQL-Server;
- Установленная роль Сервер приложений (IIS);
- Настроенная привязка https на Сервере приложений (IIS) (см. раздел 3.1);
- Установленный КриптоПро CSP и КриптоПро HSM Client (см. разделы 3.6, 3.3);
- Установленный КриптоПро .NET (см. раздел 3.6);
- Выпущенный и установленный сервисный сертификат Сервиса Подписи (см.раздел 6).

Базовая последовательность шагов по настройке (обязательные):

1. Создание экземпляра службы Сервиса Подписи (см. раздел 4.6.3.1).

На данном шаге будет создано веб-приложение на Сервере приложений IIS, развёрнуты базы данных, зарегистрированы журналы Windows.

2. Настройка сервисного сертификата Сервиса Подписи (см. раздел 6).

На данном шаге экземпляру Сервиса Подписи назначается сервисный сертификат, который используется для аутентификации при межсервисном взаимодействии.

Учетной записи, под которой работает пул приложения Сервиса Подписи, необходимо выдать права на доступ к закрытому ключу сервисного сертификата (см. раздел 6.3).

3. Ввод лицензии (см. раздел 4.1).

4. Регистрация криптопровайдеров (см. раздел 4.6.3.3).

На данном шаге в экземпляре Сервиса Подписи регистрируется криптопровайдер, который используется для создания и работы с закрытыми ключами Пользователей.

5. Регистрация обработчика, реализующего функцию по созданию запроса на сертификат (см. раздел 4.6.3.6).

6. Настройка отношений доверия с Центром Идентификации (см. раздел 4.6.3.4).

На данном шаге устанавливается отношение доверия между Центром Идентификации и Сервисом Подписи, которое необходимо для аутентификации Пользователей и Операторов на Сервисе Подписи.

Настройка выполняется в два шага:

- Регистрация на Сервисе Подписи Центра Идентификации в качестве доверенного издателя маркеров безопасности (см. раздел 4.6.3.4).
- Регистрация Сервиса Подписи в качестве доверенной стороны на Центре Идентификации (см. раздел 4.5.7.7).

К моменту выполнения шага 5 в настройке Сервиса Подписи должен быть развёрнут экземпляр Центра Идентификации.

Дополнительные действия по настройке (опционально):

- Настройка параметров подписи.

Администратор может ограничить набор форматов подписи, которые может создавать Сервис Подписи. По умолчанию доступны все форматы подписи.

Для подписи формата CAdES-T и CAdES-X Long Type 1 необходимо задать адреса служб штампов времени (см. документацию на Службы УЦ 2.0). Список настроенных служб штампов времени будет отображаться в Веб-интерфейсе Пользователя.

Администратор может настроить политику ввода ПИН-кода на закрытый ключ: требовать обязательного задания ПИН-кода, никогда не требовать задания ПИН-кода, либо сделать задание ПИН-код опциональным – на усмотрение Пользователя. По умолчанию задание ПИН-кода на закрытый ключ является опциональным.

Администратор может настроить обязательную проверку на отзыв сертификата перед подписью.

- Настройка оповещения Пользователей.

Администратор DSS может настроить SMS- или Email-оповещение Пользователей о действиях, выполненных на Сервисе Подписи. Подробнее о настройке оповещения можно узнать в разделе 5.8.

- Настройка аудита.

Администратор DSS может настроить сбор событий с Сервиса Подписи и их отправку на Сервис Аудита для ведения журнала событий.

- Настройка конечных точек.

Администратор DSS может настроить параметры взаимодействия Сервиса Подписи со интегрируемыми системами. Например, можно ограничить размер документов, которые будут подписываться и/или шифроваться на Сервисе Подписи, ограничить максимальное время отправки/получения документов по сети, задать параметры безопасности при взаимодействии с интегрируемыми системами.

4.6.2. Объекты администрирования

На Рис. 29 приведена схема объектов, доступных для администрирования на Сервисе Подписи.

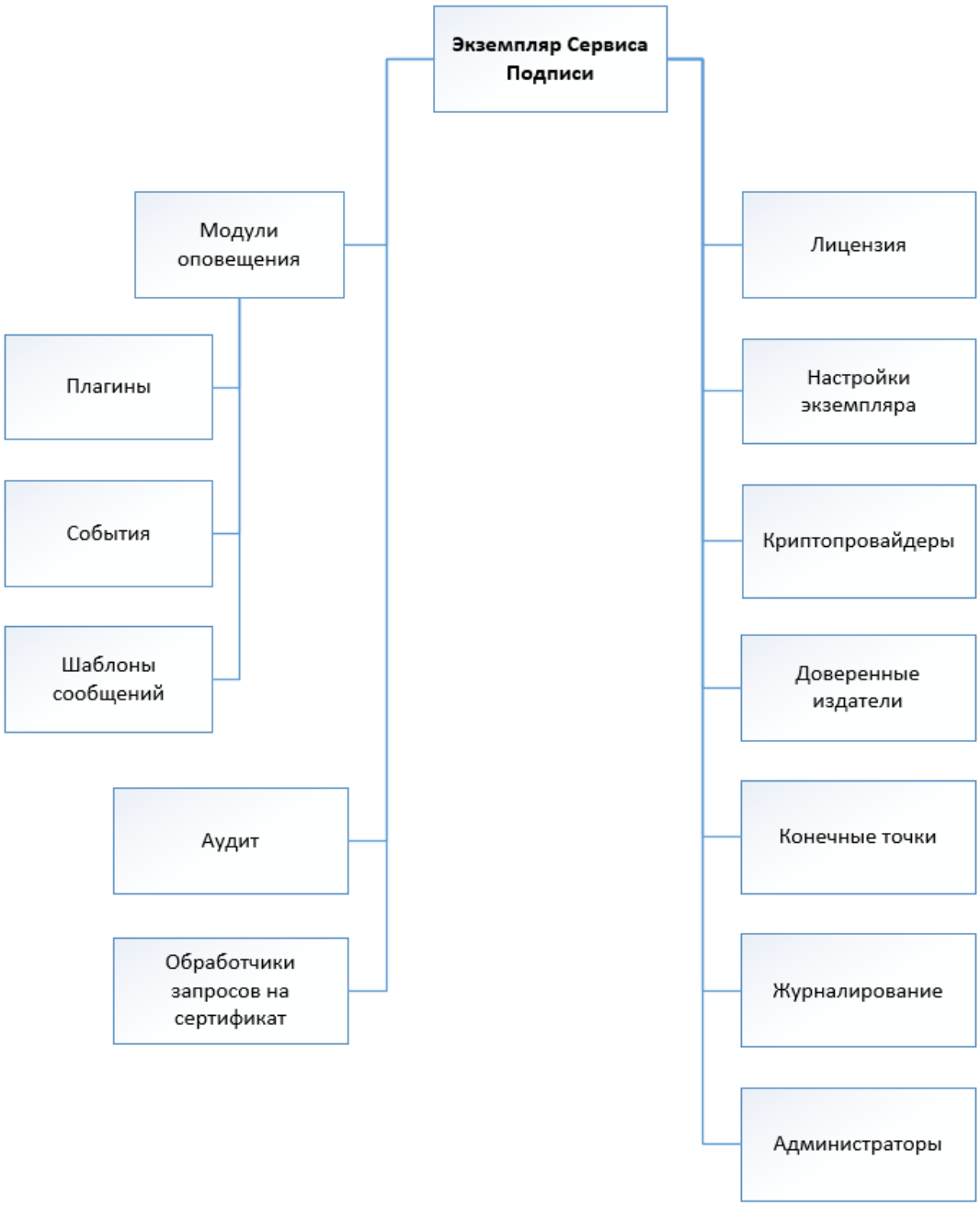

Рис. 29 – Объекты администрирования Сервиса Подписи

Таблица 62. Список командлетов компонента Сервис Подписи

Объект администрирования	Командлеты	Описание
Настройки экземпляра	New-DssSignServerInstance	Объект отвечает за управление экземплярами Сервиса Подписи.
	Remove-DssSignServerInstance	

Объект администрирования	Командлеты	Описание
	Get-DssSignServerInstance	
	Update-DssSignServerInstance	
Общие настройки	Get-DssProperties	Объект отвечает за настройку экземпляра Сервиса Подписи и строки подключения к базе данных.
	Set-DssProperties	
	Get-DssRegistryProperties	
	Set-DSSRegistryProperties	
Криптопровайдеры	Get-DssCryptoProvider	Объект отвечает за управление закрытыми ключами Пользователей.
	Get-DssCryptoProviderType	
	Add-DssCryptoProvider	
	Remove-DssCryptoProvider	
	Copy-DssCryptoProvider	
	Set-DssCryptoProvider	
	Split-DssCryptoProvider	
	Test-DssCryptoProvider	
	Enable-DssCryptoProvider	
	Disable-DssCryptoProvider	
Доверенные издатели	Add-DssClaimsProviderTrust	Объект отвечает за настройку отношений доверия с Центром Идентификации.
	Get-DssClaimsProviderTrust	
	Set-DssClaimsProviderTrust	
	Remove-DssClaimsProviderTrust	
Конечные точки	Enable-DSSEndpoint	Объект отвечает за параметры взаимодействия Сервиса Подписи с интегрируемыми системами.
	Disable-DSSEndpoint	
	Get-DSSEndpoint	

Объект администрирования	Командлеты	Описание
	Get-DssEndpointGlobalSettings	
	Set-DssEndpointGlobalSettings	
Журналирование	Get-DssSignServerTracing	Объект отвечает за журналирование сетевых взаимодействий (см. раздел 7.3).
	Set-DssSignServerTracing	
	Enable-DssSignServerTracing	
	Disable-DssSignServerTracing	
Модули оповещения	Add-DSSSignServerNotifier	Объект отвечает за рассылку уведомлений Пользователям и Операторам DSS (см. раздел 4.9.5).
	Get-DSSSignServerNotifier	
	Set-DSSSignServerNotifier	
	Remove-DSSSignServerNotifier	
	Enable-DSSSignServerNotifier	
	Disable-DSSSignServerNotifier	
Плагины	Add-DSSSignServerPlugin	Объект является частью модуля оповещения и отвечает за формирование сообщений, отправляемых Пользователям и Операторам, а также за отправку сообщений по каналу связи (SMS, Email и т.д.) (см. раздел 4.9.5).
	Get-DSSSignServerPlugin	
	Set-DSSSignServerPlugin	
	Remove-DSSSignServerPlugin	
События	Get-DSSSignServerEvent	Объект позволяет настроить список событий, о которых будут оповещаться Пользователи и Операторы, а также задать каналы отправки сообщений (SMS, Email, и т.п.) (см. раздел 4.9.5).
	Set-DSSSignServerEvent	
Шаблоны сообщений	Get-DSSSignServerFormatterTemplate	Объект позволяет просмотреть и изменить текст сообщений о

Объект администрирования	Командлеты	Описание
	Set-DSSSignServerFormatterTemplate	событиях на Сервисе Подписи, которые рассылаются Пользователям и Операторам (см. раздел 4.9.5).
Аудит	New-DSSSignServerAudit	Объект отвечает за взаимодействие с Сервисом Аудита и запись событий Сервиса Подписи в журнал Аудита (см. раздел 4.8.2).
	Remove-DSSSignServerAudit	
Лицензия	New-DSSLicense	Объект отвечает за лицензирование КриптоПро DSS. (см. раздел 4.2).
	Clear-DSSLicense	
	Update-DSSLicense	
Обработчики запросов на сертификат	Add-DssEnrollment	Объект используется для регистрации обработчика, реализующего функцию по созданию запроса на сертификат.

4.6.3. Администрирование компонента «Сервис Подписи»

Настройка компонента «Сервис Подписи» осуществляется с помощью Windows PowerShell. Команды администрирования включены в модуль **CryptoPro.DSS.PowerShell.SignServer**. Для поиска необходимого командлета перейдите в Объекты администрирования (см. Раздел 4.6.2) и выберите объект, чьи параметры необходимо настроить.

4.6.3.1. Настройки экземпляра

Командлет New-DssSignServerInstance

Используется для создания нового экземпляра Сервиса Подписи.

К основным параметрам относятся:

- название веб-сайта IIS, на котором следует развернуть веб-приложение Сервиса Подписи;
- адрес SQL-сервера, на котором следует развернуть БД Сервиса Подписи;
- отображаемое имя экземпляра Сервиса Подписи.

Синтаксис:

```
New-DssSignServerInstance -SiteName <string> [-ApplicationName <string>] -
SQLServerName <string> [-DBName <string>] -DisplayName <string>
```

Таблица 63. Параметры командлета New-DssSignServerInstance

Параметр	Тип	Описание
SiteName	string	Название веб-сайта, на котором следует развернуть веб-приложение Сервиса Подписи.
ApplicationName	string	Название веб-приложения Сервиса Подписи. Если параметр не задан используется значение SignServer.
SQLServerName	string	Имя экземпляра SQL-сервера, на котором следует развернуть экземпляр Сервиса Подписи. Формат: <SQL-сервер host>\<имя экземпляра>
DBName	string	Имя базы данных Сервиса Подписи. По умолчанию используется значение SignatureServerDB.
DisplayName	string	Отображаемое имя экземпляра Сервиса Подписи.
ConnectionInfo	SqlConnectionInfo	Расширенные данные для подключения к SQL-серверу (см. раздел 3.10).

В созданном экземпляре Сервиса Подписи зарегистрированы все форматы подписи (Общее описание КриптоПро DSS, Раздел 8). Для изменения списка предоставляемых сервисом форматов подписи, используйте командет Set-DssProperties.

Командлет Remove-DssSignServerInstance

Используется для удаления экземпляра Сервиса Подписи.

К основным параметрам относятся:

- флаг, определяющий, удалять ли БД Сервиса Подписи;
- флаг, определяющий удалять ли общую БД экземпляров Сервиса Подписи.

Синтаксис:

```
Remove-DssSignServerInstance [-DisplayName <string>] -DeleteDB <bool> -
DeleteDBCommon
```

Таблица 64. Параметры командлета Remove-DssSignServerInstance

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
DeleteDB	bool	Флаг, определяющий, требуется ли удаление БД Сервиса Подписи.

Параметр	Тип	Описание
DeleteDBCommon	Bool	Флаг, определяющий, требуется ли удаление разделяемой БД Сервиса Подписи.
ConnectionInfo	SqlConnectionInfo	Расширенные данные для подключения к SQL-серверу (см. раздел 3.10).

Командлет Get-DssSignServerInstance

Выводит на консоль список экземпляров Сервиса Подписи.

Синтаксис:

```
Get-DssSignServerInstance
```

Командлет Update-DssSignServerInstance

Обновляет экземпляр компонента Сервис Подписи после установки новых библиотек.

Синтаксис:

```
Update-DssSignServerInstance [-DisplayName <string>]
```

4.6.3.2. Общие настройки

Командлет Get-DssProperties

Используется для вывода на консоль основных параметров Сервиса Подписи.

Синтаксис:

```
Get-DssProperties [-DisplayName <string>]
```

Командлет Set-DssProperties

Используется для задания основных параметров Сервиса Подписи.

Синтаксис:

```
Set-DSSProperties [-DisplayName <string>] [-PinMode <PinCodeMode> {Required |
Forbid | Allow}] [-OperationConfirmationPolicy <MfaPolicy> {Off | On |
NotSet}] [-RequireMfaDefault <bool>] [-TSPList <List[TspService]>] [-
SignatureTypeList <List[SignatureType]> {XMLDSig | GOST3410 | CAdES | PDF |
MSOffice | CMS}] [-ActiveStsAddress <string>] [-
ValidateCertificateBeforeSignature <bool>] [-LogLevel <string> {Trace | Info
| Error}] [-MonitoringTimeout <int>] [-ServiceType <string>] [-AllowHashSigning
<bool>]
```

Таблица 65. Параметры командлета Set-DssProperties

Параметр	Тип	Значение по умолчанию	Описание
DisplayName	string	SignServer	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
PinMode	string Допустимые значения: Allow – разрешить ввод ПИН-кода (значение по умолчанию), Forbid – запретить ввод ПИН-кода, Required – требовать ПИН-код.	Allow	Режим ввода ПИН-кода.
TSPList	List<TspService> Объект TspService имеет следующие свойства: Name – строковой идентификатор службы, Title – название TSP-службы (данная строка будет отображаться в Веб-интерфейсе Пользователя), Address – URL-адрес TSP службы.	-	Задаёт доступные службы штампов времени.
SignatureTypeList	List<SignatureType> Допустимые значения: XMLDSig, GOST3410, MSOffice, PDF, CADES.	Все возможные	Поддерживаемые форматы подписи.
ServiceCertificateThumbprint	string	-	Отпечаток сертификата службы Сервиса Подписи.
ServiceCertificatePFX	string	-	Путь к PFX-файлу с сервисным сертификатом.

Параметр	Тип	Значение по умолчанию	Описание
ServiceCertificatePassword	string	-	Пароль к PFX-файлу с сервисным сертификатом. Параметр обязателен, если сертификат устанавливается из PFX-файла (параметр ServiceCertificatePFX).
ValidateCertificateBeforeSignature	bool	False	Проверять сертификат перед подписью.
MonitoringTimeout	int	10000	Период самотестирования в милисекундах. Если в значении задан 0, самотестирование будет отключено.
ServiceType	string	Server	Тип сервиса. Может принимать значения: Server, Client, ServerAndClient.
CadesUseOcspAuthorizedPolicy	bool	False	Разрешает использование групповой политики КриптоПро OCSP Client "Службы OCSP: сертификаты уполномоченных служб OCSP" при проверке полномочий службы актуальных статусов. Подробнее смотреть в Справочнике по КриптоПро OCSP SDK.
PdfSignatureSize	int	100000	Максимальный размер подписи в PDF.
TokenTimeout	int	600	Максимальное время подтверждения операций в секундах.
RequireStrongConfirmation	bool	True	Требовать строгое подтверждение операций.
TransactionCacheMode	<TransactionCacheMode> Возможные значения: DistributedCache; HalfDistributedCache; InMemoryCache.	DistributedCache	Режим работы кеша транзакций.

Параметр	Тип	Значение по умолчанию	Описание
IsAdditionalCertStore Enabled	bool	False	Использовать ли дополнительное хранилище сертификатов при подписи.
AdditionalCertStoreN ame	string	-	Название хранилища, содержащего дополнительные сертификаты и CRL для сбора доказательств действительности сертификата ЭП.
AllowHashSigning	bool	False	Получает или задает значение, показываюшее, можно ли создавать подпись хэш-значения.

Создание электронной подписи хэш-значения требует дополнительных тематических исследований и может применяться исключительно для создания усиленной неквалифицированной ЭП.

Командлет Get-DssRegistryProperties

Используется для отображения строки подключения к базе данных Сервиса Подписи.

Синтаксис:

```
Get-DSSRegistryProperties
```

Командлет Set-DSSRegistryProperties

Используется для изменения строки подключения к базе данных Сервиса Подписи.

Синтаксис:

```
Set-DSSRegistryProperties [-DisplayName <string>] [-DBConnection <string>]
```

Таблица 66. Параметры командлета Set-DSSRegistryProperties

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
DBConnection	string	Строка подключения к базе данных Сервиса Подписи.

4.6.3.3. Криптопровайдеры

Командлет Get-DssCryptoProvider

Используется для вывода на консоль информации о зарегистрированных провайдерах.

Синтаксис:

```
Get-DssCryptoProvider [-DisplayName <string>] [-Validate]
```

Таблица 67. Параметры командлета Get-DssCryptoProvider

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Validate	SwitchParameter	Флаг, определяющий, что требуется проверка работоспособности криптопровайдеров с Мастер-ключом.

Командлет Get-DssCryptoProviderType

Выводит на консоль список зарегистрированных типов криптопровайдеров.

Синтаксис:

```
Get-DssCryptoProviderType [-DisplayName <string>]
```

Командлет Add-DssCryptoProvider

Используется для регистрации нового криптопровайдера на Сервисе Подписи.

Синтаксис:

```
Add-DssCryptoProvider [-DisplayName <string>] -ProviderName <string> -
ProviderType <int> -TypeId <string> [-Order <int] [-SetMasterKeyLife [-
MasterKeyLife <int>]] [-SetUsersKeysLife [-UsersKeysLife <int>]] [-
MasterKeyName <string>]
```

Таблица 68. Параметры командлета Add-DssCryptoProvider

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Descrition	string	Описание криптопровайдера для отображения в Веб-интерфейс Пользователя.
TypeId	String Возможные значения: GostWithMasterKey Common RSAWithMasterKey	Идентификатор типа криптопровайдера.

Параметр	Тип	Описание
Order	int	Отвечает за порядок следования на Веб-интерфейсе Пользователя зарегистрированных криптопровайдеров. Чем выше номер, тем выше в списке криптопровайдер. По умолчанию параметр равен 0.
ProviderType	int	Тип провайдера, зарегистрированного в ОС (Для КриптоПро CSP – 75).
ProviderName	string	Имя провайдера, зарегистрированное в системе.
SetMasterKeyLifetime	SwitchParameter	Установить срок действия Мастер-ключа в случае, если создается провайдер с Мастер-ключом.
MasterKeyLifetime	int	Срок действия Мастер-ключа с момента создания в месяцах. По умолчанию срок действия Мастер-ключа - 36 месяцев.
SetUsersKeysLifetime	SwitchParameter	Установить срок действия пользовательских ключей.
UsersKeysLifetime	int	Срок действия пользовательских ключей, созданных на данном провайдере, в месяцах. По умолчанию срок действия пользовательского ключа 15 месяцев.
MasterKeyName	string	Имя контейнера с Мастер-ключом, если создается провайдер с уже существующим Мастер-ключом.

Зарегистрированное имя провайдера в системе предопределено заранее. Его можно увидеть в документации поставщика криптопровайдера. Для продуктов КриптоПро:

- КриптоПро HSM: **Crypto-Pro HSM Svc CSP**
- КриптоПро CSP (только для тестирования КриптоПро DSS): **Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider**

Командлет Remove-DssCryptoProvider

Используется для удаления криптопровайдера на Сервисе Подписи.

Синтаксис:

```
Remove-DssCryptoProvider [-DisplayName <string>] -ID <guid>
```

Таблица 69. Параметры командлета Remove-DssCryptoProvider

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
ID	guid	Идентификатор криптопровайдера.

Командлет Enable-DssCryptoProvider

Используется для включения криптопровайдера на Сервисе Подписи, ранее переведённого в состояние отключен.

Синтаксис:

```
Enable-DssCryptoProvider [-DisplayName <string>] -ID <int>
```

Таблица 70. Параметры командлета Enable-DssCryptoProvider

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
ID	guid	Идентификатор криптопровайдера.

Командлет Disable-DssCryptoProvider

Используется для отключения криптопровайдера на Сервисе Подписи.

Синтаксис:

```
Disable-DssCryptoProvider [-DisplayName <string>] -ID <guid>
```

Таблица 71. Параметры командлета Disable-DssCryptoProvider

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
ID	guid	Идентификатор криптопровайдера.

Командлет Copy-DssCryptoProvider

Используется для создания нового криптопровайдера, принадлежащего заданной группе криптопровайдеров. Мастер-ключ нового криптопровайдера совпадает с Мастер-ключами остальных криптопровайдеров группы.

Синтаксис:

```
Copy-DssCryptoProvider [-DisplayName <string>] -GroupID <int> -NewProvName
<string>
```

Таблица 72. Параметры командлета Copy-DssCryptoProvider

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
GroupID	Int	Идентификатор группы, которой принадлежит копируемый криптопровайдер.
NewProvName	string	Имя нового криптопровайдера.

Командлет Split-DssCryptoProvider

Используется для исключения криптопровайдера из группы.

Синтаксис:

```
Split-DssCryptoProvider [-DisplayName <string>] -ID <guid>
```

Таблица 73. Параметры командлета Split-DssCryptoProvider

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
ID	guid	Идентификатор криптопровайдера.

Командлет Set-DssCryptoProvider

Используется для вывода на консоль информации о зарегистрированных провайдерах.

Синтаксис:

```
Set-DssCryptoProvider -DisplayName <string> [-MasterKeyName <string>][-Order
<int] [-Description <string>] -ID <guid>
```

Таблица 74. Параметры командлета Set-DssCryptoProvider

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Order	int	Отвечает за порядок следования на Веб-интерфейсе Пользователя зарегистрированных криптопровайдеров. Чем выше номер, тем выше в списке криптопровайдер. По умолчанию параметр равен 0.
Description	string	Описание криптопровайдера для отображения в Веб-интерфейс Пользователя.
MasterKeyName	string	Имя контейнера с Мастер-ключом, если создается провайдер с уже существующим Мастер-ключом.
ID	guid	Идентификатор криптопровайдера.

Командлет Test-DssCryptoProvider

Используется для проверки доступности криптопровайдера.

Синтаксис:

```
Test-DssCryptoProvider [-DisplayName <string>] -ID <guid>
```

Таблица 75. Параметры командлета Test-DssCryptoProvider

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
ID	guid	Идентификатор криптопровайдера.

4.6.3.4. Доверенные издатели

Командлет Add-DssClaimsProviderTrust

Используется для добавления отпечатка сертификата доверенного издателя маркеров безопасности.

Синтаксис:

```
Add-DssClaimsProviderTrust [-DisplayName <string>] -IssuerName <string> -
Thumbprint <string>
```

Таблица 76. Параметры командлета Add-DssClaimsProviderTrust

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
IssuerName	string	Уникальное имя издателя маркеров безопасности.
Thumbprint	string	Отпечаток сертификата подписи маркеров безопасности.

Командлет Get-DssClaimsProviderTrust

Используется для вывода на консоль зарегистрированных доверенных издателей маркеров безопасности. Отображается строковой идентификатор издателя и отпечаток сертификата ключа подписи.

Синтаксис:

```
Get-DssClaimsProviderTrust [-DisplayName <string>]
```

Командлет Set-DssClaimsProviderTrust

Используется для изменения отпечатка сертификата доверенного издателя маркеров безопасности.

Синтаксис:

```
Set-DssClaimsProviderTrust [-DisplayName <string>] - IssuerName <string>
-NewThumbprint <string>
```

Таблица 77. Параметры командлета Set-DssClaimsProviderTrust

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
IssuerName	string	Уникальное имя издателя маркеров безопасности.
NewThumbprint	string	Новый отпечаток сертификата подписи маркеров безопасности.

Командлет Remove-DssClaimsProviderTrust

Используется для удаления доверенного издателя маркеров безопасности.

Синтаксис:

```
Remove-DssClaimsProviderTrust [-DisplayName <string>] – IssuerName <string>
```

Таблица 78. Параметры командлета Remove-DssClaimsProviderTrust

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
IssuerName	string	Уникальное имя издателя маркеров безопасности.

4.6.3.5. Конечные точки

Командлет Get-DssEndpointGlobalSettings

Используется для вывода на консоль общих настроек конечных точек Сервиса Подписи.

Синтаксис:

```
Get-DssEndpointGlobalSettings [-DisplayName <string>]
```

Командлет Set-DssEndpointGlobalSettings

Используется для изменения общих настроек конечных точек Сервиса Подписи. Список параметров команды указан в Таблица 26.

Синтаксис:

```
Set-DssEndpointGlobalSettings [-MaxRecieveTimeOut <int>] [-MaxSendTimeOut
<int>] [-MaxMessageSize <int>] [-DisplayName <string>]
```

Таблица 79. Параметры командлета Set-DssEndpointGlobalSettings

Параметр	Тип	Описание
MaxRecieveTimeOut	int	Максимальное время получения сообщения в секундах. По умолчанию равен 30 секунд.

Параметр	Тип	Описание
MaxSendTimeOut	int	Максимальное время отправки сообщения в секундах. По умолчанию равен 30 секунд.
MaxMessageSize	int	Максимальный размер сообщения в байтах. По умолчанию равен 5 Мбайт.
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.

Командлет Enable-DssEndpoint

Используется для включения конечных точек Сервиса Подписи. Список параметров команды указан в Таблица 80.

Синтаксис:

```
Enable-DSSEndpoint -Address <string> [-DisplayName <string>]
```

Таблица 80. Параметры командлета Enable-DSSEndpoint

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Name	string	Имя конечной точки.

Командлет Disable-DssEndpoint

Используется для отключения конечных точек Сервиса Подписи. Список параметров команды указан в Таблица 81.

Синтаксис:

```
Disable-DSSEndpoint [-DisplayName <string>]
```

Таблица 81. Параметры командлета Disable-DSSEndpoint

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Name	string	Имя конечной точки.

Командлет Get-DssEndpoint

Используется для вывода на консоль информации о конечных точках Сервиса Подписи.

Синтаксис:

```
Get-DSSEndpoint [-DisplayName <string>]
```

4.6.3.6. Обработчики запросов на сертификат

Командлет Add-DssEnrollment

Используется для регистрации обработчика, реализующего функцию по созданию запроса на сертификат.

Синтаксис:

```
-Add-DssEnrollment [-DisplayName <string>] -Type EnrollOutOfBand [-Order
<int] -EnrollDisplayName <string> [-SNChangesEnabled <bool>] [-ValidationMode
<string>] [-CertificatePrintTemplate <string>] [-RequestPrintTemplate
<string>] [-RevokeRequestPrintTemplate <string>] -RdnConfig <string> -
TemplatesConfig <string>
```

Таблица 82. Параметры командлета Add-DssEnrollment

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Type	Значение: EnrollOutOfBand	Определяет минимальный набор параметров, необходимых для регистрации обработчика.
Order	int	Отвечает за порядок следования на Веб-интерфейсе Пользователя зарегистрированных обработчиков. Чем выше номер, тем выше в списке обработчик. По умолчанию параметр равен 0.
EnrollDisplayName	string	Отображаемое имя обработчика УЦ.
SNChangesEnabled	bool	Разрешить изменять имя субъекта в сертификате.
ValidationMode	string Возможные значения: CertificateAuthority, ChainOffline, ChainOnline, NoCheck.	Режим проверки сертификата ЭП перед использованием. По БД УЦ По локально установленному CRL; По локально установленному или загруженному по сети CRL ИЛИ при помощи OCSP-службы; Не проверять
CertificatePrintTemplate	string	Путь к шаблону печати сертификата
RequestPrintTemplate	string	Путь к шаблону печати запроса на сертификат
RevokeRequestPrintTemplate	string	Путь к шаблону печати запроса на отзыв сертификата
RdnConfig	string	Путь к файлу конфигурации компонент имени Пользователя (политики имен).
TemplatesConfig	string	Путь к файлу конфигурации шаблонов сертификатов.

Командлет Enable-DssEnrollment

Данный командлет позволяет включить обработчик. Командлет принимает идентификатор зарегистрированного обработчика, либо объект в режиме конвейера.

Синтаксис:

```
Enable-DssEnrollment [-DisplayName <string>] -ID <int>
```

ИЛИ

```
Get-DssEnrollment [-DisplayName <string>] -ID <int> | Enable-DssEnrollment
```

Таблица 83. Параметры командлета Enable-DssEnrollment

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
ID	int	Идентификатор обработчика.

Командлет Disable-DssEnrollment

Данный командлет позволяет отключить обработчик. Командлет принимает идентификатор зарегистрированного обработчика, либо объект в режиме конвейера.

Синтаксис:

```
Disable-DssEnrollment [-DisplayName <string>] -ID <int>
```

ИЛИ

```
Get-DssEnrollment [-DisplayName <string>] -ID <int> | Disable-DssEnrollment
```

Таблица 84. Параметры командлета Disable-DssEnrollment

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
ID	int	Идентификатор обработчика.

Командлет Set-DssEnrollmentOob

Командлет позволяет настроить обработчик обработчик, реализующий функцию по созданию запроса на сертификат. Командлет принимает идентификатор зарегистрированного обработчика, либо объект в режиме конвейера.

Синтаксис:

```
Set-DssEnrollmentOob -ID <int> [-DisplayName <string>] [-Override] [-Order
<int>] [-EnrollDisplayName <string>] [-SNChangesEnabled <bool>] [-
ValidationMode <string>] [-CertificatePrintTemplate <string>] [-
RequestPrintTemplate <string>] [-RevokeRequestPrintTemplate <string>] [-
RdnConfig <string>] [-TemplatesConfig <string>]
```

Таблица 85. Параметры командлета Set-DssEnrollmentOob

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Override	switch	Наличие данного параметра определяет, будут ли удалены все предыдущие настройки обработчика УЦ перед записью новых. Отсутствие параметра позволяет изменить только явно указанные в командлете настройки.
Order	int	Отвечает за порядок следования на Веб-интерфейсе Пользователя зарегистрированных обработчиков. Чем выше номер, тем выше в списке обработчик. По умолчанию параметр равен 0.
ID	int	Идентификатор обработчика УЦ, для которого изменяются настройки.
EnrollDisplayName	string	Отображаемое имя обработчика УЦ. При вводе нового имени, параметр будет переопределен для настраиваемого обработчика УЦ.
SNChangesEnabled	bool	Разрешить изменять имя субъекта в сертификате.
ValidationMode	string Возможные значения: CertificateAuthority, ChainOffline, ChainOnline, NoCheck.	Режим проверки сертификата ЭП перед использованием. По БД УЦ По локально установленному CRL; По локально установленному или загруженному по сети CRL ИЛИ при помощи OCSP-службы; Не проверять
CertificatePrintTemplate	string	Путь к шаблону печати сертификата
RequestPrintTemplate	string	Путь к шаблону печати запроса на сертификат
RevokeRequestPrintTemplate	string	Путь к шаблону печати запроса на отзыв сертификата
RdnConfig	string	Путь к файлу конфигурации компонент имени Пользователя. (см. далее).
TemplatesConfig	string	Путь к файлу конфигурации шаблонов сертификатов Пользователей. (см. далее).

Командлет Get-DssEnrollment

Данный командлет позволяет вывести на консоль сведения о зарегистрированнои обработчике УЦ. Командлет принимает идентификатор зарегистрированного обработчика УЦ, либо объект в режиме конвейера.

Синтаксис:

```
Get-DssEnrollment [-DisplayName <string>] -ID <int> [-IncludeCaProperties
<switch>]
```

Таблица 86. Параметры командлета Get-DssEnrollment

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
ID	int	Идентификатор обработчика УЦ.
IncludeCaProperties	switch	Включить в вывод свойства УЦ. Данный параметр вызывается, если нужно отобразить свойства УЦ, к которому подключен обработчик.

Командлет Remove-DssEnrollment

Данный командлет позволяет удалить зарегистрированный обработчик УЦ. Командлет принимает идентификатор зарегистрированного обработчика УЦ, либо объект в режиме конвейера.

Синтаксис:

```
Remove-DssEnrollment [-DisplayName <string>] -ID <int>
```

ИЛИ

```
Get-DssEnrollment [-DisplayName <string>] -ID <int> | Remove-DssEnrollment
```

Таблица 87. Параметры командлета Remove-DssEnrollment

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
ID	int	Идентификатор обработчика УЦ.

Обработчик УЦ может быть удалён только в случае, если в базе данных Сервиса Подписи нет сертификатов и запросов на сертификаты к данному УЦ.

Файлы конфигурации шаблонов сертификатов и политики имён представляют собой текстовые файлы, содержащие строки определенного формата.

Файлы конфигурации шаблонов сертификатов и политик имен должны быть сохранены в кодировке UTF-8.

Формат строки файла конфигурации компонент имени Пользователя (политики имен):

`DisplayName='строковое значение DisplayName' Name ='Строковое значение Name' OID='Значение OID' Order='1..n' Required='true|false'`, где

- DisplayName – отображаемое имя компонента имени;
- Name – строковый идентификатор компонента имени;
- OID – соответствующий OID компонента имени;
- Order – порядок компонента имени в шаблоне имени;
- Required – флаг указывающий на обязательность компонента имени.

Пример:

```
DisplayName='Имя' Name='CN'OID='2.5.4.3' Order='1' Required='true'
DisplayName='Электронная почта' Name='E' OID='1.2.840.113549.1.9.1' Order='17' Required='false'
DisplayName='Страна/регион' Name='C'OID='2.5.4.6'Order='9'Required='false'
DisplayName='Регион' Name='S'  OID='2.5.4.8'Order='3' Required='false'
DisplayName='Населённый пункт' Name='L'  OID='2.5.4.7'Order='4' Required='false'
DisplayName='Организация' Name='O'  OID='2.5.4.10'Order='5' Required='false'
DisplayName='Подразделение' Name='OU'  OID='2.5.4.11'Order='6' Required='false'
DisplayName='ОГРН' Name='OGRN'  OID='1.2.643.100.1'Order='7' Required='false'
DisplayName='ИНН' Name='INN'  OID='1.2.643.3.131.1.1'Order='8' Required='false'
```

Формат записи файла шаблонов сертификатов:

```
[Имя шаблона TemplateName]
OID1
OID2
…
```

и т.д., где

- TemplateName – имя шаблона сертификатов;
- OID – идентификатор улучшенного использования ключа, входящий в шаблон.

Пример:

```
[Временный сертификат Пользователя УЦ]
1.2.643.2.2.34.2
1.2.643.2.2.34.6
1.3.6.1.5.5.7.3.2

[Временный сертификат Оператора УЦ]
1.2.643.2.2.34.2
1.2.643.2.2.34.5
1.3.6.1.5.5.7.3.2
```

4.6.4. Пример PowerShell-сценария для настройки Сервиса Подписи

Данный сценарий задаёт минимально необходимые настройки Сервиса Подписи.

```
# Создание нового экземпляра компонента Сервис Подписи
New-DssSignServerInstance -SiteName "Default Web Site" -ApplicationName
SignServer -SQLServerName ".\SQLEXPRESS" -DisplayName SignServer

# Ввод отпечатка сервисного сертификата
Set-DssProperties -ServiceCertificateThumbprint <Отпечаток сертификата
компонента>

#Добавление HSM-провайдера с Мастер Ключом
Add-DssCryptoProvider -TypeId < GostWithMasterKey> -ProviderName "Crypto-Pro
HSM Svc CSP" -ProviderType 75

#Регистрация обработчика, отвечающего за генерацию запроса на сертификат
Add-DssEnrollment -Type EnrollOutOfBand -EnrollName <Имя обработчика> -
RdnConfig <Путь к файлу политики имен> TemplatesConfig <Путь к файлу шаблонов
сертификатов>

# Настройка отношений доверия с Центром Идентификации
Add-DssClaimsProviderTrust -IssuerName realsts -Thumbprint <Отпечаток
сертификата Центра Идентификации>

# Ввод временной лицензии
New-DssLicense
```

Пример регистрации Сервиса Подписи в качестве доверенной стороны на Центре Идентификации:

```
Add-DssRelyingPartyTrust -Name "SignServer" -MetadataUri
http://<signserver_host>/SignServer/FederationMetadata/2007-
06/FederationMetadata.xml
```

Пример настройки адресов служб штампов времени:

```
#Задание служб штампов времени

$newTsp = New-Object -TypeName CryptoPro.DSS.Common.Service.TSPService
#Задание адреса
$newTsp.Url = "http://cryptopro.ru/tsp/tsp.srf"
#Задание идентификатора
$newTsp.Name = "testtsp"
#Задание отображаемого имени
$newTsp.Title = "Тестовая TSP служба КРИПТО-ПРО"

$newTsp2 = New-Object -TypeName CryptoPro.DSS.Common.Service.TSPService
$newTsp2.Url = "http://tsp.cryptopro.ru/tsp/tsp.srf"
$newTsp2.Name = "csptsp"
$newTsp2.Title = "TSP служба КРИПТО-ПРО"

# Формируем список служб штампов времени.
$newTspList = $newTsp, $newTsp2

# Регистрируем службы штампов времени на Севрисе Подписи
```

```
Set-DssProperties -TspList $newTspList
```

Пример настройки конечных точек:

```
# Размер входящих/исходящих сообщений увеличиваем до ~50Mb
# Time-out приёма/передачи сообщений увеличиваем до 1 минуты
Set-DSSEndpoint -MaxRecieveTimeOut 60 -MaxSendTimeOut 60 -MaxMessageSize
50000000
```

Пример включения журналирования:

```
# Настройка журналирования событий
Set-DssSignServerTracing -ServiceModelListenerLogFile
C:\dsstrace\SignServer.svclog -ServiceModelListenerSourceLevel All

# Настройка журналирования сообщений
Set-DssSignServerTracing -ServiceModelMessageLoggingListenerLogFile
C:\dsstrace\SignServerMessage.svclog -
ServiceModelMessageLoggingListenerSourceLevel All

# Включение журналирования
Enable-DssSignServerTracing
```

4.7. Настройка Веб-интерфейса Пользователя

Веб-интерфейс Пользователя предоставляет Пользователям графический интерфейс для работы с Сервисом Электронной Подписи.

4.7.1. Последовательность шагов по настройке экземпляра компонента «Веб-интерфейс Пользователя»

Данный раздел Руководства определяет последовательность и порядок действий по разворачиванию и настройке экземпляра компонента Веб-интерфейс Пользователя в режиме «с нуля».

Предварительные условия:

- Установленная роль Сервер приложений (IIS);
- Настроенная привязка https на Сервере приложений (IIS);
- Выпущенный и установленный сервисный сертификат Веб-интерфейса Пользователя (см. раздел 6.2).

Базовая последовательность шагов по настройке (обязательные):

1. Создание экземпляра Веб-интерфейса Пользователя (см. раздел 4.7.3.1)

На данном шаге будет создано веб-приложение на Сервере приложений IIS, зарегистрированы журналы Windows.

2. Настройка сервисного сертификата Веб-интерфейса Пользователя (см. раздел 4.7.3.1)

На данном шаге экземпляру Веб-интерфейса Пользователя назначается сервисный сертификат, который используется для аутентификации при межсервисном взаимодействии.

Необходимо выдать права на доступ к закрытому ключу сертификата учётной записи под которой работает пул приложения Веб-интерфейса Пользователя (см. раздел 6.2).

3. Настройка адресов Сервиса Подписи и Центра Идентификации (см. раздел 4.7.3.3).

На данном шаге задаются адреса Сервиса Подписи и Центра Идентификации для межсервисного взаимодействия.

4. Настройка параметров протокола аутентификации ws-federation passive requestor profile.

На данном шаге Администратор задаёт параметры для аутентификации на Веб-интерфейсе Пользователя при помощи комадлета Set-DssFEWSFederationSettings.

5. Настройка отношений доверия с Центром Идентификации (см. раздел 4.7.3.2)

На данном шаге устанавливаются отношения доверия между Центром Идентификации и Веб-интерфейсом Пользователя, которое необходимо для аутентификации Пользователей и Операторов на Веб-интерфейсе Пользователя.

Настройка выполняется в два шага:

- Регистрация на Веб-интерфейсе Пользователя Центра Идентификации в качестве доверенного издателя маркеров безопасности (см. раздел 4.7.3.2).
- Регистрация на Центре Идентификации Веб-интерфейса Пользователя в качестве доверенной стороны (см. раздел 4.5.7.7).

К моменту выполнения шага 5 в настройке Веб-интерфейса Пользователя должен быть развёрнут экземпляр Центра Идентификации.

После выполнения перечисленных настроек доступ к Веб-интерфейсу Пользователя осуществляется по умолчанию по следующим ссылкам:

Веб-интерфейс Сервиса Подписи:

```
https://<hostname>/Frontend
```

Личный кабинет Пользователя/Оператора:

```
https://<hostname>/STS/Users
```

Пример PowerShell-скрипта для настройки Веб-интерфейса Пользователя приведён в разделе 4.7.4.

Дополнительные действия по настройке (опционально):

- Кастомизация Веб-интерфейса Пользователя

Администратор может изменить отображаемые на Веб-интерфейсе Пользователя логотипы, цвета интерфейса, цвета шрифтов, заголовки и т.п. Подробнее о кастомизации см. раздел 4.7.3.6. Также Администратор может изменить первую страницу, которая отображается Пользователю при входе на Веб-интерфейс. По умолчанию отображается страница приветствия.

- Визуализация документов

Администратор может настроить отображение документов в Веб-интерфейсе при подписании и шифровании. Подробнее об отображении документов см. раздел 4.7.3.5.

- Настройка размера подписываемых документов

Администратор может ограничить максимальный размер документа, который может быть подписан через Веб-интерфейс Пользователя (см. раздел 4.7.3.1). По умолчанию, максимальный размер документа равен 5Mb.

- Интеграция с Сервисом Проверки Подписи (КриптоПро SVS 2.0)

Администратор может включить отображение дополнительных вкладок на Веб-интерфейсе Пользователя для проверки подписи и сертификата (см. раздел 4.7.3.1). Для выполнения данного действия необходимо, чтобы был установлен и настроен Сервис Проверки Подписи.

- Отображение журнала аудита

Администратор может включить отображение журнала Сервиса Аудита на Веб-интерфейсе Пользователя (см. раздел 4.7.3.1). Для выполнения данной операции необходимо, чтобы был установлен и настроен компонент Сервис Аудита (см. раздел 5.5).

4.7.2. Объекты администрирования

На Рис. 30 приведена схема объектов, доступных для администрирования на Веб-интерфейсе Пользователя.

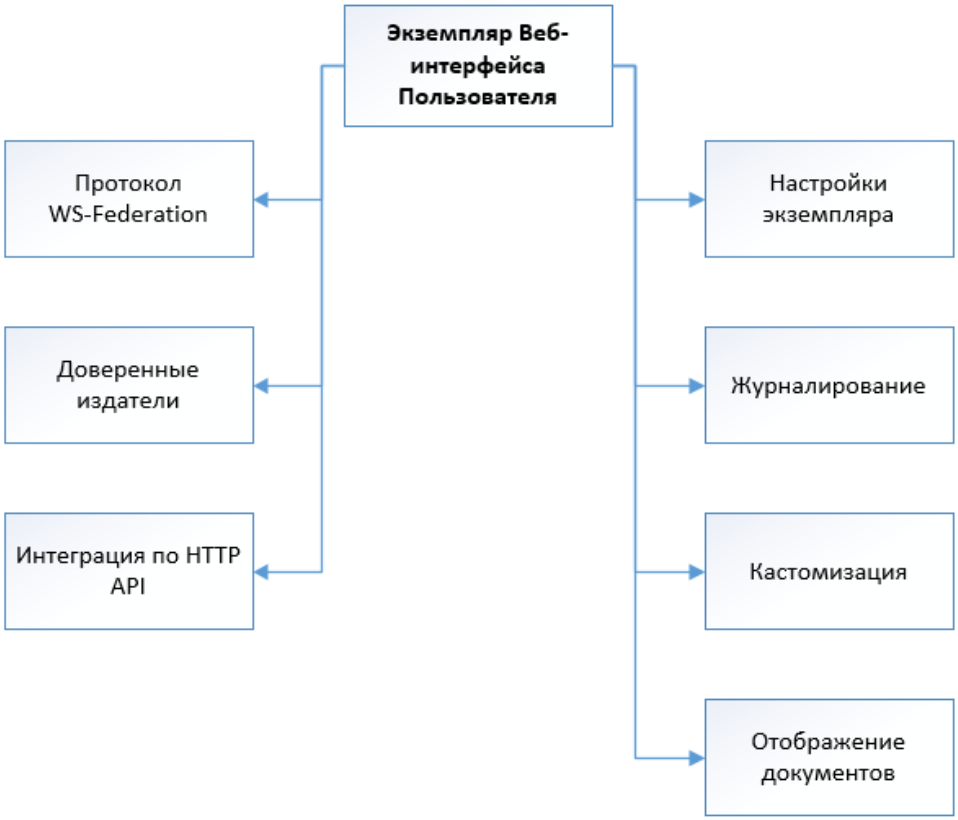

Рис. 30 – Объекты администрирования Веб-интерфейса Пользователя

Таблица 88. Список командлетов компонента Веб-интерфейс Пользователя

Объекты администрирования	Командлет	Описание
Настройки экземпляра	New-DssFEInstance	Объект отвечает за управление экземплярами Веб-интерфейса Пользователя.
	Remove-DssFEInstance	
	Get-DssFeInstance	
	Set-DssFEProperties	
	Get-DssFEProperties	
	Update-DssFEInstance	
Доверенные издатели	Add-DssFeClaimsProviderTrust	Объект отвечает за настройку отношений доверия с Центром Идентификации.
	Get-DssFEClaimsProviderTrust	
	Set-DssFEClaimsProviderTrust	

Объекты администрирования	Командлет	Описание
	Remove-DssFEClaimsProviderTrust	
Протокол WS-Federation	Get-DssFEWSFederationSettings	Объект отвечает за настройку протокола WS-Federation с ЦИ КриптоПро DSS.
	Set-DssFEWSFederationSettings	
Интеграция по HTTP-API	Add-DssFETrustedWebapplication	Объект отвечает за настройки взаимодействия с веб-интерфейсом интегрируемой системы по HTTP API.
	Enable-DssFETrustedWebapplication	
	Disable-DssFETrustedWebapplication	
	Get-DssFETrustedWebApplication	
	Remove-DssFETrustedWebApplication	
Отображение документов	Get-DssFEConverterPlugin	Объект отвечает за визуализацию документов при их загрузке в Веб-Интерфейс Пользователя.
	Add-DssFEConverterPlugin	
	Remove-DssFEConverterPlugin	
Кастомизация	Get-DssFECustomization	Объект отвечает за настройку отображения Веб-интерфейса Пользователя.
	Set-DssFECustomization	
	Reset-DssFECustomization	
Журналирование	Enable-DssFETracing	Объект «Журналирование» отвечает за журналирование сетевых взаимодействий (см. раздел 7.3).
	Disable-DssFETracing	
	Get-DssFETracing	
	Set-DssFETracing	

4.7.3. Администрирование компонента «Веб-интерфейс Пользователя»

Настройка компонента «Веб-интерфейс Пользователя» осуществляется с помощью Windows PowerShell. Команды администрирования включены в модуль **CryptoPro.DSS.PowerShell.Frontend**. Для поиска необходимого командлета перейдите в Объекты администрирования (см. Раздел 4.7.2) и выберите объект, чьи параметры необходимо настроить.

4.7.3.1. Настройки экземпляра

Командлет New-DssFEInstance

Создаёт новый экземпляр компонента Веб-интерфейс Пользователя.

К основным параметрам относятся:

- название веб-сайта IIS, на котором следует развернуть веб-приложение сервера подписи.
- отображаемое имя экземпляра Веб-интерфейса Пользователя.

Синтаксис:

```
New-DssFEInstance -SiteName <stirng> [-ApplicationName <string>] -DisplayName
<string>
```

Таблица 89. Параметры командлета New-DssFEInstance

Параметр	Тип	Описание
SiteName	string	Название веб-сайта, на котором следует развернуть веб-приложение Веб-интерфейса Пользователя.
ApplicatonName	string	Название веб-приложения Веб-интерфейса Пользователя. Если параметр не задан, используется значение Frontend.
DisplayName	string	Отображаемое имя экземпляра Веб-интерфейса Пользователя.

Командлет Remove-DssFEInstance

Удаляет созданный экземпляр компонента Веб-интерфейса Пользователя.

Синтаксис:

```
Remove-DssFEInstance [-DisplayName <string>]
```

Командлет Get-DssFEInstance

Выводит на консоль список экземпляров Веб-интерфейса Пользователя.

Синтаксис:

```
Get-DssFEInstance
```

Командлет Set-DssFEProperties

Командлет **Set-DssFEProperties** позволяет задать основные параметры компонента «Веб-интерфейс Пользователя». К основным параметрам относят:

- URL-адрес Сервиса Подписи;
- URL-адрес Центра Идентификации;
- отпечаток сертификата Веб-интерфейса Пользователя.

Синтаксис:

```
Set-DSSFEProperties [-SignServerAddress <string>] [-StsAddress <string>] [-
ServiceCertificate <string>] [-VsAddress <string>] [-CmisAddress <string>] [-
AnalyticsServiceAddress <string>] [-IndexPage <FrontendIndexPages> {Sign |
Encrypt | Decrypt | VerifySign | VerifyCertificate | CertificatesList}] [-
```

```
MaxIISContentLength <uint32>] [-RequireMutualHttps <bool>] [-DisplayName
<string>]
```

Таблица 90. Параметры командлета Set-DssFEProperties

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра Веб-интерфейса Пользователя.
SignServerAddress	string	URL-адрес Сервиса Подписи. Пример: http://<hostname>/<SignServiceAppName>/SignServiceExR.svc/token/nosc
StsAddress	string	URL-адрес Центра Идентификации: Пример: https://<hostname>/<StsAppName>/Active.svc/service
ServiceCertificate	string	Отпечаток сертификата Веб-интерфейса Пользователя.
VsAddress	string	URL-адрес Сервиса Проверки Подписи. Пример: http://<hostname>/<VerifivationServiceAppName>/service.svc
IndexPage	FrontendIndexPages Возможные значения: Sign Encrypt Decrypt VerifySign VerifyCertificate CertificatesList	Задаёт первую отображаемую страницу Веб-интерфейса Пользователя.
MaxIISContentLength	Uint32	Максимальный размер контента, который можно загрузить в веб-приложение (в байтах). По умолчанию равен 4 Мбайт.
AnalyticsServiceAddress	string	Адрес компонента «Сервис Аудита». По умолчанию адрес имеет следующий вид: http://<hostname>/<analyticsAppName>/AnalyticsService.svc
RequireMutualHttps	bool	Требовать соединения по https с двусторонней аутентификацией.

Командлет Get-DssFEProperties

Командлет **Get-DssFEProperties** позволяет отобразить основные параметры Веб-интерфейса Пользователя.

Синтаксис:

```
Get-DssFEProperties [-DisplayName <string>]
```

Командлет Update-DssFEInstance

Обновляет экземпляр компонента Веб-интерфейс Пользователя после установки новых библиотек.

Синтаксис:

```
Update-DssFEInstance [-DisplayName <string>]
```

4.7.3.2. Доверенные издатели

Командлет Add-DssFEClaimsProviderTrust

Добавляет отпечаток сертификата подписи маркеров безопасности в список доверенных издателей маркеров безопасности.

Синтаксис:

```
Add-DssFEClaimsProviderTrust [-DisplayName <string>] -IssuerName <string> -
Thumbprint <string>
```

Таблица 91. Параметры командлета Add-DssFEClaimsProviderTrust

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра Веб-интерфейса Пользователя.
IssuerName	string	Имя доверенного издателя.
Thumbprint	string	Отпечаток сертификата доверенного издателя.

Командлет Get-DssFEClaimsProviderTrust

Используется для вывода на консоль зарегистрированных доверенных издателей маркеров безопасности. Отображается строковой идентификатор издателя и отпечаток сертификата ключа подписи.

Синтаксис:

```
Get-DssFEClaimsProviderTrust [-DisplayName <string>]
```

Командлет Set-DssFEClaimsProviderTrust

Используется для изменения отпечатка сертификата доверенного издателя маркеров безопасности.

Синтаксис:

```
Set-DssFEClaimsProviderTrust [-DisplayName <string>] - IssuerName <string>
-NewThumbprint <string>
```

Таблица 92. Параметры командлета Set-DssFEClaimsProviderTrust

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Веб-интерфейса Пользователя. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
IssuerName	string	Уникальное имя издателя маркеров безопасности.
NewThumbprint	string	Новый отпечаток сертификата подписи маркеров безопасности.

КомандлетRemove-DssFEClaimsProviderTrust

Используется для удаления доверенного издателя маркеров безопасности.

Синтаксис:

```
Remove-DssFEClaimsProviderTrust [-DisplayName <string>] - IssuerName <string>
```

Таблица 93. Параметры командлета Remove-DssFEClaimsProviderTrust

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Веб-интерфейса Пользователя. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
IssuerName	string	Уникальное имя издателя маркеров безопасности.

4.7.3.3. Протокол WS-Federation

Командлет Set-DssFEWSFederationSettings

Данный командлет используется для изменения настроек WS-Federation. К ним относятся:

- адрес Центра Идентификации КриптоПро DSS;
- адрес Веб-интерфейса Пользователя КриптоПро DSS;
- адрес доверенного Центра Идентификации в домене Пользователя.

Синтаксис:

```
Set-DssFEWSFederationSettings [-DisplayName <string>] [-Issuer <string>] [-
Realm <string>] [-HomeRealm <string>] [RequireHttps <bool>]
```

Таблица 94. Параметры командлета Set-DssFEWSFederationSettings

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Веб-интерфейса Пользователя. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.

Параметр	Тип	Описание
Issuer	string	URL-адрес Центра Идентификации КриптоПро DSS. По умолчанию имеет значения: https://<host_name>/sts/sts/issue/
Realm	string	URL-адрес Веб-интерфейса Пользователя КриптоПро DSS. По умолчанию имеет значения: https://<host_name>/frontend/
HomeRealm	string	URL-адрес Центра Идентификации. По умолчанию не заполняется, зарезервирован для дальнейшего использования.
RequireHttps	bool	Требовать защищённого соединения.

Командлет Get-DssFEWSFederationSettings

Данный командлет используется для вывода на консоль настроек WS-Federation.

Синтаксис:

```
Get-DssFEWSFederationSettings [-DisplayName <string>]
```

4.7.3.4. Интеграция по HTTP-API

Командлет Add-DssFETrustedWebapplication

Командлет позволяет добавить веб-интерфейс интегрируемой системы, с которого при попытке аутентификации будет происходить перенаправление на Веб-интерфейс Пользователя. Используется для настройки интеграции с помощью HTTP-API.

Синтаксис:

```
Add-DSSFETrustedWebApplication -Name <string> [-BackPostUrls <List[string]>]
[-DisplayName <string>]
```

Таблица 95. Параметры командлета Add-DssFETrustedWebapplication

Параметр	Тип	Описание
Name	string	Название веб-сайта, с которого будет осуществляться перенаправление.
BackPostUrls	string	URL или множество URL доверенных приложений.
DisplayName	string	Отображаемое имя экземпляра Веб-интерфейса Пользователя, для которого настраивается интеграция.

Командлет Enable-DssFETrustedWebapplication

Командлет позволяет включить перенаправление на Веб-интерфейс Пользователя с добавленного ранее доверенного приложения.

Синтаксис:

```
Enable-DSSFETrustedWebApplication [-DisplayName <string>]
```

Командлет Disable-DssFETrustedWebapplication

Командлет позволяет отключить перенаправление на Веб-интерфейс Пользователя с добавленного ранее доверенного приложения.

Синтаксис:

```
Disable-DSSFETrustedWebApplication [-DisplayName <string>]
```

Командлет Get-DssFETrustedWebapplication

Командлет позволяет получить список доверенных приложений.

Синтаксис:

```
Get-DSSFETrustedWebApplication [-Name <string>] [-DisplayName <string>]
```

Командлет Remove-DssFETrustedWebapplication

Командлет позволяет удалить доверенное приложение.

Синтаксис:

```
Remove-DSSFETrustedWebApplication [-Name <string>] [-DisplayName <string>]
```

4.7.3.5. Отображение документов

Командлет Get-DssFEConverterPlugin

Данный командлет используется для вывода на консоль всех зарегистрированных плагинов для преобразования документов.

Синтаксис:

```
Get-DssFEConverterPlugin [-DisplayName <string>]
```

Командлет Add-DssFEConverterPlugin

Регистрация нового плагина для преобразования документов.

Синтаксис:

```
Add-DssFEConverterPlugin [-DisplayName <string>] -FileExtension <string> -
Assembly <string> [-Classname <string>] [-Priority <int>] [-Parameters
<Hashtable>]
```

Таблица 96. Параметры командлета Add-DssFEConverterPlugin

Параметр	Тип	Описание
FileExtension	string	Расширение документа.
Assembly	string	Полный путь до файла сборки плагина. В качестве значения данного параметра можно указать только имя dll файла сборки, в этом случае полный путь будет отсчитываться относительно директории: <Путь установки>\Plugins\Converters\<Тип плагина>.
Classname	string	Имя класса, реализующего интерфейс IDSSDocumentConverter.

Параметр	Тип	Описание
Priority	int	Приоритет плагина относительно остальных зарегистрированных для данного расширения плагинов.
Parameters	Hashtable	Дополнительные параметры плагина.

В PowerShell для задания параметра типа **Hashtable** можно применить следующую конструкцию:

```
@{paramName1=paramValue1; paramName2=paramValue2;…;paramNameN=paramValueN}
```

где **paramName$_i$**, **paramValue$_i$** – название и значение параметра соответственно.

Командлет Remove-DssFEConverterPlugin

Удаление зарегистрированного плагина для преобразования.

Синтаксис:

```
Remove-DssFEConverterPlugin [-DisplayName <string>] -FileExtension <string> -
Assembly <string> -Classname <string>
```

Таблица 97. Парметры командлета Remove-DssFEConverterPlugin

Параметр	Тип	Описание
FileExtension	string	Расширение документа.
Assembly	string	Полный путь до файла сборки плагина. В качестве значения данного параметра можно указать только имя dll файла сборки, в этом случае полный путь будет отсчитываться относительно директории: <Путь установки>\Plugins\Converters\<Тип плагина>.
Classname	string	Имя класса, реализующего интерфейс IDSSDocumentConverter.

4.7.3.6. Кастомизация

Командлет Get-DssFECustomization

Данный командлет используется для вывода на консоль всех настроек отображения экземпляра Веб-интерфейса Пользователя.

Синтаксис:

```
Get-DssFECustomization [-DisplayName <string>]
```

Командлет Set-DssFECustomization

Данный командлет используется для изменения настроек отображения экземпляра Веб-интерфейса Пользователя.

Синтаксис:

```
Set-DssFECustomization [-DisplayName <string>] [-Title <string>] [-Copyright
<string>] [-LogotypeFile <string>] [-HelpFile <string>] [-MainColor <string>]
[-AdditionalColor <string>] [-FontColor <string>] [-Font <string>]
[-FavIconFile <string>]
```

Таблица 98. Параметры командлета Set-DssFECustomization

Параметр	Тип	Описание
Title	string	Заголовок веб-приложения.
Copyright	string	Права на использование и распространение.
LogotypeFile	string	Полный путь до файла с логотипом. Размер логотипа – максимум 80 pix в высоту и 220 pix в ширину.
HelpFile	string	Полный путь до файла со справкой. Файл справки представляет собой HTML-документ.
MainColor	string	Основной цвет интерфейса веб-приложения (меню, выделенные кнопки). Цвет задается в формате HEX.
AdditionalColor	string	Дополнительный цвет интерфейса веб-приложения (выделенный элемент меню, выпадающий список под учетной записью). Цвет задается в формате HEX.
FontColor	string	Цвет шрифта заголовка, пунктов меню. Цвет задается в формате HEX.
Font	string	Тип шрифта.
FavIconFile	string	Полный путь до файла с favicon. Допустимое расширение для файла – ico.

Ниже приведён пример для настройки кастомизации Веб-интрефейса Пользователя:

```
Set-DSSFECustomization -AdditionalColor f37c20 -MainColor 02458d
Set-DSSFECustomization -FontColor f37c20 -Font Calibri
Set-DSSFECustomization -FavIconFile E:\Temp\favicon.ico -LogotypeFile
E:\Temp\logo.jpg -HelpFile E:\Temp\Help.html
Set-DSSFECustomization -Title "Сервер электронной подписи Тест" -Copyright
"Тест"
```

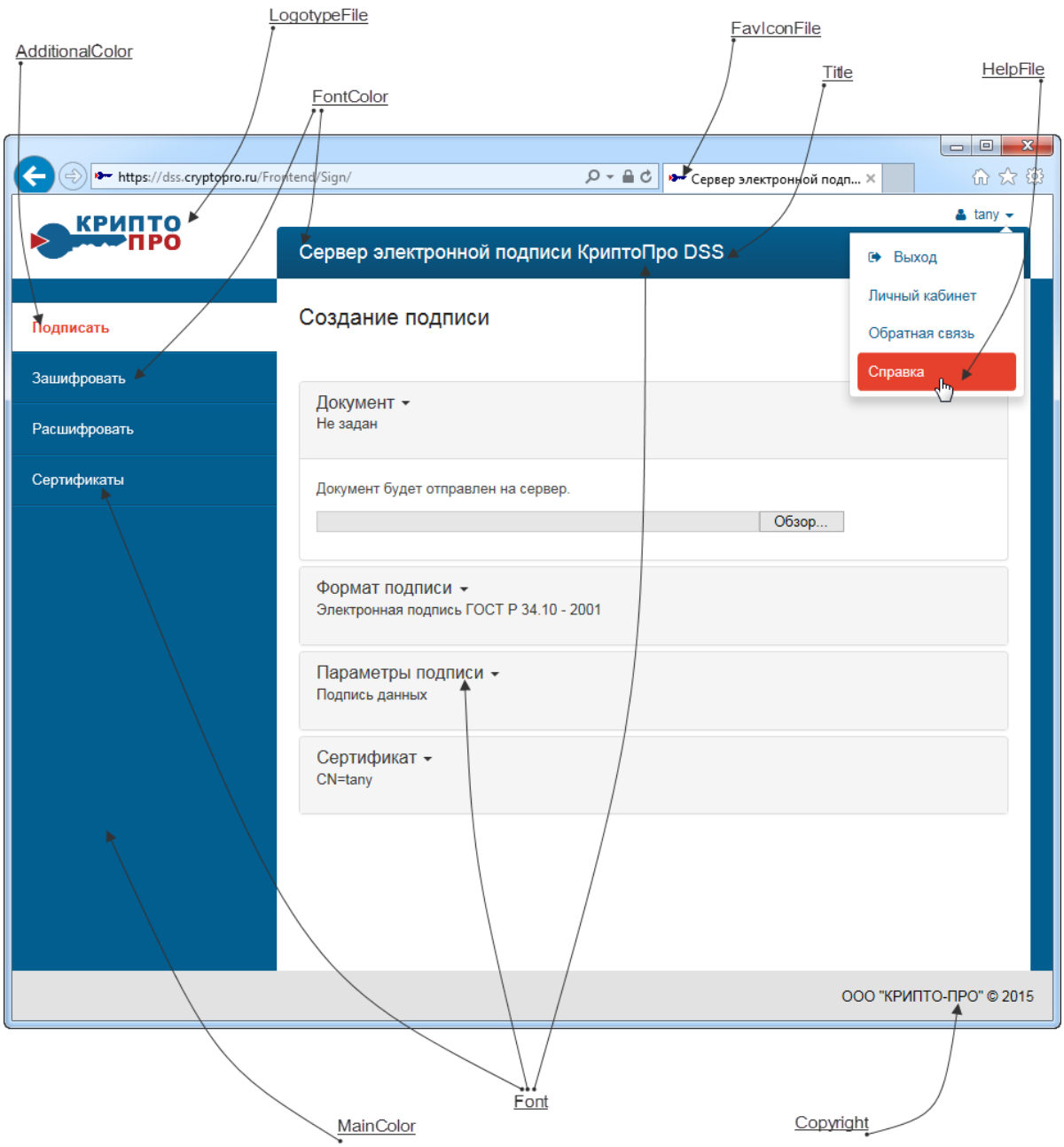

Рис. 31 – Настройки отображения Веб-интерфейса Пользователя

Командлет Reset-DssFECustomization

Данный командлет используется для восстановления настроек по умолчанию отображения экземпляра Веб-интерфейса Пользователя.

Синтаксис:

```
Reset-DssFECustomization [-DisplayName <string>]
```

4.7.4. Пример PowerShell-сценария для настройки компонента «Веб-интерфейс Пользователя»

Данный сценарий задаёт минимально необходимую настройку компонента.

```
# Добавление нового экземпляра Веб-интерфейса Пользователя
New-DssFEInstance -SiteName "Default Web Site" -DisplayName Frontend

# Добавление отпечатка сертификата Веб-интерфейса Пользователя
Set-DssFEProperties -ServiceCertificate <Отпечаток сертификата компонента>

# Настройка адресов Сервиса Подписи и Центра Идентификации
Set-DSSFEProperties -ServiceCertificate $feThumb -SignServerAddress
      "http://<hostname>/SignServer/SignServiceExR.svc/token/nosc" -StsAddress
      "https://<hostname>/STS/Active.svc/service"

# Добавление отпечатка компонента «Центр Идентификации»
Add-DssFEClaimsProviderTrust -IssuerName realsts -Thumbprint <Отпечаток
      сертификата Центра Идентификации>

# Добавление адреса ЦИ КриптоПро DSS в настройки WS-Federation
Set-DssFEWSFederationSettings -Issuer
      "https://<хост компонента STS>/STS/sts/issue/" -Realm
      https://<хост компонента Frontend>/Frontend/
```

Пример регистрации Веб-интерфейса Пользователя на Центре Идентификации.

```
# Регистрация Веб-интерфейса на Центре Идентификации

Add-DssRelyingPartyTrust -Name "Frontend" -MetadataUri
      https://<hostname>/Frontend/FederationMetadata/2007-
      06/FederationMetadata.xml
```

4.8. Настройка Сервиса Аудита

Компонент, осуществляющий аудит в СЭП «КриптоПро DSS», занимается сбором событий с других компонентов: с Сервера Подписи и Центра Идентификации. Сервис Аудита состоит из SOAP-сервиса, веб-интерфейса аудита и БД аудита. SOAP-сервис получает список записей аудита с других компонентов КриптоПро DSS (зависит от конкретных настроек сбора событий) и записывает эти события в БД. С помощью веб-интерфейса аудита Пользователь может просмотреть события аудита, а также отфильтровать их по дате и коду операции.

В состав компонента «Сервис аудита» (Рис. 32) входят:

- SOAP-сервис Аудита;
- Веб-интерфейс Сервиса Аудита;
- БД Сервиса Аудита.

Рис. 32 – Состав компонента «Сервис Аудита»

Для хранения информации о событиях используется база данных Microsoft SQL Server версии 2008 R2 или выше.

Принцип работы сервиса заключается в следующем:

1. Для записи сообщений в БД Сервиса Аудита Центр Идентификации и Сервис Подписи обращаются к службе записи сообщений аудита, входящему в состав SOAP-сервиса Сервиса Аудита. Адреса службы по умолчанию имеют вид:

- https://<hostname>/<AnalyticsAppName>/AuditWriter.svc,
- http://<hostname>/<AnalyticsAppName>/AuditWriter.svc

2. Сервис записи сообщений аудита осуществляет запись в БД всех событий аудита, которые поступают от компонентов СЭП КриптоПро DSS «Центр Идентификации» и «Сервис Подписи»;

3. Веб-интерфейс Сервиса Аудита позволяет осуществить просмотр/фильтрацию записей аудита, хранящихся в БД.

4. Сервис чтения аудита представляет собой SOAP-сервис. Веб-интерфейс Пользователя и Центр Идентификации используют данный сервис для отображения события аудита. Адреса службы по умолчанию имеют вид:

- http://<hostname>/<AnalyticsAppName>/analyticsservice.svc/token
- https://<hostname>/<AnalyticsAppName>/analyticsservice.svc/issuedtoken/transport

- https://<hostname>/<AnalyticsAppName>/analyticsservice.svc/issuedtoken/transport/nosc

Один из этих адресов должен быть настроен в командлетах **Set-DssFeProperties**, параметр **-AnalyticsServiceAddress** и в **Set-DssStsProperties**, параметр **–AnalyticsServiceAddress.**

4.8.1. Сервис Аудита

В данном разделе описывается настройка компонента КриптоПро DSS «Сервис Аудита», а также его регистрация и отображение на Веб-интерфейсе Пользователя. Настройка сбора событий при помощи Сервиса Аудита описывается в Разделе 4.8.2 Администрирование аудита.

4.8.1.1. Последовательность шагов по настройке экземпляра компонента «Сервис Аудита»

Данный раздел Руководства определяет последовательность и порядок действий по разворачиванию экземпляра Сервиса Аудита в режиме «с нуля».

Предварительные условия:

- Установленный SQL-Server;
- Установленная роль Сервер приложений (IIS);
- Настроенная привязка https на Сервере приложений (IIS);
- Выпущенный и установленный сервисный сертификат Сервиса Аудита (см. Раздел 6).

Базовая последовательность шагов по настройке (обязательные):

1. Выпуск и установка сервисного сертификата Сервиса Аудита, а также выдача прав на доступ к закрытому ключу (после выполнения п.2) (см. раздел 6).
2. Создание экземпляра приложения Сервиса Аудита (см. раздел 4.8.1.6.1).
3. Настройка параметров экземпляра Сервиса Аудита (см. раздел 4.8.1.6.1).
   На данном шаге Администратору необходимо:
   - Задать отпечаток сервисного сертификата.
   - Настроить отношения доверия с Центром Идентификации (см. раздел 4.8.1.6.2).
   - Зарегистрировать Сервис Аудита на Центре Идентификации (см. раздел 4.5.3.4).
   - Настроить параметры протокола аутентификации ws-federation passive requestor profile.

На данном шаге Администратор задаёт параметры для аутентификации на Веб-интерфейсе Пользователя при помощи командлета Set-DssAnalyticsWSFederationSettings.

- Настроить отображение пункта меню «Аудит» в Веб-интерфейсе Пользователя для:
  - Веб-интерфейса Пользователя (см. раздел 4.7.3.1);

- Центра Идентификации (см. раздел 4.5.7.2).

- Настроить аудит для:
  - Сервиса Подписи (см. раздел 4.8.2.1);
  - Центра Идентификации (см. раздел 4.8.2.2).

Дополнительные действия по настройке (опционально):

- Настроить журналирование компонента Сервис Аудита (см. раздел 7.3.3).
- Кастомизировать веб-приложение Сервиса Аудита (см. раздел 4.8.1.6.6).
- Настроить шаблоны печати Сервиса Аудита (см. раздел 4.8.1.6.5).

4.8.1.2. Объекты администрирования

На Рис. 33 приведена схема объектов, доступных для администрирования на Сервисе Аудита.

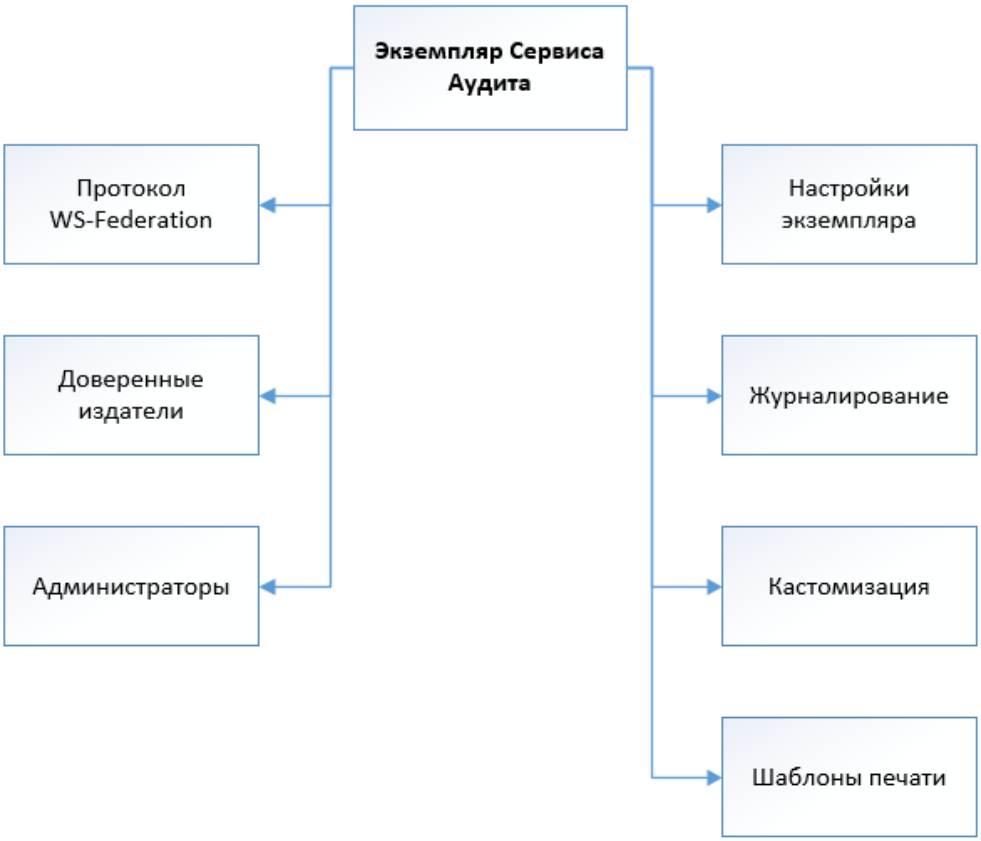

Рис. 33 – Объекты администрирования Сервиса Аудита

Таблица 99. Список командлетов компонента Сервис Аудита

Объект администрирования	Командлет	Описание
Настройки экземпляра	New-DssAnalyticsServiceInstance	Объект отвечает за управление экземплярами Сервиса Аудита.
	Remove-DssAnalyticsServiceInstance	
	Update-DssAnalyticsServiceInstance	
	Get-DssAnalyticsServiceInstance	
	Set-DssAnalyticsServiceProperties	
	Get-DssAnalyticsServiceProperties	
	Get-DssAnalyticsRegistryProperties	
	Set- DssAnalyticsRegistryProperties	
Доверенные издатели	Add-DssAnalyticsClaimsProviderTrust	Объект отвечает за настройку отношений доверия с Центром Идентификации.
	Get-DssAnalyticsClaimsProviderTrust	
	Set-DssAnalyticsClaimsProviderTrust	
	Remove-DssAnalyticsClaimsProviderTrust	
Протокол WS-Federation	Set-DssAnalyticsWSFederationSettings	Объект отвечает за настройку протокола WS-Federation с ЦИ КриптоПро DSS.
	Get-DssAnalyticsWSFederationSettings	
Шаблоны печати	Get-DssAnalyticsConverterPlugin	Объект позволяет зарегистрировать плагины, формирующие печатную форму списка событий аудита.
	Add-DssAnalyticsConverterPlugin	
	Remove-DssAnalyticsConverterPlugin	
Журналирование	Enable-DssAnalyticsServiceTracing	Объект отвечает за журналирование сетевых взаимодействий (см. раздел 7.3).
	Disable-DssAnalyticsServiceTracing	
	Get-DssAnalyticsServiceTracing	
	Set-DssAnalyticsServiceTracing	
Кастомизация	Get-DssAnalyticsCustomization	

Объект администрирования	Командлет	Описание
	Set-DssAnalyticsCustomization	Объект отвечает за настройку отображения Сервиса Аудита.
	Reset-DssAnalyticsCustomization	
Плагины отчетов	Add-DssAnalyticsReportPlugin	Объект позволяет зарегистрировать плагины, формирующие преднастроенный отчет о событиях аудита КриптоПро DSS.
	Get-DssAnalyticsReportPlugin	
	Remove-DssAnalyticsReportPlugin	
Администраторы	Add-DssAnalyticsServiceAdministrator Get-DssAnalyticsServiceAdministrator Remove-DssAnalyticsServiceAdministrator	Объект отвечает за управление учетными записями Администраторов, имеющих доступ к БД myDSS Internal Server. (См. раздел 4.2.2.1).

4.8.1.3. Отображение веб-интерфейса Сервиса Аудита для различных ролей

В КриптоПро DSS только три роли могут видеть события аудита:

- Пользователь;
- Оператор;
- Оператор аудита.

От каждой из перечисленных ролей зависит отображение веб-интерфейса Сервиса Аудита и самих событий аудита.

4.8.1.4. Плагины формирования отчетов

В Сервисе Аудита КриптоПро DSS доступна расширенная настройка различных отчетов. Эту возможность реализуют плагины формирования отчетов. Плагины настраиваются при помощи командлетов Add-DssAnalyticsReportPlugin, Get-DssAnalyticsReportPlugin, Remove-DssAnalyticsReportPlugin. В зависимости от типов отчетов, представленных в Таблица 100, к плагину нужно подключить соответствующий класс отчета.

Все предопределенные типы отчетов содержатся в сборке CryptoPro.DSS.AnalyticsService.ReportPlugins.dll. Имя сборки указывается при использовании параметра **–Assembly** (см. 4.8.1.6.7).

Таблица 100. Типы отчетов Сервиса Аудита

Тип отчета	Класс отчета	Описание
Отчеты о сертификатах	CryptoPro.DSS.AnalyticsService.ReportPlugins.CertificateReports.CreatedCertificateReport	Отчет о созданных сертификатах

Тип отчета	Класс отчета	Описание
	CryptoPro.DSS.AnalyticsService.ReportPlugins.CertificateReports.RevokedCertificateReport	Отчет об отозванных сертификатах
	CryptoPro.DSS.AnalyticsService.ReportPlugins.CertificateReports.HeldCertificateReport	Отчет о приостановленных сертификатах
	CryptoPro.DSS.AnalyticsService.ReportPlugins.CertificateReports.UnheldCertificateReport	Отчет о сертификатах с возобновленным сроком действия
Отчеты об ЭП	CryptoPro.DSS.AnalyticsService.ReportPlugins.SignatureReports.CreatedSignaturesReport	Отчет о количестве ЭП
Отчеты о Пользователях	CryptoPro.DSS.AnalyticsService.ReportPlugins.UserReports.CreatedUsersReport	Отчет о количестве созданных пользователей
Отчет о пользователях MyDSS	CryptoPro.DSS.AnalyticsService.ReportPlugins.MyDss.MyDssUserReport	Отчет о количестве пользователей MyDSS в рамках заданного периода
Отчет о пользователях Cloud CSP	CryptoPro.DSS.AnalyticsService.ReportPlugins.CloudCspReport.CloudCspReport	Отчет о количестве пользователей Cloud CSP в рамках заданного периода

При администрировании плагинов формирования отчетности (см. раздел 4.8.1.6.7) необходимо указать параметры настраиваемого плагина. Это можно сделать с помощью параметра **parameters.** Этот параметр имеет тип **hashtable.** В PowerShell для задания параметра типа **Hashtable** можно применить следующую конструкцию:

```
@{paramName1=paramValue1; paramName2=paramValue2;…;paramNameN=paramValueN}
```

где **paramName$_i$**, **paramValue$_i$** – название и значение параметра соответственно. Каждый параметр и его значение помещаются в двойные кавычки.

В Таблица 101 указаны параметры плагинов формирования отчета, которые настраиваются при добавлении плагинов разных типов.

Таблица 101. Параметры плагинов формирования отчетов

Параметр	Тип	Описание
		Отчеты о сертификатах
AuditConnectionString	string	Строка подключения к БД Сервиса Аудита.
InstanceName	string	Имя экземпляра Сервиса Подписи, по данным которого строится отчет.
Xslt	string	Путь к файлу с XSLT-преобразованием.
ReportName	string	Отображаемое имя отчета.
Delimiter	string	Символ разделения элементов при экспорте отчета в CSV-формат.

Параметр	Тип	Описание
Отчеты об ЭП		
AuditConnectionString	string	Строка подключения к БД Сервиса Аудита.
InstanceName	string	Имя экземпляра Сервиса Подписи, по данным которого строится отчет.
Xslt	string	Путь к файлу с XSLT-преобразованием.
ReportName	string	Отображаемое имя отчета.
Delimiter	string	Символ разделения элементов при экспорте отчета в CSV-формат.
Отчеты о Пользователях		
StsConnectionString	string	Строка подключения к БД Центра Идентификации.
RealmName	string	Имя ЦИ, которому принадлежат Пользователи.
RdnList	string	Спислк компонентов имени Пользователя, которые попадут в отчет.
Xslt	string	Путь к файлу с XSLT-преобразованием.
ReportName	string	Отображаемое имя отчета.
Delimiter	string	Символ разделения элементов при экспорте отчета в CSV-формат.
Отчет о пользователях MyDSS		
AuditConnectionString	string	Строка подключения к БД Сервиса Аудита.
InstanceName	string	Имя экземпляра ЦИ, по данным которого строится отчет.
Xslt	string	Путь к файлу с XSLT-преобразованием.
ReportName	string	Отображаемое имя отчета.
Delimiter	string	Символ разделения элементов при экспорте отчета в CSV-формат.
Отчет о пользователях Cloud CSP		
AuditConnectionString	string	Строка подключения к БД Сервиса Аудита.
InstanceName	string	Имя экземпляра ЦИ, по данным которого строится отчет.
Xslt	string	Путь к файлу с XSLT-преобразованием.

Параметр	Тип	Описание
ReportName	string	Отображаемое имя отчета.
Delimiter	string	Символ разделения элементов при экспорте отчета в CSV-формат.

При настройке отчета о Пользователях необходимо дать права учетной записи, под которой работает Сервис Аудита (по умолчанию – IIS AppPool\CryptoProDSS-1-AnalyticsService), на доступ к БД ЦИ (по умолчанию - IdentityServiceDB). Для этого необходимо включить учетную запись Сервиса Аудита в роль IdentityServiceInstance в БД ЦИ.

Примеры добавления плагинов отчетов на Сервисе Аудита:

Плагин отчета по количеству созданных ЭП:

```
Add-DssAnalyticsReportPlugin -FileExtension csr -Assembly CryptoPro.DSS.AnalyticsService.ReportPlugins.dll -Classname CryptoPro.DSS.AnalyticsService.ReportPlugins.SignatureReports.CreatedSignaturesReport -Parameters @{"AuditConnectionString" = "Data Source=<Имя SQL-сервера>;Initial Catalog=AnalyticsServiceDB;Integrated Security=True; Persist Security Info=False"; "InstanceName"="SignServer"; "ReportName"="Количество созданных подписей";}
```

Плагин отчета по количеству созданных Пользователей:

```
Add-DssAnalyticsReportPlugin -FileExtension cur -Assembly CryptoPro.DSS.AnalyticsService.ReportPlugins.dll -Classname CryptoPro.DSS.AnalyticsService.ReportPlugins.UserReports.CreatedUsersReport -Parameters @{"StsConnectionString" = "Data Source==<Имя SQL-сервера>;Initial Catalog=IdentityServiceDB;Integrated Security=True;Persist Security Info=False"; "ReportName"="Количество созданных пользователей"; "RealmName"="realsts";"RdnList"="CN"}
```

Плагин отчета по количеству пользователей MyDSS:

```
Add-DssAnalyticsReportPlugin -FileExtension mur -Assembly CryptoPro.DSS.AnalyticsService.ReportPlugins.dll -Classname CryptoPro.DSS.AnalyticsService.ReportPlugins.MyDss.MyDssUserReport -Parameters @{"AuditConnectionString" = "Data Source=<Имя SQL-сервера>;Initial Catalog=AnalyticsServiceDB;Integrated Security=True; Persist Security Info=False"; "InstanceName"="1/STS"; "ReportName"="Отчет о пользователях MyDss";}
```

Плагин отчета по количеству пользователей CloudCsp:

```
Add-DssAnalyticsReportPlugin -FileExtension clur -Assembly CryptoPro.DSS.AnalyticsService.ReportPlugins.dll -Classname CryptoPro.DSS.AnalyticsService.ReportPlugins.
CryptoPro.DSS.AnalyticsService.ReportPlugins.CloudCspReport.CloudCspReport -Parameters @{"AuditConnectionString" = "Data Source=<Имя SQL-сервера>;Initial Catalog=AnalyticsServiceDB;Integrated Security=True; Persist Security Info=False"; "InstanceName"="1/STS"; "ReportName"="Отчет о пользователях Cloud CSP";}
```

4.8.1.5. Контроль целостности записей аудита

Сервис Аудита КриптоПро DSS позволяет обеспечивать контроль целостности записей аудита, хранящихся в его БД. Это достигается путем создания подписи записей аудита при помощи криптопровайдера, зарегистрированного в рамках Сервиса Аудита. Регистрация криптопровайдеров на Сервисе Аудита осуществляется при помощи командлетов Add-DssAnalyticsCryptoProvider, Remove-DssAnalyticsCryptoProvider, Get-DssAnalyticsCryptoProvider, Set-DssAnalyticsCryptoProvider и т.д. (см. п. 4.8.1.6.3.).

Для включения функций контроля целостности записей аудита на Сервисе Аудита необходимо:

- Зарегистрировать криптопровайдер подписи записей аудита при помощи командлета **Add-DssAnalyticsCryptoProvider**;
- Настроить при помощи командлета **Set-DssAnalyticsServiceProperties** следующие параметры Сервиса Аудита: SignatureTimerInterval и SignatureBlockLength (см. п. 4.8.1.6.1.).

После этого Сервис Аудита начнет формирование блоков записей аудита заданного размера, которые в последствии будут подписаны при помощи криптографического провайдера, зарегистрированного на Сервисе. Вся информация о блоке и подписи затем помещается в БД Сервиса Аудита и может быть просмотрена позднее.

4.8.1.6. Администрирование компонента «Сервис Аудита»

Настройка компонента «Сервис Аудита» осуществляется с помощью Windows PowerShell. Команды администрирования включены в модуль **CryptoPro.DSS.PowerShell.AnalyticsService.**

4.8.1.6.1. Настройки экземпляра

Командлет New-DssAnalyticsServiceInstance

Создает новый экземпляр компонента «Сервис Аудита».

К основным параметра относятся:

- название веб-сайта IIS, на котором следует развернуть веб-приложение Сервиса Аудита;
- отображаемое имя экземпляра;
- адрес SQL-сервера, на котором следует развернуть БД Сервиса Аудита.

Синтаксис:

```
New-DssAnalyticsServiceInstance -SiteName <string> -DisplayName <string>
-SqlServerName <string> [-ApplicationName <string>] [-DbName <string>]
```

Таблица 102. Параметры командлета New-DssAnalyticsServiceInstance

Параметр	Тип	Описание
SiteName	string	Название веб-сайта, на котором следует развернуть веб-приложение Сервиса Аудита.

Параметр	Тип	Описание
ApplicationName	string	Название веб-приложения Сервиса Аудита Если параметр не задан, используется значение Analytics.
SQLServerName	string	Адрес экземпляра SQL-сервера, на котором следует развернуть экземпляр БД Сервиса Аудита Формат: <SQL-сервер host>\<имя экземпляра>
DBname	string	Имя базы данных Сервиса Аудита. По умолчанию DSSAudit.
DisplayName	String	Отображаемое имя экземпляра компонента Сервиса Аудита.
ConnectionInfo	SqlConnectionInfo	Расширенные данные для подключения к SQL-серверу (см. раздел 43.10).

Командлет Remove-DssAnalyticsServiceInstance

Удаляет экземпляр компонента Сервиса Аудита.

К основным параметрам относятся:

- флаг, определяющий, требуется ли удалять БД Сервиса Аудита.

Синтаксис:

```
Remove-DssAnalyticsServiceInstance [-DisplayName <string>] -DeleteDB <bool>
```

Таблица 103. Параметры командлета Remove-DssAnalyticsServiceInstance

Параметр	Тип	Описание
DisplayName	String	Отображаемое имя экземпляра компонента «Сервис Аудита». Если значение не указано, будет использовано имя экземпляра, назначенное по умолчанию.
DeleteDB	bool	Флаг, определяющий, требуется ли удалять БД Сервиса Аудита.
ConnectionInfo	SqlConnectionInfo	Расширенные данные для подключения к SQL-серверу (см. раздел 43.10).

Командлет Update-DssAnalyticsServiceInstance

Обновляет экземпляр компонента Сервиса Аудита после установки новых библиотек.

Синтаксис:

```
Update-DssAnalyticsServiceInstance [-DisplayName <string>]
```

Командлет Get-DssAnalyticsServiceInstance

Выводит на консоль список экземпляров Сервиса Аудита.

Синтаксис:

```
Get-DssAnalyticsServiceInstance
```

Командлет Set-DssAnalyticsServiceProperties

Командлет **Set-DssAnalyticsServiceProperties** позволяет задать основные параметры компонента «Сервис Аудита». К основным параметрам относят:

- отпечаток сертификата ключа подписи электронного идентификатора.

Синтаксис:

```
Set-DssAnalyticsServiceProperties -ServiceCertificate <string> [-DisplayName
<string>]
```

Таблица 104. Параметры командлета Set-DssAnalyticsServiceProperties

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента «Сервис Аудита». Если значение не указано, будет использовано имя экземпляра, назначенное по умолчанию.
ServiceCertificate	string	Отпечаток сертификата ключа подписи маркера безопасности.
AnalyticsServiceUri	string	Веб-адрес службы сервиса аналитики
ServiceIdentifier	string	Идентификатор сервиса в urn-формате.
SignatureTimerInterval	string	Интервал между операциями подписи сообщенией аудита
SignatureBlockLength	string	Размер блока, обрабатываемого за одну операцию подписи сообщений аудита

Командлет Get-DssAnalyticsServiceProperties

Командлет **Get-DssAnalyticsServiceProperties** позволяет вывести на консоль значение основных параметров экземпляра компонента Сервис Аудита.

Синтаксис:

```
Get-DssAnalyticsServiceProperties [-DisplayName <string>]
```

Командлет Set-DSSAnalyticsRegistryProperties

Используется для изменения строки подключения к базе данных Сервиса Аудита.

Синтаксис:

```
Set-DSSAnalyticsRegistryProperties [-DisplayName <string>] [-DBConnection
<string>]
```

Таблица 105. Параметры командлета Set-DSSAnalyticsRegistryProperties

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Аудита. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
DBConnection	string	Строка подключения к базе данных Сервиса Подписи.

Командлет Get-DSSAnalyticsRegistryProperties

Используется для получения информации о строке подключения к базе данных Сервиса Аудита.

Синтаксис:

```
Get-DSSAnalyticsRegistryProperties [-DisplayName <string>] [-DBConnection
<string>]
```

4.8.1.6.2. Доверенные издатели

Командлет Add-DssAnalyticsClaimsProviderTrust

Добавляет отпечаток сертификата подписи маркеров безопасности в список доверенных издателей маркеров безопасности.

Синтаксис:

```
Add-DssAnalyticsClaimsProviderTrust [-DisplayName <string>] -IssuerName
<string> -Thumbprint <string>
```

Таблица 106. Параметры командлета Add-DssAnalyticsClaimsProviderTrust

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра Сервиса Аудита.
IssuerName	string	Имя доверенного издателя.
Thumbprint	string	Сертификата доверенного издателя.

Командлет Get-DssAnalyticsClaimsProviderTrust

Используется для вывода на консоль зарегистрированных доверенных издателей маркеров безопасности. Отображается строковый идентификатор издателя и отпечаток сертификата открытого ключа.

Синтаксис:

```
Get-DssAnalyticsClaimsProviderTrust [-DisplayName <string>]
```

Командлет Set-DssAnalyticsClaimsProviderTrust

Используется для изменения отпечатка сертификата доверенного издателя маркеров безопасности.

Синтаксис:

```
Set-DssAnalyticsClaimsProviderTrust [-DisplayName <string>] -IssuerName
<string> -NewThumbprint <string>
```

Таблица 107. Параметры командлета Set-DssAnalyticsClaimsProviderTrust

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Аудита. Если значение не указано, будет использовано имя экземпляра, назначенное по умолчанию.
IssuerName	string	Уникальное имя издателя маркеров безопасности.
NewThumbprint	string	Новый отпечаток сертификата подписи маркеров безопасности.

Командлет Remove-DssAnalyticsClaimsProviderTrust

Используется для удаления доверенного издателя маркеров безопасности.

Синтаксис:

```
Remove-DssAnalyticsClaimsProviderTrust [-DisplayName <string>] -IssuerName
<string>
```

Таблица 108. Параметры командлета Remove-DssAnalyticsClaimsProviderTrust

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Аудита. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
IssuerName	string	Уникальное имя издателя маркеров безопасности.

4.8.1.6.3. Управление криптопровайдерами

Командлет Get-DssAnalyticsCryptoProvider

Используется для вывода на консоль информации о зарегистрированных провайдерах.

Синтаксис:

```
Get-DssAnalyticsCryptoProvider [-DisplayName <string>] [-Validate]
```

Таблица 109. Параметры командлета Get-DssAnalyticsCryptoProvider

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Аудита. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Validate	SwitchParameter	Флаг, определяющий, что требуется проверка работоспособности криптопровайдеров с Мастер-ключом.

Командлет Get-DssAnalyticsCryptoProviderType

Выводит на консоль список зарегистрированных типов криптопровайдеров.

Синтаксис:

```
Get-DssAnalyticsCryptoProviderType [-DisplayName <string>]
```

Командлет Add-DssAnalyticsCryptoProvider

Используется для регистрации нового криптопровайдера на Сервисе Подписи.

Синтаксис:

```
Add-DssAnalyticsCryptoProvider [-DisplayName <string>] -ProviderName <string>
-ProviderType <int> -TypeId <string> [-Order <int] [-SetMasterKeyLife [-
MasterKeyLife <int>]] [-SetUsersKeysLife [-UsersKeysLife <int>]] [-
MasterKeyName <string>]
```

Таблица 110. Параметры командлета Add-DssAnalyticsCryptoProvider

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Аудита. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Descrition	string	Описание криптопровайдера для отображения в Веб-интерфейс Пользователя.
TypeId	String Возможные значения: AuditIntegrity	Идентификатор типа криптопровайдера.
Order	int	Отвечает за порядок следования на Веб-интерфейсе Пользователя зарегистрированных криптопровайдеров. Чем выше номер, тем выше в списке криптопровайдер. По умолчанию параметр равен 0.
ProviderType	int	Тип провайдера, зарегистрированного в ОС (функции поддерживаются только для провайдеров типа 80 и 81).
ProviderName	string	Имя провайдера, зарегистрированное в системе.
SetMasterKeyLifetime	SwitchParameter	Установить срок действия Мастер-ключа в случае, если создается провайдер с Мастер-ключом.
MasterKeyLifetime	int	Срок действия Мастер-ключа с момента создания в месяцах. По умолчанию срок действия Мастер-ключа - 36 месяцев.
SetUsersKeysLifetime	SwitchParameter	Установить срок действия пользовательских ключей.
UsersKeysLifetime	int	Срок действия пользовательских ключей, созданных на данном провайдере, в месяцах. По умолчанию срок действия пользовательского ключа 15 месяцев.
MasterKeyName	string	Имя контейнера с Мастер-ключом, если создается провайдер с уже существующим Мастер-ключом.

Зарегистрированное имя провайдера в системе предопределено заранее. Его можно увидеть в документации поставщика криптопровайдера. Для продуктов КриптоПро:

- КриптоПро HSM: **Crypto-Pro GOST R 34.10-2012 HSM Svc CSP**
- КриптоПро CSP (только для тестирования КриптоПро DSS): **Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider**

Командлет Remove-DssAnalyticsCryptoProvider

Используется для удаления криптопровайдера на Сервисе Аудита.

Синтаксис:

```
Remove-DssAnalyticsCryptoProvider [-DisplayName <string>] -ID <guid>
```

Таблица 111. Параметры командлета Remove-DssAnalyticstoProvider

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Аудита. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
ID	guid	Идентификатор криптопровайдера.

Командлет Enable-DssAnalyticsCryptoProvider

Используется для включения криптопровайдера на Сервисе Аудита, ранее переведённого в состояние отключен.

Синтаксис:

```
Enable-DssAnalyticsCryptoProvider [-DisplayName <string>] -ID <int>
```

Таблица 112. Параметры командлета Enable-DssAnalyticsCryptoProvider

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Аудита. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
ID	guid	Идентификатор криптопровайдера.

Командлет Disable-DssAnalyticsCryptoProvider

Используется для отключения криптопровайдера на Сервисе Аудита.

Синтаксис:

```
Disable-DssCryptoProvider [-DisplayName <string>] -ID <guid>
```

Таблица 113. Параметры командлета Disable-DssAnalyticsCryptoProvider

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Аудита. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
ID	guid	Идентификатор криптопровайдера.

Командлет Copy-DssAnalyticsCryptoProvider

Используется для создания нового криптопровайдера, принадлежащего заданной группе криптопровайдеров. Мастер-ключ нового криптопровайдера совпадает с Мастер-ключами остальных криптопровайдеров группы.

Синтаксис:

```
Copy-DssAnalyticsCryptoProvider [-DisplayName <string>] -GroupID <int> -
NewProvName <string>
```

Таблица 114. Параметры командлета Copy-DssAnalyticsCryptoProvider

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Аудита. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
GroupID	Int	Идентификатор группы, которой принадлежит копируемый криптопровайдер.
NewProvName	string	Имя нового криптопровайдера.

Командлет Set-DssAnalyticsCryptoProvider

Используется для изменения параметров криптопровайдера, зарегистрированного на Сервисе Аудита

Синтаксис:

```
Set-DssCryptoProvider -DisplayName <string> [-MasterKeyName <string>][-Order
<int] [-Description <string>] -ID <guid>
```

Таблица 115. Параметры командлета Set-DssAnalyticsCryptoProvider

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Аудита. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Order	int	Отвечает за порядок следования на Веб-интерфейсе Пользователя зарегистрированных криптопровайдеров. Чем выше номер, тем выше в списке криптопровайдер. По умолчанию параметр равен 0.
Description	string	Описание криптопровайдера для отображения в Веб-интерфейс Пользователя.

Параметр	Тип	Описание
MasterKeyName	string	Имя контейнера с Мастер-ключом, если создается провайдер с уже существующим Мастер-ключом.
ID	guid	Идентификатор криптопровайдера.

Командлет Test-DssAnalyticsCryptoProvider

Используется для проверки доступности криптопровайдера.

Синтаксис:

```
Test-DssAnalyticsCryptoProvider [-DisplayName <string>] -ID <guid>
```

Таблица 116. Параметры командлета Test-DssAnalyticsCryptoProvider

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
ID	guid	Идентификатор криптопровайдера.

4.8.1.6.4. Протокол WS-Federation

Командлет Set-DssAnalyticsWSFederationSettings

Данный командлет используется для изменения настроек WS-Federation. К ним относятся:

- адрес Центра Идентификации КриптоПро DSS;
- адрес Веб-интерфейса Сервиса Аудита КриптоПро DSS;
- адрес доверенного Центра Идентификации в домене Пользователя.

Синтаксис:

```
Set-DssAnalyticsWSFederationSettings [-DisplayName <string>] [-Issuer
<string>] [-Realm <string>] [-HomeRealm <string>] [RequireHttps <bool>]
```

Таблица 117. Параметры командлета Set-DssAnalyticsWSFederationSettings

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Аудита. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Issuer	string	URL-адрес Центра Идентификации КриптоПро DSS. По умолчанию имеет значения: http://<host_name>/sts/sts/issue/
Realm	string	URL-адрес Веб-интерфейса Сервиса Аудита КриптоПро DSS. По умолчанию имеет значения: http://<host_name>//AnalyticsService/
HomeRealm	string	URL-адрес Центра Идентификации. По умолчанию не заполняется, зарезервирован для дальнейшего использования.

Параметр	Тип	Описание
RequireHttps	bool	Требовать защищённого соединения.

Командлет Get-DssAnalyticsWSFederationSettings

Данный командлет используется для вывода на консоль настроек WS-Federation Сервиса Аудита.

Синтаксис:

```
Get-DssAnalyticsWSFederationSettings [-DisplayName <string>]
```

4.8.1.6.5. Шаблоны печати

Командлет Get-DssAnalyticsConverterPlugin

Данный командлет используется для вывода на консоль всех зарегистрированных плагинов для преобразования документов.

Синтаксис:

```
Get-DssAnalyticsConverterPlugin [-DisplayName <string>]
```

Командлет Add-DssAnalyticsConverterPlugin

Регистрация нового плагина для преобразования документов.

Синтаксис:

```
Add-DssAnalyticsConverterPlugin [-DisplayName <string>] -FileExtension
<string> -Assembly <string> [-Classname <string>] [-Priority <int>] [-
Parameters <Hashtable>]
```

Таблица 118. Параметры командлета Add-DssAnalitycsConverterPlugin

Параметр	Тип	Описание
FileExtension	string	Расширение документа.
Assembly	string	Полный путь до файла сборки плагина. В качестве значения данного параметра можно указать только имя dll файла сборки, в этом случае полный путь будет отсчитываться относительно директории: <Путь установки>\Plugins\Converters\<Тип плагина>.
Classname	string	Имя класса, реализующего интерфейс IDSSDocumentConverter.
Priority	int	Приоритет плагина относительно остальных зарегистрированных для данного расширения плагинов.
Parameters	Hashtable	Дополнительные параметры плагина.

В PowerShell для задания параметра типа **Hashtable** можно применить следующую конструкцию:

```
@{paramName1=paramValue1; paramName2=paramValue2;…;paramNameN=paramValueN}
```

где **paramNamei**, **paramValuei** – название и значение параметра соответственно.

Командлет Remove-DssAnalyticsConverterPlugin

Удаление зарегистрированного плагина для преобразования.

Синтаксис:

```
Remove-DssAnalyticsConverterPlugin [-DisplayName <string>] -FileExtension
<string> -Assembly <string> -Classname <string>
```

Таблица 119. Параметры командлета Remove-DssFEConverterPlugin

Параметр	Тип	Описание
FileExtension	string	Расширение документа.
Assembly	string	Полный путь до файла сборки плагина. В качестве значения данного параметра можно указать только имя dll-файла сборки, в этом случае полный путь будет отсчитываться относительно директории: <Путь установки>\Plugins\Converters\<Тип плагина>.
Classname	string	Имя класса, реализующего интерфейс IDSSDocumentConverter.

4.8.1.6.6. Кастомизация

Командлет Get-DssAnalyticsCustomization

Данный командлет используется для вывода на консоль всех настроек отображения экземпляра Сервиса Аудита.

Синтаксис:

```
Get-DssAnalyticsCustomization [-DisplayName <string>]
```

Командлет Set-DssAnalyticsCustomization

Данный командлет используется для изменения настроек отображения экземпляра Сервиса Аудита.

Синтаксис:

```
Set-DssAnalyticsCustomization [-DisplayName <string>] [-Title <string>] [-
Copyright <string>] [-LogotypeFile <string>] [-HelpFile <string>] [-MainColor
<string>] [-AdditionalColor <string>] [-FontColor <string>] [-Font <string>]
[-FavIconFile <string>]
```

Таблица 120. Параметры командлета Set-DssFECustomization

Параметр	Тип	Описание
Title	string	Заголовок веб-приложения Сервиса Аудита.

Параметр	Тип	Описание
Copyright	string	Копирайт.
LogotypeFile	string	Полный путь до файла с логотипом. Размер логотипа – максимум 55 pix высоту и 220 pix в ширину.
HelpFile	string	Полный путь до файла со справкой. Файл справки представляет собой HTML-документ.
MainColor	string	Основной цвет интерфейса веб-приложения Сервиса Аудита (меню, выделенные кнопки). Цвет задается в формате HEX.
AdditionalColor	string	Дополнительный цвет интерфейса веб-приложения Сервиса Аудита (выделенный элемент меню, выпадающий список под учетной записью). Цвет задается в формате HEX.
FontColor	string	Цвет шрифта заголовка, пунктов меню. Цвет задается в формате HEX.
Font	string	Тип шрифта.
FavIconFile	string	Полный путь до файла с favicon. Допустимое расширение для файла – ico.

Командлет Reset-DssAnalyticsCustomization

Данный командлет используется для восстановления настроек по умолчанию отображения экземпляра Веб-интерфейса Сервиса Аудита.

Синтаксис:

```
Reset-DssAnalyticsCustomization [-DisplayName <string>]
```

4.8.1.6.7. Плагины формирования отчетов

Командлет Add-DssAnalyticsReportPlugin

Позволяет добавить плагин отчета о событиях аудита.

Синтаксис:

```
Add-DssAnalyticsReportPlugin [-DisplayName <string>] -FileExtension <string>
-Assembly <string> [-Classname <string>] [-Priority <int>] [-Parameters
<Hashtable>]
```

Таблица 121. Параметры командлета Add-DssAnalitycsReportPlugin

Параметр	Тип	Описание
FileExtension	string	Расширение документа. Допускается произвольное значение, не содержащее пробелов и спецсимволов.
Assembly	string	Полный путь до файла сборки плагина. В качестве значения данного параметра можно указать только имя dll файла сборки, в этом случае полный путь будет отсчитываться относительно директории: <Путь установки>\Plugins\Converters\<Тип плагина>.

Параметр	Тип	Описание
Classname	string	Имя класса, реализующего интерфейс IDSSDocumentConverter.
Priority	int	Приоритет плагина относительно остальных зарегистрированных для данного расширения плагинов.
Parameters	Hashtable	Дополнительные параметры плагина (подробно описаны в разделе 4.8.1.4).
DisplayName	string	Имя экземпляра Сервиса Аудита. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.

Командлет Get-DssAnalyticsReportPlugin

Данный командлет используется для вывода на консоль всех зарегистрированных плагинов для формирования отчетов о событиях аудита.

Синтаксис:

```
Get-DssAnalyticsReportPlugin [-DisplayName <string>]
```

Командлет Remove-DssAnalyticsReportPlugin

Удаление зарегистрированного плагина для формирования отчетов о событиях аудита.

Синтаксис:

```
Remove-DssAnalyticsReportPlugin [-DisplayName <string>] -FileExtension
<string> -Assembly <string> -Classname <string>
```

Таблица 122. Параметры командлета Remove-DssAnalitycsReportPlugin

Параметр	Тип	Описание
FileExtension	string	Расширение документа.
DisplayName	string	Имя экземпляра Сервиса Аудита. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Assembly	string	Полный путь до файла сборки плагина. В качестве значения данного параметра можно указать только имя dll-файла сборки, в этом случае полный путь будет отсчитываться относительно директории: <Путь установки>\Plugins\Converters\<Тип плагина>.
Classname	string	Имя класса, реализующего интерфейс IDSSDocumentConverter.

4.8.1.7. Пример PowerShell-сценария для настройки компонента «Сервис Аудита».

Данный сценарий задаёт минимально необходимую настройку компонента.

```
# Добавление нового экземпляра Сервиса Аудита
New-DssAnalyticsServiceInstance -SiteName "Default Web Site" -DisplayName
Analytics -SqlServerName <hostname>\SQL

# Добавление отпечатка сертификата службы
Set-DssAnalyticsServiceProperties -ServiceCertificate <Отпечаток сертификата
компонента>

# Добавление отпечатка компонента «Центр Идентификации»
Add-DssAnalyticsServiceClaimsProviderTrust -IssuerName realsts -Thumbprint
<Отпечаток сертификата Центра Идентификации>

# Добавление адреса ЦИ КриптоПро DSS в настройки WS-Federation
Set-DssAnalyticsWSFederationSettings -Issuer "http://<хост компонента
STS>/STS/sts/issue/" -Realm http://<hostname>/Analytics/

# Регистрация Веб-интерфейса на Центре Идентификации
Set-DssStsProperties -AnalyticsServiceAddress
http://<hostname>/<analyticsAppName>/AnalyticsService.svc

# Регистрация Веб-интерфейса на Веб-интерфейсе Пользователя
Set-DssFEProperties -AnalyticsServiceAddress
http://HostName/AnalyticsService/AnalyticsService.svc

# Получаем сертификат Сервиса Аудита.
Add-DssRelyingPartyTrust -Name "Analytics" -MetadataUri
http://hostname/AnalyticsService/federationmetadata/2007-
06/federationmetadata.xml
```

4.8.2. Администрирование аудита

Для администрирования аудита используются командлеты New-DssSignServerAudit и New-DssStsAudit в зависимости от компонента, для которого разворачивался Сервис Аудита. Оба командлета имеют одинаковый набор параметров. Ниже приведено описание командлетов, позволяющих настроить сбор информации о событиях с Сервиса Подписи и Центра Идентификации. Сбор и отправка событий осуществляются идентично работе системы оповещения (см. Раздел 4.9.5), однако не требуют настройки в несколько этапов, поскольку взаимодействие осуществляется внутри КриптоПро DSS.

4.8.2.1. Командлет New-DSSSignServerAudit

Командлет добавления модуля оповещения типа Аудит на Сервис Подписи. Описание параметров команды приведено в Таблица 123.

Синтаксис:

```
New-DSSSignServerAudit -AuditServiceAddress <string> [-Settings <hashtable>]
[-DisplayName <string>]
```

Таблица 123. Описание параметров командлета New-DSSSignServerAudit

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра компонента Сервиса Подписи.
AuditServiceAddress	string	Адрес сервиса записи сообщений аудита (по умолчанию http://<hostname>/<analyticsAppName>/AuditWriter.svc)
Settings	string	Словарь параметров модуля оповещения.

Список настроек, которые можно задать в параметре **Settings**, аналогичен настроек компонента уведомления о событиях, описанных в разделе 4.9.5.4.1.

4.8.2.2. Командлет New-DssStsAudit

Командлет для добавления модуля оповещения типа Аудит на Центр Идентификации. Описание параметров команды приведено в Таблица 124.

Синтаксис:

```
New-DssStsAudit -AuditServiceAddress <string> [-Settings <hashtable>]   [-
DisplayName <string>]
```

Таблица 124. Описание параметров командлета New-DssStsAudit

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра компонента Центра Идентификации.
AuditServiceAddress	string	Адрес сервиса записи сообщений аудита по умолчанию https://<hostname>/<analyticsAppName>/AuditWriter.svc
Settings	string	Словарь параметров модуля оповещения.

Список настроек, которые можно задать в параметре Settings, аналогичен настройкам компонента уведомления о событиях, описанных в разделе 4.9.5.4.1.

4.8.2.3. Командлет Remove-DSSSignServerAudit

Командлет для удаления модуля оповещения типа Аудит с Сервиса Подписи.

Синтаксис:

```
Remove-DSSSignServerAudit [-DeleteDb] [-ConnectionInfo <SQLConnectionInfo>]
[-DisplayName <string>]
```

Таблица 125. Описание параметров командлета Remove-DssSignServerAudit

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
DeleteDB	bool	Флаг, определяющий, требуется ли удаление базы данных Сервиса Подписи.
ConnectionInfo	SqlConnectionInfo	Расширенные данные для подключения к SQL-серверу (см. раздел 7).

4.8.2.4. Remove-DssStsAudit

Командлет для удаления модуля оповещения типа Аудит с Центра Идентификации.

Синтаксис:

```
Remove-DssStsAudit [-DeleteDb] [-ConnectionInfo <SQLConnectionInfo>] [-
DisplayName <string>]
```

Таблица 126. Описание параметров командлета Remove-DssSignServerAudit

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Центра Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
DeleteDB	bool	Флаг, определяющий, требуется ли удаление базы данных ЦИ.
ConnectionInfo	SqlConnectionInfo	Расширенные данные для подключения к SQL-серверу (см. раздел 7).

4.8.2.5. Пример PowerShell-сценария для настройки аудита

Ниже приводится пример разворачивания аудита для Сервиса Подписи.

```
Write-Host "Добавление системы аудита" -ForegroundColor Cyan
New-DSSSignServerAudit -AuditServiceAddress
https://<hostname>/<analyticsAppName>/AuditWriter.svc

Write-Host "Настройка отображения пункта меню «Аудит»"
Set-DssFEProperties -AnalyticsServiceAddress
http://<hostname>/<analyticsAppName>/AnalyticsService.svc/issuedtoken/transpo
rt
```

Ниже приводится пример разворачивания аудита для Центра Идентификации.

```
Write-Host "Добавление системы аудита" -ForegroundColor Cyan
New-DSSStsAudit -AuditServiceAddress
https://<hostname>/<analyticsAppName>/AuditWriter.svc
```

```
Write-Host "Настройка отображения пункта меню «Аудит»"
Set-DssStsProperties -AnalyticsServiceAddress
http://<hostname>/<analyticsAppName>/AnalyticsService.svc/issuedtoken/transpo
rt
```

4.8.2.6. Настройка генерации печатных форм списка записей аудита

Для активации возможности создания печатной формы списка записей аудита необходимо зарегистрировать нужные форматы и соответствующие плагины с помощью Windows PowerShell. Для каждого экземпляра Сервиса Аудита в директории **<Путь установки>\AnalyticsService** создается свой собственный конфигурационный файл с именем **<Имя экземпляра веб-приложения>_convert.config**.

Данный сценарий регистрирует плагины для создания печатных форм списка записей аудита в формате Html/Pdf/Word (формат XML доступен без дополнительных плагинов).

```
Add-DssAnalyticsConverterPlugin -FileExtension arh -Assembly
“DSS.DocumentConverter.AuditRecords.dll” -Classname
“DSS.DocumentConverter.AuditRecords.HtmlConverter” -Parameters
@{"Xslt"="<installDir>\Plugins\Converters\AuditTransform.xml"}

Add-DssAnalyticsConverterPlugin -FileExtension arp -Assembly
“DSS.DocumentConverter.AuditRecords.dll” -Classname
“DSS.DocumentConverter.AuditRecords.PdfConverter” -Parameters
@{"Xslt"="<installDir>\Plugins\Converters\AuditTransform.xml"}

Add-DssAnalyticsConverterPlugin -FileExtension arw -Assembly
“DSS.DocumentConverter.AuditRecords.dll” -Classname
“DSS.DocumentConverter.AuditRecords.WordConverter” -Parameters
@{"Xslt"="<installDir>\Plugins\Converters\AuditTransform.xml"}

Add-DssAnalyticsConverterPlugin -FileExtension arhe -Assembly
“DSS.DocumentConverter.AuditRecords.dll” -Classname
“DSS.DocumentConverter.AuditRecords.HtmlConverter” -Parameters
@{"Xslt"="<installDir>\Plugins\Converters\ExtendedAuditTransform.xml"}

Add-DssAnalyticsConverterPlugin -FileExtension arpe -Assembly
“DSS.DocumentConverter.AuditRecords.dll” -Classname
“DSS.DocumentConverter.AuditRecords.PdfConverter” -Parameters
@{"Xslt"="<installDir>\Plugins\Converters\ExtendedAuditTransform.xml"}

Add-DssAnalyticsConverterPlugin -FileExtension arwe -Assembly
“DSS.DocumentConverter.AuditRecords.dll” -Classname
“DSS.DocumentConverter.AuditRecords.WordConverter” -Parameters
@{"Xslt"="<installDir>\Plugins\Converters\ExtendedAuditTransform.xml"}
```

4.9. Настройка системы оповещения

СЭП «КриптоПро DSS» позволяет настроить оповещение Пользователей и Операторов о различных событиях системы. Также события могут заноситься в журнал Сервиса Аудита. Система оповещения настраивается независимо для Центра Идентификации и Сервиса Подписи и различается набором событий, о которых будут приходить оповещения.

Оповещение Пользователей требует подключения ЦИ и/или Сервиса Подписи к SMS-шлюзу оператора сотовой связи или к почтовому серверу в соответствии со схемой размещения компонентов (см документ ЖТЯИ.00046-03 90 02 КриптоПро DSS. Общее описание). и в соответствии с требованиями к подключению к сетям общего пользования, описанными в Разделе 10 ЖТЯИ.00046-03 95 01. Правила пользования.

При настройке системы оповещения требуется задать и настроить:

- Транспортный плагин.
- Плагин для формирования сообщений.
- Модуль для рассылки уведомлений.

Транспортный плагин осуществляет непосредственную отправку сообщений по SMS или электронной почте. В установку КриптоПро DSS входит несколько транспортных плагинов для отправки сообщений через различные SMS шлюзы и по электронной почте. Подробнее о транспортных плагинах можно прочитать в разделе 4.9.5.

Плагин для формирования сообщений осуществляет подготовку сообщения для отправки. Основная задача плагина сформировать сообщение в зависимости от типа события, от типа получателя (Пользователь, Оператор), от типа транспорта (SMS, электронная почта). В установку КриптоПро DSS входит плагин DSS.MessageFormatter.dll.

Модуль для рассылки уведомлений группирует транспортный плагин и плагин для формирования сообщений.

Система уведомлений позволяет использовать собственные транспортные плагины и плагины для формирования сообщений. Подробнее о написании плагинов можно прочитать в Руководстве разработчика КриптоПро DSS. Фрагмент работы системы оповещения КриптоПро DSS представлен на Рис. 34. На нем изображено оповещение Пользователей, Операторов, а также Сервиса Аудита о событиях, генерируемых Сервисом Подписи.

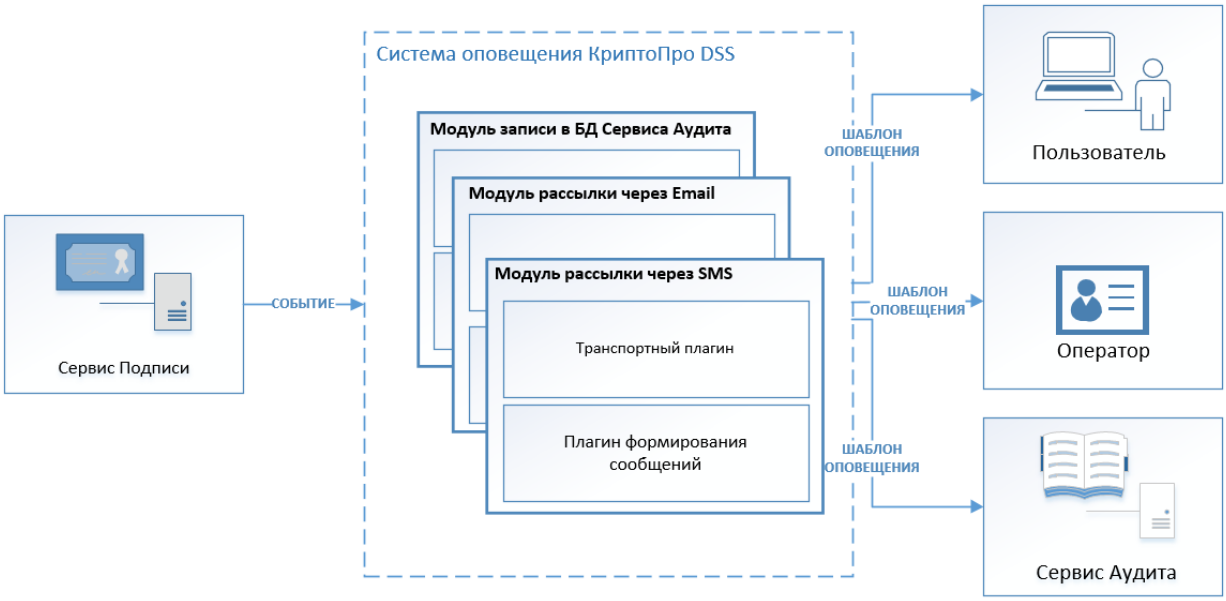

Рис. 34 – Схема работы системы оповещения

Все события, происходящие в КриптоПро DSS, генерируются Сервисом Подписи и Центром Идентификации. Подробнее о настройке этих событий см. раздел 4.9.4.

Каждое событие имеет шаблоны оповещения, текст которых при корректной настройке плагинов и модулей рассылки, упомянутых выше, может быть доставлен различным получателям. Тексты шаблонов сообщений могут быть изменены. Подробнее о настройке шаблонов сообщений о событиях см. раздел 4.9.5.7.

Существует три основных направления работы системы оповещения:

- Оповещение Пользователей и Операторов (Раздел 4.9.1).
- Шаблоны сообщений при подтверждении операций (Раздел 4.9.2).
- Шаблоны сообщений при подтверждении произвольных операций (Раздел 4.9.3).

4.9.1. Оповещение Пользователей и Операторов

В данном разделе описано оповещение Пользователей и Операторов DSS, которое является исключительно **информационным** и осуществляется через SMS-сообщения или электронную почту. В этих сообщениях содержится информация о событиях, происходящих как на Сервисе Подписи, так и на Центре Идентификации КриптоПро DSS.

Операторы DSS могут получать **информационные сообщения** следующими способами:

- О событиях Сервиса Подписи посредством SMS-сообщений (Таблица 127);
- О событиях Сервиса Подписи посредством Email-сообщений (Таблица 128);
- О событиях Центра Идентификации посредством SMS-сообщений (Таблица 129).

Таблица 127. Оповещение Операторов о событиях Сервиса Подписи посредством SMS-сообщений

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
1	RequestCreated	3	Для пользователя {0:Login} был создан запрос на сертификат.
3	RequestDeletedAll	9	Все сертификаты пользователя {0:Login} были удалены.
4	RequestDeleted	14	Запрос на сертификат пользователя {0:Login} был удален.
5	CertificateCreated	19	Для пользователя {0:Login} был выпущен сертификат.
6	CertificateDeleted	24	Сертификат пользователя {0:Login} был удален.
7	CertificateDeletedAll	29	Сертификат пользователя {0:Login} был удален.
8	CertificateHold	33	Действие сертификата пользователя {0:Login} приостановлено.
9	CertificateUnhold	38	Действие сертификата пользователя {0:Login} возобновлено.
10	CertificateRevoke	43	Сертификат пользователя {0:Login} был отозван. Причина: {0:RevocationReason}.

Таблица 128. Оповещение Операторов о событиях Сервиса Подписи посредством Email-сообщений

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
1	RequestCreated	4	Для пользователя {0:Login} был создан запрос на сертификат. Различительное имя субъекта: {0:RequestSubject}.
3	RequestDeletedAll	10	Все сертификаты пользователя {0:Login} были удалены.
4	RequestDeleted	15	Запрос на сертификат пользователя {0:Login} был удален. Различительное имя субъекта: {0:RequestSubject}.
5	CertificateCreated	20	Для пользователя {0:Login} был выпущен сертификат. Отпечаток сертификата: {0:Thumbprint}.
6	CertificateDeleted	25	Сертификат пользователя {0:Login} с отпечатком {0:Thumbprint} был удален.
7	CertificateDeleted All	30	Сертификат пользователя {0:Login} с отпечатком {0:Thumbprint} был удален.

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
8	CertificateHold	34	Действие сертификата пользователя {0:Login} приостановлено. Дата возобновления действия: {0:HoldTime}. Отпечаток сертификата: {0:Thumbprint}.
9	CertificateUnhold	39	Действие сертификата пользователя {0:Login} возобновлено.
10	CertificateRevoke	44	Сертификат пользователя {0:Login} был отозван. Причина: {0:RevocationReason}. Отпечаток сертификата: {0:Thumbprint}.

Таблица 129. Оповещение Операторов о событиях Центра Идентификации посредством SMS-сообщений

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
2	UserPhoneConfirmation	152	Был подтвержден номер телефона {0:Phone}.
3	UserCreated	155	Создана учётная запись. Логин: {0:Login}.
4	UserCreateFail	157	Не удалось создать учётную запись {0:Login}.
5	UserAccountChanged	160	Учётная запись {0:DelegateUserLogin} была изменена.
6	UserAccountChangeFail	163	Не удалось изменить учётную запись {0:DelegateUserLogin}.
11	UserDeleted	176	Учётная запись {0:DelegateUserLogin} была удалена.
12	UserDeleteFail	178	Не удалось удалить учётную запись {0:DelegateUserLogin}.
13	AdminCreated	180	Создание учётной записи администратора {0:DelegateUserLogin}.
14	AdminCreateFail	182	Не удалось создать учётную запись администратора {0:DelegateUserLogin}.
15	AdminDeleted	184	Удаление учётной записи администратора {0:DelegateUserLogin}.
16	AdminDeleteFail	186	Не удалось удалить учётную запись администратора {0:DelegateUserLogin}.
17	AdminAccountChanged	188	Учётная запись администратора {0:DelegateUserLogin} была изменена.

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
18	AdminAccountChangeFail	190	Не удалось изменить учётную запись администратора {0:DelegateUserLogin}.

Пользователи DSS могут получать **информационные сообщения** следующими способами:

- О событиях Сервиса Подписи посредством SMS-сообщений (Таблица 130);
- О событиях Сервиса Подписи посредством Email-сообщений (Таблица 131);
- О событиях Центра Идентификации посредством SMS-сообщений (Таблица 132);
- О событиях Центра Идентификации посредством Email-сообщений (Таблица 133).

Таблица 130. Оповещение Пользователей о событиях Сервиса Подписи посредством SMS-сообщений

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
1	RequestCreated	1	Для Вас был создан запрос на сертификат.
3	RequestDeletedAll	7	Были удалены все Ваши запросы на сертификат.
4	RequestDeleted	12	Был удален запрос на сертификат.
5	CertificateCreated	17	Для Вас был выпущен сертификат.
6	CertificateDeleted	22	Ваш сертификат был удален.
7	CertificateDeletedAll	27	Ваш сертификат был удален.
9	CertificateUnhold	36	Действие Вашего сертификата возобновлено.
10	CertificateRevoke	41	Ваш сертификат был отозван. Причина: {0:RevocationReason}.
11	DocumentSignSuccess	46	Документ успешно подписан.
12	DocumentSignFail	49	Не удалось подписать документ.
13	DocumentEncrypted	52	Документ успешно зашифрован.
14	DocumentEncryptionFail	55	Не удалось зашифровать документ.
15	DocumentDecrypted	58	Документ успешно расшифрован.

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
16	DocumentDecryptionFail	61	Не удалось расшифровать документ.
17	CertificatePinChanged	64	Пин-код изменен успешно.
18	CertificatePinChangeFail	67	Не удалось изменить пин-код.
19	CertificateSetDefault	70	Сертификат по умолчанию успешно назначен.
20	CertificateSetDefaultFail	73	Не удалось назначить сертификат по умолчанию.
21	CertificateResetDefault	76	Сертификат по умолчанию успешно сброшен.
22	CertificateResetDefaultFail	79	Не удалось сбросить сертификат по умолчанию.
28	CertificateInstalled	87	Сертификат успешно установлен.
38	EnhanceSignature	99	Подпись усовершенствована.
105	CertificateSetFriendlyName	102	Сертификату назначено дружественное имя : {0:CertFriendlyName}.
106	CertificateSetFriendlyNameFail	105	Не удалось назначить сертификату дружественное имя.
137	CertificateCreatedWithConfirmation	110	Для Вас был выпущен сертификат.
139	DocumentDecryptionWithConfirmation	114	Документ успешно расшифрован.
144	CertificateRevocationWithConfirmation	119	Ваш сертификат был отозван. Причина: {0:RevocationReason}.
147	CertificateHoldWithConfirmation	124	Действие Вашего сертификата было приостановлено. Дата возобновления действия: {0:HoldTime}.
150	CertificateUnholdWithConfirmation	129	Действие Вашего сертификата возобновлено.
153	CertificateDeleteWithConfirmation	134	Ваш сертификат был удален.
155	RequestCreatedWithConfirmation	138	Для Вас был создан запрос на сертификат.
157	PinChangedWithConfirmation	142	Пин-код изменен успешно.
159	CertificateDeleteAllWithConfirmation	146	Ваши сертификаты были удалены.
40	DocumentSignWithConfirmationSuccess	149	Документ успешно подписан.

Таблица 131. Оповещение Пользователей о событиях Сервиса Подписи посредством Email-сообщений

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
1	RequestCreated	2	Для Вас был создан запрос на сертификат. Различительное имя субъекта: {0:RequestSubject}.
3	RequestDeletedAll	8	Были удалены все Ваши запросы на сертификат.
4	RequestDeleted	13	Был удален запрос на сертификат. Различительное имя субъекта: {0:RequestSubject}.
5	CertificateCreated	18	Для Вас был выпущен сертификат. Отпечаток сертификата: {0:Thumbprint}.
6	CertificateDeleted	23	Ваш сертификат с отпечатком {0:Thumbprint} был удален.
7	CertificateDeletedAll	28	Ваш сертификат с отпечатком {0:Thumbprint} был удален.
8	CertificateHold	32	Действие Вашего сертификата было приостановлено. Дата возобновления действия: {0:HoldTime}. Отпечаток сертификата: {0:Thumbprint}.
9	CertificateUnhold	37	Действие Вашего сертификата возобновлено. Отпечаток сертификата: {0:Thumbprint}.
10	CertificateRevoke	42	Ваш сертификат был отозван. Причина: {0:RevocationReason}. Отпечаток сертификата: {0:Thumbprint}.
11	DocumentSignSuccess	47	Документ успешно подписан.
12	DocumentSignFail	50	Не удалось подписать документ.
13	DocumentEncrypted	53	Документ успешно зашифрован.
14	DocumentEncryptionFail	56	Не удалось зашифровать документ.
15	DocumentDecrypted	59	Документ успешно расшифрован.

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
16	DocumentDecryptionFail	62	Не удалось расшифровать документ.
17	CertificatePinChanged	65	Пин-код изменен успешно.
18	CertificatePinChangeFail	68	Не удалось изменить пин-код.
19	CertificateSetDefault	71	Сертификат по умолчанию успешно назначен.
20	CertificateSetDefaultFail	74	Не удалось назначить сертификат по умолчанию.
21	CertificateResetDefault	77	Сертификат по умолчанию успешно сброшен.
22	CertificateResetDefaultFail	80	Не удалось сбросить сертификат по умолчанию.
28	CertificateInstalled	88	Сертификат успешно установлен.
105	CertificateSetFriendlyName	103	Сертификату назначено дружественное имя : {0:CertFriendlyName}.
106	CertificateSetFriendlyNameFail	106	Не удалось назначить сертификату дружественное имя.
137	CertificateCreatedWithConfirmation	111	Для Вас был выпущен сертификат. Отпечаток сертификата: {0:Thumbprint}.
139	DocumentDecryptionWithConfirmation	115	Документ успешно расшифрован.
144	CertificateRevocationWithConfirmation	120	Ваш сертификат был отозван. Причина: {0:RevocationReason}. Отпечаток сертификата: {0:Thumbprint}.
147	CertificateHoldWithConfirmation	125	Действие Вашего сертификата было приостановлено. Дата возобновления действия: {0:HoldTime}. Отпечаток сертификата: {0:Thumbprint}.
150	CertificateUnholdWithConfirmation	130	Действие Вашего сертификата возобновлено. Отпечаток сертификата: {0:Thumbprint}.
153	CertificateDeleteWithConfirmation	135	Ваш сертификат с отпечатком {0:Thumbprint} был удален.
155	RequestCreatedWithConfirmation	139	Для Вас был создан запрос на сертификат. Различительное имя субъекта: {0:RequestSubject}.

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
157	PinChangedWithConfirmation	143	Пин-код изменен успешно.
159	CertificateDeleteAllWithConfirmation	147	Ваши сертификаты были удалены.
40	DocumentSignWithConfirmationSuccess	150	Документ успешно подписан.

Таблица 132. Оповещение Пользователей о событиях Центра Идентификации посредством SMS-сообщений

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
2	UserPhoneConfirmation	151	Был подтвержден номер телефона {0:Phone}.
3	UserCreated	154	Для Вас создана учётная запись. Логин: {0:Login}.
5	UserAccountChanged	159	Ваша учётная запись была изменена.
6	UserAccountChangeFail	162	Не удалось изменить учётную запись.
7	UserPasswordChanged	165	Пароль для Вашей учётной записи был изменён. Новый пароль: {0:Password}
8	UserPasswordChangeFail	168	Не удалось изменить пароль для Вашей учётной записи.
9	UserPhoneChangeFail	170	Не удалось изменить номер телефона.
10	UserPasswordReset	172	Пароль для Вашей учётной записи был сброшен. Новый пароль {0:Password}
11	UserDeleted	175	Ваша учётная запись была удалена.
20	UserCreatedByAdmin	194	Для Вас была создана учетная запись. Логин: {0:DelegateUserLogin}.
22	UserAuthenticationPassed	197	Пользователь успешно аутентифицирован.
26	UserPhoneChanged	202	Номер телефона был изменен. Новый номер телефона {0:Phone}.
28	UserPhoneConfirmationOtp	206	Ваш одноразовый пароль для потдверждения номера телефона: {0:OTP}
41	UserMobileAuthSecretKeyInfo	215	Код активации ключа в myDSS: {0:OTP}.
71	UserAirKeyAuthSecretKeyInfo	306	Код активации ключа в AirKey: {0:OTP}.

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
76	TestMessage	374	Тестовое сообщение (SMS)
163	SamlAuthMethodDeleted	389	Метод аутентификации SAML удален.
165	SamlAuthMethodAssigned	393	Метод аутентификации SAML назначен.
167	OtpSmsAuthMethodDeleted	397	Метод аутентификации по СМС удален.
169	OtpSmsAuthMethodAssigned	401	Метод аутентификации по СМС назначен.
171	OAthAuthMethodDeleted	405	Метод аутентификации OAth удален.
173	OAthAuthMethodAssigned	409	Метод аутентификации OAth назначен.
175	OtpEmailAuthMethodDeleted	413	Метод аутентификации при помощи электронной почты удален.
177	OtpEmailAuthMethodAssigned	417	Метод аутентификации при помощи электронной почты назначен.
179	SimAuthMethodDeleted	421	Метод аутентификации SimAuth удален.
181	SimAuthMethodAssigned	425	Метод аутентификации SimAuth назначен.
183	MobileAuthMethodDeleted	429	Метод аутентификации MobileAuth удален.
185	MobileAuthMethodAssigned	433	Метод аутентификации MobileAuth назначен.
187	MtmoAuthMethodDeleted	437	Метод аутентификации Mtmo удален.
189	MtmoAuthMethodAssigned	441	Метод аутентификации Mtmo назначен.
191	MoAuthMethodDeleted	445	Метод аутентификации Mo удален.
193	MoAuthMethodAssigned	449	Метод аутентификации Mo назначен.
195	AirkeyAuthMethodDeleted	453	Метод аутентификации AirKey удален.
197	AirkeyAuthMethodAssigned	457	Метод аутентификации AirKey назначен.
199	MyDssAuthMethodDeleted	461	Метод аутентификации MyDss удален.
201	MyDssAuthMethodAssigned	465	Метод аутентификации MyDss назначен.
204	IdOnlyAuthMethodDeleted	469	Метод аутентификации "Только идентификация" удален.

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
206	IdOnlyAuthMethodAssigned	473	Метод аутентификации "Только идентификация" назначен.
208	CertificateAuthMethodDeleted	477	Метод аутентификации по сертификату удален.
210	CertificateAuthMethodAssigned	481	Метод аутентификации по сертификату назначен.
212	PasswordAuthMethodDeleted	485	Метод аутентификации по паролю удален.
214	PasswordAuthMethodAssigned	489	Метод аутентификации по паролю назначен.

Таблица 133. Оповещение Пользователей о событиях Центра Идентификации посредством Email-сообщений

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
7	UserPasswordChanged	166	Пароль для Вашей учётной записи был изменён. Новый пароль: {0:Password}
10	UserPasswordReset	173	Пароль для Вашей учётной записи был сброшен. Новый пароль {0:Password}.
26	UserPhoneChanged	203	Номер телефона был изменен. Новый номер телефона {0:Phone}.
38	UserEmailConfirmationOtp	211	Ваш одноразовый пароль для потдверждения адреса электронной почты: {0:OTP}
39	UserEmailChanged	212	Адрес электронной почты изменен. Новый адрес {0:Email}.
41	UserMobileAuthSecretKeyInfo	216	Код активации ключа в myDSS: {0:OTP}.
44	AuthenticationSchemeChanged	219	Схема аутентификации была изменена.
71	UserAirKeyAuthSecretKeyInfo	307	Код активации ключа в AirKey: {0:OTP}.
76	TestMessage	375	Тестовое сообщение (Email)
77	UserMobileAuthSendQrCodeByEmail	378	В письме содержится QR-код с ключевой инофрмацией. Отсканируйте его с помощью приложения myDss.
163	SamlAuthMethodDeleted	390	Метод аутентификации SAML удален.

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
165	SamlAuthMethodAssigned	394	Метод аутентификации SAML назначен.
167	OtpSmsAuthMethodDeleted	398	Метод аутентификации по СМС удален.
169	OtpSmsAuthMethodAssigned	402	Метод аутентификации по СМС назначен.
171	OAthAuthMethodDeleted	406	Метод аутентификации OAth удален.
173	OAthAuthMethodAssigned	410	Метод аутентификации OAth назначен.
175	OtpEmailAuthMethodDeleted	414	Метод аутентификации при помощи электронной почты удален.
177	OtpEmailAuthMethodAssigned	418	Метод аутентификации при помощи электронной почты назначен.
179	SimAuthMethodDeleted	422	Метод аутентификации SimAuth удален.
181	SimAuthMethodAssigned	426	Метод аутентификации SimAuth назначен.
183	MobileAuthMethodDeleted	430	Метод аутентификации MobileAuth удален.
185	MobileAuthMethodAssigned	434	Метод аутентификации MobileAuth назначен.
187	MtmoAuthMethodDeleted	438	Метод аутентификации Mtmo удален.
189	MtmoAuthMethodAssigned	442	Метод аутентификации Mtmo назначен.
191	MoAuthMethodDeleted	446	Метод аутентификации Mtmo удален.
193	MoAuthMethodAssigned	450	Метод аутентификации Mo назначен.
195	AirkeyAuthMethodDeleted	454	Метод аутентификации AirKey удален.
197	AirkeyAuthMethodAssigned	458	Метод аутентификации AirKey назначен.
199	MyDssAuthMethodDeleted	462	Метод аутентификации MyDss удален.
201	MyDssAuthMethodAssigned	466	Метод аутентификации MyDss назначен.
204	IdOnlyAuthMethodDeleted	470	Метод аутентификации "Только идентификация" удален.
206	IdOnlyAuthMethodAssigned	474	Метод аутентификации "Только идентификация" назначен.
208	CertificateAuthMethodDeleted	478	Метод аутентификации по сертификату удален.

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
210	CertificateAuthMethodAssigned	482	Метод аутентификации по сертификату назначен.
212	PasswordAuthMethodDeleted	486	Метод аутентификации по паролю удален.
214	PasswordAuthMethodAssigned	490	Метод аутентификации по паролю назначен.

Настройка оповещения Пользователей и/или Операторов DSS посредством SMS-сообщений приведена в Разделе 4.9.5.5.

Настройка оповещения Пользователей и/или Операторов DSS посредством сообщений электронной почты приведена в Разделе 4.9.5.6.

Тексты шаблонов сообщений могут быть изменены. Подробнее о настройке шаблонов сообщений о событиях см. раздел 4.9.5.7.

4.9.2. Шаблоны сообщений при подтверждении операций

В данном разделе описаны шаблоны сообщений, которые получают Пользователи DSS при подтверждении операций. В этих сообщениях содержится информация о событиях, генерируемых центром Идентификации КриптоПро DSS в зависимости от настроенного метода аутентификации:

- Подтверждение операций при помощи апплета на SIM-карте (SimAuth) – Таблица 134;
- Подтверждение операций при помощи мобильного приложения myDSS (MobileAuth) – Таблица 135;
- Подтверждение операций при помощи мобильного приложения AirKey (AirKeyAuth) – Таблица 136;
- Подтверждение операций при помощи SMS-сообщений (SMS) – Таблица 137;
- Подтверждение операций при помощи Email-сообщений (Email) – Таблица 138;
- Подтверждение операций при помощи Рутокен Плагин (RuTokenAuth) – Таблица 139;

Также отдельно настраиваются сообщения, отображаемые в Веб-интерфейсе Пользователя при подтверждении операций (Challenge) – Таблица 140.

Таблица 134. Подтверждение операций при помощи апплета на SIM-карте (SimAuth)

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
51	SecondaryAuthSign	264	Подпись документа. {0:DocumentInfo}. Тип подписи: {0:SignatureType}. Сертификат: {0:CertFriendlyName}.
52	SecondaryAuthSignDocs	265	Подпись документов. Тип подписи: {0:SignatureType}. Сертификат: {0:CertFriendlyName}.
53	SecondaryAuthDecrypt	266	Расшифрование документа {0:DocumentInfo}. Сертификат: {0:CertFriendlyName}.
54	SecondaryAuthCreateRequest	267	Создание запроса на сертификат. Параметры сертификата: {0:CertSubjectName}, УЦ: {0:CAName}, шаблон сертификата: {0:CertTemplateName}.
55	SecondaryAuthChangePin	268	Изменение пин-кода на сертификат. Сертификат: {0:CertFriendlyName}.
56	SecondaryAuthRenewCert	269	Обновление сертификата. Параметры сертификата: {0:CertSubjectName}, УЦ: {0:CAName}, шаблон сертификата: {0:CertTemplateName}.
57	SecondaryAuthRevokeCert	270	Отзыв сертификата. Сертификат: {0:CertFriendlyName}.
58	SecondaryAuthHoldCert	271	Приостановление сертификата. Сертификат: {0:CertFriendlyName}.
59	SecondaryAuthUnholdCert	272	Возобновление сертификата. Сертификат: {0:CertFriendlyName}.
60	SecondaryAuthDeleteCert	273	Удаление сертификата. Сертификат: {0:CertFriendlyName}.
61	SecondaryAuthDeleteCerts	274	Удаление всех сертификатов.
62	SecondaryAuthPrivateKeyAccess	275	Доступ к закрытому ключу. Сертификат: {0:CertFriendlyName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}
50	SecondaryAuthLogin	312	Подтвердите операцию входа пользователя. Идентификатор запроса {0:SessionId}

Таблица 135. Подтверждение операций при помощи мобильного приложения myDSS (MobileAuth)

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
42	MobileAuthTransactionConfirmation	217	{0:DocumentInfo}. Подтвердите операцию.

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
43	MobileAuthUserEnterConfirmation	218	Подтвердите операцию входа пользователя.
51	SecondaryAuthSign	252	Подпись документа. {0:DocumentInfo}. Тип подписи: {0:SignatureType}. Сертификат: {0:CertFriendlyName}.
52	SecondaryAuthSignDocs	253	Подпись документов. Тип подписи: {0:SignatureType}. Сертификат: {0:CertFriendlyName}.
53	SecondaryAuthDecrypt	254	Расшифрование документа {0:DocumentInfo}. Сертификат: {0:CertFriendlyName}.
54	SecondaryAuthCreateRequest	255	Создание запроса на сертификат. Параметры сертификата: {0:CertSubjectName}, УЦ: {0:CAName}, шаблон сертификата: {0:CertTemplateName}.
55	SecondaryAuthChangePin	256	Изменение пин-кода на сертификат. Сертификат: {0:CertFriendlyName}.
56	SecondaryAuthRenewCert	257	Обновление сертификата. Параметры сертификата: {0:CertSubjectName}, УЦ: {0:CAName}, шаблон сертификата: {0:CertTemplateName}.
57	SecondaryAuthRevokeCert	258	Отзыв сертификата. Сертификат: {0:CertFriendlyName}.
58	SecondaryAuthHoldCert	259	Приостановление сертификата. Сертификат: {0:CertFriendlyName}.
59	SecondaryAuthUnholdCert	260	Возобновление сертификата. Сертификат: {0:CertFriendlyName}.
60	SecondaryAuthDeleteCert	261	Удаление сертификата. Сертификат: {0:CertFriendlyName}.
61	SecondaryAuthDeleteCerts	262	Удаление всех сертификатов.
62	SecondaryAuthPrivateKeyAccess	263	Доступ к закрытому ключу. Сертификат: {0:CertFriendlyName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}
50	SecondaryAuthLogin	311	Подтвердите операцию входа пользователя. Идентификатор запроса {0:SessionId}

Таблица 136. Подтверждение операций при помощи платформы КриптоПро AirKey (AirKeyAuth)

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
51	SecondaryAuthSign	295	Подпись документа. {0:DocumentInfo}. Тип подписи: {0:SignatureType}. Сертификат: {0:CertFriendlyName}.
52	SecondaryAuthSignDocs	296	Подпись документов. Тип подписи: {0:SignatureType}. Сертификат: {0:CertFriendlyName}.
53	SecondaryAuthDecrypt	297	Расшифрование документа {0:DocumentInfo}. Сертификат: {0:CertFriendlyName}.
54	SecondaryAuthCreateRequest	298	Создание запроса на сертификат. Параметры сертификата: {0:CertSubjectName}, УЦ: {0:CAName}, шаблон сертификата: {0:CertTemplateName}.
55	SecondaryAuthChangePin	299	Изменение пин-кода на сертификат. Сертификат: {0:CertFriendlyName}.
56	SecondaryAuthRenewCert	300	Обновление сертификата. Параметры сертификата: {0:CertSubjectName}, УЦ: {0:CAName}, шаблон сертификата: {0:CertTemplateName}.
57	SecondaryAuthRevokeCert	301	Отзыв сертификата. Сертификат: {0:CertFriendlyName}.
58	SecondaryAuthHoldCert	302	Приостановление сертификата. Сертификат: {0:CertFriendlyName}.
59	SecondaryAuthUnholdCert	303	Возобновление сертификата. Сертификат: {0:CertFriendlyName}.
60	SecondaryAuthDeleteCert	304	Удаление сертификата. Сертификат: {0:CertFriendlyName}.
61	SecondaryAuthDeleteCerts	305	Удаление всех сертификатов.
72	AirKeyAuthTransactionConfirmation	308	{0:DocumentInfo}. Подтвердите операцию.
73	AirKeyAuthUserEnterConfirmation	309	Подтвердите операцию входа пользователя.
50	SecondaryAuthLogin	310	Подтвердите операцию входа пользователя. Идентификатор запроса {0:SessionId}

Таблица 137. Подтверждение операций при помощи SMS-сообщений (SMS)

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
1	OTP	148	{0:DocumentInfo}. Ваш одноразовый пароль для подтверждения операции: {0:OTP}

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
2	UserPhoneConfirmation	151	Был подтвержден номер телефона {0:Phone}.
3	UserCreated	154	Для Вас создана учётная запись. Логин: {0:Login}.
5	UserAccountChanged	159	Ваша учётная запись была изменена.
6	UserAccountChangeFail	162	Не удалось изменить учётную запись.
7	UserPasswordChanged	165	Пароль для Вашей учётной записи был изменён. Новый пароль: {0:Password}
8	UserPasswordChangeFail	168	Не удалось изменить пароль для Вашей учётной записи.
9	UserPhoneChangeFail	170	Не удалось изменить номер телефона.
10	UserPasswordReset	172	Пароль для Вашей учётной записи был сброшен. Новый пароль {0:Password}
11	UserDeleted	175	Ваша учётная запись была удалена.
19	UserEnterConfirmation	192	Ваш одноразовый пароль для входа: {0:OTP}
20	UserCreatedByAdmin	194	Для Вас была создана учетная запись. Логин: {0:DelegateUserLogin}.
22	UserAuthenticationPassed	197	Пользователь успешно аутентифицирован.
26	UserPhoneChanged	202	Номер телефона был изменен. Новый номер телефона {0:Phone}.
28	UserPhoneConfirmationOtp	206	Ваш одноразовый пароль для потдверждения номера телефона: {0:OTP}
41	UserMobileAuthSecretKeyInfo	215	Код активации ключа в myDSS: {0:OTP}.
42	MobileAuthTransactionConfirmation	226	{0:DocumentInfo}. Подтвердите операцию.
43	MobileAuthUserEnterConfirmation	227	Подтвердите операцию входа пользователя.
51	SecondaryAuthSign	240	Подпись документа. {0:DocumentInfo}. Тип подписи: {0:SignatureType}. Сертификат: {0:CertFriendlyName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}
52	SecondaryAuthSignDocs	241	Подпись документов. Тип подписи: {0:SignatureType}. Сертификат: {0:CertFriendlyName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}.

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
53	SecondaryAuthDecrypt	242	Расшифрование документа {0:DocumentInfo}. Сертификат: {0:CertFriendlyName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}.
54	SecondaryAuthCreateRequest	243	Создание запроса на сертификат. Параметры сертификата: {0:CertSubjectName}, УЦ: {0:CAName}, шаблон сертификата: {0:CertTemplateName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}.
55	SecondaryAuthChangePin	244	Изменение пин-кода на сертификат. Сертификат: {0:CertFriendlyName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}.
56	SecondaryAuthRenewCert	245	Обновление сертификата. Параметры сертификата: {0:CertSubjectName}, УЦ: {0:CAName}, шаблон сертификата: {0:CertTemplateName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}.
57	SecondaryAuthRevokeCert	246	Отзыв сертификата. Сертификат: {0:CertFriendlyName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}.
58	SecondaryAuthHoldCert	247	Приостановление сертификата. Сертификат: {0:CertFriendlyName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}.
59	SecondaryAuthUnholdCert	248	Возобновление сертификата. Сертификат: {0:CertFriendlyName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}.
60	SecondaryAuthDeleteCert	249	Удаление сертификата. Сертификат: {0:CertFriendlyName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}.
61	SecondaryAuthDeleteCerts	250	Удаление всех сертификатов. Введите одноразовый пароль для подтверждения операции: {0:OTP}.
62	SecondaryAuthPrivateKeyAccess	251	Доступ к закрытому ключу. Сертификат: {0:CertFriendlyName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}
71	UserAirKeyAuthSecretKeyInfo	306	Код активации ключа в AirKey: {0:OTP}.
50	SecondaryAuthLogin	313	Идентификатор запроса {0:SessionId}. Ваш одноразовый пароль для входа: {0:OTP}
76	TestMessage	374	Тестовое сообщение (SMS)

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
163	SamlAuthMethodDeleted	389	Метод аутентификации SAML удален.
165	SamlAuthMethodAssigned	393	Метод аутентификации SAML назначен.
167	OtpSmsAuthMethodDeleted	397	Метод аутентификации по СМС удален.
169	OtpSmsAuthMethodAssigned	401	Метод аутентификации по СМС назначен.
171	OAthAuthMethodDeleted	405	Метод аутентификации OAth удален.
173	OAthAuthMethodAssigned	409	Метод аутентификации OAth назначен.
175	OtpEmailAuthMethodDeleted	413	Метод аутентификации при помощи электронной почты удален.
177	OtpEmailAuthMethodAssigned	417	Метод аутентификации при помощи электронной почты назначен.
179	SimAuthMethodDeleted	421	Метод аутентификации SimAuth удален.
181	SimAuthMethodAssigned	425	Метод аутентификации SimAuth назначен.
183	MobileAuthMethodDeleted	429	Метод аутентификации MobileAuth удален.
185	MobileAuthMethodAssigned	433	Метод аутентификации MobileAuth назначен.
187	MtmoAuthMethodDeleted	437	Метод аутентификации Mtmo удален.
189	MtmoAuthMethodAssigned	441	Метод аутентификации Mtmo назначен.
191	MoAuthMethodDeleted	445	Метод аутентификации Mo удален.
193	MoAuthMethodAssigned	449	Метод аутентификации Mo назначен.
195	AirkeyAuthMethodDeleted	453	Метод аутентификации AirKey удален.
197	AirkeyAuthMethodAssigned	457	Метод аутентификации AirKey назначен.
199	MyDssAuthMethodDeleted	461	Метод аутентификации MyDss удален.
201	MyDssAuthMethodAssigned	465	Метод аутентификации MyDss назначен.
204	IdOnlyAuthMethodDeleted	469	Метод аутентификации "Только идентификация" удален.
206	IdOnlyAuthMethodAssigned	473	Метод аутентификации "Только идентификация" назначен.
208	CertificateAuthMethodDeleted	477	Метод аутентификации по сертификату удален.

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
210	CertificateAuthMethodAssigned	481	Метод аутентификации по сертификату назначен.
212	PasswordAuthMethodDeleted	485	Метод аутентификации по паролю удален.
214	PasswordAuthMethodAssigned	489	Метод аутентификации по паролю назначен.

Таблица 138. Подтверждение операций при помощи Email-сообщений (Email)

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
1	OTP	149	{0:DocumentInfo}. Ваш одноразовый пароль для подтверждения операции: {0:OTP}.
7	UserPasswordChanged	166	Пароль для Вашей учётной записи был изменён. Новый пароль: {0:Password}
10	UserPasswordReset	173	Пароль для Вашей учётной записи был сброшен. Новый пароль {0:Password}.
26	UserPhoneChanged	203	Номер телефона был изменен. Новый номер телефона {0:Phone}.
19	UserEnterConfirmation	210	Ваш одноразовый пароль для входа: {0:OTP}.
38	UserEmailConfirmationOtp	211	Ваш одноразовый пароль для потдверждения адреса электронной почты: {0:OTP}
39	UserEmailChanged	212	Адрес электронной почты изменен. Новый адрес {0:Email}.
41	UserMobileAuthSecretKeyInfo	216	Код активации ключа в myDSS: {0:OTP}.
44	AuthenticationSchemeChanged	219	Схема аутентификации была изменена.
51	SecondaryAuthSign	228	Подпись документа. {0:DocumentInfo}. Тип подписи: {0:SignatureType}. Сертификат: {0:CertFriendlyName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}
52	SecondaryAuthSignDocs	229	Подпись документов. Тип подписи: {0:SignatureType}. Сертификат: {0:CertFriendlyName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}.
53	SecondaryAuthDecrypt	230	Расшифрование документа {0:DocumentInfo}. Сертификат: {0:CertFriendlyName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}.

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
54	SecondaryAuthCreateRequest	231	Создание запроса на сертификат. Параметры сертификата: {0:CertSubjectName}, УЦ: {0:CAName}, шаблон сертификата: {0:CertTemplateName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}.
55	SecondaryAuthChangePin	232	Изменение пин-кода на сертификат. Сертификат: {0:CertFriendlyName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}.
56	SecondaryAuthRenewCert	233	Обновление сертификата. Параметры сертификата: {0:CertSubjectName}, УЦ: {0:CAName}, шаблон сертификата: {0:CertTemplateName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}.
57	SecondaryAuthRevokeCert	234	Отзыв сертификата. Сертификат: {0:CertFriendlyName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}.
58	SecondaryAuthHoldCert	235	Приостановление сертификата. Сертификат: {0:CertFriendlyName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}.
59	SecondaryAuthUnholdCert	236	Возобновление сертификата. Сертификат: {0:CertFriendlyName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}.
60	SecondaryAuthDeleteCert	237	Удаление сертификата. Сертификат: {0:CertFriendlyName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}.
61	SecondaryAuthDeleteCerts	238	Удаление всех сертификатов. Введите одноразовый пароль для подтверждения операции: {0:OTP}.
62	SecondaryAuthPrivateKeyAccess	239	Доступ к закрытому ключу. Сертификат: {0:CertFriendlyName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}
71	UserAirKeyAuthSecretKeyInfo	307	Код активации ключа в AirKey: {0:OTP}.
50	SecondaryAuthLogin	314	Идентификатор запроса {0:SessionId}. Ваш одноразовый пароль для входа: {0:OTP}
76	TestMessage	375	Тестовое сообщение (Email)
77	UserMobileAuthSendQrCodeByEmail	378	В письме содержится QR-код с ключевой инофрмацией. Отсканируйте его с помощью приложения myDss.
163	SamlAuthMethodDeleted	390	Метод аутентификации SAML удален.

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
165	SamlAuthMethodAssigned	394	Метод аутентификации SAML назначен.
167	OtpSmsAuthMethodDeleted	398	Метод аутентификации по СМС удален.
169	OtpSmsAuthMethodAssigned	402	Метод аутентификации по СМС назначен.
171	OAthAuthMethodDeleted	406	Метод аутентификации OAth удален.
173	OAthAuthMethodAssigned	410	Метод аутентификации OAth назначен.
175	OtpEmailAuthMethodDeleted	414	Метод аутентификации при помощи электронной почты удален.
177	OtpEmailAuthMethodAssigned	418	Метод аутентификации при помощи электронной почты назначен.
179	SimAuthMethodDeleted	422	Метод аутентификации SimAuth удален.
181	SimAuthMethodAssigned	426	Метод аутентификации SimAuth назначен.
183	MobileAuthMethodDeleted	430	Метод аутентификации MobileAuth удален.
185	MobileAuthMethodAssigned	434	Метод аутентификации MobileAuth назначен.
187	MtmoAuthMethodDeleted	438	Метод аутентификации Mtmo удален.
189	MtmoAuthMethodAssigned	442	Метод аутентификации Mtmo назначен.
191	MoAuthMethodDeleted	446	Метод аутентификации Mtmo удален.
193	MoAuthMethodAssigned	450	Метод аутентификации Mo назначен.
195	AirkeyAuthMethodDeleted	454	Метод аутентификации AirKey удален.
197	AirkeyAuthMethodAssigned	458	Метод аутентификации AirKey назначен.
199	MyDssAuthMethodDeleted	462	Метод аутентификации MyDss удален.
201	MyDssAuthMethodAssigned	466	Метод аутентификации MyDss назначен.
204	IdOnlyAuthMethodDeleted	470	Метод аутентификации "Только идентификация" удален.
206	IdOnlyAuthMethodAssigned	474	Метод аутентификации "Только идентификация" назначен.
208	CertificateAuthMethodDeleted	478	Метод аутентификации по сертификату удален.
210	CertificateAuthMethodAssigned	482	Метод аутентификации по сертификату назначен.

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
212	PasswordAuthMethodDeleted	486	Метод аутентификации по паролю удален.
214	PasswordAuthMethodAssigned	490	Метод аутентификации по паролю назначен.

Таблица 139. Подтверждение операций при помощи Рутокен Плагин (RuTokenAuth)

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
51	SecondaryAuthSign	332	Подпись документа. {0:DocumentInfo}. Тип подписи: {0:SignatureType}. Сертификат: {0:CertFriendlyName}.
52	SecondaryAuthSignDocs	333	Подпись документов. Тип подписи: {0:SignatureType}. Сертификат: {0:CertFriendlyName}.
53	SecondaryAuthDecrypt	334	Расшифрование документа {0:DocumentInfo}. Сертификат: {0:CertFriendlyName}.
54	SecondaryAuthCreateRequest	335	Создание запроса на сертификат. Параметры сертификата: {0:CertSubjectName}, УЦ: {0:CAName}, шаблон сертификата: {0:CertTemplateName}.
55	SecondaryAuthChangePin	336	Изменение пин-кода на сертификат. Сертификат: {0:CertFriendlyName}.
56	SecondaryAuthRenewCert	337	Обновление сертификата. Параметры сертификата: {0:CertSubjectName}, УЦ: {0:CAName}, шаблон сертификата: {0:CertTemplateName}.
57	SecondaryAuthRevokeCert	338	Отзыв сертификата. Сертификат: {0:CertFriendlyName}.
58	SecondaryAuthHoldCert	339	Приостановление сертификата. Сертификат: {0:CertFriendlyName}.
59	SecondaryAuthUnholdCert	340	Возобновление сертификата. Сертификат: {0:CertFriendlyName}.
60	SecondaryAuthDeleteCert	341	Удаление сертификата. Сертификат: {0:CertFriendlyName}.
61	SecondaryAuthDeleteCerts	342	Удаление всех сертификатов.
62	SecondaryAuthPrivateKeyAccess	343	Доступ к закрытому ключу. Сертификат: {0:CertFriendlyName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}
50	SecondaryAuthLogin	345	Подтвердите операцию входа пользователя. Идентификатор запроса {0:SessionId}.

Таблица 140. Сообщения, отображаемые в Веб-интерфейсе Пользователя при подтверждении операций (Challenge)

ID события (EventID)	Имя события	ID шаблона сообщения (TemplateID)	Текст шаблона
51	SecondaryAuthSign	318	Подпись документа. {0:DocumentInfo}. Тип подписи: {0:SignatureType}. Сертификат: {0:CertFriendlyName}.
52	SecondaryAuthSignDocs	319	Подпись документов. Тип подписи: {0:SignatureType}. Сертификат: {0:CertFriendlyName}.
53	SecondaryAuthDecrypt	320	Расшифрование документа {0:DocumentInfo}. Сертификат: {0:CertFriendlyName}.
54	SecondaryAuthCreateRequest	321	Создание запроса на сертификат. Параметры сертификата: {0:CertSubjectName}, УЦ: {0:CAName}, шаблон сертификата: {0:CertTemplateName}.
55	SecondaryAuthChangePin	322	Изменение пин-кода на сертификат. Сертификат: {0:CertFriendlyName}.
56	SecondaryAuthRenewCert	323	Обновление сертификата. Параметры сертификата: {0:CertSubjectName}, УЦ: {0:CAName}, шаблон сертификата: {0:CertTemplateName}.
57	SecondaryAuthRevokeCert	324	Отзыв сертификата. Сертификат: {0:CertFriendlyName}.
58	SecondaryAuthHoldCert	325	Приостановление сертификата. Сертификат: {0:CertFriendlyName}.
59	SecondaryAuthUnholdCert	326	Возобновление сертификата. Сертификат: {0:CertFriendlyName}.
60	SecondaryAuthDeleteCert	327	Удаление сертификата. Сертификат: {0:CertFriendlyName}.
61	SecondaryAuthDeleteCerts	328	Удаление всех сертификатов.
62	SecondaryAuthPrivateKeyAccess	329	Доступ к закрытому ключу. Сертификат: {0:CertFriendlyName}. Введите одноразовый пароль для подтверждения операции: {0:OTP}
1	OTP	330	{0:DocumentInfo}. Подтвердите операцию.
50	SecondaryAuthLogin	331	Подтвердите операцию входа пользователя. Идентификатор запроса {0:SessionId}

Настройка плагинов, отвечающих за формирование и рассылку шаблонов событий, приведенных в данном разделе, описана в разделе 4.9.5.

Тексты шаблонов сообщений могут быть изменены. Подробнее о настройке шаблонов сообщений о событиях см. раздел 4.9.5.7.

4.9.3. Шаблоны сообщений при подтверждении произвольных операций

В данном разделе описана настройка собственных шаблонов событий подтверждения произвольных операций, которые могут быть доставлены Пользователям и/или интегрируемым системам. Процедура настройки состоит из следующих шагов:

1. Регистрация произвольной операции (события) при помощи командлета Add-DssScope.
2. Регистрация шаблона сообщения о произвольной операции (событии) при помощи командлета Add-DssScopeTemplate.

Далее описаны все командлеты, использующиеся при настройке собственных шаблонов событий подтверждения произвольных операций.

Для каждого созданного поизвольного события необходимо добавить столько шаблонов сообщений, сколько методов аутентификации используется. Также необходимо добавить шаблон типа **Challenge** (`-Destination List[Challenge]`), который будет отображаться в Веб-интерфейсе Пользователя, либо передаваться в веб-интерфейс интегрируемой системы.

Шаблон сообщения представляет собой текст, в котором могут быть указангы подстановочные поля (параметры). Имена подстановочных параметров указываются произвольно. Значения подстановочных паратметров должны передаваться из интегрируемой системы (подробнее см. раздел 8.7 ЖТЯИ.00096-02 97 01 КриптоПро DSS. Руководство разработчика).

Общий вид шаблона сообщения:

```
Подтверждение тестовой операции. Время: {0:<Мой параметр 1>}. Документ:
{0:<Мой параметр 2>}. Пользователь: {0:<Мой параметр 3>}.
```

4.9.3.1. Командлет Add-DssScope

Командлет отвечает за регистрацию произвольного события.

Синтаксис:

```
Add-DssScope [-DisplayName <string>] -Name <string> [-PassThru <switch>] [-
RequireConfirmation <bool>] [-ScopeDescription <string>] [-ScopeDisplayName
<string>]
```

Таблица 141. Описание параметров командлета Add-DssScope

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра компонента.
Name	string	Имя события, используемое для обращения к нему.
PassThru	switch	Флаг, показывающий следует ли передавать обект дальше по конвейеру.
RequireConfirmation	bool	Требовать подтверждение данного события.

Параметр	Тип	Описание
ScopeDescription	string	Описание события.
ScopeDisplayName	string	Понятное имя события.

4.9.3.2. Командлет Get-DssScope

Командлет позволяет вывести на консоль сведения о зарегистрированном произвольном событии.

Синтаксис:

```
Get-DssScope [-DisplayName <string>] -Name <string>
```

4.9.3.1. Командлет Set-DssScope

Командлет отвечает за настройку зарегистрированного ранее произвольного события. Может принимать на вход объект в режиме конвейера.

Синтаксис:

```
Set-DssScope [-DisplayName <string>] -ScopeName <string> [-PassThru <switch>]
[-RequireConfirmation <bool>] [-ScopeDescription <string>] [-ScopeDisplayName
<string>]
```

Таблица 142. Описание параметров командлета Set-DssScope

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра компонента.
Name	string	Имя события, используемое для обращения к нему.
PassThru	switch	Флаг, показывающий следует ли передавать обект дальше по конвейеру.
RequireConfirmation	bool	Требовать подтверждение данного события.
ScopeDescription	string	Описание события.
ScopeDisplayName	string	Понятное имя события.

4.9.3.1. Командлет Disable-DssScope

Командлет позволяет отключить уведомления о произвольном событии.

Синтаксис:

```
Disable-DssScope [-DisplayName <string>] -ScopeName <string> [-PassThru
<switch>]
```

4.9.3.1. Командлет Enable-DssScope

Командлет позволяет включить уведомления о произвольном событии.

Синтаксис:

```
Enable-DssScope [-DisplayName <string>] -ScopeName <string> [-PassThru
<switch>]
```

4.9.3.1. Командлет Remove-DssScope

Командлет позволяет удалить произвольное событие.

Синтаксис:

```
Remove-DssScope [-DisplayName <string>] -ScopeName <string> -TargetScope
<IdentityScope> [-PassThru <switch>]
```

4.9.3.2. Командлет Add-DssScopeTemplate

Командлет позволяет добавить собственный шаблон сообщения о произвольном событии и связать его с этим событием.

Синтаксис:

```
Add-DssScopeTemplate [-DisplayName <string>] -Destinations
<List[DestinationTypeEnum]> -Recipient <RecipientTypeEnum> -ScopeName
<string> -Template <string>
```

Таблица 143. Описание параметров командлета Add-DssScopeTemplate

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра компонента.
Destinations	List[DestinationTypeEnum]. Возможные значения: **SimAuth, MobileAuth, AirKeyAuth, SMS, Email, RuTokenAuth, Challenge.**	Переключать вывода информации о событиях в файл. Если параметр не задан, то вывод будет осуществлён на консоль.
Recipient	List[DestinationTypeEnum] В настоящее время рекомендуется использовать значение **User.**	Имя файла для сохранения информации о событиях.
ScopeName	string	Имя события, используемое для обращения к нему.

Параметр	Тип	Описание
Template	string	Текст шаблона сообщения.

4.9.3.3. Командлет Get-DssScopeTemplate

Командлет позволяет вывести на консоль информацию о зарегистрированном собственном шаблоне сообщения о произвольном событии.

Синтаксис:

```
Get-DssScopeTemplate [-DisplayName <string>] -ScopeName <string>
```

4.9.4. Настройка событий

4.9.4.1. Командлет Get-DssSignServerEvent

Командлет для вывода на консоль информации о событиях. Описание параметров команды приведено в Таблица 144. Также командлет может принимать объект в режиме конвейера.

Синтаксис:

```
Get-DssSignServerEvent [-File] [-FileName <string>] [-DisplayName <string>]
```

Таблица 144. Описание параметров командлета Get-DSSSignServerEvent

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра компонента
File	switch	Переключать вывода информации о событиях в файл. Если параметр не задан, то вывод будет осуществлён на консоль.
FileName	string	Имя файла для сохранения информации о событиях.

Аналогичным синтаксисом и набором параметров располагает командлет **Get-DssStsEvent.**

4.9.4.2. Командлет Set-DssSignServerEvent

Командлет для изменения настроек событий. Описание параметров команды приведено в Таблица 145.

Командлет позволяет настроить сообщения по отдельности (задавая идентификатор события) или настроить все события сразу, задав файл с настройками событий. Создать файл с настройками событий можно через командлет Get-DssSignServerEvent. Также командлет может принимать объект в режиме конвейера.

Синтаксис:

```
Set-DssSignServerEvent [-EventID <int>] [-Notify <bool>] [-NotifyAdmin
<bool>] [-Auditable <bool>] [-FileName <string>] [-DisplayName <string>]
```

Таблица 145. Описание параметров командлета Set-DSSSignServerEvent

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра компонента
EventId	int	Идентификатор события
Notify	bool	Уведомлять Пользователя о событии.
NotifyAdmin	bool	Уведомлять Оператора о событии.
Auditable	bool	Записывать событие в журнал аудита.
FileName	string	Имя файла с настройками событий.

Аналогичным синтаксисом и набором параметров располагает командлет **Set-DssStsEvent.**

4.9.5. Настройка оповещения

4.9.5.1. Последовательность действий при настройке Системы оповещения

Настройка оповещения осуществляется с помощью командлетов, входящих в состав модулей **CryptoPro.DSS.PowerShell.SignServer** и **CryptoPro.DSS.PowerShell.STS**, в зависимости от компонента для которого выполняется настройка. Оба модуля содержат однотипный набор команд для настройки оповещения. Список команд приведён в Таблица 146.

Общая схема настройки оповещения:

- Задать транспортный плагин через командлет Add-DssXXXPlugin.
- Задать плагин для формирования сообщений через командлет Add-DssXXXPlugin.
- Задать компонент для рассылки сообщений через командлет Add-DssXXXNotifier.

Здесь XXX – имя компонента, для которого настаивается оповещение: SignServer или STS.

4.9.5.2. Объекты администрирования системы оповещения

В Таблица 146 приведены основные объекты администрирования системы оповещения.

Таблица 146. Объекты администрирования системы оповещения

Командлет	Описание
Get-DssSignServerEvent Get-DssStsEvent	Вывести список событий.
Get-DssSignServerFormatterTemplate Get-DssStsFormatterTemplate	Вывести список шаблонов сообщений
Get-DssSignServerNotifier Get-DssStsNotifier	Вывести список компонентов для рассылки уведомлений.
Get-DssSignServerPlugin Get-DssStsPlugin	Вывести список плагинов.
Set-DssSignServerEvent Set-DssStsEvent	Изменить настройки события или событий.
Set-DssSignServerFormatterTemplate Set-DssStsFormatterTemplate	Изменить шаблон сообщения.
Set-DssSignServerNotifier Set-DssStsNotifier	Изменить настройки компонента для рассылки уведомлений.
Set-DssSignServerPlugin Set-DssStsPlugin	Изменить настройки плагина.
Remove-DssSignServerNotifier Remove-DssStsNotifier	Удалить компонент для рассылки уведомления.
Remove-DssSignServerPlugin Remove-DssStsPlugin	Удалить плагин.
Add-DssSignServerNotifier Add-DssStsNotifier	Добавить компонент для рассылки уведомления.
Add-DssSignServerPlugin Add-DssStsPlugin	Добавить плагин.
Enable-DssSignServerNotifier Enable-DssStsNotifier	Включить компонент для рассылки уведомлений.
Disable-DssSignServerNotifier Disable-DssStsNotifier	Отключить компонент для рассылки уведомлений.

4.9.5.3. Настройка плагинов

4.9.5.3.1. Командлет Add-DssSignServerPlugin

Данный командлет используется для добавления транспортного плагина или плагина для форматирования сообщений. Описание параметров команды приведено в Таблица 147.

Синтаксис:

```
Add-DssSignServerPlugin -PluginTypeName <string> -PluginType <string> {SMS |
Email | Formatter} -Settings <hashtable> [-DisplayName <string>]
```

Таблица 147. Описание параметров командлета Add-DssSignServerPlugin

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра компонента
PluginTypeName	string	Полное имя типа, реализующего плагин. Имя должно иметь вид: <full class name>,<assembly name>
PluginType	string	Тип плагина: SMS – плагин для рассылки сообщений по SMS. Email – плагин для рассылки сообщений по электронной почте. Formatter – плагин для формирования текста сообщений.
Settings	hashtable	Настройки плагина.

Настройки, задаваемые через параметр Settings, специфичны для каждого плагина. О настройке SMS-плагинов, включённых в установку DSS, можно прочитать в разделе 4.9.5.4, о настройке Email-плагинов – в разделе 4.9.5.6.

В установку КриптоПро DSS входит несколько плагинов для формирования сообщений:

- Плагин для формирования SMS сообщений.
- Плагин для формирования Email сообщений.
- Плагин для формирования сообщений журнала Аудита.

Ниже приводится примерный ысписок команд для регистрации плагина для формирования SMS и Email сообщений:

```
Add-DSSSignServerPlugin -PluginTypeName
"CryptoPro.DSS.MessageFormatter.SMSFormatter,DSS.MessageFormatter" -
PluginType Formatter -Settings @{Header="Крипто-Про DSS."}
```

```
Add-DSSSignServerPlugin -PluginTypeName
"CryptoPro.DSS.MessageFormatter.EmailFormatter,DSS.MessageFormatter" -
PluginType Formatter -Settings @{Header="Крипто-Про DSS."}
```

4.9.5.3.2. Командлет Get-DssSignServerPlugin

Командлет для вывода на консоль информации о зарегистрированных плагинах.

Синтаксис:

```
Get-DssSignServerPlugin [-DisplayName <string>]
```

4.9.5.3.3. Командлет Set-DssSignServerPlugin

Командлет для изменения настроек зарегистрированных плагинов. Описание параметров команды приведено в

Таблица 148.

Синтаксис:

```
Set-DssStsPlugin -Settings <hashtable> -PluginID <int> [-Override] [-
DisplayName <string>]
```

Таблица 148. Описание параметров командлета Set-DssSignServerPlugin

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра компонента
PluginId	int	Идентификатор плагина.
Settings	hashtable	Настройки плагина.
Override	SwitchParameter	Параметр определяет способ сохранения настроек плагина. Если параметр задан, то будут сохранены настройки, переданные через параметр Settings. То есть старые настройки будут удалены. Если параметр не задан, то при сохранении переданные в параметре Settings настройки будут объединены с уже имеющимися настройками.

Настройки, задаваемые через параметр Settings, специфичны для каждого плагина. О настройке SMS-плагинов, включённых в установку DSS, можно прочитать в разделе 4.9.5.4, о настройке Email-плагинов – в разделе 4.9.5.6.

4.9.5.3.4. Командлет Remove-DssSignServerPlugin

Командлет для удаления зарегистрированного плагина. Описание параметров команды приведено в Таблица 149.

Синтаксис:

```
Remove-DssSignServerPlugin -PluginID <int> [-DisplayName <string>]
```

Таблица 149. Описание параметров командлета Remove-DssSignServerPlugin

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра компонента

Параметр	Тип	Описание
PluginId	int	Идентификатор плагина.

4.9.5.4. Настройка компонентов для рассылки сообщений

4.9.5.4.1. Командлет Add-DssSignServerNotifier

Командлет для добавления компонента для рассылки сообщений. Описание параметров команды приведено в Таблица 150.

Синтаксис:

```
Add-DssSignServerNotifier -TransportPluginID <int> -FormatterPluginID <int> -
NotifierType <string> {SMS | Email} [-Settings <hashtable>] [-DisplayName
<string>]
```

Таблица 150. Описание параметров командлета Add-DssSignServerNotifier

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра компонента
TransportPluginID	int	Идентификатор транспортного плагина.
FormatterPluginID	int	Идентификатор плагина для формирования сообщений.
NotifierType	string	Тип компонента для рассылки сообщений. Значение должно быть согласовано с типом транспортного плагина. SMS – компонент для рассылки сообщений по SMS. Email – компонент для рассылки сообщений по электронной почте.
Settings	String	Настройки компонента.

Параметр **Settings** является опциональным. Рекомендуется оставить его настройки по умолчанию. Ниже приводится список настроек, которые можно задать через параметр **Settings**:

- **MinQueueSize** – приемлемый размер очереди сообщений. При превышение заданного значения обработчики будут забирать сообщения из очереди без паузы до момента уменьшения размера очереди ниже данного значения. По умолчанию параметр равен 100.

- **MaxQueueSize** – максимальный размер очереди. При достижении максимального размера очереди отправка новых сообщений блокируется, до момента снижения размера очереди ниже данного значения. По умолчанию параметр равен 10000.
- **TimerInterval** – интервал времени опроса очереди сообщений.
- **TTL** – количество повторных попыток отправки сообщения, при возникновении ошибок. По умолчанию параметр равен 3.
- **MessageWindow** – количество сообщений, забираемых из очереди для отправки за один раз. По умолчанию параметр равен 1.
- **ThreadCount** – количество обработчиков очереди сообщений. По умолчанию равен 1.
- **Enabled** – состояние компонента для рассылки сообщений: включен/отключен.

4.9.5.4.2. Командлет Get-DssSignServerNotifier

Командлет для вывода на консоль информации о зарегистрированных компонентах для рассылки уведомлений.

Синтаксис:

```
Get-DSSSignServerNotifier [-DisplayName <string>]
```

4.9.5.4.3. Командлет Set-DssSignServerNotifier

Командлет для изменения настроек компонента для рассылки уведомлений. Описание параметров команды приведено в Таблица 151.

Синтаксис:

```
Set-DssSignServerNotifier -NotifierID <int> [-Settings <hashtable>] [-
DisplayName <string>]
```

Таблица 151. Описание параметров командлета Set-DssSignServerPlugin

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра компонента
NotifierID	int	Идентификатор компонента для рассылки уведомлений.
Settings	hashtable	Настройки плагина.
Override	SwithParameter	Флаг, отвечающий за режим записи настроек. По умолчанию настройки объединяются.

Список настроек, задаваемых через параметр Settings, описан в разделе 4.9.5.4.1.

4.9.5.4.4. Командлет Remove-DssSignServerNotifier

Командлет для удаления зарегистрированного компонента для рассылки уведомлений. Описание параметров команды приведено в Таблица 152.

Синтаксис:

```
Remove-DssSignServerNotifier -NotifierID <int> [-DisplayName <string>]
```

Таблица 152. Описание параметров командлета Remove-DssSignServerPlugin

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра компонента
NotifierID	int	Идентификатор компонента для рассылки уведомлений.

4.9.5.4.5. Командлет Enable-DssSignServerNotifier

Командлет для включения компонента для рассылки уведомлений. Описание параметров команды приведено в Таблица 153.

Синтаксис:

```
Enable-DssSignServerNotifier -NotifierID <int> [-DisplayName <string>]
```

Таблица 153. Описание параметров командлета Enable-DssSignServerPlugin

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра компонента
NotifierID	int	Идентификатор компонента для рассылки уведомлений.

4.9.5.4.6. Командлет Disable-DssSignServerNotifier

Командлет для отключения компонента для рассылки уведомлений. Описание параметров команды приведено в Таблица 154.

Синтаксис:

```
Disable-DssSignServerNotifier -NotifierID <int> [-DisplayName <string>]
```

Таблица 154. Описание параметров командлета Disable-DssSignServerPlugin

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра компонента
NotifierID	int	Идентификатор компонента для рассылки уведомлений.

4.9.5.5. Настройка уведомлений по SMS

Для отправки оповещений КриптоПро DSS использует специальные SMS-плагины. SMS-плагин представляет собой сборку .NET (см. Руководство разработчика). В состав СЭП «КриптоПро DSS» входят следующие плагины:

- DSS.SmsService.StubPlugin.dll
- DSS.SmsService.DevinoSms.dll

- DSS.SmsService.MtsSms.dll
- DSS.SmsService.SmppPlugin.dll

Все плагины устанавливаются в папку <Путь установки>\DSS\Plugins\Sms.

Перед использованием плагина Администратор должен зарегистрировать плагин (см. раздел 4.9.5.3.1).

4.9.5.5.1. Плагин DSS.SmsService.StubPlugin

Данный плагин предназначен для использования в тестовых целях. Тестовый плагин записывает содержимое SMS сообщения в текстовые файлы без их отправки. Папка, в которую сохраняются файлы, задаётся параметром **WorkingDirectory**. Предварительно необходимо дать права на запись в данную директорию для Пользователя **IIS AppPool\CryptoProDSS-1-STS** и/или **IIS AppPool\CryptoProDSS-1-SignServer.**

Параметры, задаваемые при регистрации, перечислены в Таблица 155.

Таблица 155. Параметры плагина StubPlugin

Наименования параметра	Описание	Значение по умолчанию	Обязательный
WorkingDirectory	Путь к папке для сохранения файлов с текстом SMS сообщений.	<Путь установки>\DSS\<имя компонента>\fakesms, где имя компонента принимает занчения: SignServer - для сообщений, отправленных Сервисом Подписи, STS – для сообщений, отправленных Центром Идентификации	Нет

Тип плагина, указываемый при регистрации в командлете Add-DSSSignServerPlugin в параметре PluginTypeName: **CryptoPro.DSS.SmsService.StubPlugin.SmsStub,DSS.SmsService.StubPlugin**

4.9.5.5.2. Плагин DSS.SmsService.DevinoSms

Данный плагин предназначен для работы со службой рассылки SMS http://ws.devinosms.com/SmsService.asmx. Параметры, задаваемые при регистрации, перечислены в Таблица 156.

Названия параметров регистрозависимы.

Таблица 156. Параметры плагина DevinoSms

Наименования параметра	Описание	Значение по умолчанию	Обязательный
login	Логин для доступа к услуге	Нет	Да

Наименования параметра	Описание	Значение по умолчанию	Обязательный
password	Пароль для доступа к услуге.	Нет	Да
sourceaddress	Подпись отправителя. Данное значение будет подставлено вместо номера отправителя.	null	Да

Тип плагина, указываемый при регистрации в командлете Add-DSSSignServerPlugin в параметре PluginTypeName: **CryptoPro.DSS.SmsService.DevinoSms.DevinoSmsPlugin,DevinoSmsPlugin**

4.9.5.5.3. Плагин DSS.SmsService.MtsSms

Данный плагин предназначен для работы со службой рассылки SMS http://mcommunicator.ru. Параметры, задаваемые при регистрации, перечислены в Таблица 157.

Таблица 157. Параметры плагина МТС

Наименования параметра	Описание	Значение по умолчанию	Обязательный
login	Логин для доступа к услуге (представляет из себя номер телефона в формате 7XXXXXXXXXX)	Нет	Да
password	Пароль для доступа к услуге. В качестве значения можно указать пароль в открытом виде, либо MD5-хэш от пароля (определяется параметром passwordFormat)	Нет	Да
passwordFormat	Параметр определяет вид пароля, указанного в качестве значения параметра password. Может принимать два значения: raw – пароль указан в открытом виде, hashed – указано значение MD5 функции хэширования от пароля.	raw	Нет
sourceAddress	Подпись отправителя. Данное значение будет подставлено вместо номера отправителя. При использовании «Подписи отправителя» необходимо указывать подпись в точности как она была подключена (с учетом регистра).	null	Нет

Наименования параметра	Описание	Значение по умолчанию	Обязательный
serviceAddress	Адрес сервиса отправки SMS (необходим для задания адреса для доступа к сервису отличного от http://www.mcommunicator.ru/m2m/m2m_api.asmx)	http://www.mcommunicator.ru/m2m/m2m_api.asmx	Нет

Если параметр необязательный, то его можно не указывать, в этом случае будет использоваться значение по умолчанию.

Если не указывать параметр **sourceAddress**, то сообщения будут приходить с номера **4938** (сообщения будут приходить с указанного номера, даже если параметр задан, но не подключена соответствующая услуга).

Если задать параметр **sourceAddress** равным **79857707575**, то сообщения будут отправлены с федерального номера.

Тип плагина, указываемый при регистрации в командлете Add-DSSSignServerPlugin в параметре PluginTypeName: **CryptoPro.DSS.SmsService.MtsSms.MtsSmsPlugin,DSS.SmsService.MtsSms**

4.9.5.5.4. Плагин DSS.SmsService.SmppPlugin

Данный плагин предназначен для работы со службой рассылки SMS по протоколу SMPP. Параметры, задаваемые при регистрации, перечислены в Таблица 158.

Таблица 158. Параметры плагина SMPP

Наименования параметра	Описание	Значение по умолчанию	Обязательный
ServiceAddress	Адрес SMPP сервера	Нет	Да
ServicePort	Порт доступа к серверу SMPP	Нет	Да
SystemId	Логин для доступа к сервису	Нет	Да
SystemPassword	Пароль для доступа к сервису	Нет	Да
Source	Адрес отправителя	null	Нет

Тип плагина, указываемый при регистрации в командлете Add-DSSSignServerPlugin в параметре PluginTypeName: **CryptoPro.DSS.SmsService.SmppPlugin.SmppPlugin,DSS.SmsService.SmppPlugin**

4.9.5.5.5. Настройка плагина для формирования SMS-сообщений

При формировании SMS-сообщения используется специальный плагин – его задача состоит в создании текста сообщения на основе информации о выполняемом действии, подписываемом документе, одноразовом пароле и т.п. Для настройки плагина используется команды Add-DssSignServerPlugin, Set-DssSignServerPlugin.

В состав Сервиса Подписи входит плагин DSS.MessageFormatter. Его параметры представлены в Таблица 159.

Таблица 159. Параметры форматера SMS сообщений

Наименования параметра	Описание	Значение по умолчанию	Обязательный
HEADER	Заголовок сообщения. Общая часть всех SMS сообщений.	Null	Нет
XSLT	XSLT преобразование, которое следует применить над форматированным текстом, содержащим информацию о документе	Преобразование по умолчанию	Нет
XSLT_FILE	Имя файла, содержащего XSLT преобразование	Null	Нет

Плагин формирует текст SMS-сообщения на основе информации о документе. Информация о документе может представлять собой форматированный и неформатированный текст. Под форматированным тестом подразумевается некоторое XML-представление документа, к которому можно применить XSLT-преобразование.

По умолчанию используется следующее преобразование:

```
<?xml version='1.0'?>
<xsl:stylesheet version="1.0"
xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
  <xsl:output method="text"/>
  <xsl:template match="/">
    <xsl:apply-templates select="//row"/>
  </xsl:template>
  <xsl:template match="row">
    <xsl:value-of select="name"/>
    <xsl:text>: </xsl:text>
    <xsl:value-of select="value"/>
    <xsl:if test="position()!=last()">
      <xsl:text>, </xsl:text>
    </xsl:if>
    <xsl:if test="position()=last()">
      <xsl:text>.</xsl:text>
    </xsl:if>
  </xsl:template>
</xsl:stylesheet>
```

Неформатированный текст добавляется в SMS сообщение без изменений.

Тип плагина, указываемый при регистрации в командлете Add-DSSSignServerPlugin в параметре PluginTypeName: **CryptoPro.DSS.MessageFormatter.SMSFormatter,DSS.DSS.MessageFormatter**

4.9.5.5.6. Пример настройки оповещения по SMS

Пример демонстрирует настройку компонента оповещения через тестовый SMS плагин. Сообщения, отправляемые через тестовый плагин, будут сохранятся в файлы в указанной при настройке директории.

```
# Директория для сохранения файлов с сообщениями
$SMSBaseDir = "C:\tempsms\"

Write-Host "Добавление плагина для отправки СМС-сообщений"
Add-DSSSignServerPlugin -PluginTypeName
"CryptoPro.DSS.SmsService.StubPlugin.SmsStub,DSS.SmsService.StubPlugin" -
PluginType SMS -Settings @{"WorkingDirectory" = $SMSBaseDir}

Write-Host "Добавление плагина для форматирования СМС-сообщений"
Add-DSSSignServerPlugin -PluginTypeName
"CryptoPro.DSS.MessageFormatter.SMSFormatter,DSS.MessageFormatter" -
PluginType Formatter -Settings @{Header="Крипто-Про DSS."}

Write-Host "Добавление модуля оповещения для отправки СМС-сообщений"
Add-DSSSignServerNotifier -TransportPluginID 1 -FormatterPluginID 2 -
NotifierType SMS -Settings
@{"MinQueueSize"="0";"MaxQueueSize"="10000";"TimerInterval"="500";"TTL"="1";"
MessageWindow"="50";"ThreadCount"="1";"Enabled"="true"}
```

4.9.5.6. Настройка уведомлений по Email

Для отправки оповещений по электронной почте DSS использует специальные Email-плагины. Email-плагин представляет собой сборку .NET (см. Руководство разработчика). В состав СЭП «КриптоПро DSS» входят следующие плагины:

- DSS.EmailService.SmtpPlugin.dll

  Все плагины устанавливаются в папку **<Путьустановки>\DSS\Plugins\Email.**

Перед использованием плагина Администратор должен зарегистрировать плагин (см. раздел 4.9.5.3.1).

4.9.5.6.1. Плагин DSS.EmailService.SmtpPlugin

Параметры, задаваемые при регистрации, перечислены в Таблица 160. Параметры плагина SmtpPlugin.

Таблица 160. Параметры плагина SmtpPlugin

Наименования параметра	Описание	Значение по умолчанию	Обязательный
Host	Адрес SMTP-сервера.		Да

Наименования параметра	Описание	Значение по умолчанию	Обязательный
Port	Порт SMTP-сервера		Да
Login	Логин для доступа к серверу		Нет
Password	Пароль для доступа к серверу		Нет
FromAddress	Адрес отправителя		Да
Subject	Тема сообщения по умолчанию		Нет
RequireSsl	Требуется ли SSL соединение для доступа к серверу	По умолчанию false	Нет
Timeout	Время истечения ожидания при отправке сообщения в милисекундах.	По умолчанию 30 секунд	Нет

Тип плагина, указываемый при регистрации в командлете Add-DSSSignServerPlugin в параметре PluginTypeName:

CryptoPro.DSS.EmailService.SmtpPlugin.SmtpPlugin,DSS.EmailService.SmtpPlugin.

4.9.5.6.2. Настройка плагина для формирования Email-сообщений

При формировании Email-сообщения используется специальный плагин – его задача состоит в создании текста сообщения на основе информации о выполняемом действии, подписываемом документе, одноразовом пароле и т.п. Для настройки плагина используется команды Add-DssSignServerPlugin, Set-DssSignServerPlugin.

Настройки данного плагина аналогичны настройкам плагина для формирования SMS сообщений.

Тип плагина, указываемый при регистрации в командлете Add-DSSSignServerPlugin в параметре PluginTypeName: **CryptoPro.DSS.MessageFormatter.EmailFormatter,DSS.DSS.MessageFormatter**

4.9.5.6.3. Пример настройки оповещения по Email

```
# Регистрируем транспортный плагин для отправки Email сообщений
Add-DssStsPlugin -PluginTypeName
“CryptoPro.DSS.EmailService.SmtpPlugin.SmtpPlugin,DSS.EmailService.SmtpPlugin
” -PluginType Email -Settings @{“Host”=”mail_server”; “Port”=”25”;
“FromAddress”=”noreply@some_domain.com”; “RequireSsl”=”true” }

# Регистрируем плагин для формирования сообщений
Add-DssStsPlugin -PluginTypeName
“CryptoPro.DSS.MessageFormatter.EmailFormatter,DSS.MessageFormatter” -
PluginType Formatter -Settings @{}
```

```
# Регистрируем компонент для отаравки Email сообщений.
# Идентификаторы транспортного плагина и плагина для формирования сообщений
# можно посмотреть в выводе командлет Get-DssStsPlugin
Add-DssStsNotifier -TransportPluginID <Transport_Plugin_ID> -
FormatterPluginID <Formatter_Plugin_ID> -NotifierType Email
```

4.9.5.7. Настройка шаблонов сообщений

4.9.5.7.1. Последовательность шагов при настройке шаблонов сообщений

Стандартные тексты шаблонов сообщений, приведенные в разделах 4.9.1–4.9.3, можно изменить. Для этого необходимо выполнить следующую последовательность действий:

3. Выберите событие, текст которого хотите изменить. Списки событий представлены в таблицах разделов 4.9.1–4.9.3, либо выводятся на консоль командлетами **Get-DssSignServerEvent** и **Get-DssStsEvent** (см. раздел 4.9.4).
4. Определите ID события (параметр ID в выводе на консоль) и выберите идентификатор шаблона оповещения о событии (один из шаблонов, если их несколько), который хотите изменить. Идентификатор шаблона(-ов) оповещения содержится в параметре **MessageTemplates** в выводе на консоль. Просмотреть свойства шаблонов, если их несколько, можно при помощи команды `(Get-DssStsEvent -EventID <идентификатор шаблона>).MessageTemplates`.
5. Используя командлет **Set-DSSSignServerFormatterTemplate,** задайте в параметре **–Template** новый текст сообщения о событии, указав также в параметре **–TemplateID** идентификатор выбранного шаблона оповещения.

4.9.5.7.2. Командлет Get-DSSSignServerFormatterTemplate

Командлет для вывода на консоль информации о шаблонах сообщений.

Синтаксис:

```
Get-DSSSignServerFormatterTemplate [-DisplayName <string>]
```

4.9.5.7.3. Командлет Set-DSSSignServerFormatterTemplate

Командлет для изменения шаблона сообщения о событии. Описание параметров команды приведено в Таблица 161.

Синтаксис:

```
Set-DSSSignServerFormatterTemplate -TemplateID <int> -Template <string> [-
DisplayName <string>]
```

Таблица 161. Описание параметров командлета Set-DSSSignServerFormatterTemplate

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра компонента

Параметр	Тип	Описание
TemplateID	int	Идентификатор шаблона сообщения.
Template	string	Шаблон сообщения.

4.9.5.8. Пример настройки системы оповещения

Пример демонстрирует настройку компонента оповещения через тестовый SMS-плагин. Сообщения, отправляемые через тестовый плагин, будут сохранятся в файлы в указанной при настройке директории.

```
# Директория для сохранения файлов с сообщениями
$SMSBaseDir = "C:\tempsms\"

Write-Host "Добавление плагина для отправки СМС-сообщений"
Add-DSSSignServerPlugin -PluginTypeName
"CryptoPro.DSS.SmsService.StubPlugin.SmsStub,DSS.SmsService.StubPlugin" -
PluginType SMS -Settings @{"WorkingDirectory" = $SMSBaseDir}

Write-Host "Добавление плагина для форматирования СМС-сообщений"
Add-DSSSignServerPlugin -PluginTypeName
"CryptoPro.DSS.MessageFormatter.SMSFormatter,DSS.MessageFormatter" -
PluginType Formatter -Settings @{Header="Крипто-Про DSS."}

Write-Host "Добавление модуля оповещения для отправки СМС-сообщений"
Add-DSSSignServerNotifier -TransportPluginID 1 -FormatterPluginID 2 -
NotifierType SMS -Settings
@{"MinQueueSize"="0";"MaxQueueSize"="10000";"TimerInterval"="500";"TTL"="1";"
MessageWindow"="50";"ThreadCount"="1";"Enabled"="true"}
```

4.10. Преобразование документов

В КриптоПро DSS документы, которые Пользователь загружает для подписи или шифрования, могут быть визуализированы. Для этого используются плагины преобразования документов. Преобразование документов может происходить на следующих компонентах КриптоПро DSS в зависимости от выполняемой операции:

- на Веб-интерфейсе Пользователя (визуализация документов при подписании или шифровании, отображение документов формата XML);
- на Центре Идентификации (используются для отображения документа в мобильном приложении myDSS).

Далее описаны настройки для визуализации документов в каждом из перечисленных случаев.

4.10.1. Визуализация документов при подписании на Веб-интерфейсе Пользователя

Веб-интерфейс Пользователя предоставляет Пользователям возможность визуализации документов перед созданием подписи. Поддерживается просмотр документов следующих форматов: PDF, XML, ODT.

Также обеспечивается техническая поддержка форматов DOC, DOT, DOCM, DOTM, DOCX, DOTX, FlatOpc, FlatOpcMacroEnabled, FlatOpcTemplate, FlatOpcTemplateMacroEnabled, OTT, OOXML, WordML, RTF, HTML, XHTML, MHTML и TXT, однако в их отношении в рамках проведения оценки влияния требуется проверять допустимость использования в конечной системе. Подробнее об этом в п. 1.5 документа ЖТЯИ.00096-02 30 01. КриптоПро HSM. Формуляр.

Настройка визуализации документов перед созданием ЭП осуществляется при помощи специальных плагинов. Чтобы воспользоваться плагином в КриптоПро DSS, его необходимо сначала зарегистрировать. Работа с плагинами визуализации документов на Веб-интерфейсе Пользователя осуществляется при помощи командлетов, описанных в **разделе 4.7.3.5.**

Плагины, позволяющие визуализировать документы данных форматов, находятся в директории **<Путь установки>\DSS\Plugins\Converters** и имеют следующие названия:

- DSS.DocumentConverter.PdfStub.dll – отвечает за отображение документов формата PDF;
- DSS.DocumentConverter.Word.dll - отвечает за отображение документов форматов DOC, DOT, DOCM, DOTM, DOCX, DOTX, FlatOpc, FlatOpcMacroEnabled, FlatOpcTemplate, FlatOpcTemplateMacroEnabled, XML, ODT, OTT, OOXML, WordML, RTF, HTML, XHTML, MHTML, TXT, PNG, JPG, BMP, JPEG, TIFF, GIF.

Для активации возможности просмотра документов необходимо зарегистрировать нужные форматы и соответствующие плагины с помощью Windows PowerShell. Для каждого экземпляра веб-приложения в директории **<Путь установки>\Frontend** создается свой собственный конфигурационный файл с именем **<Имя экземпляра веб-приложения>_convert.config.**

Пример:

Данный сценарий регистрирует форматы документов, для которых возможен просмотр с помощью установленных плагинов.

```
Add-DssFEConverterPlugin -FileExtension pdf -Assembly
DSS.DocumentConverter.PdfStub.dll

Add-DssFEConverterPlugin -FileExtension doc -Assembly
DSS.DocumentConverter.Word.dll

Add-DssFEConverterPlugin -FileExtension dot -Assembly
DSS.DocumentConverter.Word.dll

Add-DssFEConverterPlugin -FileExtension docm -Assembly
DSS.DocumentConverter.Word.dll

Add-DssFEConverterPlugin -FileExtension dotm -Assembly
DSS.DocumentConverter.Word.dll

Add-DssFEConverterPlugin -FileExtension docx -Assembly
DSS.DocumentConverter.Word.dll

Add-DssFEConverterPlugin -FileExtension dotx -Assembly
DSS.DocumentConverter.Word.dll

Add-DssFEConverterPlugin -FileExtension FlatOpc -Assembly
DSS.DocumentConverter.Word.dll

Add-DssFEConverterPlugin -FileExtension FlatOpcMacroEnabled -Assembly
DSS.DocumentConverter.Word.dll

Add-DssFEConverterPlugin -FileExtension FlatOpcTemplate -Assembly
DSS.DocumentConverter.Word.dll

Add-DssFEConverterPlugin -FileExtension FlatOpcTemplateMacroEnabled -Assembly
DSS.DocumentConverter.Word.dll

Add-DssFEConverterPlugin -FileExtension xml -Assembly
DSS.DocumentConverter.Word.dll

Add-DssFEConverterPlugin -FileExtension odt -Assembly
DSS.DocumentConverter.Word.dll

Add-DssFEConverterPlugin -FileExtension ott -Assembly
DSS.DocumentConverter.Word.dll

Add-DssFEConverterPlugin -FileExtension ooxml -Assembly
DSS.DocumentConverter.Word.dll

Add-DssFEConverterPlugin -FileExtension WordML -Assembly
DSS.DocumentConverter.Word.dll

Add-DssFEConverterPlugin -FileExtension rtf -Assembly
DSS.DocumentConverter.Word.dll

Add-DssFEConverterPlugin -FileExtension html -Assembly
DSS.DocumentConverter.Word.dll

Add-DssFEConverterPlugin -FileExtension xhtml -Assembly
DSS.DocumentConverter.Word.dll

Add-DssFEConverterPlugin -FileExtension mhtml -Assembly
DSS.DocumentConverter.Word.dll
```

```
Add-DssFEConverterPlugin -FileExtension txt -Assembly
DSS.DocumentConverter.Word.dll

Add-DssFEConverterPlugin -FileExtension png -Assembly
DSS.DocumentConverter.Image.dll

Add-DssFEConverterPlugin -FileExtension jpg -Assembly
DSS.DocumentConverter.Image.dll

Add-DssFEConverterPlugin -FileExtension bmp -Assembly
DSS.DocumentConverter.Image.dll

Add-DssFEConverterPlugin -FileExtension jpeg -Assembly
DSS.DocumentConverter.Image.dll

Add-DssFEConverterPlugin -FileExtension tiff -Assembly
DSS.DocumentConverter.Image.dll
```

Если просмотр загруженного документа поддерживается установленными плагинами и выполнена регистрация в конфигурационном файле, то документ отображается во вкладке «Загрузка документа». (Рис. 35).

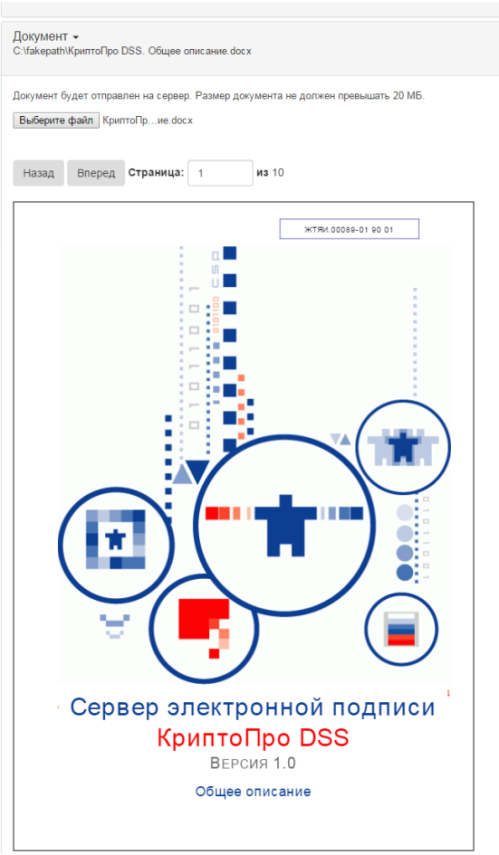

Рис. 35 – Визуализация загруженного документа

Для поддержки отображения документов особых форматов необходимо реализовать и зарегистрировать соответствующий плагин, отвечающий описанным в Руководстве разработчика требованиям.

4.10.2. Визуализация документов на мобильном приложении myDSS

Мобильное приложение myDSS имеет возможность отображать документ при подтверждении операции с этим документом. Настройка соответствующих плагинов преобразования документов осуществляется при помощи командлетов, входящих в состав PowerShell-модуля ЦИ **CryptoPro.DSS.PowerShell.STS.** Эти командлеты описаны в **разделе 4.5.7.11.**

Центр Идентификации предоставляет Пользователям возможность визуализации документов в мобильном предложении myDSS перед созданием подписи. Поддерживается просмотр документов следующих форматов: PDF, XML, ODT.

Также обеспечивается техническая поддержка форматов DOC, DOT, DOCM, DOTM, DOCX, DOTX, FlatOpc, FlatOpcMacroEnabled, FlatOpcTemplate, FlatOpcTemplateMacroEnabled, OTT, OOXML, WordML, RTF, HTML, XHTML, MHTML и TXT, однако в их отношении в рамках проведения оценки влияния требуется проверять допустимость использования в конечной системе. Подробнее об этом в п. 1.5 документа ЖТЯИ.00096-02 30 01. КриптоПро HSM. Формуляр.

Плагины, позволяющие визуализировать документы данных форматов, находятся в директории **<Путь установки>\DSS\Plugins\Converters** и имеют следующие названия:

- DSS.DocumentConverter.PdfStub.dll – отвечает за отображение документов формата PDF;
- DSS.DocumentConverter.Word.dll - отвечает за отображение документов форматов DOC, DOT, DOCM, DOTM, DOCX, DOTX, FlatOpc, FlatOpcMacroEnabled, FlatOpcTemplate, FlatOpcTemplateMacroEnabled, XML, ODT, OTT, OOXML, WordML, RTF, HTML, XHTML, MHTML, TXT, PNG, JPG, BMP, JPEG, TIFF, GIF.

Для активации возможности просмотра документов необходимо зарегистрировать нужные форматы и соответствующие плагины с помощью Windows PowerShell. Для каждого экземпляра веб-приложения в директории **<Путь установки>\Sts** создается свой собственный конфигурационный файл с именем **<Имя экземпляра веб-приложения>_convert.config.**

Если плагин преобразования настроен верно, в мобильном приложении myDSS в области «Данные операции» отобразится документ, операцию с которым требуется подтвердить (Рис. 36).

Рис. 36 – Отображение документа в мобильном приложении myDSS

Пример:

```
Add-DssSTSConverterPlugin -FileExtension pdf -Assembly
DSS.DocumentConverter.PdfStub.dll

Add-DssSTSConverterPlugin -FileExtension doc -Assembly
DSS.DocumentConverter.Word.dll

Add-DssSTSConverterPlugin -FileExtension dot -Assembly
DSS.DocumentConverter.Word.dll

Add-DssSTSConverterPlugin -FileExtension docm -Assembly
DSS.DocumentConverter.Word.dll

Add-DssSTSConverterPlugin -FileExtension dotm -Assembly
DSS.DocumentConverter.Word.dll

Add-DssSTSConverterPlugin -FileExtension docx -Assembly
DSS.DocumentConverter.Word.dll

Add-DssSTSConverterPlugin -FileExtension dotx -Assembly
DSS.DocumentConverter.Word.dll

Add-DssSTSConverterPlugin -FileExtension FlatOpc -Assembly
DSS.DocumentConverter.Word.dll

Add-DssSTSConverterPlugin -FileExtension FlatOpcMacroEnabled -Assembly
DSS.DocumentConverter.Word.dll
```

```
Add-DssSTSConverterPlugin -FileExtension FlatOpcTemplate -Assembly
DSS.DocumentConverter.Word.dll

Add-DssSTSConverterPlugin -FileExtension FlatOpcTemplateMacroEnabled -
Assembly DSS.DocumentConverter.Word.dll

Add-DssSTSConverterPlugin -FileExtension xml -Assembly
DSS.DocumentConverter.Word.dll

Add-DssSTSConverterPlugin -FileExtension odt -Assembly
DSS.DocumentConverter.Word.dll

Add-DssSTSConverterPlugin -FileExtension ott -Assembly
DSS.DocumentConverter.Word.dll

Add-DssSTSConverterPlugin -FileExtension ooxml -Assembly
DSS.DocumentConverter.Word.dll

Add-DssSTSConverterPlugin -FileExtension WordML -Assembly
DSS.DocumentConverter.Word.dll

Add-DssSTSConverterPlugin -FileExtension rtf -Assembly
DSS.DocumentConverter.Word.dll

Add-DssSTSConverterPlugin -FileExtension html -Assembly
DSS.DocumentConverter.Word.dll

Add-DssSTSConverterPlugin -FileExtension xhtml -Assembly
DSS.DocumentConverter.Word.dll

Add-DssSTSConverterPlugin -FileExtension mhtml -Assembly
DSS.DocumentConverter.Word.dll

Add-DssSTSConverterPlugin -FileExtension txt -Assembly
DSS.DocumentConverter.Word.dll

Add-DssStsConverterPlugin -FileExtension png -Assembly
DSS.DocumentConverter.Image.dll

Add-DssStsConverterPlugin -FileExtension jpg -Assembly
DSS.DocumentConverter.Image.dll

Add-DssStsConverterPlugin -FileExtension bmp -Assembly
DSS.DocumentConverter.Image.dll

Add-DssStsConverterPlugin -FileExtension jpeg -Assembly
DSS.DocumentConverter.Image.dll

Add-DssStsConverterPlugin -FileExtension tiff -Assembly
DSS.DocumentConverter.Image.dll
```

4.10.3. Отображение документов формата XML

КриптоПро DSS предоставляет Пользователям возможность отображения документов формата XML на Веб-интерфейсе Пользователя перед созданием подписи или шифрованием документа. Отображение этих документов возможно также в мобильном приложении myDSS, если на Центре Идентификации настроены соответствующие плагины (см. раздел 4.10.2). Плагин, позволяющий отобразить эту информацию,

находится в директории **<Путь установки>\DSS\Plugins\Converters** и называется **DSS.DocumentConverter.Dtbs.dll.**

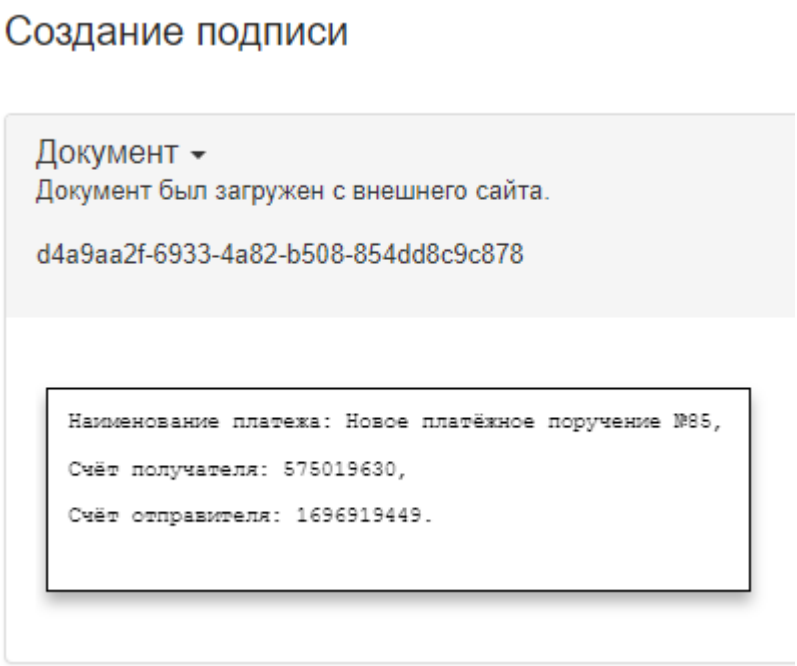

Рис. 37 - Отображение документов формата XML

Работа с плагином производится при помощи командлетов, описанных в **разделе 4.7.3.5.** При добавлении плагина необходимо также задать настройки, перечисленные в Таблица 162. Эти настройки задаются внутри параметра **Parameters** типа **Hashtable**:

```
@{paramName1=paramValue1; paramName2=paramValue2;…;paramNameN=paramValueN}
```

где **paramName$_i$**, **paramValue$_i$** – название и значение параметра соответственно.

Таблица 162. Параметры плагина DSS.DocumentConverter.Dtbs.dll

Параметр	Описание
PageSetup.LeftMargin	Отступ в документе слева.
PageSetup.TopMargin	Отступ в документе сверху.
PageSetup.RightMargin	Отступ в документе справа.
PageSetup.BottomMargin	Отступ в документе снизу.
PageSetup.PageHeight	Высота страницы документа.
PageSetup.PageWidth	Ширина страницы документа.

Параметр	Описание
PageSetup.PaperSize	Размеры отображаемого документа. Данный параметр позволяет выбрать стандартные размеры по обозначению формата из Таблица 163. Для ввода пользовательских параметров используется значение **Custom.**
PageSetup.Gutter	Расстояние между строками.
xslt	Путь к файлу с XSLT-преобразованием. Опциональный параметр.

Таблица 163. Стандартные размеры документов

Формат бумаги	Размеры
A3	297x420мм
A4	210x297мм
A5	148x210мм
B4	250x353мм
B5	176x250мм
Executive	7.25x10.5”
Folio	8x13”
Ledger	11x17”
Legal	8.5x14”
Letter	8.5x11”
EnvelopeDL	110x220мм
Quarto	8x10”
Statement	8.5x5.5”
Tabloid	11x17”
Paper10x14	10x14”
Paper11x17	11x17”

Формат бумаги	Размеры
Custom	При выборе данного размера необходимо самостоятельно задать размеры страницы при помощи параметров из Таблица 162.

Пример регистрации плагина для отображения документов формата XML:

```
Add-DssFeConverterPlugin -FileExtension dtbs -Assembly
DSS.DocumentConverter.Dtbs.dll -Parameters @{ "PageSetup.LeftMargin"="10";
"PageSetup.PageWidth"="350"; "PageSetup.TopMargin"="10";
"PageSetup.PageHeight"="100"; "PageSetup.RightMargin"="10";
"PageSetup.PaperSize"="Custom"; "PageSetup.BottomMargin"="0";
"PageSetup.Gutter"="0"}
```

Расширение, указанное в параметре **–FileExtension** при регистрации плагина, и расширение файла отображаемым документом должны совпадать.

Пример содержимого XML-файла, который необходимо отобразить:

```
<?xml version="1.0" encoding="utf-8"?>
<dtbs xmlns="http://www.cryptopro.ru/schemas/2014/08/dtbs">
    <row>
        <name>Наименование документа</name>
        <value>Платёжное поручение</value>
    </row>
    <row>
        <name>Банк получателя</name>
        <value>АКБ "Рога и копыта"</value>
    </row>
    <row>
        <name>Счёт получателя</name>
        <value>40781032100000000000</value>
    </row>
    <row>
        <name>Сумма платежа</name>
        <value>100 RUB</value>
    </row>
</dtbs>
```

Xsd-схема файла, который необходимо отобразить:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema targetNamespace="http://www.cryptopro.ru/schemas/2014/08/dtbs"
    elementFormDefault="qualified"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
```

```
    xmlns:dtbs="http://www.cryptopro.ru/schemas/2014/08/dtbs"
>
    <xs:element name="dtbs" type="dtbs:dtbsType" />
    <xs:complexType name="dtbsType">
        <xs:sequence>
            <xs:element ref="dtbs:row" minOccurs="0" maxOccurs="unbounded" />
        </xs:sequence>
        <xs:attribute name="unattendedSign" type="xs:boolean">
            <xs:annotation>
                <xs:documentation>
                    Если 'true', то документ подписывается без отображения и
                    подтверждения пользователем. В этом случае элементы row
                    должны отсутствовать.
                </xs:documentation>
            </xs:annotation>
        </xs:attribute>
    </xs:complexType>

    <xs:element name="row" type="dtbs:rowType" />
    <xs:complexType name="rowType">
        <xs:sequence>
            <xs:element name="name" type="xs:string">
                <xs:annotation>
                    <xs:documentation>
                        Название ключевого поля с XML-документом, который
необходимо отобразить
                    </xs:documentation>
                </xs:annotation>
            </xs:element>
            <xs:element name="value" type="xs:string">
                <xs:annotation>
                    <xs:documentation>
                        Значение ключевого поля с XML-документом, который
необходимо отобразить
                    </xs:documentation>
                </xs:annotation>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
</xs:schema>
```

4.11. Настройка myDSS

Модуль аутентификации myDSS для СЭП «КриптоПро DSS» является обособленной частью Центра Идентификации и позволяет подтверждать волеизъявление Пользователя на выполнение различных операций с помощью мобильного приложения, а также может применяться в качестве вспомогательной аутентификации.

Модуль аутентификации myDSS имеет следующую структуру:

1. Серверная часть

a. Сервис взаимодействия с ЦИ.

Интегрируется с ЦИ КриптоПро DSS и выполняет следующие функции:

- генерация и обновление ключевой информации Пользователей myDSS при взаимодействии с ЦИ КриптоПро DSS;
- управление процессом подтверждения операций.

b. Сервис взаимодействия с мобильным приложением myDSS.

Выполняет функции по взаимодействию с мобильными приложениями, включая:

- регистрацию устройств пользователей для отправки PUSH-уведомлений;
- отправку PUSH-уведомлений;
- предоставление информации о операциях, необходимых для подтверждения пользователем;
- прием и проверку кодов подтверждения при помощи Сервиса взаимодействия с ЦИ.

2. Клиентская часть:

Клиентская часть представлена мобильным приложением myDSS, доступным в операционных системах iOS и Android. Приложение myDSS выполняет следующие функции:

- управление ключевой информацией Пользователя (считывание, хранение, использование, обновление, удаление);
- получение информации для подтверждения от серверной части в режиме онлайн или офлайн;
- отображение подтверждаемой информации на экране мобильного телефона;
- выработка кода подтверждения на основе данных транзакции, ключа пользователя, времени выработки и (опционально) отпечатка устройства;
- отправка кода подтверждения в серверную часть в режиме онлайн или отображение пользователю в режиме офлайн.

Схема взаимодействия компонентов, отображающая описанные логические компоненты myDSS и их взаимодействие с другими компонентами и продуктами, приведена на Рис. 38.

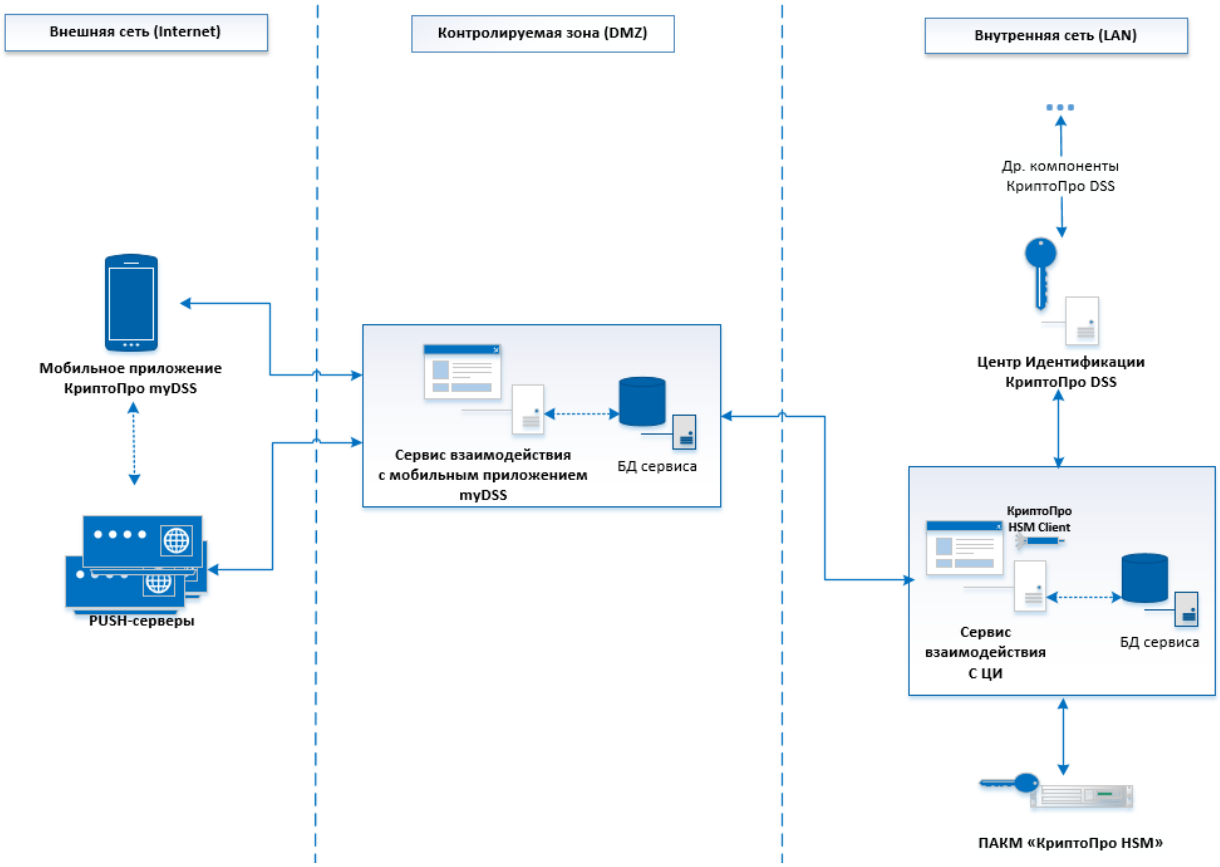

Рис. 38 - Схема взаимодействия компонентов при использовании myDSS

4.11.1. Последовательность шагов по настройке экземпляров myDSS

Данный раздел Руководства Администратора определяет последовательность и порядок действий по разворачиванию и настройке экземпляров модуля аутентификации myDSS в режиме «с нуля».

Предварительные условия:

- Установленный SQL-Server;
- Установленная роль Сервер приложений (IIS);
- Настроенная привязка https на сервере приложений (IIS);
- Установленный и настроенный экземпляр ЦИ КриптоПро DSS (см. Раздел 4.5);
- Доступность адресов PUSH-серверов с сервера, где будет разворачиваться экземпляр Сервиса взаимодействия с мобильным приложением myDSS.

Возможные PUSH-серверы:

- Firebase Cloud Messaging Server.
  URL: **https://fcm.googleapis.com/fcm/send**

- Apple Push Notification Service.
  Необходимо открыть доступ TCP на
  gateway.push.apple.com:2195
  И
  feedback.push.apple.com:2196

Для отправки PUSH-уведомлений на устройства Apple требуется **сертификат с клиентской аутентификацией** на Apple Push Notification Service. Получить данный сертификат можно по запросу на mydss@cryptopro.ru.

Для отправки PUSH-уведомлений на устройства Android требуется получить **ключ доступа** к Firebase Cloud Messaging Server. Получить данный ключ можно по запросу на mydss@cryptopro.ru.

Базовая последовательность шагов по настройке (обязательные):

1. Создание экземпляра Сервиса взаимодействия с ЦИ (см. раздел 4.11.4.2.1).

На данном шаге будет создано веб-приложение на сервере приложений IIS, развёрнуты базы данных, зарегистрированы журналы Windows.

2. Создание экземпляра Сервиса взаимодействия с мобильным приложением myDSS (см. раздел 4.11.4.3.1).

На данном шаге будет создано веб-приложение на сервере приложений IIS, развёрнуты базы данных, зарегистрированы журналы Windows.

Необходимо переключить в режим автоматического запуска службу **КриптоПро myDSS (External Service).**

3. Регистрация криптопровайдеров (см. раздел 4.6.3.3).

На данном шаге в экземпляре Сервиса взаимодействия с ЦИ регистрируется криптопровайдер, который используется для выработки векторов аутентификации Пользователей.

4. Регистрация Мастер-ключа, используемого для выработки вектора аутентификации. Регистрация производится при помощи комадлета Set-MyDssServerInternalProperties.

5. Настройка Сервиса взаимодействия с ЦИ.

На данном шаге выполняется настройка экземпляра Сервиса взаимодействия с ЦИ. Настройка осуществляется при помощи командлета Set-MyDssServerInternalProperties. Данный шаг состоит из следующих этапов:

- Задание адреса сервиса рассылки PUSH-уведомлений. Настройка производится при помощи командлета Set-MyDssServerInternalProperties.
- Задание адреса сервиса, с которым связывается мобильное приложение. Настройка производится при помощи командлета Set-MyDssServerInternalProperties.

Адрес сервиса, с которым связывается мобильное приложение, должен быть доступен из сети Интернет.

- Задание адреса ЦИ КриптоПро DSS. Настройка данного этапа происходит при помощи командлета Set-DssMobileAuthProperties.

6. Настройка Сервиса взаимодействия с мобильным приложением myDSS.

На данном шаге выполняется настройка экземпляра Сервиса взаимодействия с мобильным приложением myDSS. Данный шаг состоит из задания адреса Сервиса взаимодействия с ЦИ. Настройка осуществляется при помощи командлета Set-MyDssInteractionServiceProperties.

4.11.2. Пример PowerShell-сценария для настройки компонента myDSS

Данный сценарий выполняет минимально необходимую настройку экземпляров серверов myDSS внешнего и внутреннего взаимодействия.

```
# Создание экземпляра Сервиса взаимодействия с ЦИ
New-MyDssServerInternalInstance -SiteName "Default Web Site" -SQLServerName
".\SQLEXPRESS2012" -DisplayName InternalService


# Создание экземпляра Сервиса взаимодействия с мобильным приложением myDSS
New-MyDssServerExternalInstance -SiteName "Default Web Site" -SQLServerName
".\SQLEXPRESS2012" -DisplayName ExternalService


# Добавление криптопровайдера
Add-MyDssServerInternalCryptoProviders -TypeId <Common> -ProviderName
"Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider" -ProviderType
75


#Получение информации о зарегистрированном криптопровайдере с целью
определения его идентификатора
Get-MyDssServerInternalCryptoProviders


#Регистрация Мастер-ключа, используемого для выработки вектора аутентификации
Set-MyDssServerInternalProperties -CryptoProviderId <Id криптопровайдера>
```

```
#Задание адреса сервиса рассылки PUSH-уведомлений
Set-MyDssServerInternalProperties -InteractionPushServiceAddress "http://
<hostname>/MyDssServerExternal/InteractionPushService.svc"


#Задание адреса Сервиса взаимодействия с мобильным приложением myDSS
Set-MyDssServerInternalProperties -InteractionServiceAddress
"http://<hostname>/MyDssServerExternal/InteractionService.svc"


#Получение списка настроенных параметров Сервиса взаимодействия с ЦИ
Get-MyDssServerInternalProperties


#Задание адреса Сервиса взаимодействия с ЦИ
Set-MyDssInteractionServiceProperties -InteractionService -ServiceAddress
"http://<hostname>/MyDssServerInternal/Service.svc"


#Задание на ЦИ КриптоПро DSS адреса Сервиса взаимодействия с ЦИ
Set-DssMobileAuthProperties -DisplayName <Имя экземпляра ЦИ> -ServiceAddress
"http://<hostname>/MyDssServerInternal/service.svc"
```

Зарегистрированное имя провайдера в системе предопределено заранее. Его можно увидеть в документации поставщика криптопровайдера. Для продуктов КриптоПро:

- КриптоПро HSM: **Crypto-Pro HSM Svc CSP**
- КриптоПро CSP (только для тестирования КриптоПро DSS): **Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider**

Модуль аутентификации myDSS может оповещать интегрируемую систему о результате подтверждения операции в мобильном приложении, отправляя в интегрируемую систему соответствующие сообщения. Для настройки такого оповещения необходимо зарегистировать сооветствующие плагины (транспортный и форматирования) и модуль оповещения.

```
#Настройка транспортного плагина
Add-DssStsPlugin -PluginTypeName
"CryptoPro.DSS.Identity.Authentication.Notification.HttpTransportPlugin,Crypt
oPro.DSS.Identity.Authentication.Notification" -PluginType
AuthenticationResult -Settings @{}


#Настройка плагина форматирования
Add-DssStsPlugin -PluginTypeName
"CryptoPro.DSS.Identity.Authentication.Notification.AuthenticationResultForma
tter,CryptoPro.DSS.Identity.Authentication.Notification" -PluginType
Formatter -Settings @{}


#Добавление модуля оповещения
Add-DssStsNotifier -TransportPluginID <ID транспортного плагина> -
FormatterPluginID <ID плагина форматирования> -NotifierType
AuthenticationResultCallback -Settings @{}
```

ID плагинов присваиваются автоматически после их добавления.

4.11.3. Объекты администрирования

На Рис. 27 приведена схема объектов, доступных для администрирования в myDSS.

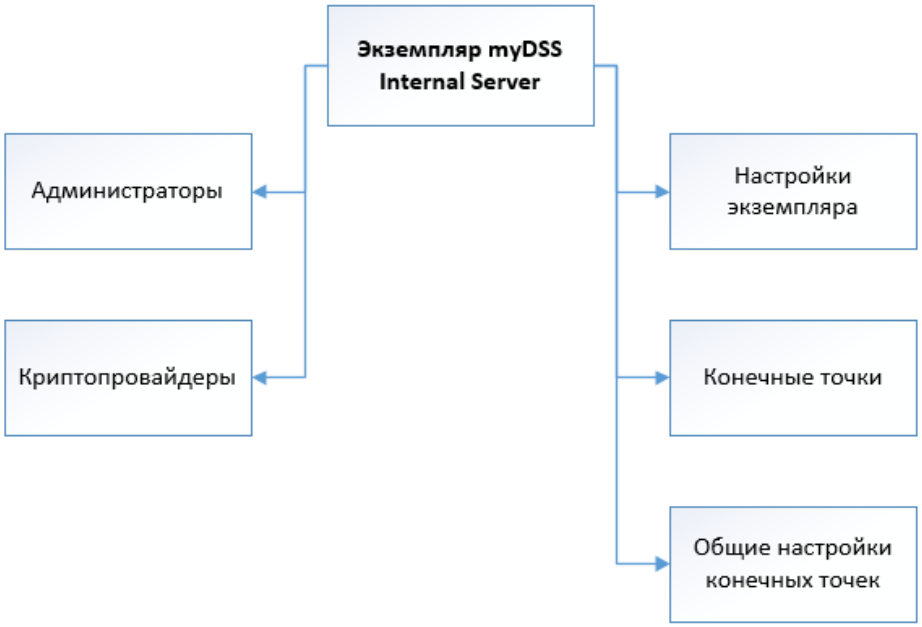

Рис. 39 – Объекты администрирования Сервиса взаимодействия с ЦИ

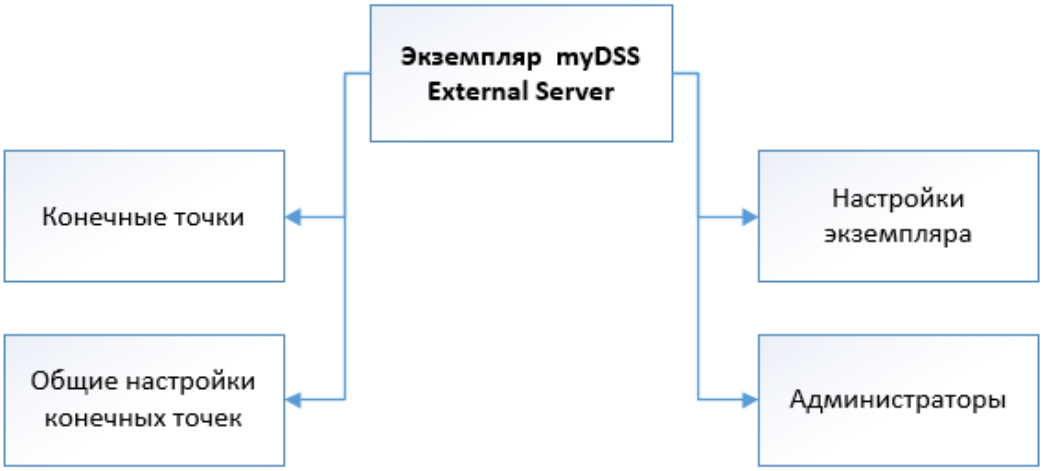

Рис. 40 – Объекты администрирования Сервиса взаимодействия с мобильным приложением myDSS

Таблица 164. Объекты администрирования myDSS Internal Server

Объект администрирования	Командлеты	Описание
Администраторы	Add-MyDssInternalAdministrator Get-MyDssInternalAdministrator Remove-MyDssInternalAdministrator	Объект отвечает за управление учетными записями Администраторов, имеющих доступ к БД myDSS Internal Server. (См. раздел 4.3.4.1).
Экземпляр myDSS Internal Server	New-MyDssServerInternalInstance Remove-MyDssServerInternalInstance Update-MyDssServerInternalInstance Get-MyDssServerInternalInstance	Объект «Экземпляр» отвечает за управление экземплярами myDSS External Server.
Настройки экземпляра	Set-MyDssServerInternalRegistryProperties Get-MyDssServerInternalRegistryProperties Set-MyDssServerInternalProperties Get-MyDssServerInternalProperties	Объект «Настройки экземпляра» отвечает за настройку строки подключения к базе данных и редактирование свойств экземпляра.
Криптопровайдеры	Add-MyDssServerInternalCryptoProviders Get-MyDssServerInternalCryptoProviders Set-MyDssServerInternalCryptoProviders Copy-MyDssServerInternalCryptoProviders Enable-MyDssServerInternalCryptoProviders Disable-MyDssServerInternalCryptoProviders Remove-MyDssServerInternalCryptoProviders Test-MyDssServerInternalCryptoProviders	Объект «Криптопровайдеры» отвечает за управление закрытыми ключами myDSS при взаимодействии с ПАКМ «КриптоПро HSM». Настройки идентичны настройкам криптопровайдеров на Сервисе Подписи (См. Раздел 4.6.3.3).
Конечные точки	Enable-MyDssServerInternalEndpoint Disable-MyDssServerInternalEndpoint Get-MyDssServerInternalEndpoint	Объект «Конечные точки» отвечает за параметры взаимодействия myDSS Internal Server с ЦИ КриптоПро DSS и с myDSS External Server. Настраиваемые параметры идентичны настройкам конечных точек на Сервисе Подписи (См. Раздел 4.6.3.5).

Объект администрирования	Командлеты	Описание
Общие настройки конечных точек	Get-EndpointGlobalSettings Set-EndpointGlobalSettings	Объект отвечает за общие настройки параметров взаимодействия myDSS Internal Server с интегрируемыми системами. Настраиваемые параметры идентичны общим настройками конечных точек на ЦИ (См. раздел 4.5.7.3).

Таблица 165. Объекты администрирования myDSS External Server

Объект администрирования	Командлеты	Описание
Администраторы	Add-MyDssExternalAdministrator Get-MyDssExternalAdministrator Remove-MyDssExternalAdministrator	Объект отвечает за управление учетными записями Администраторов, имеющих доступ к БД myDSS External Server. (См. раздел 4.3.4.1).
Экземпляр myDSS External Server	New-MyDssServerExternalInstance Remove-MyDssServerExternalInstance Get-MyDssServerExternalInstance Update-MyDssServerExternalInstance	Объект «Экземпляр» отвечает за управление экземплярами myDSS External Server.
Настройки экземпляра	Get-MyDssInteractionServiceProperties Set-MyDssInteractionServiceProperties Get-MyDssPushServiceProperties Set-MyDssPushServiceProperties Set-MyDssServerExternalRegistryProperties Get-MyDssServerExternalRegistryProperties	Объект «Настройки экземпляра» отвечает за настройку строки подключения к базе данных и редактирование свойств служб экземпляра.

Объект администрирования	Командлеты	Описание
Конечные точки	Get-MyDssServerInteractionPushServiceEndpoint Enable-MyDssServerInteractionPushServiceEndpoint Disable-MyDssServerInteractionPushServiceEndpoint Get-MyDssServerInteractionServiceEndpoint Enable-MyDssServerInteractionServiceEndpoint Disable-MyDssServerInteractionServiceEndpoint	Объект «Конечные точки» отвечает за параметры взаимодействия служб myDSS External Server с входящими сообщениями с мобильных устройств и с myDSS Internal Server. Настраиваемые параметры идентичны настройкам конечных точек на Сервисе Подписи (См. Раздел 4.6.3.5).
Общие настройки конечных точек	Get-MyDssServerInteractionPushServiceEndpointGlobalSettings Set-MyDssServerInteractionPushServiceEndpointGlobalSettings Get-MyDssServerInteractionServiceEndpointGlobalSettings Set-MyDssServerInteractionServiceEndpointGlobalSettings	Объект отвечает за общие настройки параметров взаимодействия myDSS External Server с интегрируемыми системами. Настраиваемые параметры идентичны общим настройками конечных точек на ЦИ (См. раздел 4.5.7.3).

4.11.4. Администрирование компонента myDSS

Настройка компонента myDSS осуществляется с помощью Windows PowerShell. Команды администрирования включены в модули **CryptoPro.DSS.PowerShell.MyDssServerInternal** и **CryptoPro.DSS.PowerShell.MyDssServerExternal.**

4.11.4.1. Командлет Set-DssMobileAuthProperties

Командлет позволяет настроить взаимодействие myDSS с ЦИ КриптоПро DSS. Входит в состав PowerShell-модуля ЦИ КриптоПро DSS. (см.раздел 4.5.2).

К основным параметрам относятся:

- Отображаемое имя экземпляра ЦИ КриптоПро DSS;
- Адрес Сервиса взаимодействия с ЦИ myDSS.

Синтаксис:

```
Set-DssMobileAuthProperties -DisplayName <Имя экземпляра ЦИ> -ServiceAddress
"http://localhost/MyDssServerInternal/service.svc"
```

Таблица 166. Параметры командлета Set-DssMobileAuthProperties

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра ЦИ КриптоПро DSS.
AuthnLockoutEnabled	bool	Есть ли ограничение по числу неправильных попыток ввода кода подтверждения.
CallbackUriPrefix	string	Адрес экземпляра ЦИ КриптоПро DSS. Пример: https://<имя хоста>/Sts
ConfirmationCodeLength	int	Длина кода подтверждения операции.
DeviceFingerprintRequired	bool	Требуется ли отпечаток устройства.
KeyInfoDivideRequired	bool	Требуется ли высылать код активации Пользователю в случае генерации вектора аутентификации Оператором
KeyInfoDivideByUserRequired	bool	Требуется ли высылать код активации Пользователю в случае самостоятельной генерации им вектора аутентификации.
OfflineKeyGenerationOnly	bool	Является ли выбор вектора аутентификации из сгенерированных Администратором ранее единственным вариантом генерации.
PrefixUserId	string	Префикс идентификатора Пользователя.
SecondKeyPartLength	int	Длина кода активации (отправляемая Пользователю).
ServiceAddress	string	Адрес Сервиса взаимодействия с ЦИ myDSS.
QrCodeDisplayFormat	**File**: сохранение в файл; **Frame**: отображение в отдельном окне; **Screen**: отображение в Веб-интерфейсе Оператора	Формат отображения QR-кода оператору.
SendQrCodeByEmailPermitted	bool	Отправлять ли QR-код по электронной почте.

Параметр	Тип	Описание
HideDownloadAppLinks	bool	Скрывать ли ссылки на скачивание мобильного приложения.

4.11.4.2. Администрирование Сервиса взаимодействия с ЦИ (Internal Interaction Server)

4.11.4.2.1. Экземпляр Сервиса взаимодействия с ЦИ

Командлет New-MyDssServerInternalInstance

Создаёт экземпляр компонента myDSS Internal Interaction Server.

К основным параметрам относятся:

- название веб-сайта IIS, на котором следует развернуть веб-приложение myDSS Internal Interaction Service;
- адрес SQL-сервера, на котором следует развернуть БД myDSS Internal Interaction Server;
- отображаемое имя экземпляра myDSS Internal Interaction Server.

Синтаксис:

```
New-MyDssServerInternalInstance -SiteName <string> [-ApplicationName <string>
-DBname <string> -ConnectionInfo <SqlConnectionInfo>] -SQLServerName <string>
-DisplayName <string>
```

Таблица 167. Параметры командлета New-MyDssServerInternalInstance

Параметр	Тип	Описание
SiteName	string	Название веб-сайта, на котором следует развернуть веб-приложение.
ApplicationName	string	Название веб-приложения Сервиса взаимодействия с ЦИ. Если параметр не задан, используется значение MyDssServerInternal.
SQLServerName	string	Адрес экземпляра SQL-сервера, на котором следует развернуть экземпляр БД myDSS Internal Interaction Service. Формат: <SQL-сервер host>\<имя экземпляра>
DBname	string	Имя базы данных myDSS Internal Interaction Service. По умолчанию InternalServiceDB.
DisplayName	String	Отображаемое имя экземпляра myDSS Internal Interaction Service.

Параметр	Тип	Описание
ConnectionInfo	SqlConnectionInfo	Расширенные данные для подключения к SQL-серверу.

Командлет Remove-MyDssServerInternalInstance

Используется для удаления экземпляра myDSS Internal Interaction Service.

К основным параметрам относятся:

- флаг, определяющий, удалять ли БД myDSS Internal Interaction Service;
- флаг, определяющий удалять ли общую БД экземпляров myDSS Internal Interaction Service.

Синтаксис:

```
Remove-MyDssServerInternalInstance [-DisplayName <string> -ConnectionInfo
<SqlConnectionInfo>] -DeleteDB <bool>
```

Таблица 168. Параметры командлета Remove-MyDssServerInternalInstance

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра myDSS Internal Interaction Service. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
DeleteDB	bool	Флаг, определяющий, требуется ли удаление БД myDSS Internal Interaction Service.
ConnectionInfo	SqlConnectionInfo	Расширенные данные для подключения к SQL-серверу.

Командлет Update-MyDssServerInternalInstance

Обновляет экземпляр компонента myDSS Internal Server после установки новых библиотек.

Синтаксис:

```
Update-MyDssServerInternalInstance [-DisplayName <string>]
```

Командлет Get-MyDssServerInternalInstance

Выводит на консоль список экземпляров myDSS Internal Server.

Синтаксис:

```
Get-MyDssServerInternalInstance
```

4.11.4.2.1. Настройки экземпляра

Командлет Set-MyDssServerInternalRegistryProperties

Используется для изменения строки подключения к базе данных myDSS Internal Server.

Синтаксис:

```
Set-MyDssServerInternalRegistryProperties [-DisplayName <string>] [-
DBConnection <string>]
```

Таблица 169. Параметры командлета Set-MyDssServerInternalRegistryProperties

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра myDSS Internal Server. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
DBConnection	string	Строка подключения к базе данных myDSS Internal Server.

Командлет Get-MyDssServerInternalRegistryProperties

Используется для отображения строки подключения к базе данных myDSS Internal Server.

Синтаксис:

```
Get-MyDssServerInternalRegistryProperties
```

Командлет Set-MyDssServerInternalProperties

Используется для задания основных параметров Сервиса взаимодействия с ЦИ myDSS.

Синтаксис:

```
Set-MyDssServerInternalProperties [-DisplayName <string> -AuthCodeTimeout
<uint32> -ConfirmCodeTimeout <uint32> -CryptoProviderGroupId <guid> -
InteractionServiceAddress <string> -InteractionPushServiceAddress <string>]
```

Таблица 170. Параметры командлета Set-MyDssServerInternalProperties

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра myDSS Internal Server. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
AuthCodeTimeout	uint32	Таймаут действия кода аутентификации.

Параметр	Тип	Описание
ConfirmCodeTimeout	uint32	Таймаут действия кода подтверждения.
TransactionTimeOut	uint32	Таймаут подтверждения операции.
CryptoProviderGroupId	guid	Идентификатор группы криптопровайдеров.
InteractionServiceAddress	string	Адрес сервиса InteractionService на сервере внешнего взаимодействия.
InteractionPushServiceAddress	string	Адрес сервиса рассылки PUSH-уведомлений InteractionPushService.
CryptoProvidersMonitoringTimeout	int	Таймаут проверки работоспособности криптопровайдеров. По умолчанию равен 10 сек.

В параметре **–InteractionServiceAddress** задается адрес сервиса InteractionService, который записывается в QR-код, несущий ключевую информацию. Данный адрес будет использован для связи мобильного приложения с Сервисом взаимодействия с мобильным приложением myDSS, поэтому адрес должен быть доступен из сети Интернет.

Командлет Get-MyDssServerInternalProperties

Командлет **Get-MyDssServerInternalProperties** позволяет вывести на консоль значение основных параметров компонента myDSS Internal Server.

Синтаксис:

```
Get-MyDssServerInternalProperties [-DisplayName <string>]
```

4.11.4.3. Администрирование Сервиса взаимодействия с мобильным приложением (External Interaction Server)

4.11.4.3.1. Экземпляр Сервиса взаимодействия с мобильным приложением

Командлет New-MyDssServerExternalInstance

Создаёт экземпляр компонента myDSS External Interaction Server.

К основным параметрам относятся:

- название веб-сайта IIS, на котором следует развернуть веб-приложение myDSS External Interaction Server;
- адрес SQL-сервера, на котором следует развернуть БД myDSS External Interaction Server;
- отображаемое имя экземпляра myDSS External Interaction Server.

Синтаксис:

```
New-MyDssServerExternalInstance -SiteName <string> [-ApplicationName <string>
-DBname <string> -ConnectionInfo <SqlConnectionInfo>] -SQLServerName <string>
-DisplayName <string>
```

Таблица 171. Параметры командлета New-MyDssServerExternalInstance

Параметр	Тип	Описание
SiteName	string	Название веб-сайта, на котором следует развернуть веб-приложение.
ApplicationName	string	Название веб-приложения Сервиса взаимодействия с мобильным приложением. Если параметр не задан, используется значение MyDssServerExternal.
SQLServerName	string	Адрес экземпляра SQL-сервера, на котором следует развернуть экземпляр БД myDSS External Interaction Server. Формат: <SQL-сервер host>\<имя экземпляра>
DBname	string	Имя базы данных myDSS External Interaction Server. По умолчанию InternalServiceDB.
DisplayName	String	Отображаемое имя экземпляра myDSS External Interaction Server.
ConnectionInfo	SqlConnectionInfo	Расширенные данные для подключения к SQL-серверу.

Командлет Remove-MyDssServerExternalInstance

Используется для удаления экземпляра myDSS External Interaction Server.

К основным параметрам относятся:

- флаг, определяющий, удалять ли БД myDSS External Interaction Server;
- флаг, определяющий удалять ли общую БД экземпляров myDSS External Interaction Server.

Синтаксис:

```
Remove-MyDssServerExternalInstance [-DisplayName <string> -ConnectionInfo
<SqlConnectionInfo>] -DeleteDB <bool>
```

Таблица 172. Параметры командлета Remove-MyDssServerExternalInstance

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра myDSS External Interaction Server. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
DeleteDB	bool	Флаг, определяющий, требуется ли удаление БД myDSS External Interaction Server.
ConnectionInfo	SqlConnectionInfo	Расширенные данные для подключения к SQL-серверу.

Командлет Get-MyDssServerExternalInstance

Выводит на консоль список экземпляров myDSS External Server.

Синтаксис:

```
Get-MyDssServerExternalInstance
```

Командлет Update-MyDssServerExternalInstance

Обновляет экземпляр компонента myDSS External Server после установки новых библиотек.

Синтаксис:

```
Update-MyDssServerExternalInstance [-DisplayName <string>]
```

4.11.4.3.1. Настройки экземпляра

Командлет Set-MyDssInteractionServiceProperties

Позволяет задать адрес Сервиса взаимодействия с ЦИ.

Синтаксис:

```
Set-MyDssInteractionServiceProperties -ServiceAddress <string> [-DisplayName
<string>]
```

Таблица 173. Параметры командлета Set-MyDssInteractionServiceProperties

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра myDSS External Server. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
ServiceAddress	string	Адрес Сервиса взаимодействия с ЦИ.

Командлет Set-MyDssPushServiceProperties

Позволяет настроить основные параметры рассылки PUSH-уведомлений.

Синтаксис:

```
Set-MyDssPushServiceProperties [-DisplayName <string>] -ApnClientCertPassword
<string> -ApnClientCertPath <string> -GoogleServerKey <string> -PushTTL <int>
```

Таблица 174. Параметры командлета Set-MyDssPushServiceProperties

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра myDSS External Server. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
ApnClientCertPassword	string	Пароль от PFX-файла, задаваемого в параметре **ApnClientCertPath.**
ApnClientCertPath	string	Путь к PFX-файлу, содержащему сертификат и закрытый ключ доступа к Apple Push Notification Service.
GoogleServerKey	string	Ключ доступа к Firebase Cloud Messaging Server.
PushTTL	int	Время жизни PUSH-уведомлений в секундах.

Командлет Get-MyDssServerExternalProperties

Командлет **Get-MyDssServerExternalProperties** позволяет вывести на консоль значение основных параметров компонента myDSS External Server.

Синтаксис:

```
Get-MyDssServerExternalProperties [-DisplayName <string>]
```

Командлет Set-MyDssServerExternalRegistryProperties

Используется для изменения строки подключения к базе данных myDSS External Server.

Синтаксис:

```
Set-MyDssServerExternalRegistryProperties [-DisplayName <string>] [-
DBConnection <string>]
```

Таблица 175. Параметры командлета Set-MyDssServerInternalRegistryProperties

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра myDSS External Server. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.

Параметр	Тип	Описание
DBConnection	string	Строка подключения к базе данных myDSS External Server.

Командлет Get-MyDssServerExternalRegistryProperties

Используется для отображения строки подключения к базе данных myDSS External Server.

Синтаксис:

```
Get-MyDssServerExternalRegistryProperties
```

5. Аутентификация в КриптоПро DSS

КриптоПро DSS поддерживает несколько методов аутентификации Пользователей DSS. Все методы аутентификации делятся на две группы:

- Первичная аутентификация.
- Вторичная атентификация.

Первичная аутентификация используется при входе в Веб-интерфейс Пользователя и Личный Кабинет Пользователя на Центре Идентификации. Вспомогательная аутентификация может использоваться:

- при аутентификации Пользователя на Веб-интерфейсе Пользователя и Личном Кабинете ЦИ, как дополнительная мера безопасности (далее «Подтверждение входа»);
- при выполнении операции, требующих доступа к закрытому ключу (см. раздел 4.5.5. Подтверждение операций).

Вторичная аутентификация в КриптоПро DSS является **вспомогательной** и не ослабляет требований первичной аутентификации.

При настройке вторичной аутентификации необходимо обратить особое внимание на регистрацию Сервиса Подписи в качестве доверенной стороны на Центре Идентификации при помощи параметра **-BackChannelUrl** (см. раздел 4.5.3.3).

Список доступных методов аутентификации приводится в выводе командлета Get-DssAuthenticationMethod. Администратор DSS может сделать доступными только необходимые методы аутентификации с помощью командлетов Enable-DssAuthenticationMethod и Disable-DssAuthenticationMethod. Все неиспользуемые методы аутентификации должны быть отключены.

Таблица 176. Список методов первичной аутентификации

Метод	Описание
Аутентификация по паролю	Аутентификация по паролю, хранимому в базе данных Центра Идентификации DSS.
Аутентификация по сертификату	Аутентификация с помощью двустороннего TLS-соединения.
Аутентификация с помощью мобильного приложения myDSS	Аутентификация с помощью мобильного приложения myDSS.

Метод	Описание
Аутентификация с помощью апплета на SIM-карте	Аутентификация по ключу SIM-карты. Присутствует в двух исполнениях: **QES** –аутентификация Пользователя при доступе к КЭП для создания квалицифированной ЭП. **M2M** - аутентификация Пользователя при доступе к КЭП для создания усиленной неквалифицированной ЭП.

Таблица 177. Список методов вторичной (вспомогательной) аутентификации

Метод	Описание
Аутентификация по SMS	Аутентификация с использованием одноразовых паролей, доставляемых в SMS-сообщении.
Аутентификация по протоколу OATH	Аутентификация с помощью одноразовых паролей, полученных по протоколу OATH (TOTP и HOTP).
Аутентификация по электронной почте	Аутентификация с использованием одноразовых паролей, доставляемых по электронной почте.

5.1. Аутентификация по паролю

Идентификатор:

http://dss.cryptopro.ru/identity/authenticationmethod/password

Аутентификация по паролю является основным методом аутентификации локальных Пользователей Центра Идентификации DSS.

К настройке аутентификации по паролю относится следующий набор параметров, задаваемых через командлет Set-DssStsProperties:

Таблица 178. Параметры для настройки аутентификации с помощью командлета Set-DssStsProperties

Параметр	Описание
PasswordType	Тип паролей: Парольные фразы; Символьные пароли.
PasswordSource	Источник паролей: Только Пользователь задаёт пароль; Пароль генерируется только на стороне сервера; Смешанный режим.
PasswordComplexity	Сложность символьных паролей.
PasswordLength	Длина символьных паролей.

Параметр	Описание
PasswordPhraseComplexity	Сложность парольной фразы.
InvalidPasswordAttempts	Количество попыток ввода пароля.
PasswordLifetime	Срок действия пароля Пользователя.
ChangePasswordAfterReset	Требование смены пароля Пользователя при первом входе.

Параметр **PasswordType** определяет тип паролей, генерируемых на сервере. Данный параметр влияет на поведение кабинета Оператора на Центре Идентификации DSS. В зависимости от значения параметра **PasswordType** будет генерироваться тот или иной тип пароля Пользователя, когда Оператор:

- создаёт учётную запись Пользователя и назначает аутентификацию по логину и паролю;
- сбрасывает пароль для существующей учётной записи Пользователя.

Если в качестве паролей используются парольные фразы, то при вводе пароля Пользователем должен соблюдать следующие правила:

- Разрешается вводить не менее трёх букв от каждого слова.
- Введённые слова или части слов должны быть разделены пробелами.
- Разрешается вводить парольную фразу полностью.
- Парольная фраза не чувствительна к регистру букв.
- Парольная фраза на чувствительная к языку ввода.

По умолчанию значение **PasswordType** предполагает использование парольных фраз. При изменении данной настройки, а также любых других настроек по умолчанию, необходимо данное действие согласовывать с руководителем подразделения, а также внести запись в соответствующий журнал с указанием причины изменения настроек.

Параметр **PasswordSource** влияет на поведение Веб-интерфейса Центра Идентификации при работе от имени Пользователя. Если задано значение **ServerOnly** (пароли генерируются только на сервере), то при самостоятельной смене пароля Пользователь может только запросить новый пароль с сервера. Сгенерированный сервером пароль будет отображен Пользователю в веб-интерфейсе. Если задано значение **ClientOnly**, то при смене пароля Пользователю будет предложено самостоятельно придумать новый пароль. Пользователь может самостоятельно задать только символьный пароль. Пароль должен соответствовать требованиям длины и сложности заданными администраратором. Соответствующие требования к паролю отображаются Пользователю в веб-интерфейсе. Если включен смешанный режим (**ClientAndServer**), то Пользователь может как придумать пароль самостоятельно, так и запросить пароль на сервере.

Параметры **PasswordComplexity** и **PasswordLength** определяют сложности и длину символьных паролей. Для сложности пароля определены следующие значения:

- **Weak** – цифры и заглавные латинские буквы. Минимально возможная длина пароля – 2.
- **Fair** – цифры, заглавные и строчные латинские буквы. Минимально возможная длина пароля – 3.

- **Strong** – цифры, заглавные и строчные латинские буквы, спец символы. Минимально возможная длина пароля – 4.

Данные параметры задают требования к символьным паролям, генерируемым на сервере, и паролям, задаваемым Пользователем при смене пароля.

Параметр **InvalidPasswordAttempts** задаёт количество неверных попыток ввода пароля. Если значение параметра установлено на 0, то отключается контроль количества неверных попыток ввода пароля. Если значение данного параметра больше 0, то при превышении количества неверных попыток ввода долговременного пароля учётная запись Пользователя будет заблокирована. Разблокировать учётную запись может только Оператор DSS.

Параметр **PasswordLifetime** задаёт срок действия пароля Пользователя. Если значение параметра установлено в 0, то срок действия пароля не контролируется. Если срок действия пароля установлен, то после его истечения Пользователь должен сменить пароль.

Параметр **ChangePasswordAfterReset** отвечает за требование смены пароля Пользователя при первом входе. Данное правило применяется только в том случае, если учётная запись Пользователя была создана Оператором DSS или пароль Пользователя был сброшен Оператором DSS.

5.2. Аутентификация по сертификату

Идентификатор:

http://dss.cryptopro.ru/identity/authenticationmethod/certificate

Если в качестве метода первичной аутентификации Пользователю назначен вход по сертификату, то вход в Веб-интерфейс Пользователя или личный кабинет на Центре Идентификации требуется осуществляется по двустороннему TLS-соединению с клиентской аутентификацией.

Пользователь может быть успешно аутентифицирован по сертификату при выполнении следующих условий:

- Сертификат Пользователя является доверенным для сервера DSS.
- Значение поля Субъект в сертификате совпадает с отличительным именем Пользователя DSS.
- В сертификате должно содержаться расширение Enhanced Key Usage: 1.3.6.1.5.5.7.3.2 (Проверка подлинности клиента).

Для удобства выполнения второго условия аутентификации отличительное имя Пользователя может быть автоматически заполнено правильными значениями из сертификата Пользователя.

Если в качестве метода первичной аутентификации пользователю назначен вход по сертификату, то необходимо включить требование уникальности различительного имени:

```
Set-DssStsProperties -RequireUniqueDn
```

При выполнении данного командлета будет проверена база данных на наличие дублирующихся различительных имён пользователей. Если будут найдены два и более пользователей с совпадающими различительными именами, то соответствующее требование уникальности не может быть включено.

КриптоПро DSS поддерживает выделенное хранилище издателей сертификатов аутентификации. Имя хранилища можно посмотреть в выводе параметра **ClientAuthenticationIssuersStoreName** командлета **Get-DssStsProperties** (по умолчанию – STS Client Authentication Issuers). Использование данного хранилища регулируется параметром **IsClientAuthenticationIssuersStoreEnabled** (см. раздел 4.5.7.2).

5.3. Аутентификация с помощью апплета на SIM-карте

Идентификатор:

http://dss.cryptopro.ru/identity/authenticationmethod/simauth

Вторичная аутентификация в КриптоПро DSS может осуществляться с использованием специально подготовленной SIM-карты. В этом случае Сервис Подписи присылает на телефон Пользователя бинарное SMS-сообщение, которое принимается и обрабатывается установленным на SIM-карту при производстве компонентом. Результат своей работы этот компонент возвращает на Сервис Подписи, что подтверждает вход/операцию.

Вторичная аутентификация с использованием SIM-карты присутствует в двух комплектациях КриптоПро DSS:

- DSS + SIM (QES) – аутентификация Пользователя при доступе к КЭП для создания усиленной квалифицированной ЭП.
- DSS + SIM (M2M) – аутентификация Пользователя при доступе к КЭП для создания усиленной неквалифицированной ЭП.

Предварительные условия для настройки аутентификации с использованием SIM-карты:

- Развернутые и настроенные основные компоненты КриптоПро DSS.
- КриптоПро HSM Client.

Для настройки аутентификации при помощи SIM-карты необходимо выполнить следующие действия:

1. **Настройка оповещения интегрируемой системы.**

На данном шаге происходит настройка уведомления интегрируемой системы о результатах аутентификации Пользователя. Настройка подробно описана в разделе 5.3.1.

2. **Настройка подключения к OTA-платформе.**

Настройка подробно описана в разделе 5.3.2.

3. **Регистрация набора криптопровайдеров.**

На данном шаге регистрируются криптопровайдеры, которые будут использованы для создания в ПАКМ «КриптоПро HSM» двух Мастер-ключей. Один Мастер-ключ будет использоваться для выработки векторов аутентификации Пользователей, а другой – для выработки Security Domain- (SD) ключей.

Добавление набора криптопровайдеров осуществляется при помощи командлета Add-DssSimAuthCryptoProviderProfile. Для изменения настроек уже зарегистрированных криптопровайдеров необходимо использовать командлеты Get-DssSimAuthCryptoProviderProfile, Get-DssStsCryptoProvider, Get-DssStsCryptoProviderType, Remove-DssStsCryptoProvider, Copy-DssStsCryptoProvider, Test-DssStsCryptoProvider, Enable-DssStsCryptoProvider, Disable-DssStsCryptoProvider.

4. **Настройка параметров создания файлов персонализации.**

На данном шаге выполняется настройка параметров, с которыми будет создан файл персонализации.

Файлом персонализации называются сведения о партии SIM-карт, которые передаются их изготовителю. Эти сведения содержат в себе серийные номера SIM-карт, контейнеры с ключевой информацией, SD-ключи и коды активации (для доступа к ключевому контейнеру).

Настройка параметров создания файла персонализации производится при помощи командлетов Add-DssSimAuthKeyProfile, Set-DssSimAuthKeyProfile, Get-DssSimAuthKeyProfile, Remove-DssSimAuthKeyProfile. Основные параметры, которые должны быть настроены перед созданием файла персонализации:

- Идентификатор набора криптопровайдеров (по нему происходит идентификация нужного набора).
- Имя профиля с параметрами файла персонализации.
- Тип файла персонализации.
- Шаблон файла персонализации.
- Доп. параметры (если шаблон не используется).

Полный список параметров находится в описании командлета Add-DssSimAuthKeyProfile.

5. **Создание файла персонализации и регистрация SIM-карт в БД ЦИ КриптоПро DSS.**

На данном шаге выполняется создание файла персонализации для партии SIM-карт. Одновременно с этим производится регистрация SIM-карт в БД ЦИ. Эти действия выполняются при помощи командлета Get-DssSimAuthKey. Основные параметры, которые необходимо указать при создании файла:

- Базовый серийный номер партии (впоследствии включается в серийный номер каждой SIM-карты при производстве).
- Количество SIM-карт в партии.
- Имя партии SIM-карт.
- Описание партии SIM-карт.
- Имя профиля с параметрами файла персонализации. (по нему происходит идентификация нужного профиля).
- Путь, по которому будет создан файл персонализации.

Для просмотра зарегистрированных партий SIM-карт используется командлет Get-DssTokenProfile. Для просмотра сведений об одной партии SIM-карты необходимо явно указать ID этой партии в параметре TokenProfileId. Для удаления сведений о зарегистрированных в БД ЦИ SIM-картах используется командлет Remove-DssTokenProfile.

Для просмотра сведений о конкретной SIM-карте можно использовать командлет Get-DssAuthenticationToken с параметром TokenProfileId или передать на нее объект в режиме конвейера.

5.3.1. Настройка оповещения интегрируемой системы

Модуль оповещения интегрируемой системы отвечает за уведомление интегрируемой системы о результатах аутентификации Пользователя. В Центре Идентификации DSS может быть зарегистрирован только один модуль оповещения интегрируемой системы.

Управление модулями оповещения интегрируемой системы производится через набор командлетов, используемых для управления модулями оповещения DSS. Настройка модулей оповещения подробно описана в разделе 4.9.

Для включения оповещения интегрируемой системы необходимо выполнить действия, описанные в Таблица 179.

Таблица 179. Последовательность шагов по настройке модуля оповещения интегрируемой системы

Шаг 1	**Добавление плагина форматирования сообщений**
Командлет	**Add-DssStsPlugin**
Параметры	
PluginTypeName	
Значение	CryptoPro.DSS.SimAuth.Notification.SimAuthFormatterPlugin, DSS.SimAuth.Notification
Описание	Название типа плагина форматирования. Параметр может иметь только указанное значение.
PluginType	
Значение	Formatter
Описание	Тип плагина – плагин форматирования. Параметр может иметь только указанное значение.
Settings	
Значение	@{}
Описание	Пустой словарь. Данный плагин не имеет настраиваемых параметров.
Пример	
`Add-DssStsPlugin -PluginTypeName "CryptoPro.DSS.SimAuth.Notification.SimAuthFormatterPlugin,DSS.SimAuth.Notification" -PluginType Formatter -Settings @{}`	
Шаг 2	**Добавление транспортного плагина**
Командлет	**Add-DssStsPlugin**

Параметры	
PluginTypeName	
Значение	CryptoPro.DSS.SimAuth.Notification.SimAuthTransportPlugin, DSS.SimAuth.Notification
Описание	Название типа транспортного плагина. Параметр может иметь только указанное значение.
PluginType	
Значение	SimAuth
Описание	Тип плагина – транспортный плагин для отправки уведомлений в интегрируемую систему. Параметр может иметь только указанное значение.
Settings	
Значение	@{ "Address" = “http://<адрес_сервиса_уведомлений_интегрируемой_системы>/mes-notification/notification” }
Описание	Единственный настраиваемый параметр данного плагина – адрес интерфейса интегрируемой системы для отправки уведомлений.
Пример	

```
Add-DssStsPlugin -PluginTypeName
"CryptoPro.DSS.SimAuth.Notification.SimAuthTransportPlugin,DSS.SimAuth.Notif
ication" -PluginType SimAuth -Settings @{"Address" = "http://<hostname>/mes-
notification/notification" }
```

Шаг 3	**Добавление модуля оповещения**
Командлет	**Add-DssStsNotifier**
Параметры	
TransportPluginId	
Значение	Целое положительное число
Описание	Идентификатор транспортного плагина SimAuth. Данный идентификатор можно посмотреть с помощью командлета Get-DssStsPlugin
FormatterPluginId	
Значение	Целое положительное число
Описание	Идентификатор плагина форматирования. Данный идентификатор можно посмотреть с помощью командлета Get-DssStsPlugin
NotifierType	
Значение	SimAuth

Описание	Тип модуля оповещения. Параметр может иметь только указанное значение.
Пример	
`Add-DssStsNotifier -TransportPluginId 1 -FormatterPluginId 2 -NotifierType SimAuth`	

Ниже приводится полная последовательность вызовов командлетов PowerShell для регистрации модуля.

```
#Добавление плагина формирования сообщений
Add-DssStsPlugin -PluginTypeName
"CryptoPro.DSS.SimAuth.Notification.SimAuthFormatterPlugin,DSS.SimAuth
.Notification" -PluginType Formatter -Settings @{}


#Добавление транспортного плагина
Add-DssStsPlugin -PluginTypeName
"CryptoPro.DSS.SimAuth.Notification.SimAuthTransportPlugin,DSS.SimAuth
.Notification" -PluginType SimAuth -Settings @{"Address" =
"http://<hostname>/mes-notification/notification" }


#Добавление модуля оповещения
Add-DssStsNotifier -TransportPluginId 1 -FormatterPluginId 2 -
NotifierType SimAuth
```

5.3.2. Настройка взаимодействия с OTA-платформой

OTA-платформа отвечает за взаимодействие КриптоПро DSS с апплетом на SIM-карте. Для этого требуется настроить соответствующие модули оповещения. В Центре Идентификации DSS может быть зарегистрирован только один модуль оповещения OTA-платформы.

Управление взаимодействием с OTA-платформой производится через набор командлетов, используемых для управления модулями оповещения DSS. Настройка модулей оповещения подробно описана в разделе 4.9.

Взаимодействие КриптоПро DSS с апплетом на SIM-карте организовано в соответствии со схемой, приведённой на Рис. 41.

Рис. 41 – Взаимодействие КриптоПро DSS с OTA-платформой

Последовательность действий при взаимодействии DSS с апплетом:

1. КриптоПро DSS при необходимости взаимодействия с апплетом инициирует отправку SMS-сообщения с соответствующей командой через OTA-платформу. В OTA-платформу передаётся текст сообщения с командой, номер телефона (MSISDN) и ключи SD соответствующей SIM-карты.
2. OTA-платформа готовит пакет 3GPP TS 23.048 для апплета с исходным сообщением и отправляет его.
3. Апплет на SIM-карте получает команду, выполняет необходимое действие и отправляет ответное SMS-сообщение.
4. OTA-платформа принимает ответное сообщение и передаёт его в КриптоПро DSS вместе с MSISDN пользователя.

Для настройки взаимодействия с OTA-платформой необходимо выполнить действия, описанные в Таблица 180.

Таблица 180. Последовательность шагов по настройке взаимодействия с OTA-платформой

Шаг 1	**Добавление плагина форматирования сообщений**
Командлет	**Add-DssStsPlugin**
Параметры	
PluginTypeName	

Значение	CryptoPro.DSS.SimAuth.Notification. OtaFormatterPlugin, DSS.SimAuth.Notification
Описание	Название типа плагина форматирования. Параметр может иметь только указанное значение.
PluginType	
Значение	Formatter
Описание	Тип плагина – плагин форматирования. Параметр может иметь только указанное значение.
Settings	
Значение	@{"UseQuatedValue" = "true"}
Описание	Данный плагин определяет формат сообщений, которыми обменивается DSS с OTA-платформой.
Пример	

```
Add-DssStsPlugin -PluginTypeName
"CryptoPro.DSS.SimAuth.Notification.OtaFormatterPlugin,DSS.SimAuth.Notificat
ion" -PluginType Formatter -Settings @{ "UseQuatedValue" = "true" }
```

Шаг 2	**Добавление транспортного плагина**
Командлет	**Add-DssStsPlugin**
Параметры	
PluginTypeName	
Значение	CryptoPro.DSS.SimAuth.Notification.OtaTransportPlugin, DSS.SimAuth.Notification
Описание	Название типа транспортного плагина. Параметр может иметь только указанное значение.
PluginType	
Значение	Ota
Описание	Тип плагина – транспортный плагин для отправки уведомлений в МЭП. Параметр может иметь только указанное значение.
Settings	
Значение	@{ "Address" = "http://<otaAddress>" }
Описание	Единственный настраиваемый параметр данного плагина – OTA-платформы для отправки уведомлений.
Пример	

```
Add-DssStsPlugin -PluginTypeName
"CryptoPro.DSS.SimAuth.Notification.OtaTransportPlugin,DSS.SimAuth.Notificat
ion" -PluginType Ota -Settings @{ "Address" = "http://<otaAddress>" }
```

Шаг 3	Добавление модуля оповещения
Командлет	**Add-DssStsNotifier**
Параметры	
TransportPluginId	
Значение	Целое положительное число
Описание	Идентификатор транспортного плагина OTA. Данный идентификатор можно посмотреть с помощью командлета Get-DssStsPlugin
FormatterPluginId	
Значение	Целое положительное число
Описание	Идентификатор плагина форматирования. Данный идентификатор можно посмотреть с помощью командлета Get-DssStsPlugin
NotifierType	
Значение	Ota
Описание	Тип модуля оповещения Параметр может иметь только указанное значение.
Пример	
`Add-DssStsNotifier -TransportPluginId 1 -FormatterPluginId 2 -NotifierType Ota`	

Ниже приводится полная последовательность вызовов командлетов PowerShell для регистрации модуля.

```
#Добавление плагина формирования сообщений
Add-DssStsPlugin -PluginTypeName
"CryptoPro.DSS.SimAuth.Notification.OtaFormatterPlugin,DSS.SimAuth.Not
ification" -PluginType Formatter -Settings @{ "UseQuatedValue" =
"true" }


#Добавление транспортного плагина
Add-DssStsPlugin -PluginTypeName
"CryptoPro.DSS.SimAuth.Notification.OtaTransportPlugin,DSS.SimAuth.Not
ification" -PluginType Ota -Settings @{ "Address" =
"http://<otaAddress>" }


#Добавление модуля оповещения
Add-DssStsNotifier -TransportPluginId 1 -FormatterPluginId 2 -
NotifierType Ota
```

5.3.3. Настройка аутентификации при помощи апплета на SIM-карте

Настройка аутентификации при помощи апплета на SIM-карте осуществляется с помощью Windows PowerShell. Команды администрирования включены в модуль **CryptoPro.DSS.PowerShell.STS** .

Командлет Add-DssSimAuthCryptoProviderProfile

Командлет позволяет добавить набор криптопровайдеров

Синтаксис:

```
Add-DssSimAuthCryptoProviderProfile [-GroupId <int>] [-DisplayName <string>]
```

Таблица 181. Параметры командлета Add-DssSimAuthCryptoProviderProfile

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра ЦИ. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Description	string	Описание набора криптопровайдеров.
Name	string	Имя набора криптопровайдеров.
PrimaryProviderName	string	Имя провайдера, зарегистрированное в системе.
PrimaryProviderType	string	Тип провайдера, зарегистрированного в ОС.
Settings	hashtable	Дополнительные настройки

При добавлении набора криптопровайдеров возможно также задать дополнительные настройки. Эти настройки задаются внутри параметра **Settings** типа **Hashtable**:

```
@{paramName1=paramValue1; paramName2=paramValue2;…;paramNameN=paramValueN}
```

где **paramName$_i$**, **paramValue$_i$** – название и значение параметра соответственно.

Описание дополнительных настроек набора криптопровайдеров при помощи параметра **Settings** приведено в Таблица 182.

Таблица 182. Дополнительные настройки набора криптопровайдеров

Параметр	Описание	Значение параметра
Header	Заголовки файла персонализации. Указание заголовков определяет наличие таких столбцов в файле. Порядок следования заголовков определяет их порядок следования в файле.	**var_out: <F1>/<F2>/.../<Fn>**, где <Fi>: **ICCID** - серийный номер SIM-карты; **KIC** - SD-ключ 1; **KID** - SD-ключ 2; **KIK** - SD-ключ 3 (для смены); **DCKA** - блоб с вектором аутентификации; **Password** (или **PUK**) - код активации.
PRF	Идентификатор алгоритма PRF для выработки транспортного ключа, на котором зашифровывается код аутентификации.	**AESCMAC**; **HMACSHA1**; **AESCMAC_Legacy**; **HMACSHA1_Legacy**. Значения параметра с постфиксом **Legacy** подходят только для использования в Windows Server 2008 R2.
BlobType	Тип блоба для передачи DCKA-ключа.	**17** – для QES **18** – для M2M
BlobVersion	Версия блоба для передачи DCKA-ключа.	**1** – для типа блоба 0x12; **2** – для типа блоба 0x11 (1 вектор аутентификации); **3** – для типа блоба 0x11 (2 вектора аутентификации).
IsRandomPassword	Режим генерации паролей (ПИН-кодов), используемых для выработки транспортных ключей.	Случайный: **True**; Фиксированный: **False**.
ICCIDFileFormat	Формат записи ICCID в файл персонализации.	**NoCS** – записывать файл персонализации IccId без контрольной суммы; **CS** – с контрольной суммой.
UseKeyVersion	Использовать версию при генерации ключей.	**True/False.**
FixedPassword	Значение фиксированного пароля (код аутентификации на все ключи). (Взаимоисключающие с **RandomPasswordLength**)	Строка с паролем.
RandomPasswordLength	Длина кода активации. При наличии данного параметра создается случайный код активации. Взаимоисключающие с **FixedPassword**)	Целое положительное число.

Параметр	Описание	Значение параметра
PasswordFormat	Формат записи кода активации.	Шестнадцатеричный: **Hex**; Десятичный: **Numeric**.
GlonassMaxBlobCount	Максимальное количество ключевых блобов в файле персонализации. Только для шаблона M2M.	Целое положительное число.
GlonassKeyCount	Количество ключей, которые требуется сгенерировать для файла персонализации. Только для шаблона M2M	Целое положительное число
GlonassDisableMask	Не накладывать маску на ключи. Только для шаблона M2M	**True/False.**
GlonassTestDataRows	Количество строк в файле с тестовыми данными ГЛОНАСС. Только для шаблона M2M. По умолчанию число строк составляет 10.	Целое положительное число.
UseExtendedICCID	ICCID представлен в расширенном формате, в то время как базовый ICCID - 19 цифр.	**True** – если IccId длиннее 19 цифр; **False** – в остальных случаях.

Командлет Get-DssSimAuthCryptoProviderProfile

Командлет позволяет вывести на консоль сведения о зарегистрированных наборах криптопровайдеров.

Синтаксис:

```
Get-DssSimAuthCryptoProviderProfile [-DisplayName <string>]
```

Командлет Get-DssStsCryptoProvider

Используется для вывода на консоль информации о зарегистрированных криптопровайдерах.

Синтаксис:

```
Get-DssStsCryptoProvider [-DisplayName <string>] [-Validate] -ID <guid>
```

Таблица 183. Параметры командлета Get-DssStsCryptoProvider

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Центра Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Validate	SwitchParameter	Флаг, определяющий, что требуется проверка работоспособности криптопровайдеров с Мастер-ключом.
ID	guid	Идентификатор криптопровайдера.

Командлет Get-DssStsCryptoProviderType

Выводит на консоль список зарегистрированных типов криптопровайдеров.

Синтаксис:

```
Get-DssStsCryptoProviderType [-DisplayName <string>]
```

Командлет Remove-DssStsCryptoProvider

Используется для удаления криптопровайдера на Центре Идентификации. Командлет принимает на вход идентификатор криптопровайдера в БД ЦИ, либо объект в режиме конвейера.

Синтаксис:

```
Remove-DssStsCryptoProvider [-DisplayName <string>] -ID <guid>
```

Таблица 184. Параметры командлета Remove-DssStsCryptoProvider

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Центра Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
ID	guid	Идентификатор криптопровайдера.

Командлет Copy-DssStsCryptoProvider

Используется для создания нового криптопровайдера, принадлежащего заданной группе криптопровайдеров. Мастер-ключ нового криптопровайдера совпадает с Мастер-ключами остальных криптопровайдеров группы. Командлет принимает на вход идентификатор криптопровайдера в БД ЦИ, либо объект в режиме конвейера.

Синтаксис:

```
Copy-DssStsCryptoProvider [-DisplayName <string>] -GroupID <int> -NewProvName
<string>
```

Таблица 185. Параметры командлета Copy-DssStsCryptoProvider

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Центра Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
GroupID	Int	Идентификатор группы, которой принадлежит копируемый криптопровайдер.
NewProvName	string	Имя нового криптопровайдера.

Командлет Enable-DssStsCryptoProvider

Используется для включения криптопровайдера на ЦИ, ранее переведённого в состояние отключен. Командлет принимает на вход идентификатор криптопровайдера в БД ЦИ, либо объект в режиме конвейера.

Синтаксис:

```
Enable-DssStsCryptoProvider [-DisplayName <string>] -ID <int>
```

Таблица 186. Параметры командлета Enable-DssStsCryptoProvider

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Центра Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
ID	guid	Идентификатор криптопровайдера.

Командлет Disable-DssStsCryptoProvider

Используется для отключения криптопровайдера на ЦИ. Командлет принимает на вход идентификатор криптопровайдера в БД ЦИ, либо объект в режиме конвейера.

Синтаксис:

```
Disable-DssStsCryptoProvider [-DisplayName <string>] -ID <guid>
```

Таблица 187. Параметры командлета Disable-DssStsCryptoProvider

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Центра Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
ID	guid	Идентификатор криптопровайдера.

Командлет Test-DssStsCryptoProvider

Используется для проверки доступности криптопровайдера. Командлет принимает на вход идентификатор криптопровайдера в БД ЦИ, либо объект в режиме конвейера.

Синтаксис:

```
Test-DssStsCryptoProvider [-DisplayName <string>] -ID <guid>
```

Таблица 188. Параметры командлета Test-DssStsCryptoProvider

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Центра Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
ID	guid	Идентификатор криптопровайдера.

Командлет Add-DssSimAuthKeyProfile

Используется для добавления комплекта параметров создания файла персонализации серии SIM-карт.

Синтаксис:

```
Add-DssSimAuthKeyProfile [-DisplayName <string>] -CryptoProfileId <guid> -
Name <string> [-Parameters <hashtable>] [-PassThru] [-PredefinedProfileType
<string>] -Type <string>
```

Таблица 189. Параметры командлета Add-DssSimAuthKeyProfile

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Центра Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Type	string	Тип файла персонализации. Доступные значения: **SIM** – для создания квалифицированной ЭП (исполнение DSS + SIM (QES)); **M2M** – для создания неквалифицированной ЭП (исполнение DSS + SIM (M2M)); **M2MTest** – для генерации данных, позволяющих протестировать апплет на производстве.
CryptoProfileId	guid	Идентификатор набора криптопровайдеров. Применяется для указания криптопровайдеров, которые будут использованы при выработке векторов аутентификации и SD-ключей.
Name	string	Имя комплекта настроек создания файла персонализации.
PredefinedProfileType	string	Шаблон файла персонализации. Доступные значения: **BasicFixPassword**; **BasicRandomPassword8**; **M2M**; **M2MTest**; **LegacyFixPassword**; **LegacyRandomPassword8**.
Parameters	hashtable	Параметры файла персонализации, если не указан ни один шаблон.
PassThru	switch	Позволяет передать объект, над которым совершается действие, в следующий командлет.

Параметр **PredefinedProfileType** позволяет выбрать предопределенный шаблон файла персонализации. Доступные шаблоны характеризуются параметрами, представленными в Таблица 190.

Таблица 190. Шаблоны файла персонализации

Шаблон	Параметр	Значение	Описание
BasicFixPassword	BlobType	17	Тип блоба для передачи DCKA-ключа.
	BlobVersion	2	Версия блоба для передачи DCKA-ключа.

Шаблон	Параметр	Значение	Описание
	UseKeyVersion	True	Использовать версию при генерации ключей.
	PRF	AESCMAC	Идентификатор алгоритма PRF для выработки транспортного ключа, на котором зашифровывается код аутентификации.
	PasswordFormat	Numeric	Формат записи кода активации.
	IsRandomPassword	False	Режим генерации паролей (ПИН-кодов), используемых для выработки транспортных ключей.
	FixedPassword	12345678	Значение фиксированного пароля (код аутентификации на все ключи).
	Header	"var_out: ICCID/KIC/KID/KIK/DCKA/PUK"	Заголовки файла персонализации. Указание заголовков определяет наличие таких столбцов в файле. Порядок следования заголовков определяет их порядок следования в файле.

Отличающиеся параметры для других шаблонов

Шаблон	Параметр	Значение	Описание
LegacyFixPassword	PRF	AESCMAC_Legacy	Идентификатор алгоритма PRF для выработки транспортного ключа, на котором зашифровывается код аутентификации.
BasicRandomPassword8	IsRandomPassword	True	Режим генерации паролей (ПИН-кодов), используемых для выработки транспортных ключей.
	RandomPasswordLength	8	Длина кода активации. При наличии данного параметра создается случайный код активации.
LegacyRandomPassword8	PRF	AESCMAC_Legacy	Идентификатор алгоритма PRF для выработки транспортного ключа, на котором зашифровывается код аутентификации.
	IsRandomPassword	True	Режим генерации паролей (ПИН-кодов), используемых для выработки транспортных ключей.
	RandomPasswordLength	8	Длина кода активации. При наличии данного параметра создается случайный код активации.

Командлет Set-DssSimAuthKeyProfile

Используется для изменения комплекта параметров создания файла персонализации серии SIM-карт.

Синтаксис:

```
Set-DssSimAuthKeyProfile [-DisplayName <string>] [-ID <guid>] [-
CryptoProfileId <guid>] [-InputObject <SimAuthKeyProfile>] [-Name <string>]
[-Parameters <hashtable>] [-PassThru]
```

Таблица 191. Параметры командлета Set-DssSimAuthKeyProfile

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Центра Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
CryptoProfileId	guid	Идентификатор набора криптопровайдеров. Применяется для указания криптопровайдеров, которые будут использованы при выработке векторов аутентификации и SD-ключей.
Name	string	Имя комплекта настроек создания файла персонализации.
Parameters	hashtable	Параметры файла персонализации, если не указан ни один шаблон.
PassThru	switch	Позволяет передать объект, над которым совершается действие, в следующий командлет.

Командлет Get-DssSimAuthKeyProfile

Используется для вывода на консоль сведений о комплекте настроек файла персонализации.

Синтаксис:

```
Get-DssSimAuthKeyProfile [-DisplayName <string>] [-Name <string>]
```

Таблица 192. Параметры командлета Get-DssSimAuthKeyProfile

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Центра Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Name	string	Имя комплекта настроек создания файла персонализации.

Командлет Remove-DssSimAuthKeyProfile

Используется для удаления комплекта параметров для создания файла персонализации.

Синтаксис:

```
Remove-DssSimAuthKeyProfile [-DisplayName <string>] [-Name <string>]
```

Таблица 193. Параметры командлета Remove-DssSimAuthKeyProfile

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Центра Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Name	string	Имя комплекта настроек создания файла персонализации.

Командлет Get-DssSimAuthKey

Используется для создания файла персонализации и регистрации партии SIM-карт в DSS.

Синтаксис:

```
Get-DssSimAuthKey [-DisplayName <string>] -IccId <string> -FilePath <string>
[-LotDescription <string>] -LotName <string> [-Password <string>] [-
PersoFileOnly] -ProfileId <string> [-Quantity <int>]
```

Таблица 194. Параметры командлета Get-DssSimAuthKey

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Центра Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
FilePath	string	Путь записи файла персонализации.
IccId	string	Базовый серийный номер партии SIM-карт.
Quantity	int	Количество SIM-карт в партии.
LotDescription	string	Описание партии SIM-карт.
LotName	string	Имя партии SIM-карт.
ProfileId	string	Имя комплекта настроек создания файла персонализации.
Password	string	Фиксированный код активации для партии SIM-карт.
PersoFileOnly	switch	Сформировать только файл персонализации. (без регистрации SIM-карт в базе данных).

Командлет Get-DssTokenProfile

Используется для вывода на консоль сведений о зарегистрированных в DSS партиях SIM-карт.

Синтаксис:

```
Get-DssTokenProfile [-DisplayName <string>] [-TokenProfileId <int>] [-
Quantity <int>]
```

Таблица 195. Параметры командлета Get-DssSimAuthKey

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Центра Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
TokenProfileId	int	Идентификатор партии SIM-карт, зарегистрированных в DSS.

Командлет Remove-DssTokenProfile

Используется для удаления зарегистрированных в DSS партий SIM-карт.

Синтаксис:

```
Remove-DssTokenProfile [-DisplayName <string -TokenProfileId <int> [-Quantity
<int>]
```

Таблица 196. Параметры командлета Remove-DssSimAuthKey

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Центра Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
TokenProfileId	int	Идентификатор партии SIM-карт, зарегистрированных в DSS.

Командлет Get-DssAuthenticationToken

Используется для вывода на консоль сведений о SIM-картах, содержащихся в партии.

Синтаксис:

```
Get-DssAuthenticationToken [-DisplayName <string>] [-TokenProfileId <int>] [-
Quantity <int>]
```

Таблица 197. Параметры командлета Get-DssAuthenticationToken

Параметр	Тип	Описание
DisplayName	string	Имя экземпляра Центра Идентификации. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
TokenProfileId	int	Идентификатор партии SIM-карт, зарегистрированных в DSS.

5.4. Аутентификация при помощи мобильного приложения myDSS

Командлеты для настройки аутентификации при помощи мобильного приложения myDSS описаны в разделе 4.11.

5.4.1. Аутентификация по логину и паролю и подтверждением операций с помощью мобильного приложения myDSS

Данный метод требует установки защищенного TLS-соединения с односторонней аутентификацией. Аутентификация производится по паролю, хранимому в БД Центра Идентификации КриптоПро DSS.

Кроме аутентификации по паролю, данный метод аутентификации подтверждает операции с помощью мобильного приложения myDSS следующими способами:

- С помощью сравнения уникального идентификатора.

КриптоПро DSS генерирует для подписываемого документа уникальный идентификатор, который отображается как в Веб-интерфейсе DSS, так и в мобильном приложении. Пользователь сравнивает идентификаторы и в случае их совпадения подтверждает операцию путем нажатия соответствующей кнопки в myDSS, после чего ему потребуется ввести ПИН-код в мобильном приложении. Такой метод подтверждения применим для создания ЭП любых документов.

- С помощью отображения самого документа.

Документ, для которого планируется создать электронную подпись, отображается в мобильном приложении myDSS. Пользователь просматривает его, убеждается, что хочет выполнить операцию именно с этим документом, и подтверждает ее путем нажатия соответствующей кнопки в myDSS, после чего ему потребуется ввести ПИН-код в мобильном приложении. Такой метод подтверждения применим для создания ЭП только неконфиденциальных документов.

Описанные в данном разделе способы аутентификации реализуются в комплектации КриптоПро DSS «DSS + myDSS» (см. раздел 2.4 ЖТЯИ.00096-02 90 02 КриптоПро DSS. Общее Описание).

5.4.2. Аутентификация с помощью мобильного приложения myDSS

При данном методе аутентификации Пользователь не имеет прямого доступа к Веб-Интерфейсу DSS. Интегрированная с КриптоПро DSS информационная система инициализирует операцию создания ЭП документа, после чего подписываемый документ отображается в мобильном приложении myDSS. Пользователь просматривает его,

убеждается, что хочет выполнить операцию именно с этим документом, и подтверждает ее путем нажатия соответствующей кнопки в myDSS, после чего ему потребуется ввести ПИН-код в мобильном приложении. Такой сценарий возможен для работы только с неконфиденциальными документами.

Описанный метод аутентификации реализуется в комплектации КриптоПро DSS «DSS + myDSS» (см. раздел 2.4 ЖТЯИ.00096-02 90 02 КриптоПро DSS. Общее Описание).

5.4.3. Настройка оповещения интегрируемой системы об операциях в myDSS

Модуль аутентификации myDSS может оповещать интегрируемую систему о результате подтверждения операции в мобильном приложении, отправляя в интегрируемую систему соответствующие сообщения. Для настройки такого оповещения необходимо зарегистировать сооветствующие плагины (транспортный и форматирования) и модуль оповещения.

Управление модулями оповещения интегрируемой системы производится через набор командлетов, используемых для управления модулями оповещения DSS. Настройка модулей оповещения подробно описана в разделе 4.9.

Для включения оповещения интегрируемой системы необходимо выполнить действия, описанные в Таблица 198.

Таблица 198. Последовательность шагов по настройке оповещения интегрируемой системы об операциях в myDSS

Шаг 1	**Добавление плагина форматирования сообщений**
Командлет	**Add-DssStsPlugin**
Параметры	
PluginTypeName	
Значение	CryptoPro.DSS.Identity.Authentication.Notification.AuthenticationResultFormatter,CryptoPro.DSS.Identity.Authentication.Notification
Описание	Название типа плагина форматирования. Параметр может иметь только указанное значение.
PluginType	
Значение	Formatter
Описание	Тип плагина – плагин форматирования. Параметр может иметь только указанное значение.
Settings	
Значение	@{}

Шаг 1	Добавление плагина форматирования сообщений
Описание	Пустой словарь. Данный плагин не имеет настраиваемых параметров.
Пример	

```
Add-DssStsPlugin -PluginTypeName
"CryptoPro.DSS.Identity.Authentication.Notification.AuthenticationResultForm
atter,CryptoPro.DSS.Identity.Authentication.Notification" -PluginType
Formatter -Settings @{}
```

Шаг 2	Добавление транспортного плагина
Командлет	**Add-DssStsPlugin**
Параметры	
PluginTypeName	
Значение	CryptoPro.DSS.Identity.Authentication.Notification.HttpTransportPlugin,CryptoPro.DSS.Identity.Authentication.Notification
Описание	Название типа транспортного плагина. Параметр может иметь только указанное значение.
PluginType	
Значение	AuthenticationResult
Описание	Тип плагина – транспортный плагин для отправки уведомлений в интегрируемую систему. Параметр может иметь только указанное значение.
Settings	
Значение	@{}
Описание	Пустой словарь. Данный плагин не имеет настраиваемых параметров.
Пример	

```
Add-DssStsPlugin -PluginTypeName
"CryptoPro.DSS.Identity.Authentication.Notification.HttpTransportPlugin,Cryp
toPro.DSS.Identity.Authentication.Notification" -PluginType
AuthenticationResult -Settings @{}
```

Шаг 3	Добавление модуля оповещения
Командлет	**Add-DssStsNotifier**
Параметры	
TransportPluginId	
Значение	Целое положительное число

Шаг 1	Добавление плагина форматирования сообщений
Описание	Идентификатор транспортного плагина SimAuth. Данный идентификатор можно посмотреть с помощью командлета Get-DssStsPlugin
FormatterPluginId	
Значение	Целое положительное число
Описание	Идентификатор плагина форматирования. Данный идентификатор можно посмотреть с помощью командлета Get-DssStsPlugin
NotifierType	
Значение	AuthenticationResultCallback
Описание	Тип модуля оповещения. Параметр может иметь только указанное значение.
Settings	
Значение	@{}
Описание	Пустой словарь. Данный плагин не имеет настраиваемых параметров.
Пример	
`Add-DssStsNotifier -TransportPluginID <ID транспортного плагина> -FormatterPluginID <ID плагина форматирования> -NotifierType AuthenticationResultCallback -Settings @{}`	

Ниже приводится полная последовательность вызовов командлетов PowerShell для регистрации модуля.

```
#Настройка транспортного плагина
Add-DssStsPlugin -PluginTypeName
"CryptoPro.DSS.Identity.Authentication.Notification.HttpTransportPlugin,Crypt
oPro.DSS.Identity.Authentication.Notification" -PluginType
AuthenticationResult -Settings @{}


#Настройка плагина форматирования
Add-DssStsPlugin -PluginTypeName
"CryptoPro.DSS.Identity.Authentication.Notification.AuthenticationResultForma
tter,CryptoPro.DSS.Identity.Authentication.Notification" -PluginType
Formatter -Settings @{}


#Добавление модуля оповещения
Add-DssStsNotifier -TransportPluginID <ID транспортного плагина> -
FormatterPluginID <ID плагина форматирования> -NotifierType
AuthenticationResultCallback -Settings @{}
```

ID плагинов присваиваются автоматически после их добавления.

5.5. Настройка аутентификации с использованием одноразовых паролей

При использовании в качестве метода вспомогательной аутентификации одноразовых паролей, доставляемых в SMS сообщениях, требуется наличие корректного номера телефона в профиле учётной записи Пользователя.

В настройках ЦИ параметр **PhoneConfirmation** позволяет включить или отключить подтверждение номера телефона.

Пример:

```
Set-DssStsProperties -PhoneConfirmation $true
```

Подтверждать номер телефона требуется при изменении номера через личный кабинет Пользователя. В этом случае одноразовый пароль будет отправлен на новый номер телефона.

При создании Пользователя Оператором подтверждение номера телефона не требуется.

5.5.1. Общие настройки одноразовых паролей

К управлению одноразовыми паролями относится следующий набор параметров, задаваемых через командлет Set-DssPasswordPolicy:

- InvalidOtpAttempts
- TransactionTimeOut
- OtpConfirmationTimeOut
- MinOtpConfirmationTimeOut
- OtpComplexity
- OtpLength

OtpComplexity и **OtpLength** определяют сложность и длину одноразовых паролей, передаваемых через SMS или Email. По умолчанию создаются одноразовый пароли, состоящие из 5 цифр.

InvalidOtpAttempts определяет количество неверных попыток ввода одноразового пароля. По умолчанию Пользователю предоставляется 3 попытки неверного ввода одноразового пароля. Если значение параметра InvalidOtpAttempts установлено на 0, то количество попыток ввода одноразового пароля не ограничено.

Поведение Центра Идентификации при превышении количества неверных попыток ввода зависит от параметров **OtpConfirmationTimeOut** и **MinOtpConfirmationTimeOut**.

OtpConfirmationTimeOut определяет период времени, в течение которого Пользователь должен подтвердить одноразовый пароль. Если в течение данного периода одноразовый пароль не был подтвержден, то Пользователь должен запросить новый одноразовый пароль для подтверждения. Также в течение периода **OtpConfirmationTimeOut** действует счётчик неверных попыток ввода одноразового пароля; при запросе нового одноразового пароля счётчик обнуляется.

MinOtpConfirmationTimeOut определяет интервал времени, через который Пользователь может запросить новый одноразовый пароль. Другими словами, если в течение интервала времени **MinOtpConfirmationTimeOut** Пользователь превысил

количество неверных попыток ввода одноразового пароля, то новый пароль он сможет запросить не раньше истечения периода времени **MinOtpConfirmationTimeOut**. По умолчанию значения параметров **MinOtpConfirmationTimeOut** и **OtpConfirmationTimeOut** совпадают и равны 5 минутам. Если значение параметра MinOtpConfirmationTimeOut установлено на 0, то Пользователь может запрашивать новые одноразовые пароли без ограничения.

Параметр **TransactionTimeOut** определяет период времени, в течение которого Пользователь должен выполнить подтверждённую операцию (подпись, расшифрование документа, создание запроса на сертификат и т.п.). Если в течение данного периода времени Пользователь не выполнил операцию, то потребуется выполнить подтверждение операции повторно.

5.5.2. Аутентификация с использованием одноразовых SMS-паролей.

При использовании данного метода для подтверждения входа и операций у Пользователя дополнительно будет запрашиваться ввод одноразового пароля, доставляемого в SMS-сообщении на телефон Пользователя.

Данный вид вспомогательной аутентификации требует подключения к SMS-шлюзу оператора сотовой связи в соответствии со схемой размещения компонентов (см раздел 5.2 ЖТЯИ.00046-03 90 02. КриптоПро DSS. Общее описание) и в соответствии с требованиями к подключению к сетям общего пользования, описанными в Разделе 10 ЖТЯИ.00046-03 95 01. Правила пользования.

Для использования данного метода двухфакторной аутентификации необходимо:

1. Включить с помощью командлета Enable-DssAuthenticationMethod метод аутентификации с идентификатором http://dss.cryptopro.ru/identity/authenticationmethod/otpviasms.
2. Зарегистрировать компонент для рассылки сообщений через SMS. Данная процедура описана в разделе 4.9.5.4.

Для успешной аутентификации в профиле Пользователя должен быть задан номер телефона.

5.5.3. Аутентификация с использованием одноразовых Email-паролей

При использовании данного метода для подтверждения входа и операций дополнительно у Пользователя будет запрашиваться ввод одноразового пароля, доставляемого по электронной почте.

Данный вид вспомогательной аутентификации требует подключения к почтовому серверу в соответствии со схемой размещения компонентов (см раздел 5.2 ЖТЯИ.00046-03 90 02. КриптоПро DSS. Общее описание) и в соответствии с требованиями к подключению к сетям общего пользования, описанными в Разделе 10 ЖТЯИ.00046-03 95 01. Правила пользования.

Для использования данного метода двухфакторной аутентификации необходимо:

1. Включить с помощью командлета Enable-DssAuthenticationMethod метод аутентификации с идентификатором http://dss.cryptopro.ru/identity/authenticationmethod/otpviaemail.
2. Зарегистрировать компонент для рассылки сообщений через Email. Данная процедура описана в разделе 4.9.5.6.

Для успешной аутентификации в профиле Пользователя должен быть задан адрес электронной почты.

5.5.4. Аутентификация с использованием протокола OATH

При использовании данного метода двухфакторной аутентификации у Пользователя будет запрашиваться ввод одноразового пароля, полученного с помощью OATH-токена.

СЭП «КриптоПро DSS» поддерживает работу с токенами, работающими по алгоритму HOTP (соответствующая спецификация RFC доступна по адресу http://tools.ietf.org/html/rfc4226).

Для использования данного метода необходимо:

1. Включить с помощью командлета Enable-DssAuthenticationMethod метод аутентификации с идентификатором http://dss.cryptopro.ru/identity/authenticationmethod/oath.
2. Зарегистрировать плагин для чтения файлов инициализации токенов с помощью командлета Add-DssStsConverterPlugin.
3. Импортировать файл инициализации токенов с помощью командлета Import-DssStsOtpTokenData.
4. Назначить OATH-токен Пользователю.

Назначение OATH-токена происходит на странице редактирования учётной записи Пользователя (см. Рис. 42). После нажатия на кнопку «Назначить» открывается диалог для ввода серийного номера токена и двух первых OTP.

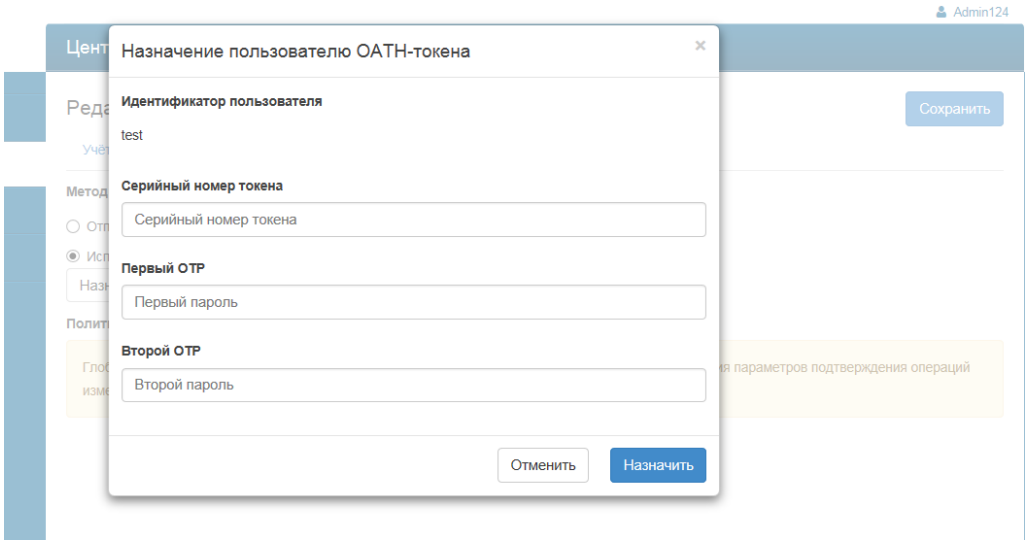

Рис. 42 – Назначение OATH-токена Пользователю

После успешного назначения токена требуется сохранить изменения учетной записи Пользователя, нажав кнопку «Сохранить».

Просмотр зарегистрированных токенов осуществляется на странице «Общие настройки» (см. Рис. 43).

На этой же странице доступен функционал по восстановлению синхронизации токена. Соответствующий диалог открывается при нажатии на кнопку «Восстановить синхронизацию». Для выполнения данной операции необходимо ввести два последовательных пароля, выданных OATH-токеном.

Поиск в отображаемой на странице таблице осуществляется по полям «Идентификатор», «Серийный номер», «Идентификатор Пользователя» и «Тип токена». Сортировка возможна по первым трём полям.

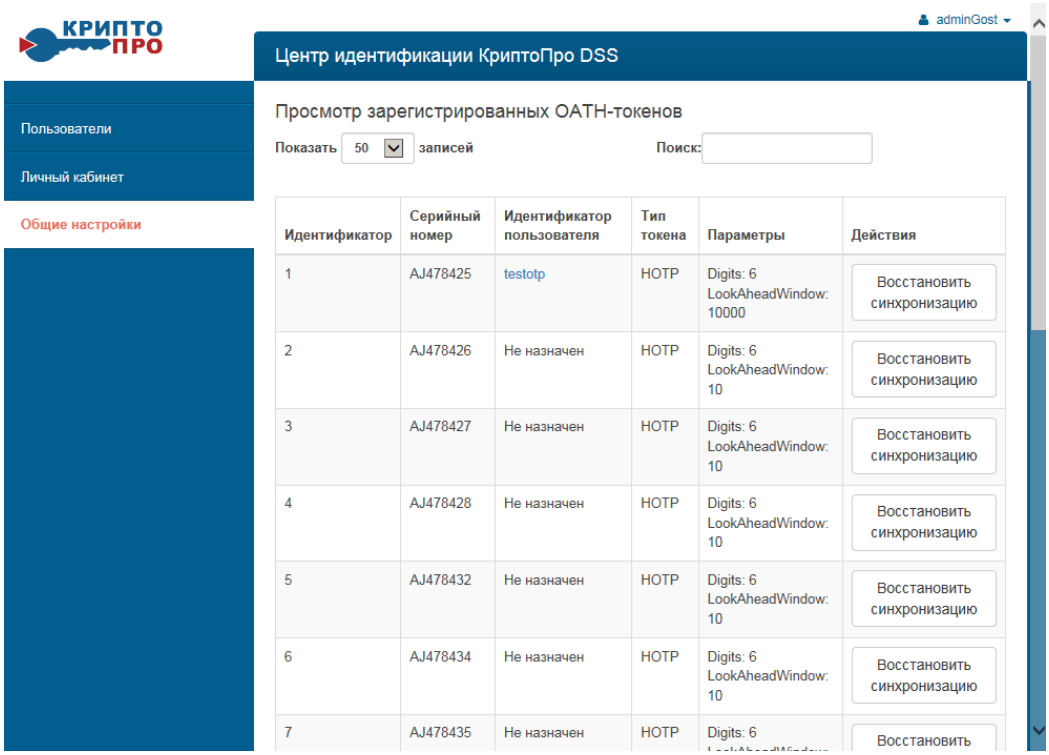

Рис. 43 – Просмотр списка зарегистрированных OATH-токенов

5.5.4.1. Регистрация oath-токенов eToken Pass

Ниже приведён пример PowerShell сценария для включения двухфакторной аутентификации для всех Пользователей с использованием одноразовых паролей, получаемых с помощью OATH-токенов eToken Pass. КриптоПро DSS умеет работать с двумя типами токенов eToken Pass: HOTP и TOTP.

Пример:

```
Set-DssStsProperties -MfaPolicy On
Enable-DssAuthenticationMethod -Uri
http://dss.cryptopro.ru/identity/authenticationmethod/oath
Add-DssStsConverterPlugin -Assembly
DSS.DocumentConverter.eTokenPass.dll -FileExtension dat
Import-DssStsOtpTokenData -FilePath C:\importAlpine.dat
```

Ниже представлен пример файла инициализации токенов eToken Pass.

Пример:

```
# ===== SafeWord Authenticator Records $Version: 100$ =====
dn: sccAuthenticatorId=AA000000
objectclass: sccCompatibleToken
sccAuthenticatorId: AA000000
sccTokenType: eToken-PASS-ES
sccTokenData:
sccKey=0000000000000000000000000000000000000000;sccMode=E;sccPwLen=6;crypto=H
macSHA1;sccVer=6.2;
sccSignature:
MC0CFQDAzhIZ3NYTU42RiGKALvfNTKuunAIUFG8f7grd239knrNUOaHdfhhaSa0=t
```

5.5.4.2. Регистрация oath-токенов Gemalto Lava

Ниже приведён пример PowerShell-сценария для включения двухфакторной аутентификации для всех Пользователей с использованием одноразовых паролей, получаемых с помощью OATH-токенов Gemalto Lava. КриптоПро DSS умеет работать с одним типом токенов Gemalto Lava: TOTP. При импорте файлов инициализации Gemalto требуется задать пароль для расшифрования данных.

Пример:

```
Set-DssStsProperties -MfaPolicy On
Enable-DssAuthenticationMethod -Uri
http://dss.cryptopro.ru/identity/authenticationmethod/oath
Add-DssStsConverterPlugin -Assembly
DSS.DocumentConverter.Gemalto.dll -FileExtension xml
Import-DssStsOtpTokenData -FilePath C:\importGemaltoLavaTB.xml -Parameters @{
"password" = "your password"}
```

Ниже представлен пример файла инициализации токенов Gemalto Lava.

Пример:

```
<SecretContainer xmlns="http://www.w3.org/2001/XMLSchema" xmlns:oath-
pskc="http://www.openauthentication.org/OATH/2006/10/PSKC"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.openauthentication.org/OATH/2006/10/PSKC/oath_
pskc_schema_v1.2.xsd" version="1.0">
      <EncryptionMethod algorithm="PBE-AES128-CBC">
            <PBESalt>EW0h0yUcDX72WU9UiKiCwDpXsJg=</PBESalt>
            <PBEIterationCount>128</PBEIterationCount>
            <IV>ixYgnjjY58RNacxZHwxgBQ==</IV>
      </EncryptionMethod>
      <DigestMethod algorithm="HMAC-SHA1"></DigestMethod>
      <Device>
            <DeviceId>
                  <Manufacturer>Gemalto</Manufacturer>
                  <SerialNo>GAKT0000A7EF</SerialNo>
                  <Model>EZIO</Model>
            </DeviceId>
            <Secret SecretAlgorithm="HOTP" SecretId="GAKT0000A7EF">
                  <Issuer>Gemalto</Issuer>
                  <Usage otp="true">
                        <AlgorithmIdentifier>
                              <Algorithm>OCRA-HOTP</Algorithm>
                              <CryptoFunction>HMAC-SHA1</CryptoFunction>
                              <Truncation>6</Truncation>
                              <Pin>false</Pin>
                              <Counter>false</Counter>
                              <Time>true</Time>
                              <Session>false</Session>
                              <Challenge>false</Challenge>
                        </AlgorithmIdentifier>
                        <ResponseFormat format="DECIMAL" length="6" />
                  </Usage>
                  <Data Name="SECRET">

      <Value>MxbBpkI2UQVUlWUoYlVa0n3sbchSD7dT5wwzGQQFqK8=</Value>

      <ValueDigest>KAZnz0QJuRxJEpctzfFnHRe/uhs=</ValueDigest>
                  </Data>
                  <Data Name="TIME">
                        <Value>MA==</Value>
                  </Data>
                  <Data Name="TIME_INTERVAL">
                        <Value>MzA=</Value>
                  </Data>
                  <Data Name="CLOCK_DRIFT">
                        <Value>NA==</Value>
```

```
                  </Data>
            </Secret>
      </Device>
</SecretContainer>
```

5.5.4.3. Регистрация oath-токенов Feitian

Ниже приведён пример PowerShell-сценария для включения двухфакторной аутентификации для всех Пользователей с использованием одноразовых паролей, получаемых с помощью OATH-токенов Feitian. КриптоПро DSS умеет работать с двумя типами токенов Feitian: c100, c200.

Пример:

```
Set-DssStsProperties -MfaPolicy On
Enable-DssAuthenticationMethod -Uri
http://dss.cryptopro.ru/identity/authenticationmethod/oath
Add-DssStsConverterPlugin -Assembly
DSS.DocumentConverter.Feitian.dll -FileExtension xml
Import-DssStsOtpTokenData -FilePath C:\importFeitian.xml
```

Ниже представлен пример файла инициализации токенов Feitian.

Пример:

```
<KeyContainer Version="1.0" xmlns ="urn:ietf:params:xml:ns:keyprov:pskc">
  <KeyPackage>
    <DeviceInfo>
      <Manufacturer>FeiTianOfChina</Manufacturer>
      <SerialNo>3600314100014</SerialNo>
    </DeviceInfo>
    <Key Id="3600314100014"
Algorithm="urn:ietf:params:xml:ns:keyprov:pskc:totp">
      <AlgorithmParameters>
        <ResponseFormat Length="8" Encoding="DECIMAL"/>
      </AlgorithmParameters>
      <Data>
        <Secret>
          <PlainValue>fEq9ZhqLxYo6rjgMW92Uav0bIzc=</PlainValue>
        </Secret>
        <Time>
          <PlainValue>0</PlainValue>
        </Time>
        <TimeInterval>
          <PlainValue>60</PlainValue>
        </TimeInterval>
      </Data>
      <Policy>
        <StartDate>2015-03-27T05:43:25Z</StartDate>
        <ExpiryDate>2018-02-22T07:14:50Z</ExpiryDate>
```

```
      </Policy>
    </Key>
  </KeyPackage>
```

6. Управление сервисными сертификатами

На Рис. 44 отображена настройка сервисных сертификатов в компонентах КриптоПро DSS. Рисунок иллюстрирует следующие требования к настройке и взаимодействию компонент КриптоПро DSS:

1. Каждому компоненту КриптоПро DSS назначается сервисный сертификат.
2. Между Центром Идентификации и остальными компонентами КриптоПро DSS необходимо установить отношение доверия. Установка отношений доверия осуществляется путём регистрации сервисного сертификата ЦИ в каждом из оставшихся компонент КриптоПро DSS.
3. Доверенные стороны должны быть зарегистрированы на Центре Идентификации.
4. В КриптоПро DSS должны быть настроены требования аутентификации доверенной стороны (подробнее про доверенные стороны см. раздел 4.5.3).

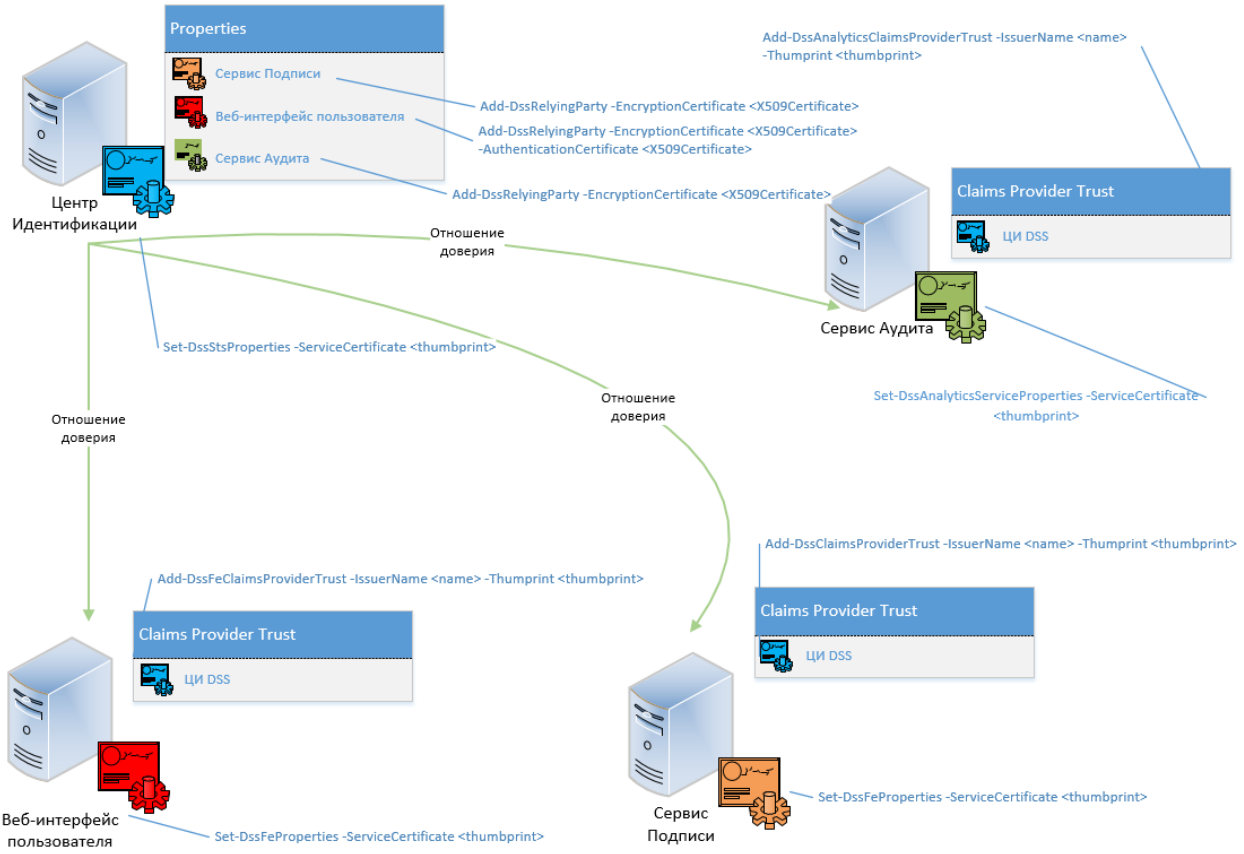

Рис. 44 – Сервисные сертификаты

Назначение сервисных сертификатов осуществляется с помощью командлетов, приведённых в Таблица 199.

Таблица 199. Командлеты для настройки сервисных сертификатов

Компонент	Командлет
Веб-интерфейс Пользователя	Set-DssFEProperties
Центр Идентификации	Set-DssStsProperties
Сервис Подписи	Set-DssProperties
Сервис Аудита	Set-DssAnalyticsServiceProperties

Для установления отношений доверия между Центром Идентификации и остальными компонентами КриптоПро DSS используются командлеты, приведённые в Таблица 200.

Таблица 200. Командлеты для установления отношений доверия с ЦИ DSS

Компонент	Командлет
Веб-интерфейс Пользователя	Add-DssFEClaimsProviderTrust
Сервис Подписи	Add-DssClaimsProviderTrust
Сервис Аудита	Add-DssAnalyticsClaimsProviderTrust

Установление отношений доверия между компонентами КриптоПро DSS и Центром Идентификации необходимо для проверки издателя маркера безопасности, с которым аутентифицируется Пользователь. Только маркеры безопасности, подписанные доверенным издателем, будут приняты на компонентах СЭП.

Для взаимодействия Веб-интерфейса Пользователя с Центром Идентификации необходимо дополнительное действие: зарегистрировать сервисный сертификат Веб-интерфейса Пользователя на Центре Идентификации. Веб-интерфейс Пользователя использует сервисный сертификат для аутентификации на Центре Идентификации при проверке прав доступа Пользователей и Операторов к Сервису Подписи. Данная настройка выполняется с помощью командлета Set-DssRelyingPartyTrust с параметром **AuthenticationCertificate**.

В некоторых сценариях взаимодействия компонентов КриптоПро DSS может применяться шифрование SAML-токенов. В активном сценарии взаимодействия с Сервисом Подписи (через SOAP-интерфейс) можно настроить на Центре Идентификации DSS шифрование SAML-токен, выпускаемых Пользователю. В этом случае содержимое SAML-токена будет недоступно Пользователю, так как SAML-токен зашифрован в сторону Сервиса Подписи. Для настройки шифрования SAML-токенов необходимо задать сертификат Сервиса Подписи на Центре Идентификации DSS. Данная настройка выполняется с помощью командлета Set-DssRelyingPartyTrust с параметром **EncryptionCertificate**.

Шифрование SAML-токенов не является обязательным требованием.

Необходимо, чтобы алгоритм открытого ключа хотя бы одного сертификата веб-сервера (IIS) и алгоритм открытого ключа сервисного сертификата ЦИ совпадали.

6.1. Требования к сервисным сертификатам

Сервисные сертификаты должны содержать в поле «Использование ключа» значения:

- Шифрование ключей (KEY ENCIPHERMENT);
- Цифровая подпись (DIGITAL SIGNATURE);
- Неотрекаемость (NON REPUDIATION).

В свойстве «Улучшенный ключ» должны быть заданы значения:

- Проверка подлинности сервера (1.3.6.1.5.5.7.3.1);
- Проверка подлинности клиента (1.3.6.1.5.5.7.3.2).

Требований к содержимому поля «Субъект» нет. В значении компоненты CN можно указать назначение сертификата, например, **DSS Sign Service Certificate**.

В качестве сервисного сертификата можно использовать самоподписанный сертификат большого срока действия. Его отзыв осуществляется организационными мерами. Пример создания самоподписанного сертификата приведён в разделе 6.2.

После получения сертификата его следует установить в хранилище «Личные» локального компьютера с привязкой к закрытому ключу.

После получения сертификата его следует установить в хранилище **Личные** локального компьютера с привязкой к закрытому ключу и в хранилище **Trusted People** без привязки к закрытому ключу.

После того, как будет создан экземпляр компонента, необходимо выдать учетной записи, от имени которой работает компонент, права на доступ к закрытому ключу сертификата. Подробнее о назначении прав см. раздел 6.2. Имена учетных записей компонентов КриптоПро DSS приведены в Таблица 201.

Таблица 201. Имена учётных записей компонент КриптоПро DSS по умолчанию

Компонент	Имя учётной записи
Веб-интерфейс Пользователя	IIS AppPool\CryptoProDSS-1-Frontend

Компонент	Имя учётной записи
Сервис Подписи	IIS AppPool\CryptoProDSS-1-SignServer
Центр Идентификации	IIS AppPool\CryptoProDSS-1-STS
Сервис Аудита	IIS AppPool\CryptoProDSS-1-AnalitycsService

6.2. Пример создания самоподписанного сервисного сертификата

Пример демонстрирует создание сервисного самоподписанного сертификата с помощью утилиты **certreq.exe**. Справку по использованию утилиты certreq.exe можно посмотреть по ссылке https://technet.microsoft.com/ru-ru/library/Cc725793(v=WS.10).aspx#BKMK_examples. Справку по формату файлов с шаблоном запроса на сертификат можно посмотреть по ссылке https://technet.microsoft.com/en-us/library/cc736326(v=ws.10).aspx.

Последовательность шагов по созданию сервисного сертификата:

1. Сохраните в файл с именем **template.txt** следующий блок текста:

```
[NewRequest]
Subject="CN=DSS Service Certificate"
KeyLength=2048
ProviderName="Microsoft Enhanced Cryptographic Provider v1.0"
ProviderType=1
; Generate Exchange key
KeySpec=1
; the private key can be exported
Exportable = TRUE
; Key Usage: DIGITAL SIGNATURE, NON REPUDIATION, KEY ENCIPHERMENT (e0)
KeyUsage=0xe0
; install keys under machine
MachineKeySet=true
; Generate self-signed certificate
RequestType=Cert
SMIME=FALSE
; EKU: Server Authentication
[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1
OID=1.3.6.1.5.5.7.3.2
```

В приведенном шаблоне сертификата можно отредактировать значение ключа **Subject**.

2. Запустите интерпретатор командной строки **cmd.exe** от имени Администратора.
3. Перейдите в каталог, где был сохранён шаблон сертификата **template.txt.**

4. Выполните команду:

```
%Windir%\System32\certreq.exe -new template.txt outcert.cer
```

5. При выполнении данной команды будет создан и установлен в хранилище Личное Локального компьютера сервисный сертификат. Также сертификат будет сохранён в файл **outcert.cer**.

6. Для использования данного сертификата необходимо будет выдать права на закрытый ключ, как описано в разделе 6.3.

6.3. Назначение прав доступа к закрытому ключу сертификата

Данное действие необходимо выполнять после развертывания экземпляров служб. (см. раздел 3).

Назначить права доступа к закрытому ключу можно в оснастке «Сертификаты». Для запуска оснастки выполните следующие шаги: Пуск – Выполнить – mmc. В открывшейся консоли управления выберите: **Файл – Добавить или удалить оснастку».** В открывшемся окне выберите оснастку «Сертификаты» и нажмите кнопку «Добавить (Рис. 45).

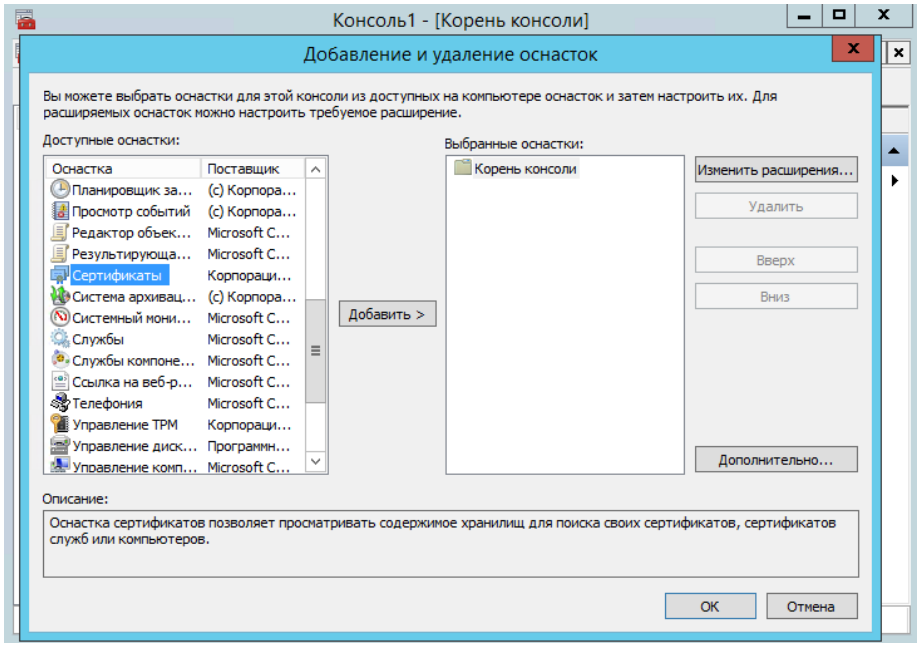

Рис. 45 – Диалог добавления и удаления оснасток

Далее в диалоге "Оснастка диспетчера сертификатов» выберите пункт «Учетной записи компьютера» и нажмите «Далее» (Рис. 46).

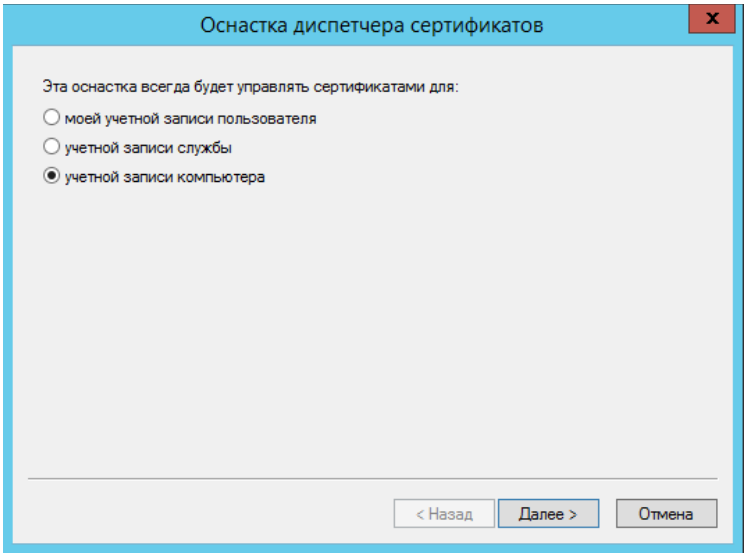

Рис. 46 – Оснастка диспетчера сертификатов

В качестве компьютера, которым будет управлять данная оснастка, необходимо указать локальный компьютер (Рис. 47)

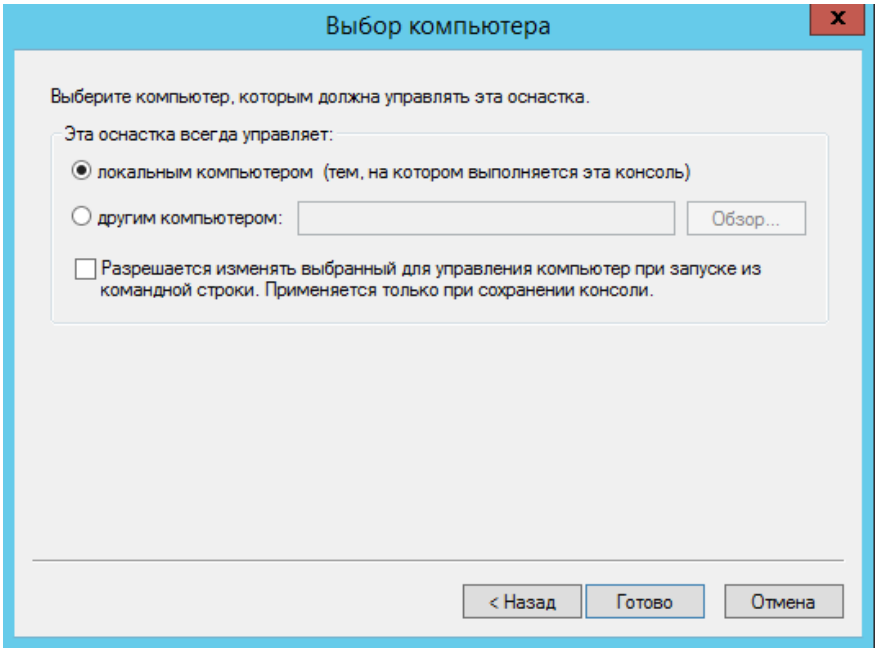

Рис. 47 – Выбор компьютера

Далее в разделе **Сертификаты (локальный компьютер) – Личное – Сертификаты** выберите нужный сертификат. Нажмите правой кнопкой мыши по выбранному сертификату и выберите: Все действия – Управление закрытыми ключами (Рис. 48).

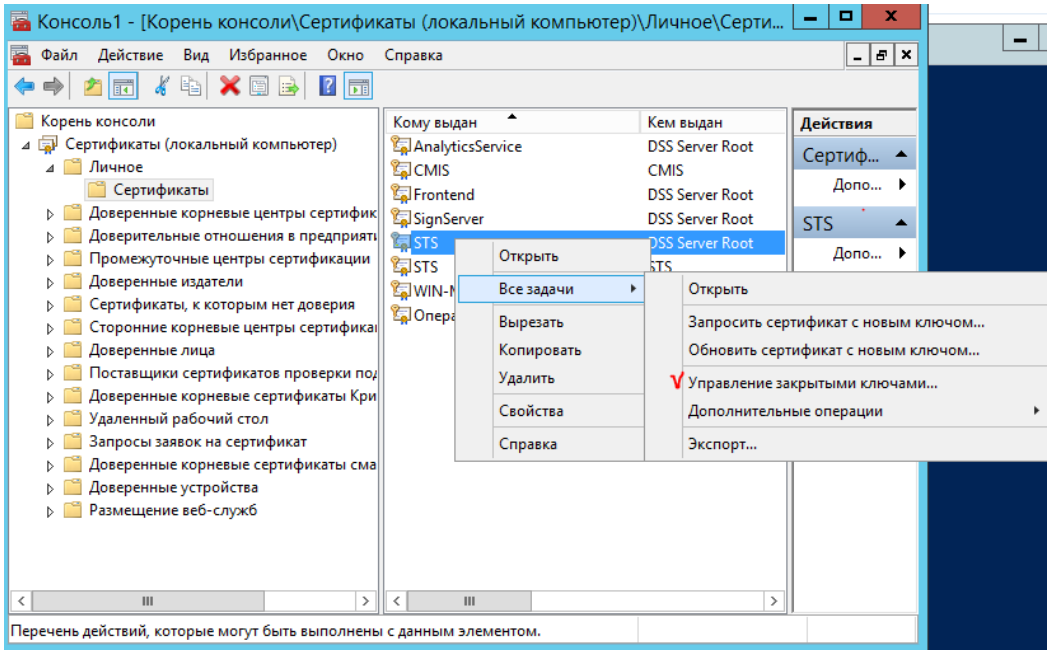

Рис. 48 – Настройка прав доступа к управлению закрытыми ключами

В открывшемся окне (Рис. 49) необходимо добавить учётную запись пула приложений и установить для неё полные права на доступ к закрытому ключу.

Имя учетной записи пула приложений имеет формат: **IIS AppPool\<Application Pool Name>**, где **«<Application Pool Name>»** - имя пула веб-приложения. Имя пула приложений можно посмотреть в оснастке управления IIS в разделе «Пулы приложений» или в основных настройках веб-приложения, которому требуется доступ к закрытому ключу сертификата. Чтобы запустить оснастку управления IIS выполните: **Пуск – Выполнить – inetmgr.**

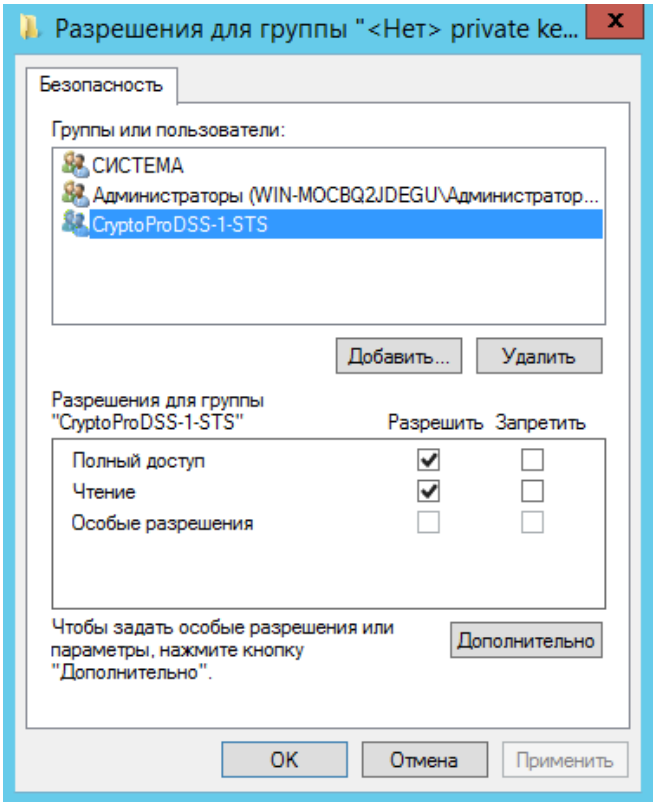

Рис. 49 – Установка прав на доступ к закрытому ключу

6.4. Примеры назначения и смены сервисных сертификатов

6.4.1. Пример назначения и смены сертификата Центра Идентификации

Назначение и/или смена сервисного сертификата Центра Идентификации происходит в два этапа:

- Назначение и/или смена сервисного сертификата Центра Идентификации.
- Назначение и/или смена сертификата подписи маркеров безопасности в компонентах DSS (Сервис Подписи, Веб-интерфейс Пользователя, Сервис Аудита).

Ниже приводится пример Powershell-сценария, демонстрирующий смену сертификата Центра Идентификации.

Пример:

```
# Назначение сервисного сертификата Центра Идентификации
Set-DssStsProperties –ServiceCertificate <thumbprint>

# (!) Примечание
# Пулу приложений Центра Идентификации необходимо выдать права на доступ к
закрытому
# ключу нового сервисного сертификата

# Назначение нового сертификата подписи маркеров безопасности на Сервисе
Подписи
# (если данных компонент установлен и развёрнут)
Set-DSSClaimsProviderTrust -IssuerName realsts –NewThumbprint <thumbprint>

# Назначение нового сертификата подписи маркеров безопасности на Сервисе
Подписи
# (если данных компонент установлен и развёрнут)
Set-DSSClaimsProviderTrust -IssuerName realsts –NewThumbprint <thumbprint>

# Назначение нового сертификата подписи маркеров безопасности
# на Веб-интерфейсе Пользователя
# (если данных компонент установлен и развёрнут)
Set-DSSFeClaimsProviderTrust -IssuerName realsts –NewThumbprint <thumbprint>

# Назначение нового сертификата подписи маркеров безопасности на Сервисе
Аудита
# (если данных компонент установлен и развёрнут)
Set-DssAnalyticsClaimsProviderTrust -IssuerName realsts –NewThumbprint
<thumbprint>

# (!) Примечание
```

```
# Значение параметра IssuerName можно посмотреть в выводе командлетов:
# Get-DSSClaimsProviderTrust
# Get-DSSFeClaimsProviderTrust
# Get-DSSCmisClaimsProviderTrust
# Get-DSSAnalyticsClaimsProviderTrust
# Имя издателя маркеров безопасности будет выведено в столбце «Имя»
```

Если сертификат Центра Идентификации подписи маркеров безопасности ещё не был зарегистрирован в компонентах DSS, то необходимо выполнить команды, приведённые ниже.

Пример:

```
# Регистрация сертификата подписи маркеров безопасности на Сервисе Подписи
# (если данный компонент установлен и развёрнут)
Add-DSSClaimsProviderTrust -IssuerName realsts –Thumbprint <thumbprint>

# Регистрация сертификата подписи маркеров безопасности на Веб-интерфейсе
Пользователя
# (если данных компонент установлен и развёрнут)
Add-DSSFeClaimsProviderTrust -IssuerName realsts –Thumbprint <thumbprint>

# Регистрация сертификата подписи маркеров безопасности на Сервисе Аудита
# (если данных компонент установлен и развёрнут)
Add-DSSAnalyticsClaimsProviderTrust -IssuerName realsts –Thumbprint
<thumbprint>
```

6.4.2. Пример назначения и смены сертификата Сервиса Подписи

Назначение и/или смена сервисного сертификата Сервиса Подписи происходит в два этапа:

- Назначение и/или смена сервисного сертификата Сервиса Подписи.
- Назначение и/или смена сертификата доверенной стороны на Центре Идентификации.

Если в качестве сервисного сертификата Сервиса Подписи используется сертификат с ключом ГОСТ Р 34.10-2001, то в настройках доверенной стороны необходимо задать требование шифрования маркеров безопасности.

Пример:

```
Set-DssRelyingPartyTrust –Id <signserver_id> -EncryptionCertificate <
X509Certificate2 ИЛИ путь к нему> -DisableTokenEncryption 0
```

где

<signserver_id> – идентификатор доверенной стороны.

< X509Certificate2 ИЛИ путь к нему > – Сертификат шифрования маркера безопасности для доверенной стороны X509Certificate2 или путь к файлу с сертификатом.

Ниже приводится пример Powershell-сценария, демонстрирующий смену сертификата Сервиса Подписи.

Пример:

```
# Назначение сервисного сертификата Сервиса Подписи
Set-DssProperties -ServiceCertificateThumbprint <thumbprint>

# (!) Примечание
# Пулу приложений Сервиса Подписи необходимо выдать права на доступ к
закрытому
# ключу нового сервисного сертификата

# (!) Примечание
# Перед выполнением следующей команды необходимо перезапустить
# Сервис Подписи для того, чтобы изменения вступили в силу
# Для перезапуска только пула приложений Сервиса Подписи выполните команду:
# Restart-WebAppPool CryptoProDSS-1-<AppName>
# <AppName> - имя веб-приложения Сервиса Подписи. По умолчанию - SignServer
# Для перезапуска IIS полностью выполните команду:
# iisreset

# Назначение нового сертификата доверенной стороны на Центре Идентификации
Set-DssRelyingPartyTrust -Id <signserver_ID> -MetadataUri
http://<hostname>/<AppName>/FederationMetadata/2007-06/FederationMetadata.xml

# в примере выше:
# <hostname> - имя хоста, на котором развёрнут экземпляр Сервиса Подписи
# <AppName> - имя веб-приложения Сервиса Подписи. По умолчанию - SignServer
# <signserver_ID> - идентификатор доверенной стороны. Значение параметра
можно
#                   посмотреть в выводе командлета Get-DssRelyingPartyTrust
# Доступность метаданных Сервиса Подписи можно проверить через браузер
# обратившись по адресу:
# http://<hostname>/<AppName>/FederationMetadata/2007-
06/FederationMetadata.xml
```

Если Сервис Подписи ещё не был зарегистрирован на Центре Идентификации в качестве доверенной стороны, то необходимо выполнить команду:

```
Add-DssRelyingPartyTrust -Name "Сервис электронной подписи" -MetadataUri
http://<hostname>/<AppName>/FederationMetadata/2007-06/FederationMetadata.xml

# в примере выше:
# <hostname> - имя хоста, на котором развёрнут экземпляр Сервиса Подписи
# <AppName> - имя веб-приложения Сервиса Подписи. По умолчанию - SignServer
```

6.4.3. Пример назначения и смены сертификата Веб-интерфейса Пользователя

Назначение и/или смена сервисного сертификата Веб-интерфейса Пользователя происходит в два этапа:

- Назначение и/или смена сервисного сертификата Веб-интерфейса Пользователя.
- Назначение и/или смена сертификата доверенной стороны на Центре Идентификации.

Ниже приводится пример Powershell-сценария, демонстрирующий смену сертификата Веб-интерфейса Пользователя.

Пример.

```
# Назначение сервисного сертификата Веб-интерфейса Пользователя
Set-DSSFEProperties -ServiceCertificate <thumbprint>

# (!) Примечание
# Пулу приложений Веб-интерфейса Пользователя необходимо выдать
# права на доступ к закрытому нового сервисного сертификата

# (!) Примечание
# Перед выполнением следующей команды необходимо перезапустить
# Веб-интерфейс Пользователя для того чтобы изменения вступили в силу
# Для перезапуска только пула приложений Веб-интерфейса Пользователя
# Выполните команду:
# Restart-WebAppPool CryptoProDSS-1-<AppName>
# <AppName> - имя веб-приложения Веб-интерфейса Пользователя.
# По умолчанию - Frontend
# Для перезапуска IIS полностью выполните команду:
# iisreset

# Назначение нового сертификата доверенной стороны на Центре Идентификации
Set-DssRelyingPartyTrust -Id <frontend_ID> -MetadataUri
https://<hostname>/<AppName>/FederationMetadata/2007-
06/FederationMetadata.xml

# в примере выше:
# <hostname> - имя хоста, на котором развёрнут экземпляр
#              Веб-интерфейса Пользователя.
# <AppName> - имя веб-приложения веб-интерфейса Пользователя. По умолчанию -
SignServer
# <frontend_ID> - идентификатор доверенной стороны. Значение параметра можно
#                   посмотреть в выводе командлета Get-DssRelyingPartyTrust
# Доступность метаданных Веб-интерфейса Пользователя можно проверить через
браузер
# обратившись по адресу:
# https://<hostname>/<AppName>/FederationMetadata/2007-
06/FederationMetadata.xml
```

6.4.4. Пример назначения и смены сертификата Сервиса Аудита

Назначение и/или смена сервисного сертификата Сервиса Аудита происходит в два этапа:

- Назначение и/или смена сервисного сертификата Сервиса Аудита.
- Назначение и/или смена сертификата доверенной стороны на Центре Идентификации.

Ниже приводится пример Powershell-сценария, демонстрирующий смену сертификата Сервиса Аудита.

Пример.

```
# Назначение сервисного сертификата Сервиса Аудита
Set-DSSAnalyticsServiceProperties -ServiceCertificateThumbprint <thumbprint>

# (!) Примечание
# Пулу приложений Сервиса Аудита необходимо выдать
# права на доступ к закрытому нового сервисного сертификата

# (!) Примечание
# Перед выполнением следующей команды необходимо перезапустить
# Сервис Аудита для того чтобы изменения вступили в силу
# Для перезапуска только пула приложений Сервиса Аудита выполните команду:
# Restart-WebAppPool CryptoProDSS-1-<AppName>
# <AppName> - имя веб-приложения Сервиса Аудита. По умолчанию -
AnalyticsService
# Для перезапуска IIS полностью выполните команду:
# iisreset

# Назначение нового сертификата доверенной стороны на Центре Идентификации
Set-DssRelyingPartyTrust -Id <AnalyticsService> -MetadataUri
http://<hostname>/<AppName>/FederationMetadata/2007-06/FederationMetadata.xml

# в примере выше:
# <hostname> - имя хоста, на котором развёрнут экземпляр Сервиса Аудита.
# <AppName> - имя веб-приложения Сервиса Аудита. По умолчанию -
AnalyticsService
# <AnalyticsService> - идентификатор доверенной стороны. Значение параметра
можно
#             посмотреть в выводе командлета Get-DssRelyingPartyTrust
# Доступность метаданных Сервиса Аудита можно проверить через браузер
# обратившись по адресу:
# http://<hostname>/<AppName>/FederationMetadata/2007-
06/FederationMetadata.xml
```

7. Диагностика

7.1. Устранение неполадок

В случае неверной настройки компонентов КриптоПро DSS, его веб-сервисы могут быть недоступны. Для первоначального определения службы, которая была настроена неправильно, можно проверить ее работоспособность путем обращения к ее базовой странице запуска. Базовые страницы запуска перечислены в Таблица 202.

Таблица 202. Базовые страницы запуска WCF-служб КриптоПро DSS

Компонент	Служба	Страница запуска
Центр Идентификации	Служба выпуска маркеров безопасности	http://<host_name>/STS/active.svc
	Служба управления Пользователями	http://<host_name>/STS/usermanagement.svc
Сервис Подписи	Служба Сервиса Подписи	http://<host_name>//signserver/signservice.svc
Сервис Аудита	Служба обработки событий аудита	http://<host_name>/AnalyticsService/analyticsservice.svc
	Служба записи событий аудита	http://<host_name>/AnalyticsService/AuditWriter.svc
myDSS	Служба Сервиса взаимодействия с ЦИ	http://<host_name>//MyDssServerInternal/service.svc
	Службы Сервиса взаимодействия с мобильным приложением	http://<host_name>//MyDssServerExternal/InteractionPushService.svc
		http://<host_name>//MyDssServerExternal/InteractionService.svc

В случае правильной настройки компонента служба успешно запустится, и будет выведена страница примерно следующего содержания (см. Рис. 50):

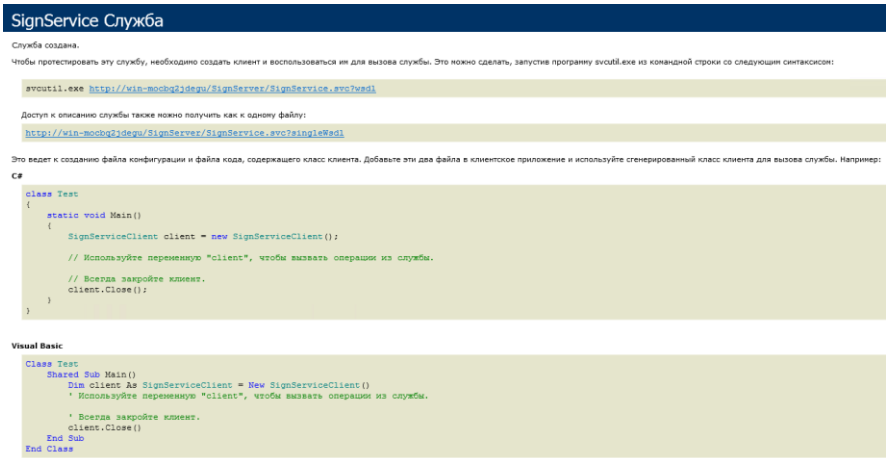

Рис. 50 - Страница успешного запуска WCF-службы

Если страница успешного запуска службы не появляется, необходимо обратиться к журналам Windows, где регистрируются ошибки запуска служб и другие системные события (см. раздел 7.2).

7.2. Журналы Windows

Основным средством диагностики СЭП «КриптоПро DSS» являются журналы Windows. При создании экземпляра каждого компонента СЭП «КриптоПро DSS» регистрируются два журнала: Admin и Operational (Рис. 51). Журнал Admin предназначен для Администраторов СЭП «КриптоПро DSS». Журнал Operational предназначен для сбора журналирования при диагностике и исправлении сложных ошибок. Ошибки на ранних стадиях запуска СЭП «КриптоПро DSS» могут быть записаны в Журнал Приложений (Applications). Источником событий в данном случае будут являться: System.ServiceModel 4.0.0.0, ASP.NET 4.0.

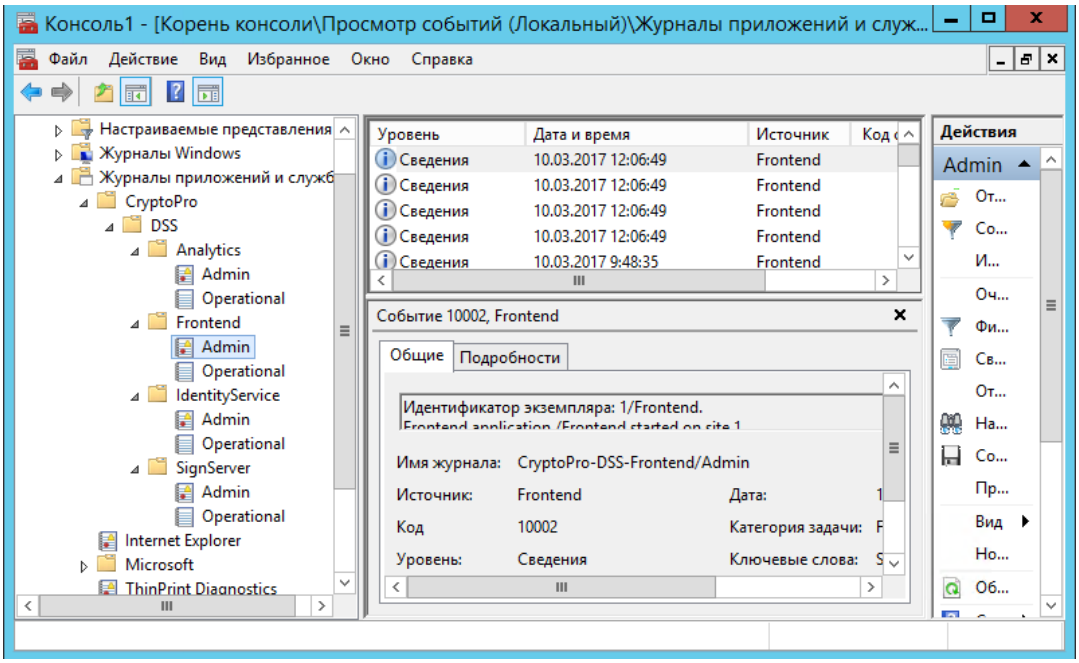

Рис. 51 – Журналы СЭП

7.3. Журналирование

СЭП «КриптоПро DSS» позволяет вести журналирование и протоколирование сообщений, которыми обмениваются веб-клиент и веб-службы СЭП «КриптоПро DSS».

Журналирование используется для вывода информации о потоке выполнения и отдельных действий различных компонентов распределенного приложения. Механизм протоколирования сообщений, в свою очередь, предназначен для сохранения содержимого сообщений, которыми обмениваются веб-клиент и веб-служба.

В СЭП «КриптоПро DSS» возможности журналирования предоставляются технологией Windows Communication Foundation (WCF). Основными источниками журналирования WCF являются **System.ServiceModel** и **System.ServiceModel.MessageLogging.** Источник журналирования **System.ServiceModel** — наиболее общий источник журналирования WCF,

записывающий основные этапы приложения по всему стеку связи WCF: от входа и выхода из транспорта до входа и выхода из пользовательского кода. Источник журналирования **System.ServiceModel.MessageLogging** записывает все сообщения, проходящие через систему.

СЭП «КриптоПро DSS» позволяет настроить журналирование из вышеуказанных источников отдельно для каждого из своих компонентов. Для каждого из источников журналирования можно настроить уровень журналирования и путь к файлу, в который будет записываться журналирование. Файлы журналирования имеют расширение «.svclog», и для просмотра таких файлов используется программа SvcTraceViewer.exe (дистрибутив поставляется в составе Windows SDK на официальном сайте Microsoft).

Настройка журналирования осуществляется с помощью командлетов, входящих в состав модулей **CryptoPro.DSS.PowerShell.SignServer**, **CryptoPro.DSS.PowerShell.Frontend.dll** и **CryptoPro.DSS.PowerShell.STS**, в зависимости от компонента для которого выполняется настройка. Все три модуля содержат однотипный набор команд для настройки журналирования. Список команд приведён в Таблица 203.

Для каждого из источников журналирования определен набор настраиваемых параметров:

- глобальная настройка для включения/отключения журналирования (с помощью командлетов **Enable/Disable-DssXXXTracing**);
- уровень журналирования, путь к файлу журналирования, максимальный размер одного файла трасировки и найстройка циклической перезаписи файла журналирования (с помощью командлетов **Set-DssXXXTracing**).

Здесь XXX – имя компонента для которого настаивается оповещение: SignServer, FE (Frontend), CMIS, AnalyticsService, UMS (User Management Service) или STS.

Таблица 203. Список команд для настройки журналирования

Командлет	Описание
Get-DssSignServerTracing Get-DssStsTracing Get-DssFeTracing Get-DssUmsTracing Get-DssAnalyticsServiceTracing Get-DssCmisTracing	Вывести список настраиваемых параметров.
Set-DssSignServerTracing Set-DssStsTracing Set-DssFeTracing Set-DssUmsTracing Set-DssAnalyticsServiceTracing Set-DssCmisTracing	Изменить настройки журналирования.
Enable-DssSignServerTracing Enable-DssStsTracing Enable-DssFeTracing Enable-DssUmsTracing Enable-DssAnalyticsServiceTracing Enable-DssCmisTracing	Включить журналирование.

Командлет	Описание
Disable-DssSignServerTracing Disable-DssStsTracing Disable-DssFeTracing Disable-DssUmsTracing Disable-DssAnalyticsServiceTracing Disable-DssCmisTracing	Отключить журналирование.

7.3.1. Командлет Set-DssSignServerTracing

Командлет **Set-DssSignServerTracing** позволяет установить значения параметров журналирования Сервиса Подписи.

Синтаксис:

```
Set-DssSignServerTracing [-ServiceModelListenerLogFile <string>]
[-ServiceModelListenerSourceLevel <SourceLevels> {Off | Critical | Error |
Warning | Information | Verbose | ActivityTracing | All}]
[-ServiceModelListenerMaxLogFileSize <int>]
[-ServiceModelListenerCircularFilesCount <int>]
[-ServiceModelMessageLoggingListenerLogFile <string>]
[-ServiceModelMessageLoggingListenerSourceLevel <SourceLevels> {Off |
Critical | Error | Warning | Information | Verbose | ActivityTracing | All}]
[-ServiceModelMessageLoggingListenerMaxLogFileSize <int>]
[-ServiceModelMessageLoggingListenerCircularFilesCount <int>]
[-DisplayName <string>]
```

Таблица 204. Параметры командлета Set-DssSignServerTracing

Параметр	Тип	Описание
DisplayName	string	Отображаемое имя экземпляра компонента Сервис Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
ServiceModelListenerLogFile	string	Путь к файлу журналирования из источника ServiceModel.
ServiceModelListenerSourceLevel	SourceLevels	Уровень журналирования из источника ServiceModel.
ServiceModelListenerMaxLogFileSize	int	Максимальный размер файла журналирования из источника ServiceModel (в байтах). Размер файла журналирования может принимать значение от ~5Mb до ~50Mb.
ServiceModelListenerCircularFilesCount	int	Максимальное количество создаваемых файлов журналирования от источника ServiceModel. Если значение выставлено в 0, то количество создаваемых файлов журналирования не ограничено.

Параметр	Тип	Описание
ServiceModelMessageLoggingListenerLogFile	string	Путь к файлу журналирования из источника ServiceModelMessageLogging.
ServiceModelMessageLoggingListenerSourceLevel	SourceLevels	Уровень журналирования из источника ServiceModelMessageLogging.
ServiceModelMessageLoggingListenerMaxLogFileSize	int	Максимальный размер файла журналирования из источника ServiceModelMessageLogging (в байтах). Размер файла журналирования может принимать значение от ~5Mb до ~50Mb.
ServiceModelMessageLoggingListenerCircularFilesCount	int	Максимальное количество создаваемых файлов журналирования от источника ServiceModelMessageLogging. Если значение выставлено в 0, то количество создаваемых файлов журналирования не ограничено.

SourceLevels — перечисление уровней журналирования, принимающее значения **All**, **Off**, **Critical**, **Error**, **Warning**, **Information**, **Verbose**, **ActivityTracing**. Более подробную информацию о данном перечислении можно узнать на сайте MSDN.

Параметры **ServiceModelListenerCircularFilesCount** и **ServiceModelMessageLoggingListenerCircularFilesCount** определяют количество создаваемых файлов журналирования. Значение «0» данных параметров означает отсутствие ограничения на количество создаваемых файлов журналирования. По достижению максимального размера файла (определяется параметрами **ServiceModelMessageLoggingListenerMaxLogFileSize** и **ServiceModelListenerMaxLogFileSize**) будет создан новый файл, в который в дальнейшем будет продолжаться запись журналирования. При достижении максимального количества файлов журналирования запись вновь начнётся с первого файла.

К моменту включения журналирования каталог для записи файлов журналирования должен существовать. В противном случае при запуске Сервиса Проверки Подписи произойдет критическая ошибка.

Учётной записи Сервиса Проверки Подписи требуется выдать права на запись в указанный каталог.

Командлеты **Set-DssFETracing**, **Set-DssAnalyticsServiceTracing**, **Set-DssCmisTracing**, **Set-DssUMSTracing** и **Set-DssStsTracing** работают аналогично.

7.3.2. Командлет Get-DssSignServerTracing

Командлет **Get-DssSignServerTracing** позволяет вывести на экран значения параметров журналирования Сервиса Подписи.

Синтаксис:

```
Get-DssSignServerTracing [-DisplayName <string>]
```

Командлеты **Get-DssFETracing, Get-DssAnalyticsServiceTracing, Get-DssCmisTracing, Get-DssUMSTracing** и **Get-DssStsTracing** работают аналогично.

7.3.3. Командлет Enable-DssSignServerTracing

Командлет Enable-DssSignServerTracing включает журналирование Сервиса Подписи.

Синтаксис:

```
Enable-DssSignServerTracing [-DisplayName <string>]
```

Командлеты **Enable-DssFETracing, Enable-DssAnalyticsServiceTracing, Enable-DssCmisTracing, Enable-DssUMSTracing** и **Enable-DssStsTracing** работают аналогично.

7.3.4. Командлет Disable-DssSignServerTracing

Командлет **Enable-DssSignServerTracing** отключает журналирование Сервиса Подписи.

Синтаксис:

```
Disable-DssSignServerTracing [-DisplayName <string>]
```

Командлеты **Disable-DssFETracing, Disable-DssAnalyticsServiceTracing, Disable-DssCmisTracing, Disable-DssUMSTracing** и **Disable-DssStsTracing** работают аналогично.

7.3.5. Пример PowerShell-сценария для настройки журналирования Сервиса Подписи

Данный сценарий задаёт необходимую настройку журналирования компонента Сервис Подписи. Для Веб-интерфейса Пользователя, Сервиса Аудита, Сервиса управления Пользователями и Центра Идентификации настройка журналирования выполняется аналогично.

```
# Настройка параметров журналирования
Set-DssSignServerTracing
-ServiceModelListenerLogFile "C:\DssLogs\ss_trace.svclog"
-ServiceModelListenerSourceLevel All
-ServiceModelListenerMaxLogFileSize 10000000
-ServiceModelMessageLoggingListenerLogFile "C:\DssLogs\ss_msg.svclog"
-ServiceModelMessageLoggingListenerSourceLevel All
-ServiceModelMessageLoggingListenerMaxLogFileSize 10000000
-ServiceModelListenerCircularFilesCount 10
-ServiceModelMessageLoggingListenerCircularFilesCount 10

# Включение журналирования
Enable-DssSignServerTracing
```

СВЕДЕНИЯ О РАЗРАБОТЧИКЕ

Компания КриптоПро создана в 2000 году и в настоящее время занимает лидирующее положение по распространению средств криптографической защиты информации и электронной цифровой подписи.

Основное направление деятельности компании - разработка средств криптографической защиты информации и развитие Инфраструктуры Открытых Ключей (Public Key Infrastructure) на основе использования международных рекомендаций и российских криптографических алгоритмов.

Компания разработала полный спектр программных и аппаратных продуктов для обеспечения целостности, авторства и конфиденциальности информации с применением ЭП и шифрования для использования в различных средах (Windows, Unix, Java). Новое направление продуктов компании – программно-аппаратные средства криптографической защиты информации и использованием смарт-карт и USB ключей, позволяющих существенно повысить безопасность систем, использующих ЭП.

Компания КриптоПро является разработчиком и поставщиком средств применения ЭП в автоматизированных информационных системах. Кроме этого, компания оказывает консультационные услуги по обеспечению деятельности удостоверяющих центров и применению ЭП в автоматизированных информационных системах предприятий различных форм собственности.

Удостоверяющий центр компании КриптоПро предоставляет организациям (юридическим лицам) услуги по изготовлению и управлению открытыми и закрытыми ключами Пользователей информационных систем, включая процедуру подачи и обработки запросов на сертификаты, верификацию запросов на сертификаты, формирования сертификатов, их получения, использования и отзыва. Также Удостоверяющим центром предоставляются иные сервисные функции, связанные с использованием электронных подписей, шифрованием, обеспечением электронного юридически-значимого документооборота.

Контакты:

ООО «КРИПТО-ПРО»

127018, Москва, ул. Сущёвский вал, 18

Телефон: (495) 995 4820

Факс: (495) 995 4820

URL: http://www.CryptoPro.ru

E-mail: info@CryptoPro.ru