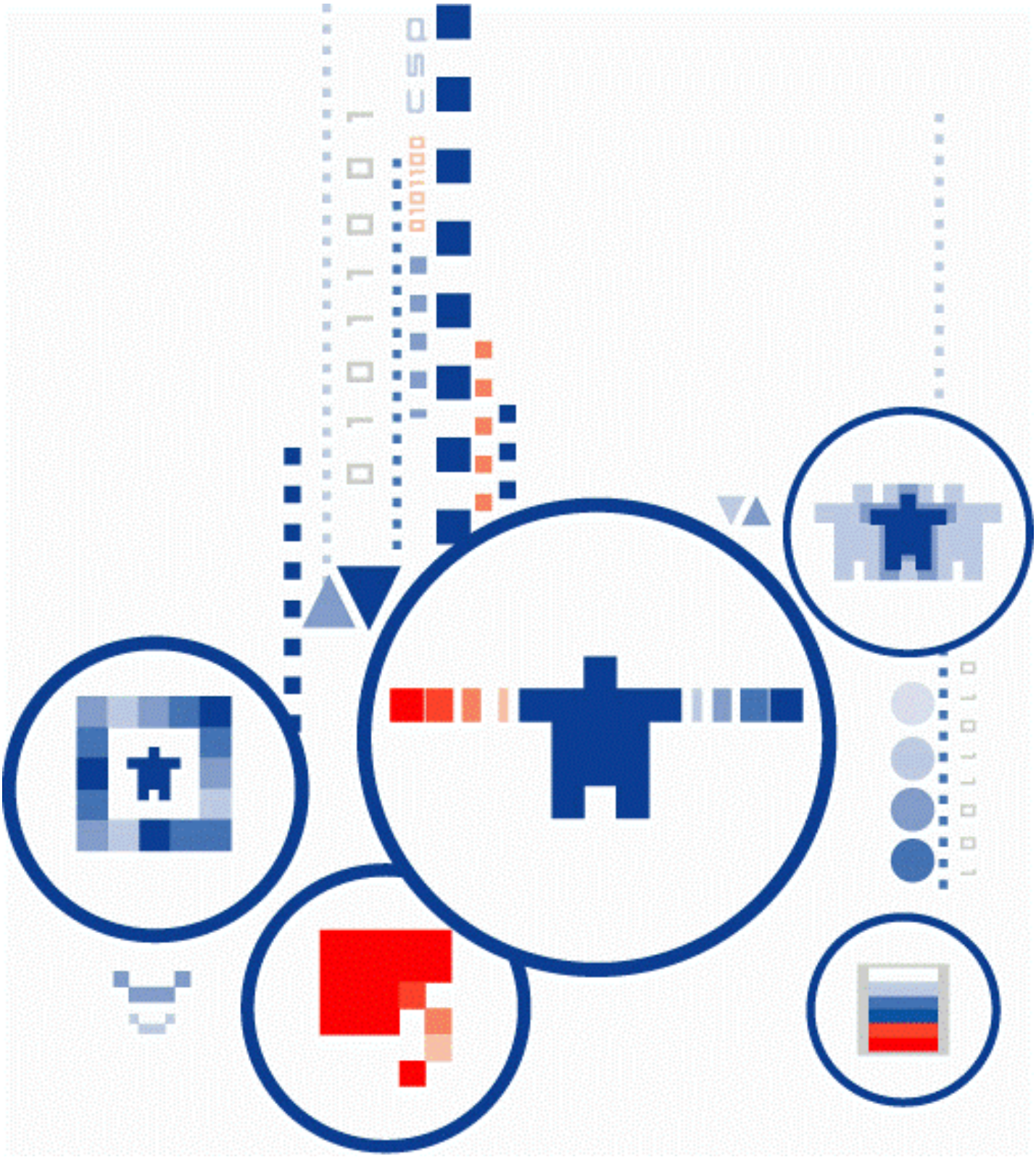


Сервер Электронной Подписи

"КриптоПро DSS"

Руководство Администратора

Содержание

Руководство Администратора КриптоПро DSS

Настоящий документ содержит Руководство Администратора Сервера Электронной Подписи (СЭП) «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».

Руководство Администратора КриптоПро DSS

Настоящий документ содержит Руководство Администратора Сервера Электронной Подписи (СЭП) «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».

Системные требования

В данном разделе описаны системные требования к СЭП «КриптоПро DSS».

- Аппаратные требования.
- Программные требования
- Требования к компонентам ОС, установленной на веб-сервере.

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 таблице ниже приведены минимальные требования к техническим средствам, которые обеспечивают установку компонентов СЭП и их работу при 1000 Пользователях:

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.

Требования к программному обеспечению

В таблице ниже 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.

Примечание

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.

НАЗВАНИЕ	СЕРВИС ПОДПИСИ	ЦЕНТР ИДЕНТИФИКАЦИИ	ВЕБ-ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ	СЕРВИС АУДИТА	MYDSS
Windows Server 2008 R2/2012/2012R2 (x64)/2016/2019	+	+	+	+	+, кроме Windows Server 2008 R2
Microsoft SQL Server 2008 R2/2012/2014/2016/2017/2019	+	+	-	+	+
КриптоПро HSM Client	+	-	-	-	+ (Internal Interaction Server)

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 компонентов, описанных ниже.

[!INCLUDE["Microsoft Windows Server 2008 R2"](../deploy/shared/Win2008.md)] [!INCLUDE["Microsoft Windows Server 2012, 2012 R2, 2016, 2019"](../deploy/shared/Win20122016.md)]

Развертывание КриптоПро DSS

В данном разделе описывается развертывание СЭП «КриптоПро DSS». Развертывание КриптоПро DSS осуществляется в следующем порядке:

1. Развертывание веб-сервера.
2. Установка КриптоПро CSP (входит в комплект поставки). Последние версии документации могут быть загружены с официального сайта.
3. Установка КриптоПро DSS и дополнительного ПО (включая автоматическую установку с диска Microsoft .NET Framework версии 4.6.1 и PowerShell версии 3.0).
4. Установка ПАКМ «КриптоПро HSM».
5. Развертывание ЦИ.
6. Развертывание Сервиса Подписи.
7. Развертывание Веб-интерфейса Пользователя (при необходимости).
8. Развертывание Сервиса Аудита (при необходимости).
9. Развертывание myDSS (при необходимости).
10. Развертывание Сервиса Обработки Документов (при необходимости).
11. Развертывание Сервиса Взаимодействия с DSS SDK (mDAG) (при необходимости).
12. Развертывание баз данных служб (при использовании для СЭП нескольких серверов).

Развертывание веб-сервера

В данном разделе описывается настройка компонентов и ролей Internet Information Services для следующих ОС:

- Microsoft Windows Server 2008 R2;
- Microsoft Windows Server 2012;
- Microsoft Windows Server 2012 R2, 2016, 2019.

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).

Примечание

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
```

Развертывание веб-сервера на ОС Microsoft Windows Server 2012

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

- ASP.NET 4.5 (3.5 достаточно для Windows Server 2012);
- Расширяемость .NET (.NET Extensibility 4.5) (3.5 достаточно для Windows Server 2012);
- 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 (NetFx4Extended-ASPNET45);
- Активация по HTTP (HTTP Activation).

Для автоматической настройки работы веб-сервера необходимо в командной строке, запущенной от имени администратора, выполнить 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:NetFx4Extended-ASPNET45 /FeatureName:WAS-ConfigurationAPI /FeatureName:netfx3serverfeatures
```

Развертывание веб-сервера на ОС Microsoft Windows Server 2012 R2, 2016

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

- ASP.NET 4.5 (3.5 достаточно для Windows Server 2012);
- Расширяемость .NET (.NET Extensibility 4.5) (3.5 достаточно для Windows Server 2012);
- 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 (NetFx4Extended-ASPNET45);
- Активация по HTTP (HTTP Activation).

Для автоматической настройки работы веб-сервера необходимо в командной строке, запущенной от имени администратора, выполнить 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:IIS-
NetFxExtensibility45 /FeatureName:NetFx4Extended-ASPNET45 /FeatureName:WAS-ConfigurationAPI
```

Развертывание веб-сервера на ОС Microsoft Windows Server 2012 R2, 2016

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

- ASP.NET 4.5 (3.5 достаточно для Windows Server 2012);
- Расширяемость .NET (.NET Extensibility 4.5) (3.5 достаточно для Windows Server 2012);
- 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 (NetFx4Extended-ASPNET45);
- Активация по HTTP (HTTP Activation).

Для автоматической настройки работы веб-сервера необходимо в командной строке, запущенной от имени администратора, выполнить 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:IIS-
NetFxExtensibility45 /FeatureName:NetFx4Extended-ASPNET45 /FeatureName:WAS-ConfigurationAPI
```

Установка, удаление и обновление КриптоПро DSS

Установка КриптоПро DSS

Для установки компонентов сервера электронной подписи «КриптоПро DSS» запустите установку пакета **DSSInstall.exe**, расположенного на компакт-диске.

Если на сервере, где устанавливается КриптоПро DSS, отсутствует необходимое дополнительное ПО (Microsoft .NET Framework, PowerShell 3.0, SQL Server Features Pack и Microsoft Visual C++ Redistributable Packages for Visual Studio 2015), будет предложена его установка. Для выполнения данного действия потребуются права администратора.

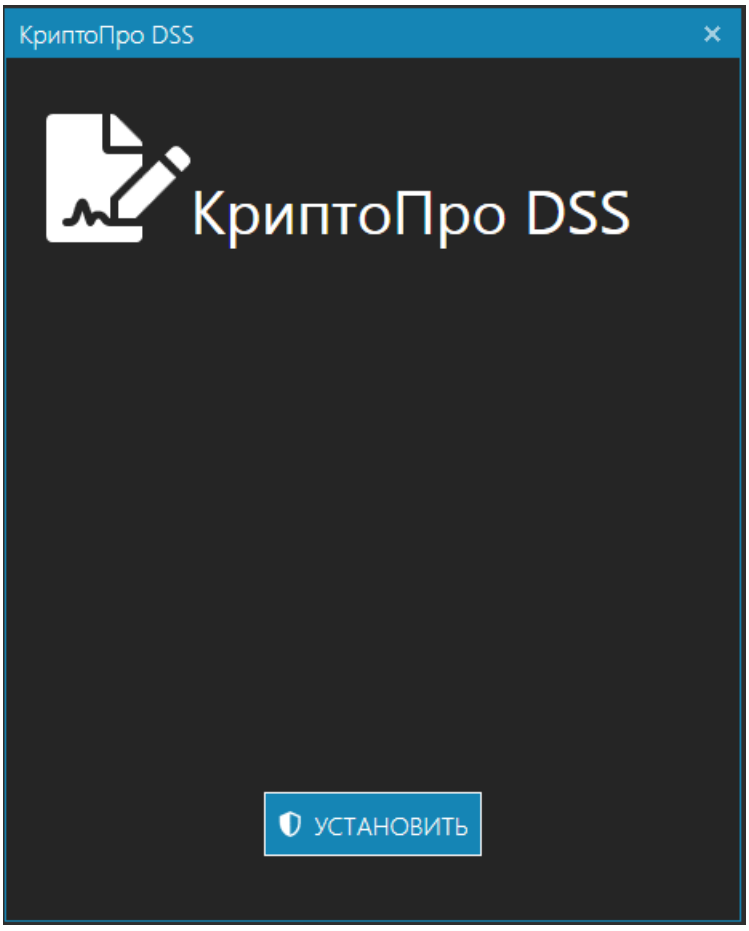
Примечание

Дальнейшая установка КриптоПро DSS возможна только после того, как соответствующее ПО будет установлено.

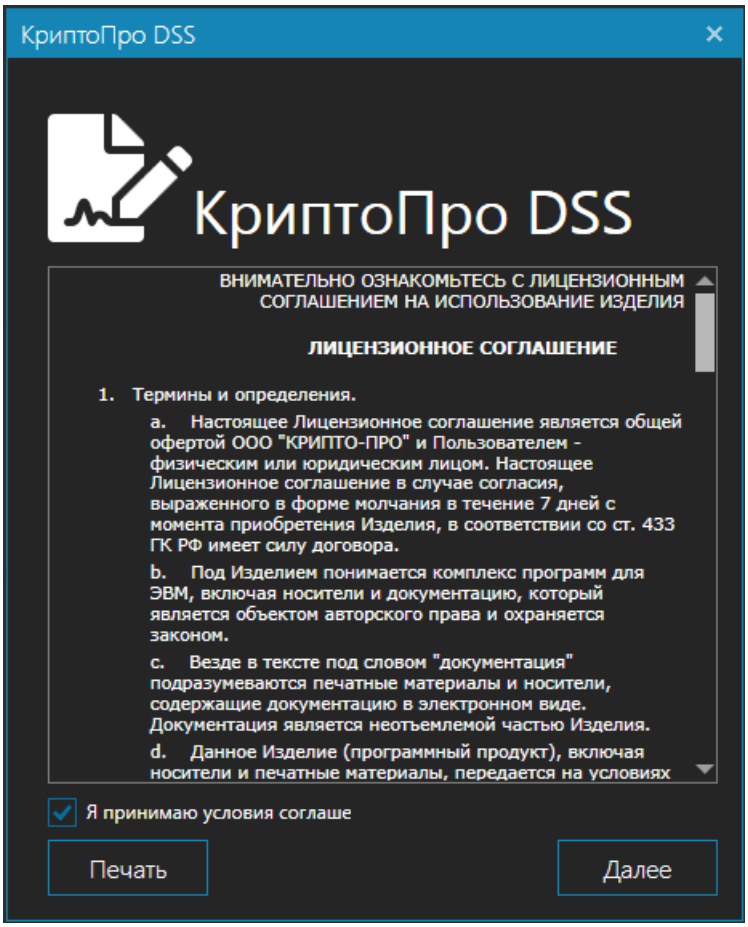
Примечание

При установке дополнительного ПО может потребоваться перезагрузка рабочей станции.

Как только дополнительное ПО будет установлено, запустится установщик КриптоПро DSS. Установка КриптоПро DSS должна осуществляться с правами администратора. После коротких подготовительных процедур на экране появится окно Мастера установки. Для начала установки нажмите кнопку "Установить".



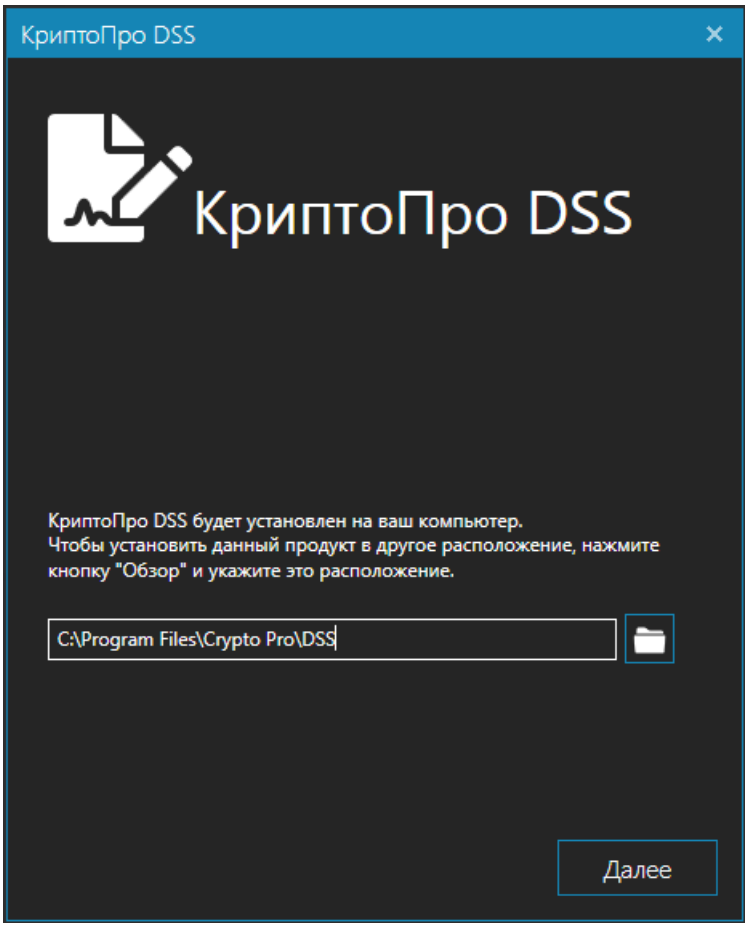
Ознакомьтесь с лицензионным соглашением на КриптоПро DSS. Если Вы согласны со всеми пунктами соглашения, выделите пункт «Я принимаю условия этого соглашения», и нажмите «Далее».



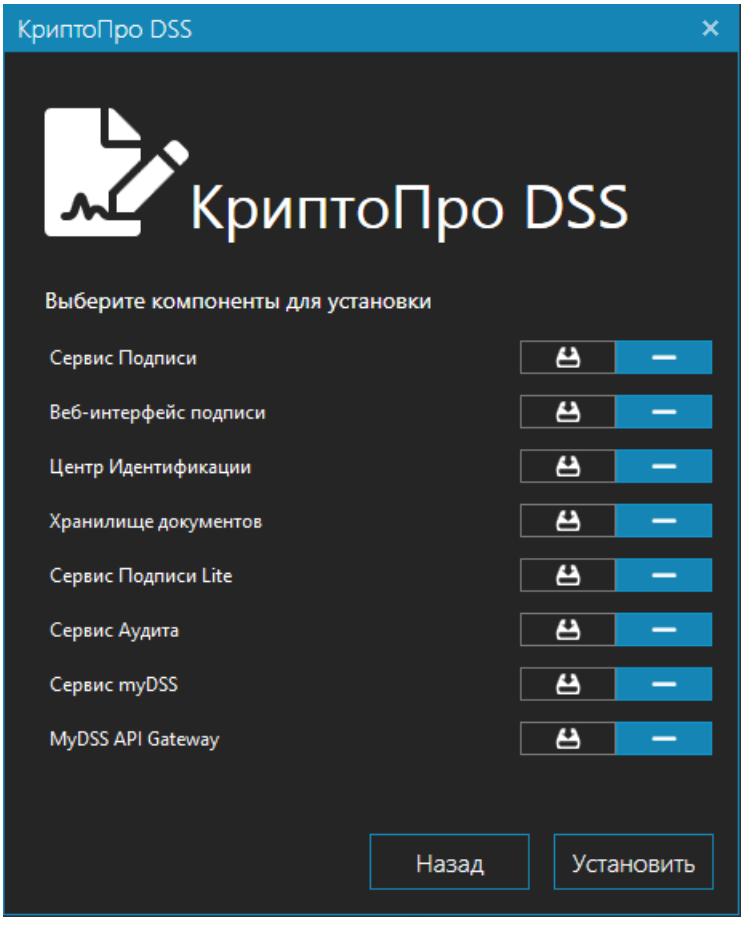
Выберите директорию, куда будет установлен КриптоПро DSS, и нажмите кнопку "Далее".

Примечание

Директорией по умолчанию является `C:\Program Files\Crypto Pro\DSS`. Не рекомендуется без крайней необходимости изменять директорию установки.

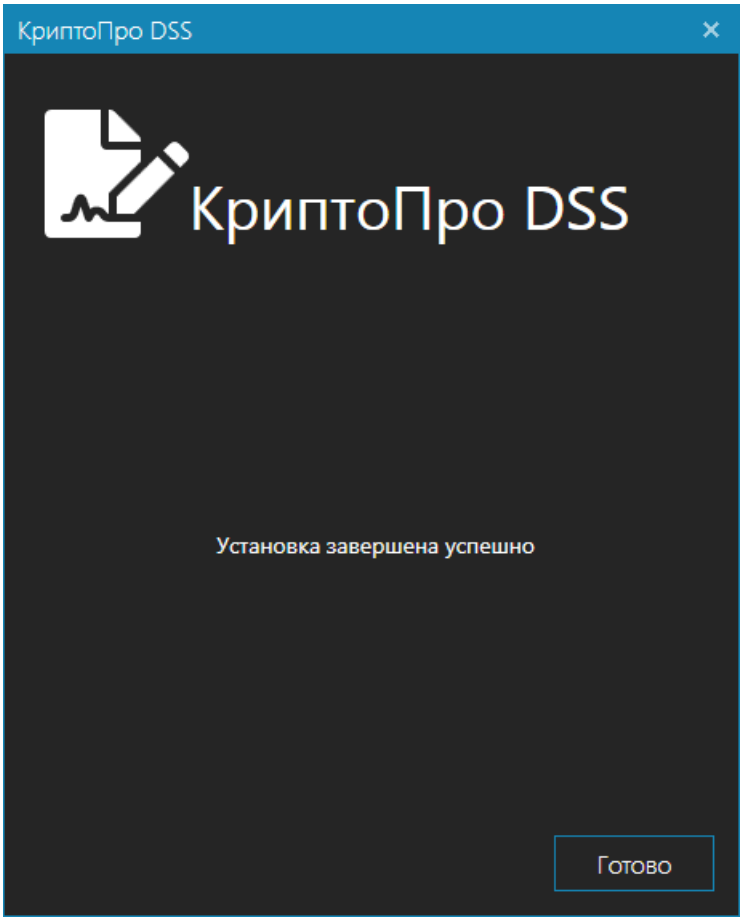


Выберите компоненты СЭП «КриптоПро DSS», которые будут установлены. Для этого переключите соответствующий значок компонента в "Компонент будет установлен" По умолчанию не выбран ни один из компонентов. Нажмите кнопку "Установить".



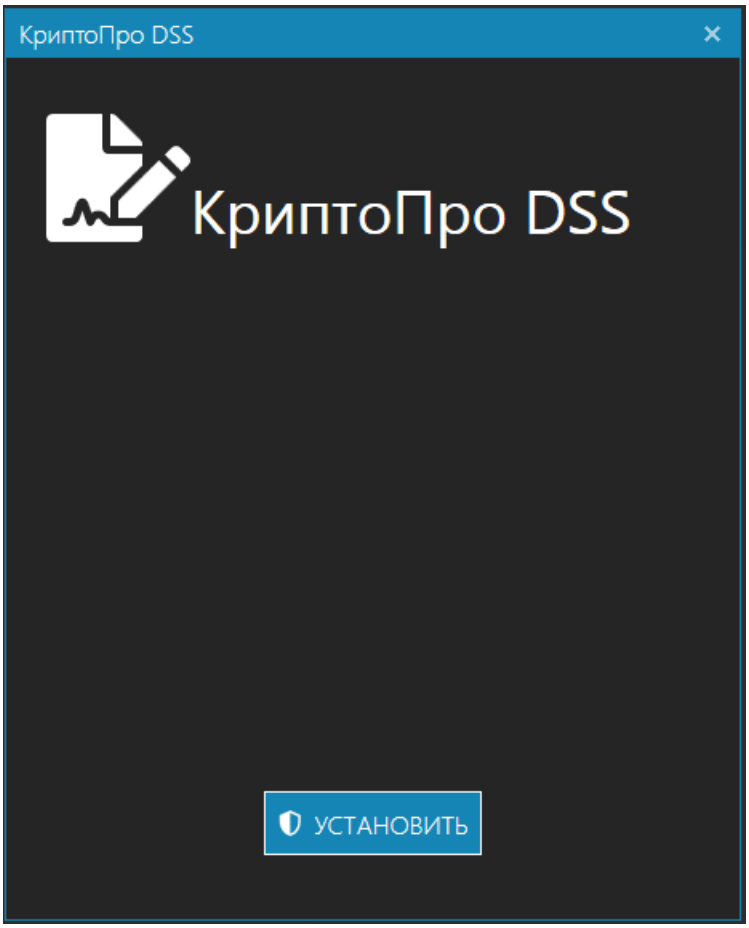
Далее начнется установка выбранных компонентов КриптоПро DSS. После ее завершения нажмите кнопку "Готово", чтобы

выйти из программы установки.



Добавление/удаление отдельных компонентов КриптоПро DSS

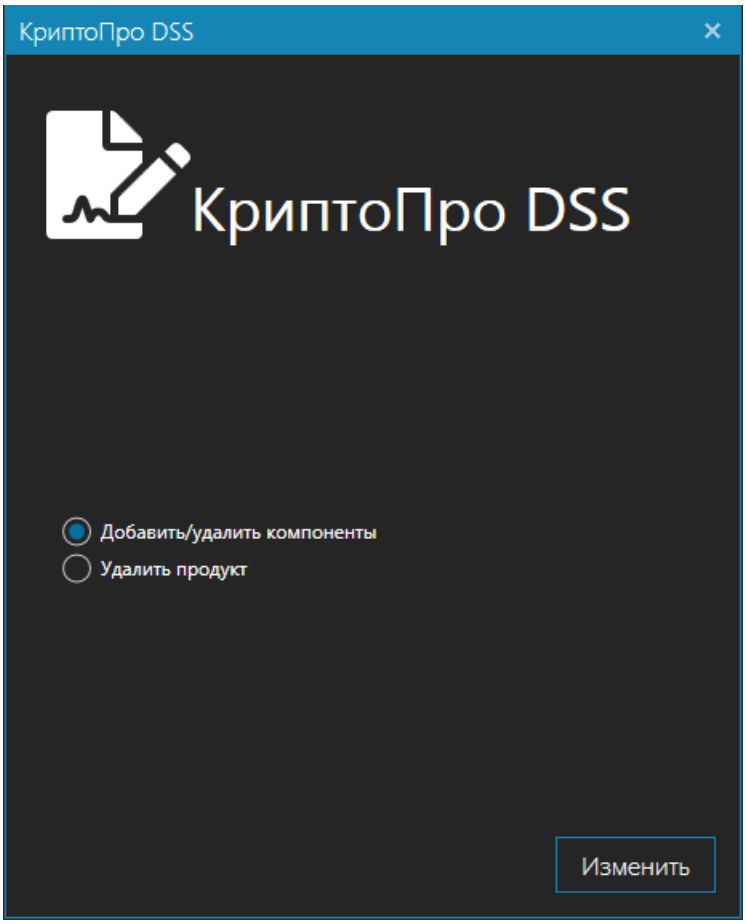
Для добавления или удаления компонентов сервера электронной подписи «КриптоПро DSS» запустите установку пакета **DSSInstall.exe**, расположенного на компакт-диске, и нажмите «Установить». Данное действие должно осуществляться от имени пользователя с правами администратора.



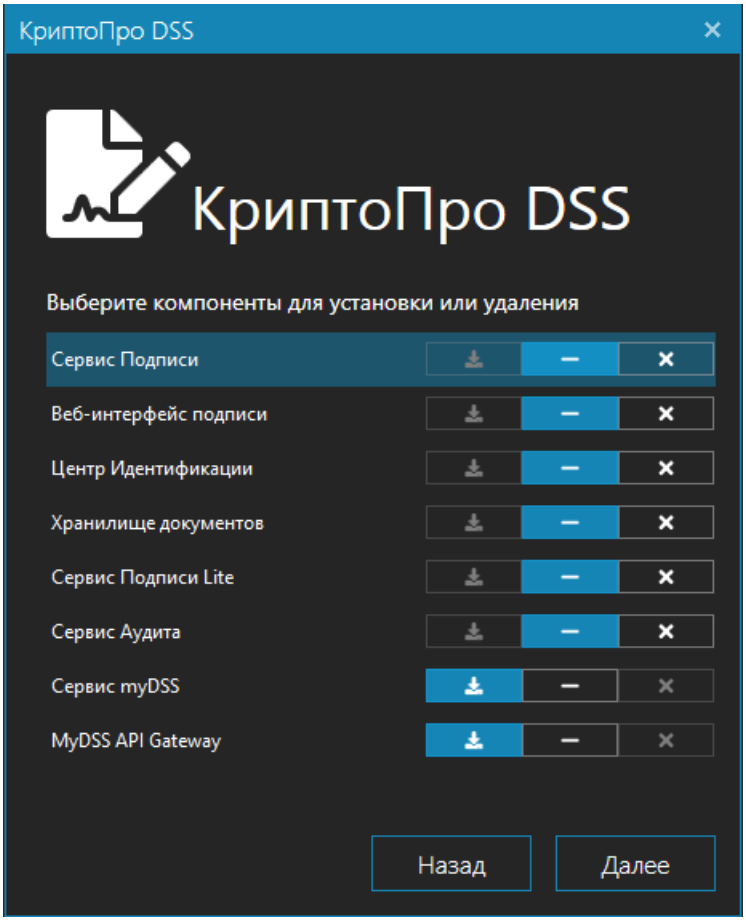
На следующей странице мастера установки выберите «Добавить/удалить компоненты» и нажмите кнопку «Изменить».

Примечание

Выбор удаления на данном этапе какого-либо компонента DSS НЕ удаляет созданные ранее экземпляры этого компонента. Для удаления экземляров воспользуйтесь полным удалением КриптоПро DSS.

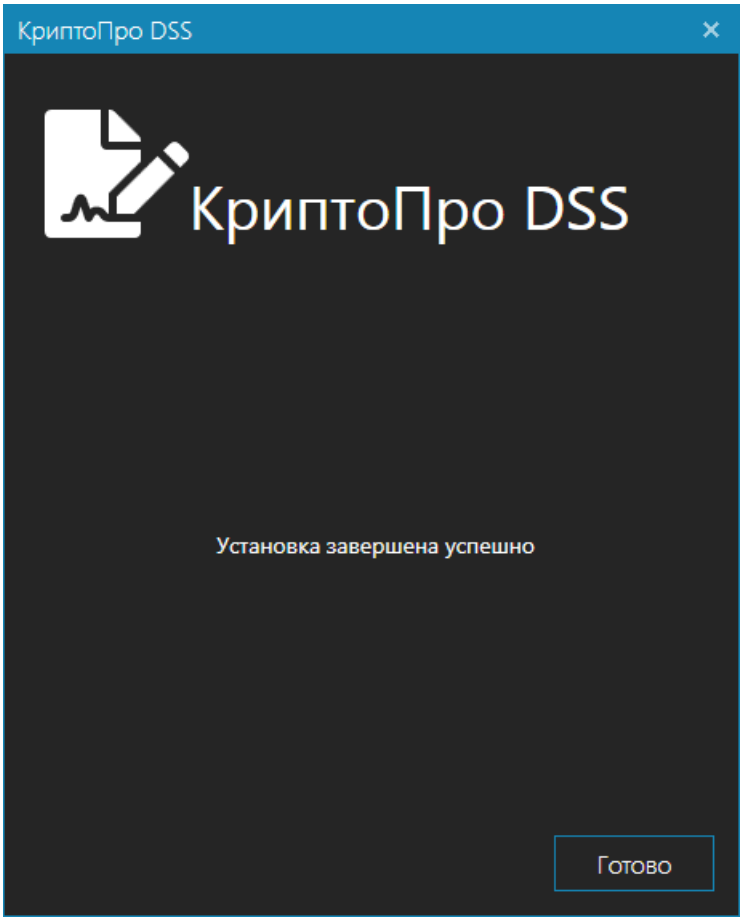


Выберите компоненты СЭП «КриптоПро DSS», которые будут добавлены или удалены. Для этого переключите соответствующий значок компонента в "Компонент будет установлен" или "Компонент будет удален". По умолчанию для каждого компонента выбрано значение "Состояние компонента не будет изменено". Нажмите кнопку "Далее".



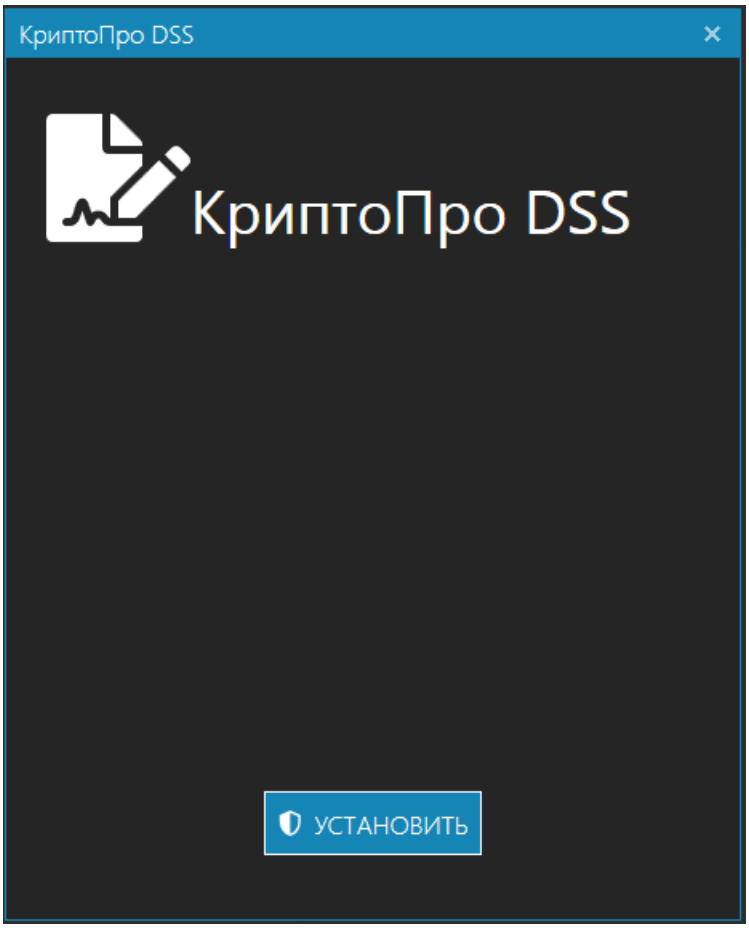
Далее начнется установка/удаление выбранных компонентов КриптоПро DSS. После ее завершения нажмите кнопку

"Готово", чтобы выйти из программы установки.



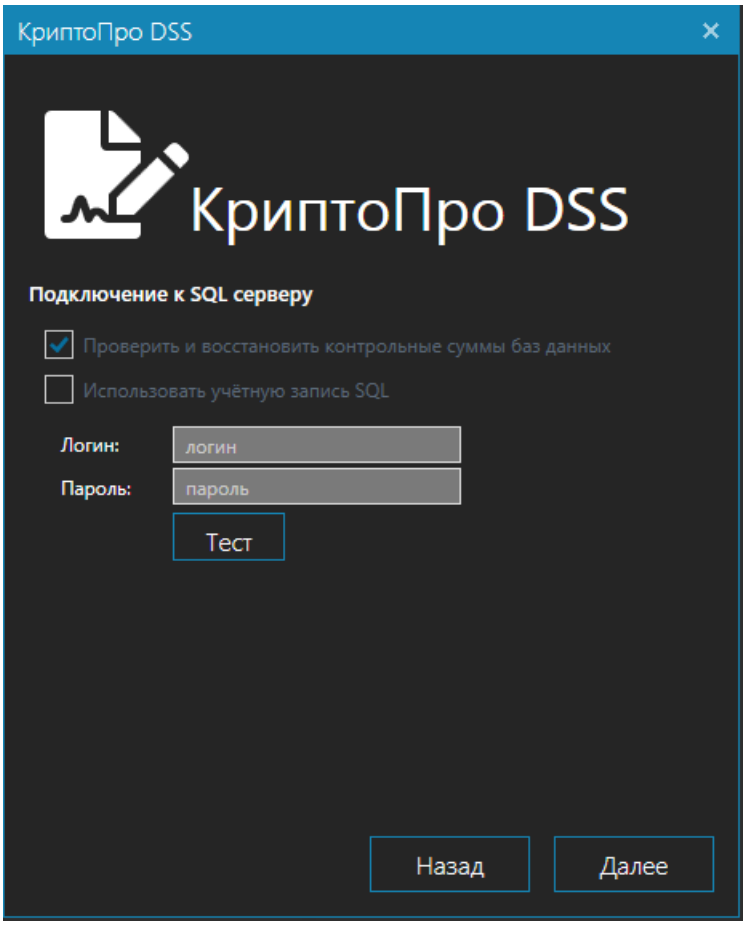
Удаление КриптоПро DSS

Для удаления всех установленных компонентов КриптоПро DSS и их экземпляров запустите установку пакета **DSSInstall.exe**, расположенного на компакт-диске, и нажмите «Установить». Удаление КриптоПро DSS должно осуществляться от имени пользователя с правами администратора.

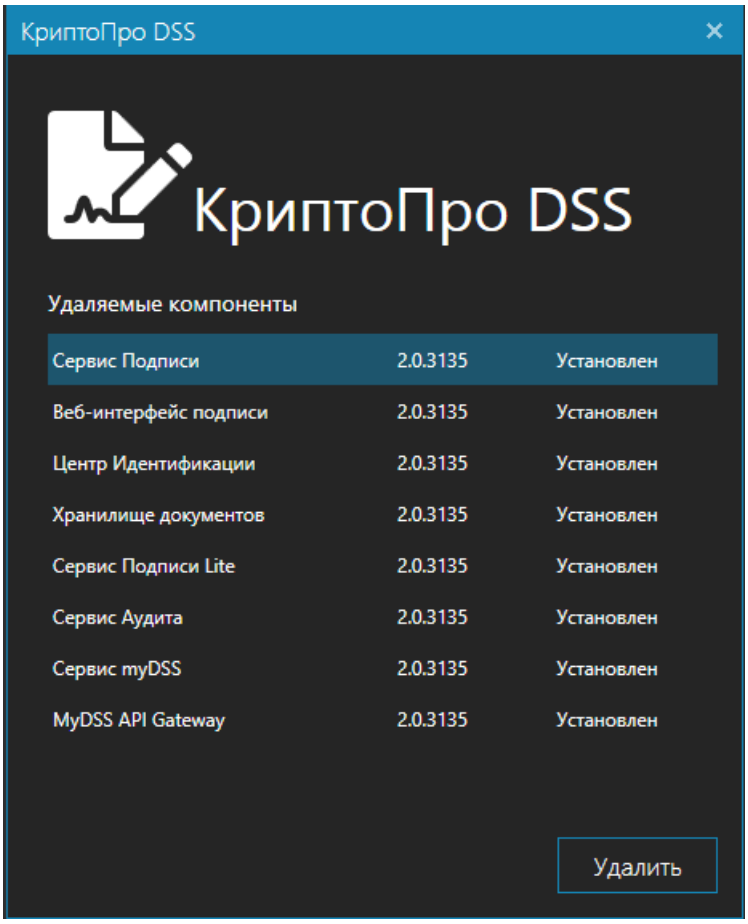


На следующей странице мастера установки выберите «Удалить продукт» и нажмите кнопку «Изменить».

Введите учетные записи для доступа к SQL-серверу, чтобы удалить базы данных экземпляров компонентов. Нажмите кнопку "Далее".

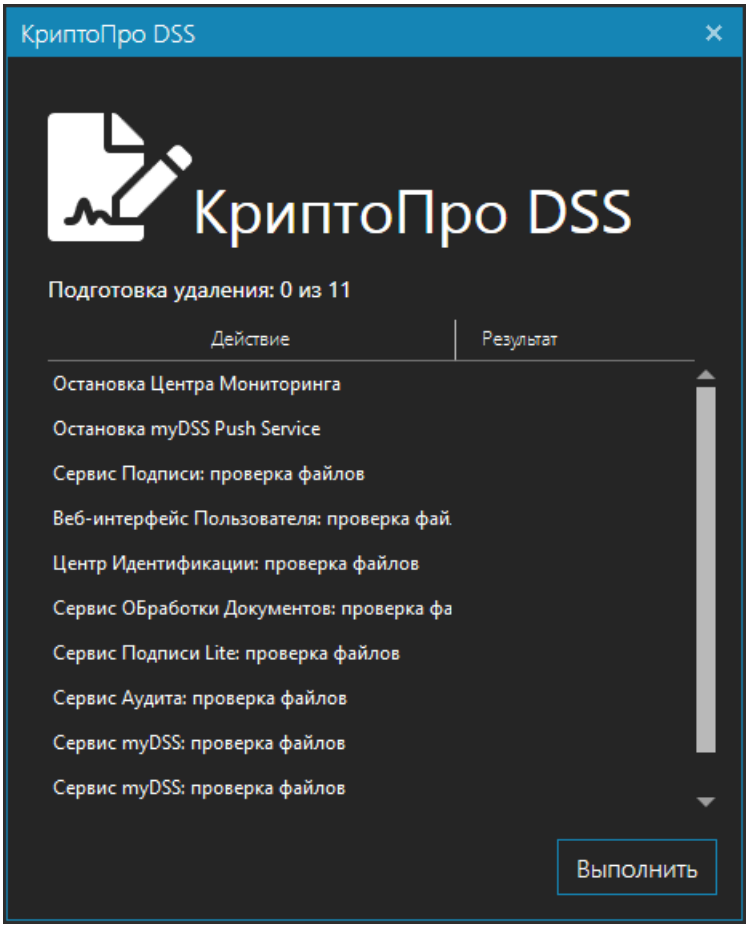


Проверьте список удаляемых компонентов КриптоПро DSS и нажмите кнопку "Удалить". Произойдет удаление установленных компонентов.

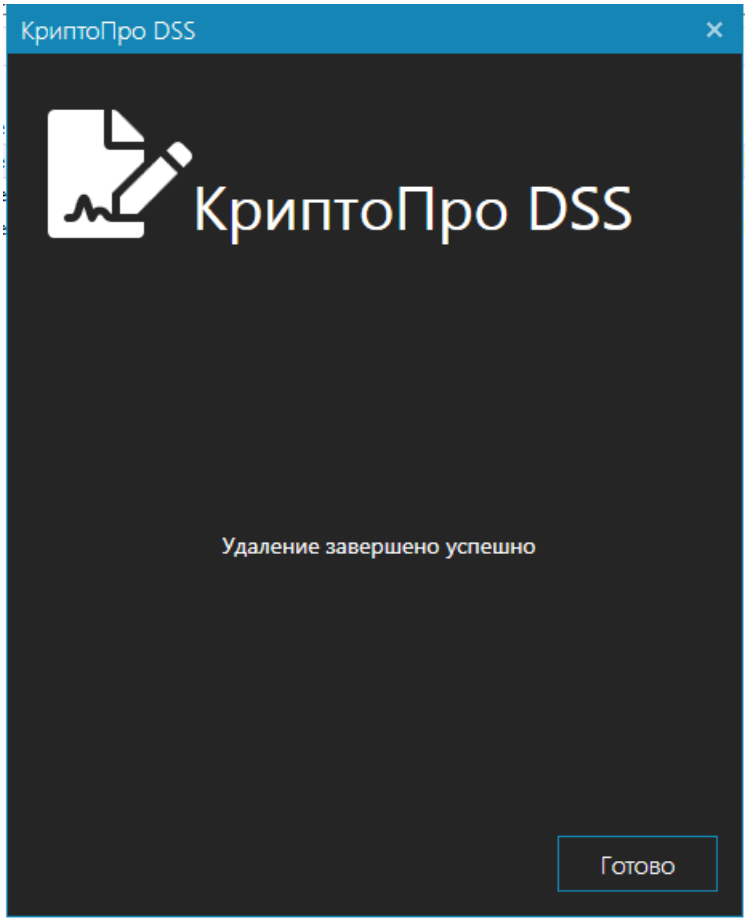


Проверьте список затрагиваемых при удалении продукта экземпляров компонентов и нажмите кнопку "Выполнить". Произойдет удаление экземпляров компонентов. Ознакомьтесь со статусом удаления компонентов и нажмите кнопку

"Далее".



После завершения всех действий нажмите кнопку "Готово", чтобы выйти из программы установки.

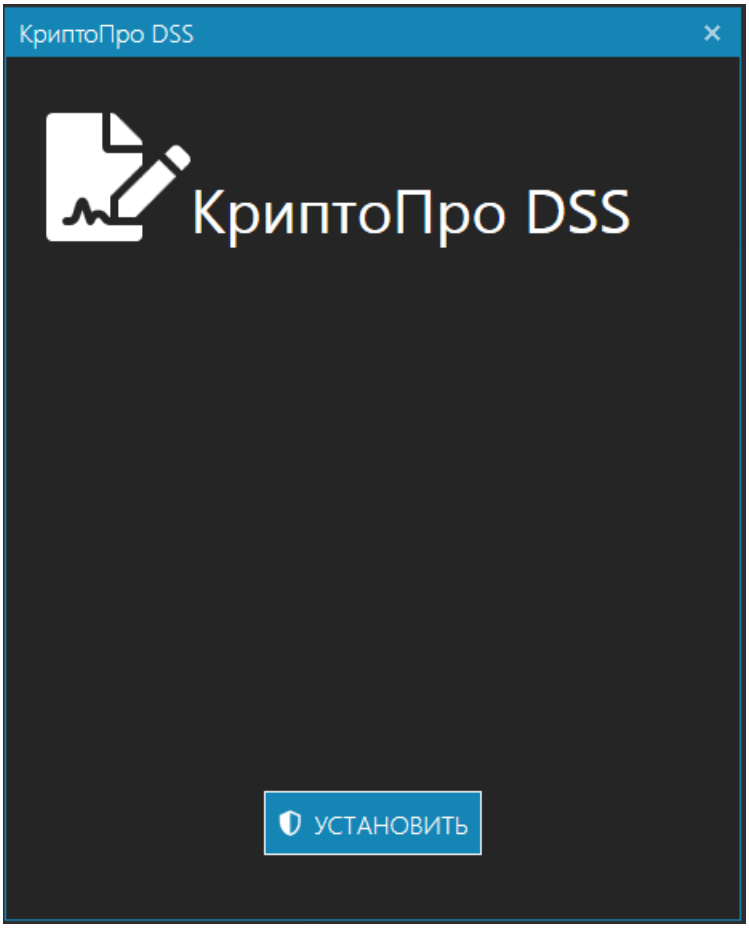


Обновление КриптоПро DSS

Для обновления КриптоПро DSS запустите установку пакета **DSSInstall.exe**, расположенного на компакт-диске, и нажмите «Установить». Обновление КриптоПро DSS должно осуществляться от имени пользователя с правами администратора.

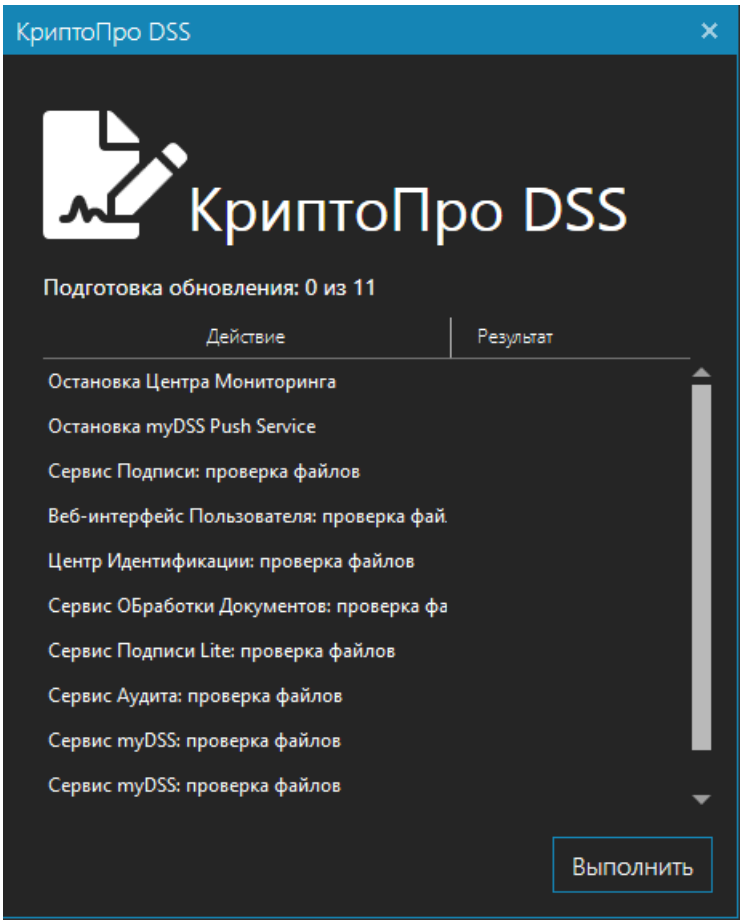
Примечание

Режим обновления активируется автоматически при запуске установщика и доступен только при запуске установщика КриптоПро DSS более новой версии.

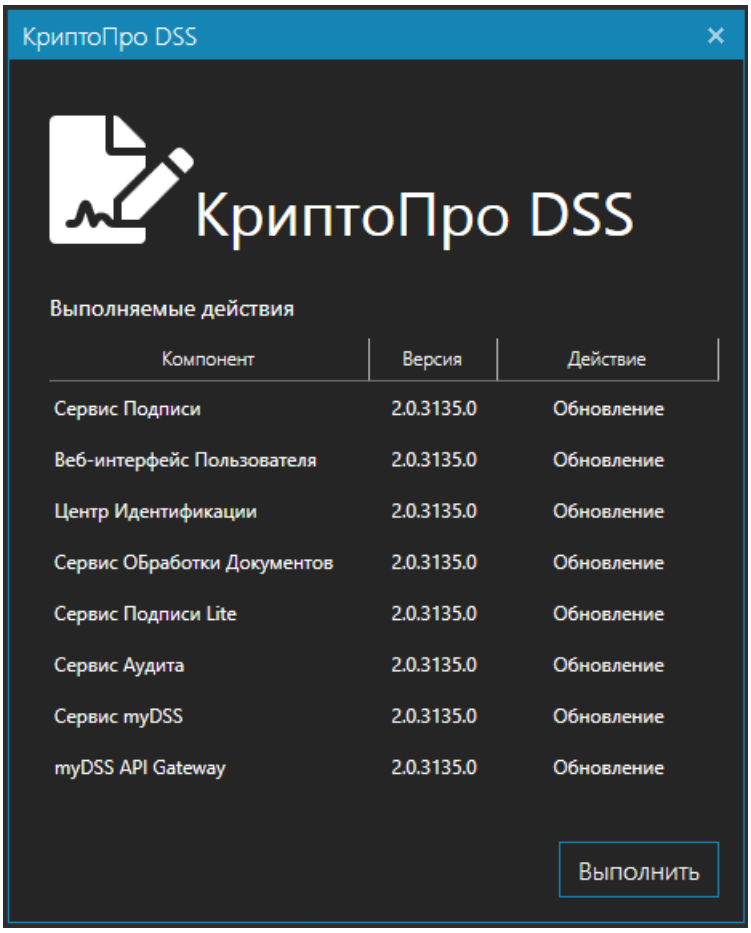


Ознакомьтесь с предупреждениями о смене версии КриптоПро DSS, активируйте чекбокс "Я ознакомлен с требованиями" и нажмите кнопку "Далее", чтобы перейти к подготовке к обновлению.

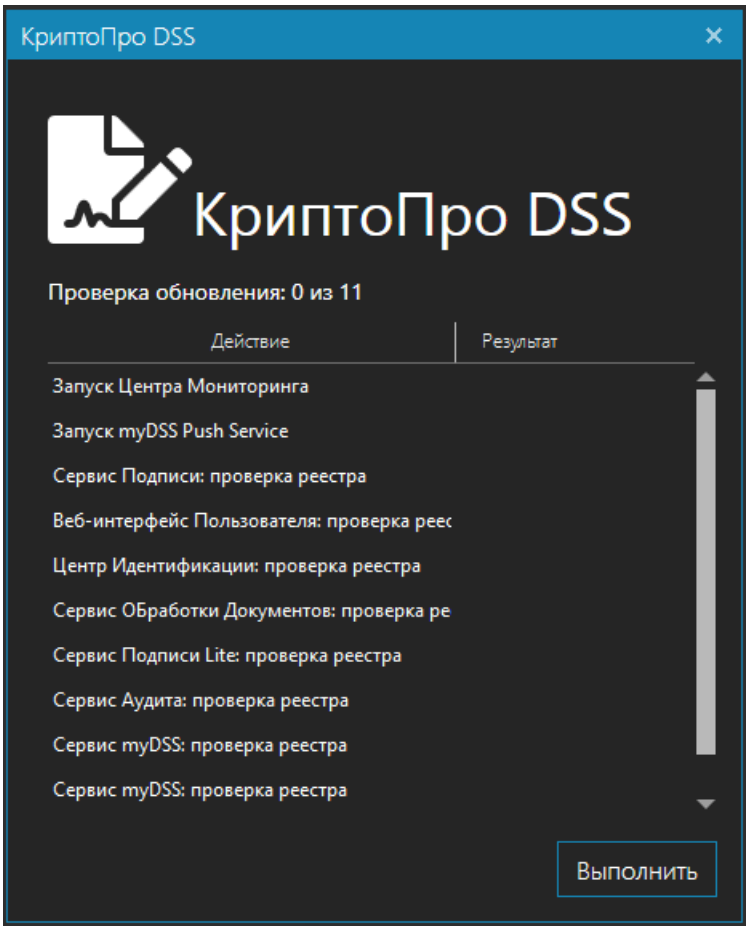
На странице подготовки к обновлению отображаются необходимые проверки файлов и служб. Чтобы выполнить данные проверки, нажмите кнопку «Выполнить». Ознакомьтесь с результатами проверок и нажмите кнопку "Далее".



Ознакомьтесь со списком компонентов КриптоПро DSS, которые будут обновлены, и нажмите кнопку "Выполнить", чтобы обновить компоненты.

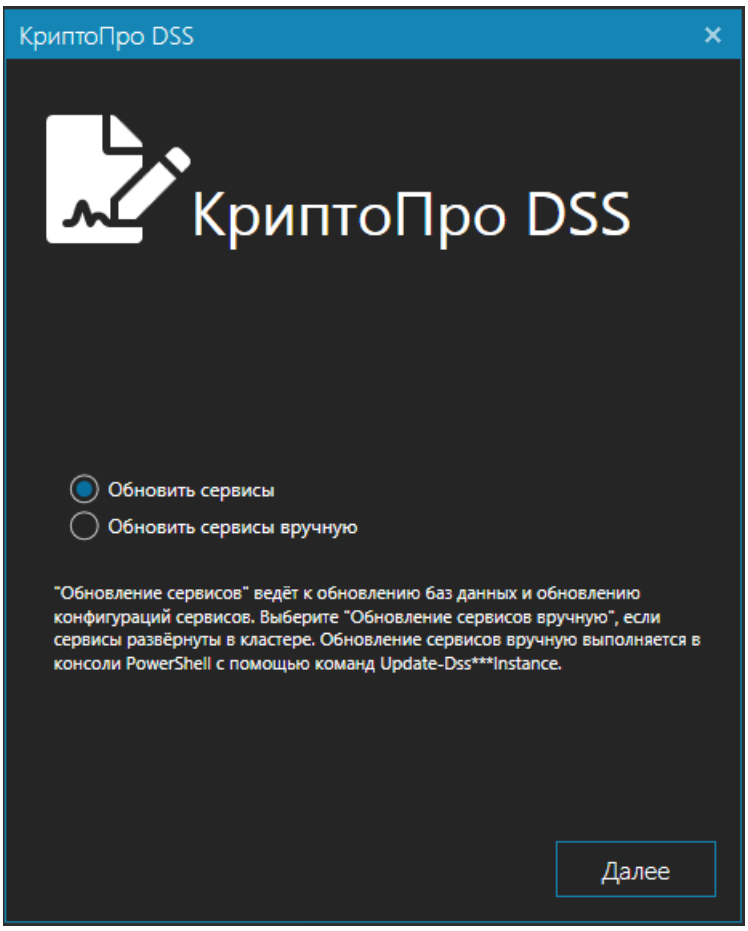


Ознакомьтесь со списком проверок файлов и служб после обновления и нажмите кнопку "Выполнить". После завершения проверок нажмите кнопку "Далее".

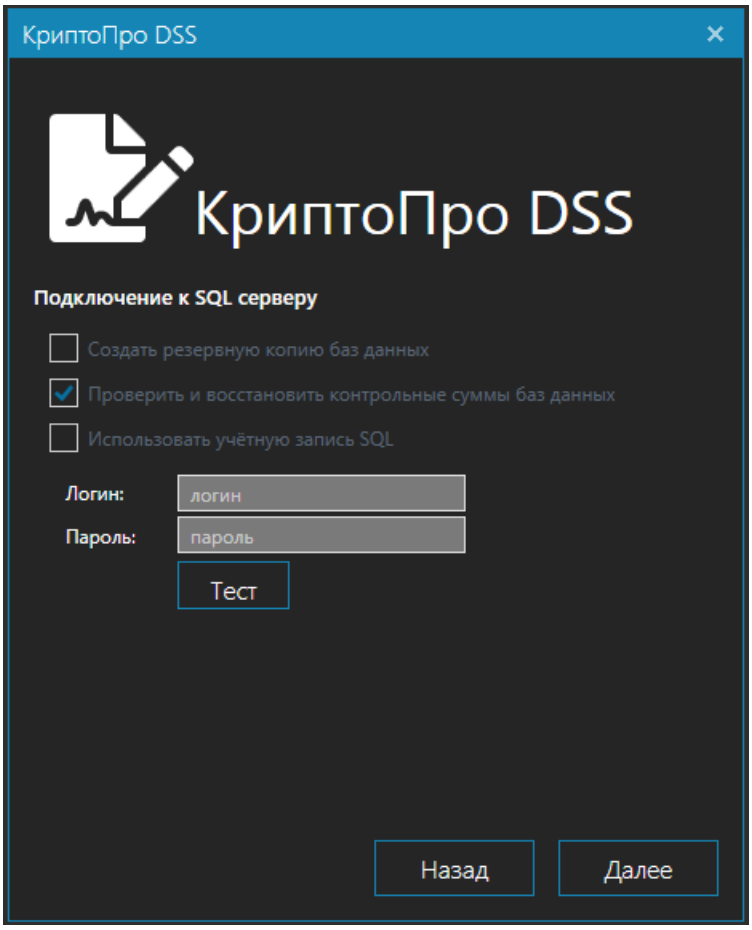


Выберите режим обновления развернутых ранее экземпляров компонентов. Рекомендуется выбрать "Обновить сервисов",

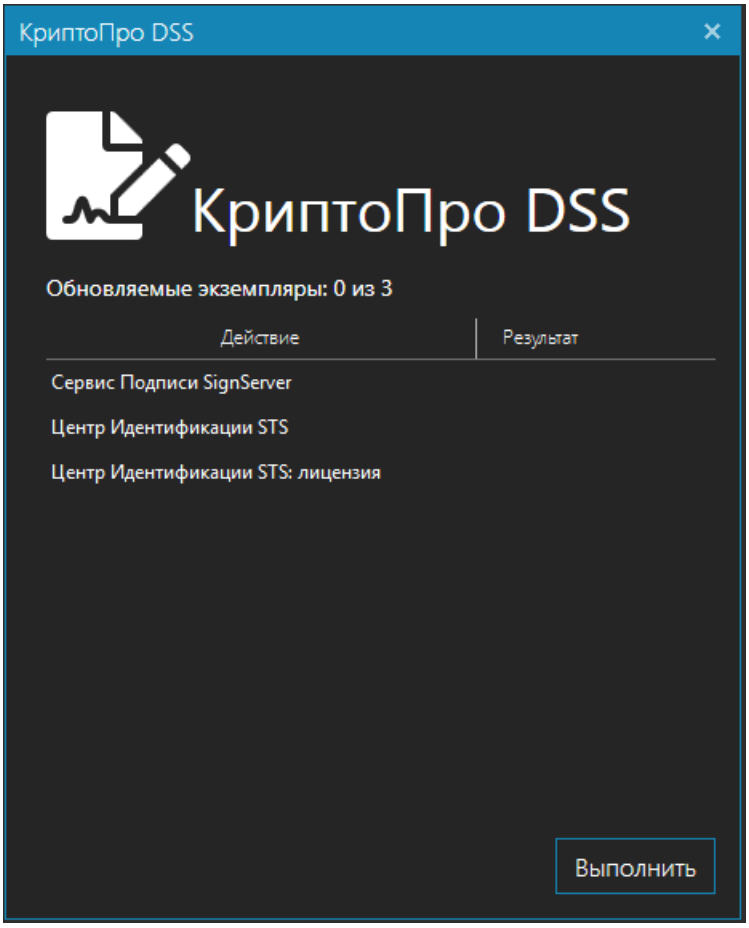
если экземпляры не были развернуты в кластере. В противном случае необходимо выбрать "Обновить сервисы вручную". Нажмите кнопку "Далее".



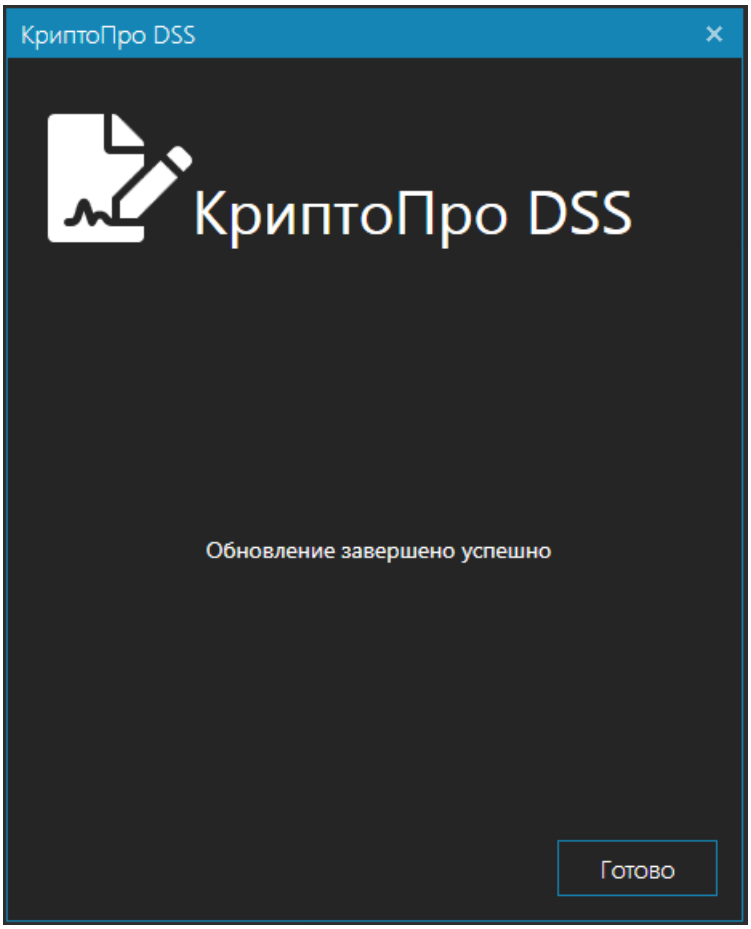
Введите учетные записи для доступа к SQL-серверу, чтобы обновить конфигурации баз данных экземпляров. Также возможно создать резервную копию БД при помощи включения соответствующего чекбокса. Нажмите кнопку "Далее".



Проверьте список обновляемых компонентов КриптоПро DSS и нажмите кнопку "Выполнить". Произойдет обновление развернутых экземпляров компонентов. Ознакомьтесь с результатами обновления и нажмите кнопку "Далее".



После завершения всех действий нажмите кнопку "Готово", чтобы выйти из программы установки.



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 со следующими криптопровайдерами:

- Crypto-Pro HSM Svc CSP (тип 75);
- Crypto-Pro GOST R 34.10-2012 HSM Svc CSP (тип 80);
- Crypto-Pro GOST R 34.10-2012 Strong HSM Svc CSP (тип 81).

Для регистрации криптопровайдера на Сервисе Подписи используйте командлет Add-DssCryptoProvider.

Примечание

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.

Развертывание Центра Идентификации

Развёртывание Центра Идентификации КриптоПро DSS осуществляется в следующем порядке:

1. Развертывание веб-сервера Microsoft IIS с необходимыми компонентами.
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.
5. Настройка Центра Идентификации.

Развертывание Сервиса Подписи

Развёртывание Сервиса Подписи осуществляется в следующем порядке:

1. Развертывание веб-сервера Microsoft IIS с необходимыми компонентами.
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.
5. Установка «КриптоПро .NET».
6. Установка Сервиса Подписи.
7. Настройка Сервиса Подписи.

Примечание

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»).

Развертывание Веб-интерфейса Пользователя

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

1. Развертывание веб-сервера Microsoft IIS с необходимыми компонентами.
2. Установка Веб-интерфейса Пользователя КриптоПро DSS.
3. Настройка Веб-интерфейса Пользователя.

Развертывание Сервиса Аудита

Развертывание Сервиса Аудита КриптоПро DSS осуществляется в следующем порядке:

1. Развертывание веб-сервера Microsoft IIS с необходимыми компонентами.
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.
4. Настройка Сервиса Аудита.

Развертывание myDSS

Развёртывание компонента myDSS осуществляется в следующем порядке:

1. Развертывание веб-сервера Microsoft IIS с необходимыми компонентами.
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.
5. Настройка компонента myDSS.

Развертывание Сервиса Обработки Документов

Развёртывание компонента myDSS осуществляется в следующем порядке:

1. Развертывание веб-сервера Microsoft IIS с необходимыми компонентами.
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 Сервиса Обработки Документов.
5. Настройка компонента Сервис Обработки Документов.

Развертывание Сервиса Обработки Документов

Развёртывание компонента myDSS осуществляется в следующем порядке:

1. Развертывание веб-сервера Microsoft IIS с необходимыми компонентами.
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 Сервиса Обработки Документов.
5. Настройка компонента Сервис Обработки Документов.

Развертывание баз данных экземпляров компонентов

Сервис Подписи, Центр Идентификации, Сервис Аудита, Сервис Обработки Документов и модуль аутентификации myDSS для своей работы требуют подключения к базам данных на SQL-сервере. Базы данных создаются при разворачивании экземпляров компонентов:

- Центр Идентификации - командлет New-DssStsInstance,
- Сервис Подписи - командлет New-DssSignServerInstance,
- Сервис Аудита - командлет New-DssAnalyticsServiceInstance,
- Сервис Обработки Документов - командлет New-DssDocumentStoreInstance,
- Модуль аутентификации myDSS:
  - Сервис взаимодействия с ЦИ - командлет New-MyDssServerInternalInstance
  - Сервис взаимодействия с мобильным приложением myDSS - командлет New-MyDssServerExternalInstance,

При этом существует два варианта размещения базы данных экземпляра компонента:

- **Локально** - на том же сервере, что и экземпляр компонента;
- **Удаленно** - кластер SQL-сервера AlwaysOn.

Также в этом разделе:

- Права доступа к удаленному SQL-серверу
- Настройка параметров подключения к SQL-серверу
- Развертывание экземпляров DSS в кластере
- Примеры создания экземпляров DSS с настройкой подключения к БД

Локальный SQL-сервер

При разворачивании экземпляров DSS на локальном SQL-сервере в командлетах `New-Dss...Instance` достаточно указать имя SQL-сервера в параметре `-SQLServerName`.

Пример:

```
New-DssSignServerInstance -SiteName "Default Web Site" -ApplicationName SignServer -SQLServerName
“.\SQLEXPRESS” –DisplayName SignServer
```

При этом для возможности подключения экземпляров компонентов DSS к SQL будут созданы следующие учетные данные на SQL-сервере:

1. Логин на уровне веб-сервера (соответствует имени пула приложений на IIS)
2. Логин на уровне БД (соответствует имени пула приложений на IIS)

Указанные учетные данные совпадают с именем пула приложений на IIS. Например, `IIS AppPool/CryptoProDSS-1-STS`.

> **Примечание**
>
> Администратор DSS, который разворачивает экземпляры компонентов, на SQL-сервере должен обладать следующими правами:
>
> - dbcreator,
> - securityadmin.

Удаленный SQL-сервер

При разворачивании экземпляров DSS на удаленном SQL-сервере вначале необходимо выбрать схему аутентификации:

- **учетные данные Windows**;
- **учетные данные SQL Server**.

> **Примечание**
>
> Управление доступом на уровне домена позволяет упростить администрирование учетных записей. По возможности рекомендуется использовать аутентификацию Windows.

От типа выбранной аутентификации зависит набор параметров подключения к БД.

Windows-аутентификация

> **Примечание**
>
> При аутентификации на удаленном SQL-сервере по учетным данным Windows сервера с экземплярами DSS и SQL-сервера должны находиться в одном домене Windows.

В случае аутентификации на удаленном SQL-сервере по учетным данным Windows, необходимо перед разворачиванием создать для экземпляров DSS учетные записи в домене.

> **Примечание**
>
> Рекомендуется использовать `gMSA (Group Managed Service Accounts)` для учетных данных экземпляров в домене.

Общее описание gMSA

Пример настройки gMSA

Разворачивание экземпляров DSS с Windows-аутентификацией на удаленном SQL-сервере производится при помощи командлета `New-Dss...Instance` (в зависимости от экземпляра компонента). При этом необходимо использовать параметр `-ConnectionInfo`, в который нужно передать параметры подключения к БД. Эти параметры заполняются при помощи командлета `New-DssSql...ConnectionInfo` (в зависимости от экземпляра компонента).

> **Внимание!**
>
> Необходимо учитывать наличие у Администратора DSS прав доступа к SQL-серверу.

Описание структуры SqlConnectionInfo

Параметры при создании экземпляра DSS с Windows-аутентификацией

Примеры

SQL-аутентификация

Разворачивание экземпляров DSS с Windows-аутентификацией на удаленном SQL-сервере производится при помощи командлета `New-Dss...Instance` (в зависимости от экземпляра компонента). При этом необходимо использовать параметр `-ConnectionInfo`, в который нужно передать параметры подключения к БД. Эти параметры заполняются при помощи командлета `New-DssSql...ConnectionInfo` (в зависимости от экземпляра компонента).

После выполнения командлета `New-Dss...Instance` на SQL-сервере будут созданы учетные записи с указанными данными.

> **Внимание!**
>
> Необходимо учитывать наличие у Администратора DSS прав доступа к SQL-серверу.

Описание структуры SqlConnectionInfo

Параметры при создании экземпляра DSS с SQL-аутентификацией

Примеры

Перед использованием командлетов в консоли PowerShell необходимо задать учетные данные Администратора DSS для

подключения к SQL-серверу. Учетные данные передаются через параметры `$DssAdmin`, `$DssAdminPwd`.

Права доступа к удаленному SQL-серверу

Если у Администратора DSS есть права `dbcreator` и `securityadmin` на удаленном SQL-сервере, то разворачивание экземпляров DSS и их БД производится как это описано выше для Windows-аутентификации и SQL-аутентификации.

Если у Администратора DSS нет прав `dbcreator` и `securityadmin`, то разворачивание экземпляров DSS и их БД состоит из следующих шагов:

1. Администратор SQL-сервера создает заготовки БД на SQL-сервере. При этом необходимо создать на уровне SQL-сервера следующее:

- логин для Администратора DSS. Администратор DSS должен быть включен в роль `db_owner` в созданных заготовках БД.
- логины для экземпляров DSS.

Имена БД по умолчанию представлены в таблице ниже.

КОМПОНЕНТ DSS	ИМЯ БД ПО УМОЛЧАНИЮ
Сервис Аудита	`AnalyticsServiceDB`
Сервис Обработки Документов	`DocumentStoreDB`
Сервис Обработки Операций*	`DssOperationsDb`
Центр Идентификации	`IdentityServiceDB`
Сервис взаимодействия с мобильным приложением myDSS	`MyDssServerExternalDB`
Сервис взаимодействия с ЦИ (myDSS)	`MyDssServerInternalDB`
Сервис Подписи**	`SignatureServerCommonDB`
Сервис Подписи	`SignatureServerDB`

Примечание

*Сервис Операций входит в состав и Сервиса Подписи, и Центра Идентификации. Соответственно, данная БД требуется в одном экземпляре для обоих компонентов.

Сервис Подписи имеет 2 базы данных: `SignatureServerCommonDB` **имеет **фиксированное** имя и будет использоваться всеми развернутыми экземплярами Сервиса Подписи. Имена остальных БД можно изменять, оповестив об этом Администратора DSS.

1. Администратор DSS создает экземпляры DSS с указанием имени БД и параметров подключения к ней. При этом необходимо указать флаг `BeginUseEmpty`. Если БД создавалась не с именем по умолчанию, в параметрах подключения также необходимо заполнить параметр `DatabaseName`.

2. Администратор DSS включает учетные данные экземпляров DSS в роли соответствующих баз данных. Для этого необходимо выполнить следующие действия:

- Создать на SQL-сервере пользователей SQL для экземпляров DSS в соответствующих БД.
- Созданных пользователей включить в роли соответствующих БД.

Имена ролей приведены в таблице ниже.

КОМПОНЕНТ DSS	ИМЯ РОЛИ
Сервис Аудита	`auditinstance`
Сервис Обработки Документов	`documentstoreserverinstance`
Сервис Операций*	`operationmanager`
Центр Идентификации	`identityserverinstance`
Сервис взаимодействия с мобильным приложением myDSS	`mydssserverexternalinstance`
Сервис взаимодействия с ЦИ (myDSS)	`mydssserverinstance`
Сервис Подписи**	`signserverinstance`

Примечание

*Сервис Операций входит в состав и Сервиса Подписи, и Центра Идентификации. Соответственно, в роль необходимо включать обе их учетные записи.

**Сервис Подписи имеет 2 базы данных: `SignatureServerCommonDB` и `SignatureServerDB`. Соответственно, учетную запись экземпляра необходимо включать в нужную роль в каждой из этих БД.

Настройка параметров подключения к SQL-серверу

Для указания параметров подключения к SQL-серверу при разворачивании экземпляров DSS необходимо использовать командлеты `New-Dss...SqlConnectionInfo`.

ПАРАМЕТР	ТИП	ОПИСАНИЕ
`AccountType`	string	Тип аутентификации в экземпляре SQL сервера для учётной записи, от имени которой будет выполняться подключение к БД: `AutoDetect` - автоматическая попытка определения типа аутентификации (по умолчанию) `SqlAccount` - SQL-аутентификация `Windows` - Windows-аутентификация. Если DSS неверно определил тип аутентификации, необходимо использовать параметр `SkipValidation`.
`AsUser`	string	(Только при SQL-аутентификации) Имя учётной записи Администратора DSS на SQL-сервере
`AsUserPassword`	string	(Только при SQL-аутентификации) Пароль учётной записи Администратора DSS на SQL-сервере
`BeginUseEmpty`	bool	Использовать существующую пустую БД. Используется, если БД создавалась заранее.
`CreateBackUp`	bool	Создавать резервную копию базы данных перед обновлением экземпляров DSS
`DatabaseName`	string	Название базы данных

ПАРАМЕТР	ТИП	ОПИСАНИЕ
`RepairDatabaseChecksums`	bool	Восстановить контрольные суммы при обновлении экземпляров DSS
`RestoreAccessModeAfterError`	bool	Будет ли БД возвращена в `MULTI_USER` режим после обновления
`ServerName`	string	Адрес экземпляра SQL-сервера, на котором следует развернуть базу данных.
`ServiceAccountName`	string	Имя учетной записи экземпляра DSS
`ServiceAccountPassword`	string	Пароль учетной записи экземпляра DSS
`SkipValidation`	bool	Не определять автоматически способ аутентификации на SQL-сервере
`TraceLogPath`	string	Путь к журналам обновления базы данных (на сервере, где разворачивается экземпляр DSS)
`UseExclusiveAccessMode`	bool	Будет ли БД переведена в `SINGLE_USER` режим на время обновления
`UseExistingDB`	bool	Использовать существующую базу данных. Используется при разворачивании дополнительных экземпляров DSS в кластере.
`UseNetworkService`	bool	(Только при удаленной Windows-аутентификации) Использовать учётную запись `Network Service` в качестве учётной записи экземпляра, если нет возможности создать учетные записи в домене Windows или использовать `gMSA`.

Параметры для Windows-аутентификации

- `AccountType` (Заполняется, если отключена автоматическая попытка определения типа аутентификации)
- `BeginUseEmpty`
- `DatabaseName` (Заполняется, если требуется заполнить имя БД для экземпляра самостоятельно, либо экземпляр создается повторно на одном сервере)
- `ServerName`
- `ServiceAccountName`
- `SkipValidation` (Устанавливается в случае нестандартных размещений SQL. Например, домен Windows и SQL-аутентификация)
- `UseExistingDB`
- `UseNetworkService`

Параметры для SQL-аутентификации

- `AccountType` (если отключена автоматическая попытка определения типа аутентификации)
- `AsUser`
- `AsUserPassword`
- `BeginUseEmpty`
- `DatabaseName` (Заполняется, если требуется заполнить имя БД для экземпляра самостоятельно, либо экземпляр создается повторно на одном сервере)
- `ServerName`
- `ServiceAccountName`
- `ServiceAccountPassword`
- `SkipValidation` (Устанавливается в случае нестандартных размещений SQL. Например, домен Windows и SQL-аутентификация)
- `UseExistingDB`

Параметры при обновлении экземпляров DSS

Обновление экземпляров DSS их баз данных производится при помощи командлетов `Update-Dss...Instance` (в зависимости от экземпляра компонента). При этом указанные ниже параметры должны быть переданы в параметр `-ConnectionInfo`. Параметры заполняются при помощи командлетов `New-DssSql...ConnectionInfo` (в зависимости от экземпляра компонента).

- `AsUser` - если была настроена SQL-аутентификация
- `AsUserPassword` - если была настроена SQL-аутентификация
- `CreateBackUp`
- `RepairDatabaseChecksums`
- `RestoreAccessModeAfterError`
- `SkipValidation` (Устанавливается в случае нестандартных размещений SQL. Например, домен Windows и SQL-аутентификация)
- `TraceLogPath`
- `UseExclusiveAccessMode`

Параметры при удалении экземпляров DSS

Удаление экземпляров DSS их баз данных производится при помощи командлетов `Remove-Dss...Instance` (в зависимости от экземпляра компонента). При этом указанные ниже параметры должны быть переданы в параметр `-ConnectionInfo`. Параметры заполняются при помощи командлетов `New-DssSql...ConnectionInfo` (в зависимости от экземпляра компонента).

- `AsUser` - если была настроена SQL-аутентификация
- `AsUserPassword` - если была настроена SQL-аутентификация
- `SkipValidation` (Устанавливается в случае нестандартных размещений SQL. Например, домен Windows и SQL-аутентификация)

Развертывание экземпляров DSS в кластере

Если необходимо развернуть дополнительные экземпляры DSS на отдельном сервере, то при заполнении параметров подключения к БД требуется указать имя существующей базы данных основного экземпляра и выставить параметр `-UseExistingDB` в значение `$true`.

Примеры создания экземпляров DSS с настройкой подключения к БД

```
# БД расположена на локальном сервере
New-DssSignServerInstance -SQLServerName .\SQLServer -DBName SignatureServerDb
```

```
# БД расположена на удаленном сервере
$connInfo = New-DssSqlConnectionInfo -ServerName .\SQLServer -DatabaseName SignatureServerDb -
ServiceAccountName SignServerAccount

New-DssSignServerInstance -ConnectionInfo $connInfo -DisplayName SignServer -SiteName "Default Web Site"
```

Изменение строки подключения к БД

В случаях, когда необходимо изменить строку подключения к БД, в зависимости от типа экземпляра используются командлеты `Set-DSS...RegistryProperties`.

Строка подключения к БД задается в параметре -DBConnection и должна быть заполнена с использованием допустимых имен для значений ключевых слов в строке подключения (ConnectionString).

Пример:

```
Set-DssSignServerRegistryProperties -DBConnection "Data Source=.\DSS2008R2;Initial
Catalog=SignatureServerDB;Integrated Security=True;Persist Security Info=False"
```

Лицензирование КриптоПро DSS

В данном разделе приведена информация о лицензировании КриптоПро DSS. КриптоПро DSS является программно-аппаратным комплексом, поэтому на некоторое ПО, входящее в его состав, лицензия активируется автоматически при покупке основных лицензий (например, на КриптоПро CSP, КриптоПро .NET, КриптоПро OCSP Client, КриптоПро TSP Client).

Список доступных лицензий находится на странице Форма заказа в разделе "КриптоПро DSS".

> **Примечание**
>
> Лицензия на Cloud CSP может быть приобретена как Оператором DSS в составе КриптоПро DSS (см. раздел ПАК КриптоПро DSS - КриптоПро Cloud CSP версии 2.0 Формы заказа), так и Пользователем в составе СКЗИ КриптоПро CSP (см. раздел СКЗИ «КриптоПро CSP/JCP» Формы заказа).

В КриптоПро DSS для администрирования (ввода и удаления Администратором) доступны следующие лицензии:

- Лицензии на Сервис Подписи;
- Лицензии на компоненты ЦИ:
  - На модуль аутентификации myDSS;
  - На средство аутентификации SimAuth;
  - На модуль доступа Cloud CSP (см. примечание выше);
  - На модуль аутентификации DSS Client.

Лицензия на Сервис Подписи

Существуют следующие типы лицензий на модуль аутентификации myDSS:

- **Демонстрационная.** Рассчитана на 10 Пользователей и не ограничена по сроку действия. Задается при помощи командлета Add-DssLicense без параметров. 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.** *Данная лицензия может быть выдана только для тестирования работы Сервиса Подписи.* В лицензии прописан явно срок окончания действия, а также может быть ограничено количество Пользователей. Данная лицензия может быть введена после Демонстрационной. 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.
- **Ограниченная по сроку действия на дополнительный сервер.** *Данная лицензия может быть выдана только для тестирования создания сервера репликации.*

Для ввода, удаления и получения сведений о лицензии используются следующие командлеты:

- Add-DssLicense
- Get-DssLicense
- Remove-DssLicense

> **Примечание**
>
> После внесения изменений в конфигурацию экземпляра необходимо перезапустить пул веб-приложения при помощи соответствующей команды.

Пример перезапуска:

```
# Перезапуск пула приложений Сервиса Подписи:
Restart-DssSignServerInstance -DisplayName <string>
```

Соответствие типов лицензий форме заказов

Перечисленные в данной статье названия типов лицензий используются для краткости. Точное соответствие типов лицензий на КриптоПро myDSS версии 2.0 названиям из Формы заказов представлено в таблице ниже.

> **Примечание**
>
> Соответствие Демонстрационной лицензии в данной таблице не приводится, т.к. данный тип лицензии доступен сразу после установки и настройки КриптоПро DSS вне зависимости от других приобретенных лицензий.

ТИП ЛИЦЕНЗИИ	НАИМЕНОВАНИЕ ПОЗИЦИИ В ФОРМЕ ЗАКАЗОВ
Базовая	Лицензия на право использования ПАК "КриптоПро DSS" версии 2.0 на одном сервере до <количество> пользователей

ТИП ЛИЦЕНЗИИ	НАИМЕНОВАНИЕ ПОЗИЦИИ В ФОРМЕ ЗАКАЗОВ
На расширение Базовой лицензии	Лицензия на расширение права использования ПАК "КриптоПро DSS" версии 2.0 на одном сервере на <количество> пользователей
На дополнительный сервер	Лицензия на право использования ПАК "КриптоПро DSS" версии 2.0 на одном дополнительном сервере

Примечание

Возможны расхождения данной таблицы с Формой заказа. Информацию в Форме заказа следует считать приоритетной.

Лицензия на компоненты ЦИ

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

- **На модуль аутентификации myDSS** (аутентификация пользователей с помощью мобильного приложения myDSS);
- **На модуль аутентификации DSS Client** (аутентификация Пользователей с помощью набора средств для мобильного приложения);
- **На средство аутентификации SimAuth** (аутентификация Пользователей с помощью апплета на SIM-карте);
- **На модуль доступа Cloud CSP** (облачный криптопровайдер Cloud CSP).

Для каждого из 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.

> **Примечание**
>
> Демонстрационная лицензия не уничтожается в версиях DSS 2.0.2849 и выше.

- **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.

- **Подписка (только для myDSS и DSS Client).** В лицензии типа Подписка ограничен как срок действия лицензии, так и количество Пользователей (кол-во активаций). Особенности лицензии:

    - Срок действия лицензии отсчитывается индивидуально с момента активации каждого Пользователя. Активацией Пользователя называется включение данному Пользователю метода аутентификации myDSS.
    - При включении Пользователю метода аутентификации myDSS тратится одно использование лицензии (одна активация). Если срок действия лицензии для данного Пользователя истек и у него по-прежнему включён метод аутентификации myDSS, тратится еще одно использование лицензии (одна активация). Данный процесс происходит автоматически и повторяется, пока метод аутентификации myDSS остаётся включённым для данного Пользователя.
    - Активация лицензии закрепляется за Пользователем. В течение срока действия активированной лицензии включение/отключение для данного Пользователя метода аутентификации myDSS не тратит новую активацию.
    - Лицензия может быть введена, даже если Базовая лицензия отсутствует.

> **Примечание**
>
> 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 (касается только Демонстрационной, Базовой лицензии и лицензии На расширение).

Совместимость с предыдущими версиями

Некоторые Пользователи, использующие метод аутентификации myDSS, могли быть присоединены к **Ограниченной по сроку действия** лицензии. В данном типе лицензии прописан явно срок окончания действия (общий для всех пользователей, начинает отсчитываться с момента ввода лицензии), а также может быть ограничено количество Пользователей. Данная лицензия не требует обязательного наличия Базовой и/или лицензии На расширение, но может их дополнять. Ограниченная по сроку действия лицензия может быть введена только одна.

Примечание

Ограниченная по сроку лицензия перестает полноценно действовать в версиях DSS 2.0.2849 и выше. При этом невозможны:

- Ввод и удаление лицензии данного типа.
- Присоединение к действующей лицензии новых Пользователей.

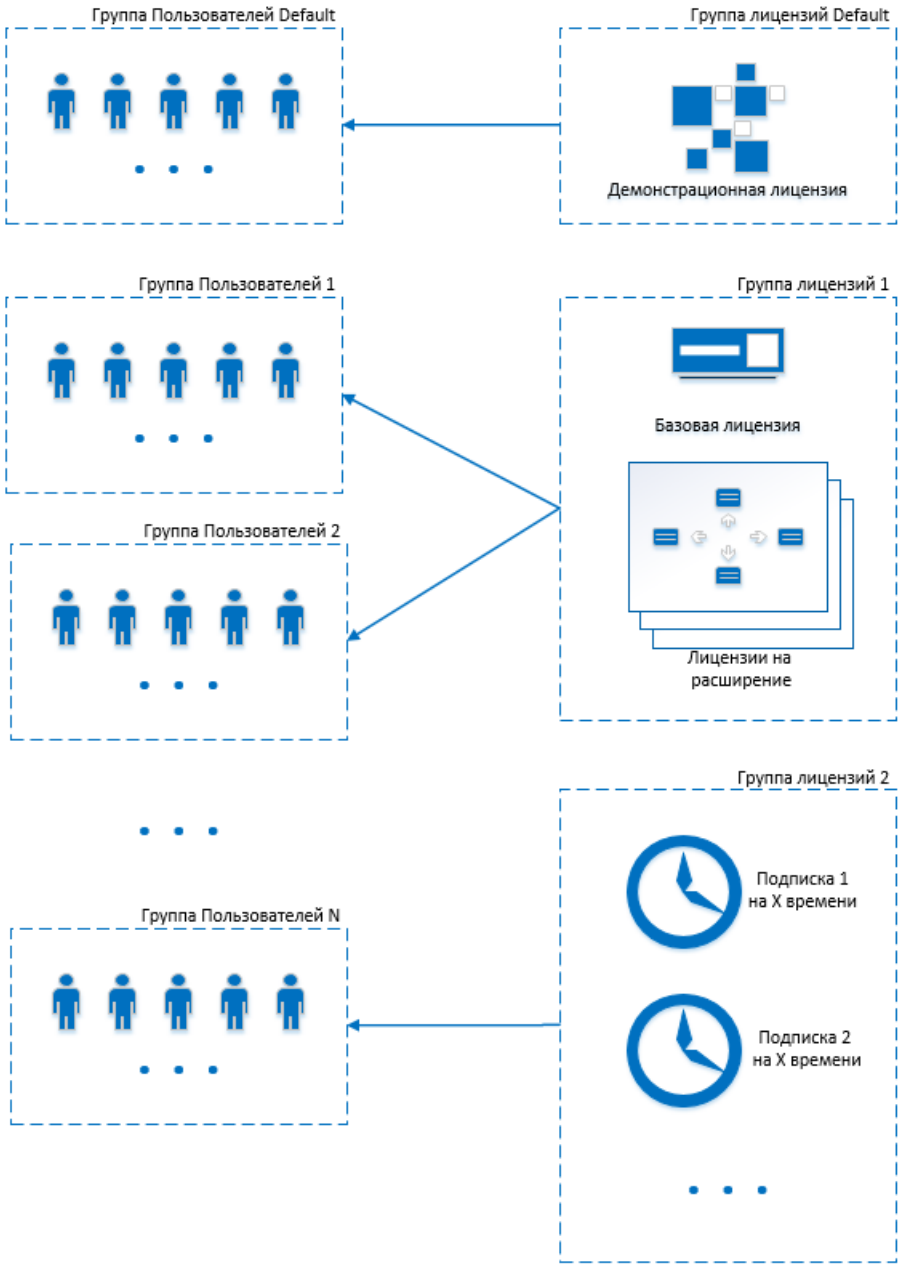
Примечание

Особенности использования ограниченной по сроку лицензии в версиях DSS 2.0.2849 и выше:

- Прикрепленные к действующей лицензии пользователи могут пользоваться ей до истечения срока действия при условии неотключения метода аутентификации myDSS.
- Если отключить пользователю, прикрепленному к ограниченной по сроку лицензии, метод аутентификации myDSS, следующее назначение ему этого метода прикрепляет его к имеющейся свободной лицензии (Приоритет: Базовая, На расширение, Подписка).

Ввод лицензий

В общем виде схема лицензирования компонентов ЦИ КриптоПро DSS выглядит следующим образом:



Ввод лицензии осуществляется в следующей последовательности:

1. Создание группы лицензий и ее привязка к группе Пользователей.

```
# Создание группы лицензий и привязка их к группе Пользователей
Add-DssStsLicenseGroup -Name "<Отображаемое имя группы лицензий 1>" -LicenseeGroups <Имя группы Пользователей 1>
Add-DssStsLicenseGroup -Name "<Отображаемое имя группы лицензий 2>" -LicenseeGroups <Имя группы Пользователей 2>
```

, где `Имя группы Пользователей` - значение строки `Name` в выводе командлета `Get-DssIdentityGroup`

Внимание!

- Одна группа лицензий **МОЖЕТ** быть привязана к нескольким группам Пользователей (в т.ч. `Default`).
- К одной группе Пользователей **НЕ МОЖЕТ** быть привязано более одной группы лицензий.

2. Ввод номера лицензии с одновременным включением данной лицензии в группу.

Внимание!

Некоторые типы лицензий не могут находиться в одной и той же группе. Возможные комбинации лицензий описаны в соответствующем разделе.

```
$licenseSerial1 = "%aaaa-aaaa-aaaa-aaaa%"
$licenseSerial2 = "%bbbb-bbbb-bbbb-bbbb%"
$companyName = "%Company_Name%"

# Добавление лицензии в группу лицензий
Add-DssStsLicense -SerialNumber $licenseSerial1 -CompanyName $companyName -LicenseGroupId <ID группы лицензий 1>
Add-DssStsLicense -SerialNumber $licenseSerial2 -CompanyName $companyName -LicenseGroupId <ID группы лицензий 2>
```

, где `LicenseGroupId` - значение строки `Name` в выводе командлета `Get-DssStsLicense`

Примечание

После внесения изменений в конфигурацию экземпляра необходимо перезапустить пул веб-приложения при помощи соответствующей команды.

Пример перезапуска:

```
# Перезапуск пула приложений ЦИ:
Restart-DssStsInstance -DisplayName <string>
```

Первый ввод лицензии

При первом вводе лицензии на модуль аутентификации myDSS или myDSS Client можно воспользоваться следующим сценарием.

```
foreach ($licenseGroup in Get-DssStsLicenseGroup)
{
   Set-DssStsLicenseGroup -LicenseGroupId $licenseGroup.Id -LicenseeGroups @{}
}

$licGroup = Add-DssStsLicenseGroup -Name "Default Lic Group" -LicenseeGroups Default

$licenseSerial1 = "%aaaa-aaaa-aaaa-aaaa%"
$companyName = '%Company_Name%'

Add-DssStsLicense -SerialNumber $licenseSerial1 -CompanyName $companyName -LicenseGroupId $licGroup.ID

Restart-DssStsInstance -DisplayName <string>
```

Сочетания лицензий

Каждая из введенных лицензий принадлежит некоторой группе лицензий. При этом следует учитывать следующие свойства лицензий при распределении их по группам:

- Компонент ЦИ, на который вводится лицензия
- Тип лицензии

В таблице ниже на пересечениях столбцов и полей символом "+" или "-" указаны возможности размещения типов лицензий в одной группе. При этом необходимо учитывать следующее:

- Демонстрационная лицензия (на любой компонент ЦИ) не сочетается с другими типами лицензий. При создании нового экземпляра ЦИ Демонстрационная лицензия не прикреплена к какой-либо группе. При этом при назначении метода аутентификации Пользователю использование этой лицензии тратится. Если выполнялось обновление экземпляра DSS более ранней версии, Демонстрационная лицензия помещается в группу лицензий `Default` и назначается группе Пользователей `Default`. Для назначения группе Пользователей `Default` другой группы лицензий необходимо удалить привязку.
- Лицензии на myDSS и DSS Client **НЕ МОГУТ** находиться в одной группе. При этом лицензия на myDSS включает в себя лицензию на DSS Client.
- Базовые лицензии и лицензии На расширение **МОГУТ** комбинироваться в одной группе на различные методы аутентификации и на различное число Пользователей в каждой.
- Лицензии типа Подписка могут комбинироваться только при условии, что их сроки действия в пределах одной группы одинаковы (например, каждая на 1 месяц).

ТИПЫ ЛИЦЕНЗИЙ	БАЗОВАЯ	НА РАСШИРЕНИЕ	ПОДПИСКА
Демонстрационная	-	-	-
Базовая	+	+	-
На расширение	+	+	-
Подписка	-	-	+ (только с одинаковым сроком действия)

Устранение неполадок

При включении лицензии в группу лицензий, где присутствуют некомбинирующиеся с ней типы, могут возникать ошибки. В данном случае необходимо сбросить привязки групп лицензий к группам Пользователей:

```
foreach ($licenseGroup in Get-DssStsLicenseGroup)
{
   Set-DssStsLicenseGroup -LicenseGroupId $licenseGroup.Id -LicenseeGroups @{}
}
```

Примечание

Данная команда уничтожает все ранее созданные привязки групп лицензий к группам Пользователей. Необходимо назначить лицензиям новые группы при помощи следующей команды:

```
Set-DssStsLicenseGroup -LicenseGroupId <ID группы лицензий> -LicenseeGroups <"Имя группы Пользователей 1","Имя группы Пользователей 2">
```

, где `Имя группы Пользователей` - значение строки `Name` в выводе командлета `Get-DssIdentityGroup`. После завершения настройки необходимо перезапустить пул приложений Центра Идентификации.

Нештатные ситуации

Примечание

Обработка нештатных ситуаций применяется для лицензии на модуль аутентификации myDSS и DSS Client.

Нештатные ситуации с использованием лицензий на модуль аутентификации myDSS или DSS Client могут возникать при использовании одной и той же учетной записи для создания подписи документов от имени различных Пользователей.

К нештатным ситуациям относится следующее:

1. Добавление нового устройства.
2. Обновление вектора аутентификации ранее чем через год от момента создания.
3. Отключение метода аутентификации, в том числе при удалении Пользователя DSS или при удалении единственного вектора аутентификации Пользователя.

В связи с этим в КриптоПро DSS применяются ограничения по количеству нештатных ситуаций, при этом количество указанных нештатных ситуаций должно составлять **не более 10%** от общего числа Пользователей в введенных лицензиях одного и того же типа. Количество нештатных ситуаций подсчитывается за период продолжительностью 30 суток.

При превышении числа нештатных ситуаций за последние 30 суток становится невозможным добавление нового устройства и/или обновление вектора аутентификации Пользователя.

Соответствие типов лицензий форме заказов

Перечисленные в данной статье названия типов лицензий используются для краткости. Точное соответствие типов лицензий названиям из формы заказов представлено в таблице ниже.

Примечание

Соответствие Демонстрационной лицензии в данной таблице не приводится, т.к. данный тип лицензии доступен сразу после установки и настройки КриптоПро DSS вне зависимости от других приобретенных лицензий.

ТИП ЛИЦЕНЗИИ	НАИМЕНОВАНИЕ ПОЗИЦИИ В ФОРМЕ ЗАКАЗОВ
Базовая	Лицензия на право использования ПО "<имя компонента ЦИ> для ПАК "КриптоПро DSS" версии 2.0 до <количество> пользователей
На расширение Базовой лицензии	Лицензия на расширение права использования ПО "<имя компонента ЦИ> для ПАК "КриптоПро DSS" версии 2.0 на <количество> пользователей
Подписка (ранее - Ограниченная по времени)	Лицензия на право использования ПО "<имя компонента ЦИ> для ПАК "КриптоПро DSS" версии 2.0 до <количество> пользователей (<срок, например "годовая">)

Примечание

Доступные лицензии в форме заказа (количество пользователей, условия и др.) могут быть изменены. Информацию в

Форме заказа следует считать приоритетной.

Определение типа лицензии

В данном разделе приведена информация, позволяющая определить тип лицензии по ее серийному номеру. В таблице ниже собраны типы лицензий как Сервиса Подписи, так и компонентов ЦИ. При этом использованы короткие наименования типов лицензий. Соответствие коротких наименований типов лицензий Форме заказов приведено в соответствующих разделах:

- Компоненты ЦИ;
- Сервис Подписи.

ТИП ЛИЦЕНЗИИ	КОД ПРОДУКТА	ПРИЗНАК ТИПА	КОММЕНТАРИЙ
Лицензия на Сервис Подписи, **Базовая**	D5	D5100-x**1**xxx	
Лицензия на Сервис Подписи, **На расширение**	D5	D5100-x**2**xxx	
Лицензия на Сервис Подписи, **Временная**	D5	D5100-x**4**xxx	
Лицензия на Сервис Подписи, доп. сервер, **Базовая**	D1	D1100-x**1**xxx	
Лицензия на Сервис Подписи, доп. сервер, **Временная**	D1	D1100-x**4**xxx	
Лицензия на компонент ЦИ, **Базовая**	A5	A5100-`X`**1**xxxx	где `X`: `M`-SIM, `D`-myDSS, `C`-Cloud CSP
Лицензия на компонент ЦИ, **На расширение**	A5	A5100-`X`**2**xxx	где `X`: `M`-SIM, `D`-myDSS, `C`-Cloud CSP
Лицензия на компонент ЦИ, **Временная** `Поддерживается только для совместимости с предыдущими версиями.`	A5	A5100-`X`4xxx	где `X`: `M`-SIM, `D`-myDSS, `C`-Cloud CSP
Лицензия на компонент ЦИ, **Подписка**	A5	A5200-D1`XX`0	Только для myDSS и DSS SDK; `XX` - количество месяцев подписки.

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 ниже.

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
```

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
```

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 ниже.

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
```

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
```

Отказоустойчивое подключение КриптоПро HSM

Для выполнения криптографических операций и хранения ключевой информации (Мастер ключи) КриптоПро DSS должен быть подключен к КриптоПро HSM. DSS использует следующие Мастер-ключи:

- Мастер-ключ Сервиса Подписи
- Мастер-ключи модуля SIM-аутентификации
- Мастер-ключ myDSS Сервера
- Мастер-ключи модуля myDSS Client
- Мастер-ключ Сервиса Аудита

  Мастер-ключи имеют ограниченный срок жизни - 3 года. Мастер-ключи использовуются для создания и хранения различных ключей пользователей. Ключи пользователя имеют ограниченный срок жизни - не более 15 месяцев.

  За 15 месяцев до окончания срока жизни Мастер-ключ переходит в состояние "Только для чтения". В данном состоянии Мастер-ключ может быть использован только для работы с ранее созданными ключами пользователей.

> **Примечание**
>
> На Мастер-ключе в состоянии "Только для чтения" новые ключи пользователей создаваться не могут.

Для обеспечения бесперебойной работы перед истечением срока действия Мастер-ключа должен быть создан новый Мастер ключ.

Мастер-ключ Сервиса Подписи

Мастер-ключ Сервиса Подписи используется для безопасного хранения ключей пользователей в Базе данных Сервиса Подписи.

Команды для управления Мастер-ключами: `*-DssCryptoProvider`

Мастер-ключи SIM-аутентификации

Модуль SIM-аутентификации использует несколько Мастер-ключей, объединённых в профиль.

В профиль входят 4 Мастер-ключа:

- Для ключей аутентификации пользователей
- Для обновления ключей аутентификации пользователей
- Для защищённого обмена сообщениями с SIM-картой
- Для защищенного хранения данных для смены ключей пользователей

  Команды для управления Мастер-ключами: `*-DssStsCryptoProvider` Команды для управления профилем: `*-DssCryptoProviderProfile`

  ### Мастер ключ myDSS Сервера

  Модуль myDSS Сервера использует использует мастер ключи для выработки ключей аутентификации пользователей и проверке кодов аутентификации (HMAC), вырабатываемых на данных ключах.

  Команды для управления Мастер-ключами: `-MyDssServerInternalCryptoProviders`

  ### Мастер ключи myDSS Client

  Модуль myDSS Client использует несколько Мастер-ключей, объединённых в профиль.

  В профиль входят 2 Мастер-ключа:

  - Для подтверждения операций

- Для аутентификации

Команды для управления Мастер ключами: `*-DssStsCryptoProvider`

Команды для управления профилем: `*-DssCryptoProviderProfile`

Мастер ключ Сервиса Аудита

Мастер-ключ используется для подписи журнала Аудита и контроля целостности журнала Аудита.

Команды для управления Мастер-ключами: `-DssAnalyticsCryptoProvider`

Подключение КриптоПро HSM

Возможны две схемы подключения DSS к HSM:

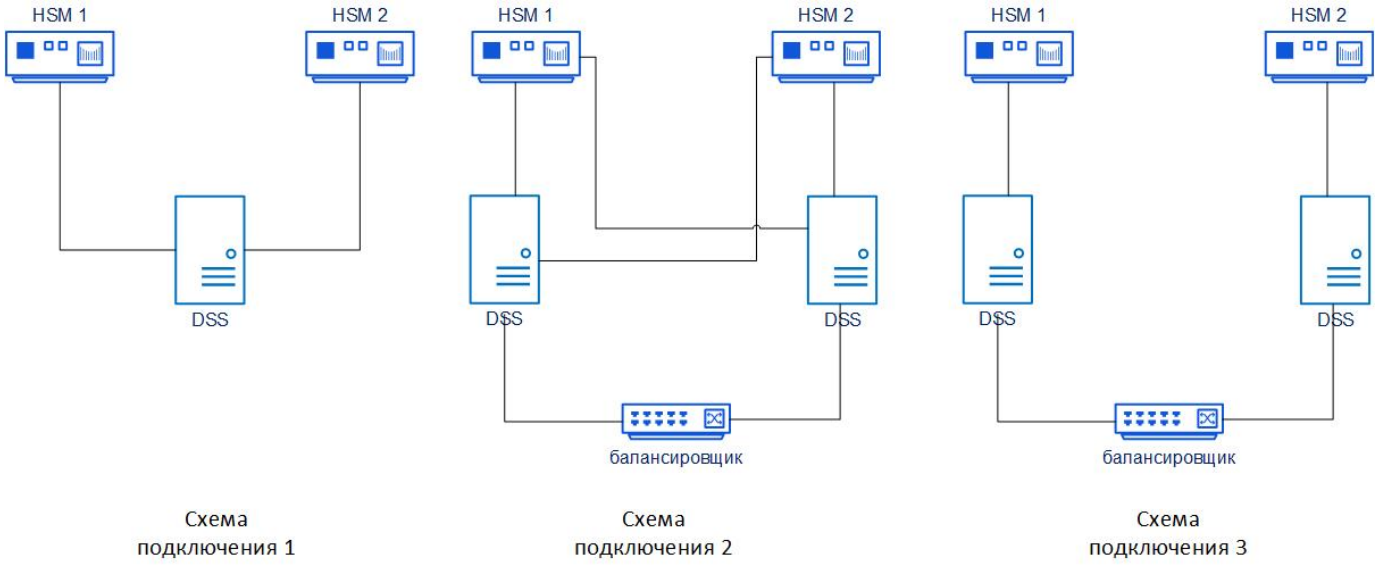
- крест-на-крест (с резервированием) - схема 1, 2
- один-к-одному - схема 3

В случае подключения крест-на-крест переключение между HSM в случае сбоя выполняет непосредственно сам DSS. DSS переодически проверяет доступность каждого из подключенных HSM. В случае недоступности HSM временно переводится в стмтус "Недоступен" и не используется для выполнения криптографических операций. После восстановления доступности DSS автоматически переведёт HSM в стмтус "Активен".

Период проверки доступности HSM настраивается в каждом компоненте DSS. Период проверки задаётся в миллисекундах.

КОМПОНЕНТ	КОМАНДА
Сервис Подписи	Set-DssProperties -MonitoringTimeout 5000
Центр Идентификации	Set-DssCpProperties -CpMonitoringTimeout 5000
myDSS Сервер	Set-MyDssServerInternalProperties -CryptoProvidersMonitoringTimeout 5000
Сервис Аудита	Set-DssAnalyticsServiceProperties -ProviderMonitoringInterval 5000

В случае подключения один-к-одному переключение должно выполняться между узлами DSS на балансировщике. Для принятия решения о переключении между узлами может использоваться КриптоПро Центр Мониторинга.



Копирование Мастер-ключей между HSM может быть выполнено:

- Средствами КриптоПро HSM - с помощью функций резервного копирования
- Средствами КриптоПро DSS

Подключение "крест-на-крест"

Последовательность действий:

- Создание экспортируемого Мастер-ключа на основном HSM
- Копирование Мастер-ключа на резервный HSM
- Перевод Мастер-ключа на основном HSM в неэкспортируемое состояние

Пример копирования Мастер-ключа Севриса Подписи

```
# Создание Мастер-ключа

$prov = Add-DssCryptoProvider -ProviderName "Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider"
-ProviderType 80 -Description "Тестовый провайдер 01.01.2020" -TypeId GostWithMasterKey -Exportable

# Копирование Мастер-ключа

Copy-DssCryptoProvider -NewProvName "Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider" -ID
$prov.ID

# Перевод Мастер-ключа неэкспортируемое состояние

Set-DssCryptoProvider -NotExportable -ID $prov.ID
```

Для myDSS Сервер последовательность действий аналогичная.

Для модуля SIM-аутентификации и модуля myDSS Client копирование ключа выполняется с помощью команд `-DssCryptoProviderProfile`

```
# Создание профиля myDSS Client

$profile = Add-DssCryptoProviderProfile -PrimaryProviderName "Crypto-Pro GOST R 34.10-2012 Cryptographic
Service Provider" -PrimaryProviderType 80 -Name "Тестовый профиль 01.01.2020" -Description "Test Export
mydss" -Type MyDss -Exportable

# Копирование Мастер-ключей

Copy-DssCryptoProviderProfile -ID $profile.ID -NewProvName "Crypto-Pro GOST R 34.10-2012 Cryptographic
Service Provider"
```

Подключение "один-к-одному"

Последовательность действий:

- Создание экспортируемого Мастер-ключа на основном HSM
- Экспорт Мастер-ключа на основном HSM
- Импорт Мастер-ключа на резервный HSM
- Перевод Мастер-ключа на основном HSM в неэкспортируемое состояние

> **Примечание**
>
> На обоих узлах DSS должен быть зарегистрирован криптопровайдер с одинаковым именем. Мастер-ключи на обоих HSM должен иметь одинаковое имя.

Пример копирования Мастер-ключа Сервиса Подписи

```
# Создание Мастер-ключа

$prov = Add-DssCryptoProvider -ProviderName "Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider" -
ProviderType 80 -Description "Тестовый провайдер 01.01.2020" -TypeId GostWithMasterKey -Exportable

# Экспорт Мастер-ключа

Export-DssCryptoProvider -ID -ID $prov.ID -OutFile C:\tmp\export3.xml

# Консоль powershell предложит ввести пароль для защиты экспортируемых данных

# Полученный файл необходимо перенести на второй узел DSS
# Импорт Мастер-ключа

Import-DssCryptoProvider -InputFile C:\tmp\export.xml

# Консоль powershell предложит ввести пароль

Set-DssCryptoProvider -NotExportable -ID $prov.ID
```

Для myDSS Сервер последовательность действий аналогичная.

Для модуля SIM-аутентификации и модуля myDSS Client копирование ключа выполняется с помощью команд `-DssCryptoProviderProfile`

```
# Создание Мастер-ключа

$profile = Add-DssCryptoProviderProfile -PrimaryProviderName "Crypto-Pro GOST R 34.10-2012 Cryptographic
Service Provider" -PrimaryProviderType 80 -Name "Тестовый профиль 01.01.2020" -Description "Test Export mydss"
-Type MyDss -Exportable

# Экспорт Мастер-ключа

Export-DssCryptoProviderProfile -ID -ID $profile.ID -OutFile C:\tmp\export3.xml
# Консоль powershell предложит ввести пароль для защиты экспортируемых данных

# Полученный файл необходимо перенести на второй узел DSS
# Импорт Мастер-ключа

Import-DssCryptoProviderProfile -InputFile C:\tmp\export.xml

# Консоль powershell предложит ввести пароль
```

Использование существующего мастер ключа

Если Мастер-ключ переносится средствами резервного копирования HSM, то последовательность действий:

- Добавить криптопровайдер с существующим Мастер-ключом

  ```
  $prov = Add-DssCryptoProvider -ProviderName "Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider"
  -ProviderType 80 -Description "Тестовый провайдер 01.01.2020" -TypeId GostWithMasterKey -MasterKeyName
  <existingKeyName>
  ```

- Включить новый криптопровайдер в существующую группу

  ```
  Join-DssCryptoProvider -GroupId <existingGroupId> -ID $prov.ID
  ```

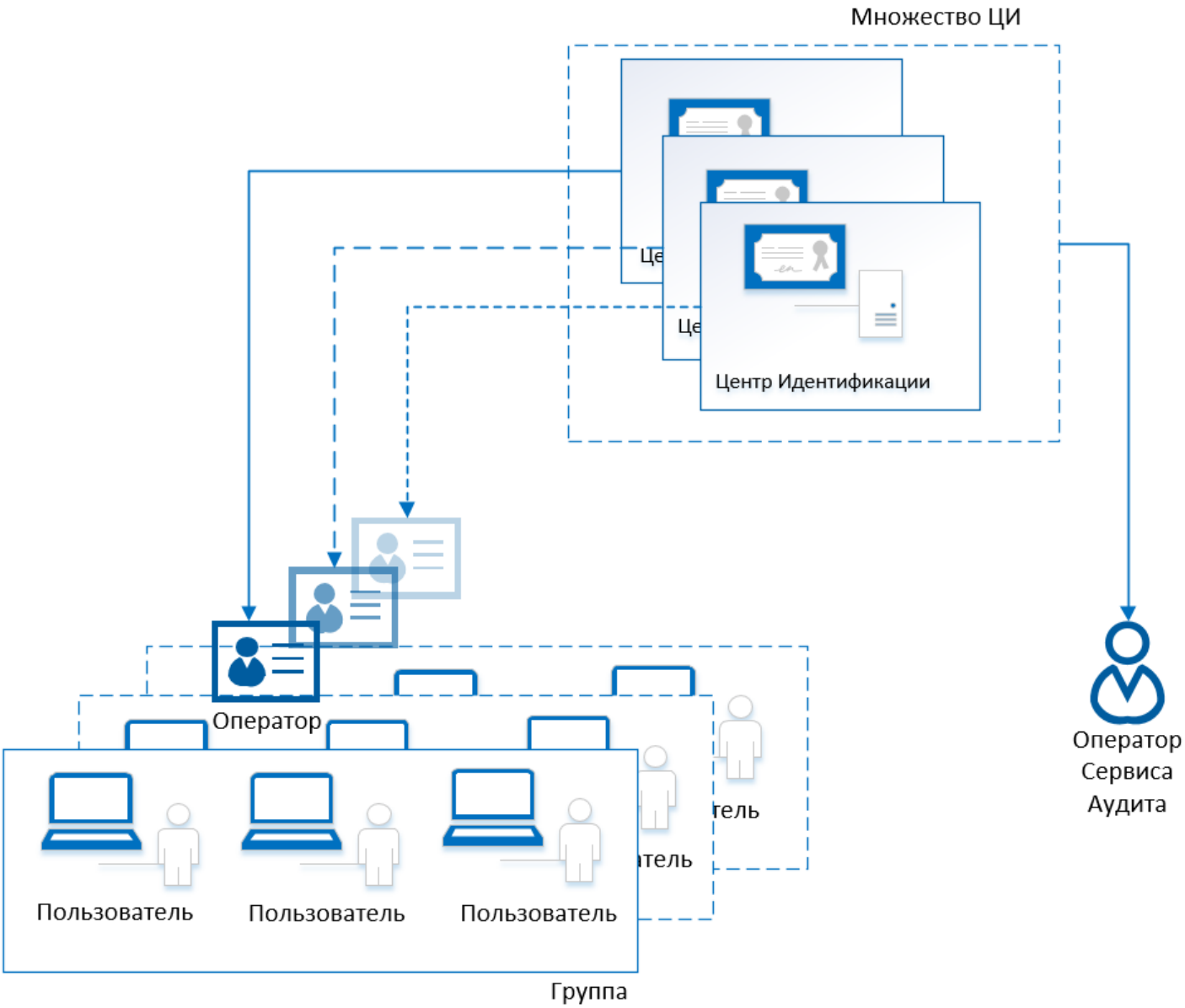
> **Примечание**
>
> В случае профиля Мастер-ключей для модулей SIM-аутентификации и myDSS Client данную операцию необходимо будет выполнить для каждого Мастер-ключа, входящего в профиль.

Учетные записи

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

- Пользователь;
- Операторы:
  - Оператор;
  - Оператор Аудита;
  - Оператор-наблюдатель;
- 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, на данной схеме она не отображается.



Согласно перечисленным ролям, в КриптоПро DSS можно создавать учетные записи выбранного типа. Учетная запись может принадлежать к конкретному экземпляру (экземплярам) ЦИ, на котором была создана, а также к группе.

Учетные записи Пользователей

Пользователь СЭП «КриптоПро DSS» - любой пользователь, получивший учетные данные для входа от Оператора. Ему доступны основные функции 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.

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 аутентификации, подтверждения операций, а также политика компонентов имени, в которой указывается, какие компоненты имени обязательно должны присутствовать при регистрации Пользователя.

Пользователи, вне зависимости от того, к какому экземпляру ЦИ они относятся, могут быть разделены на группы под управлением Операторов. Пользователю может быть назначена только одна группа. Группа Пользователей также характеризуется различными общими настройками и политиками, действующими для всех входящих в нее Пользователей и Операторов. Если на Центре Идентификации разрешена самостоятельная регистрация (в тестовом режиме), то при создании Пользователем своей учётной записи он будет включен в группу по умолчанию (Default).

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

Учетные записи Операторов

В КриптоПро DSS существуют следующие виды Операторов:

- Оператор;
- Оператор Аудита;
- Оператор-наблюдатель.

> **Примечание**
>
> Одна и та же учетная запись не может выполнять роль Оператора, Оператора-наблюдателя и Оператора Аудита одновременно.

Аутентификация Оператора в КриптоПро DSS осуществляется при помощи сертификата.

КриптоПро DSS поддерживает выделенное хранилище издателей сертификатов для аутентификации. Имя хранилища можно получить в выводе командлета Get-DssStsProperties (без параметров) напротив параметра `ClientAuthenticationIssuersStoreName` (по умолчанию – STS Client Authentication Issuers). Использование данного хранилища регулируется параметром `IsClientAuthenticationIssuersStoreEnabled` командлета Set-DssStsProperties.

Для проверки подлинности сертификата Оператора DSS веб-сервером необходимо добавить корневой сертификат издателя сертификата оператора DSS в хранилище `«Доверенные корневые центры сертификации»` локального компьютера.

Для проверки подлинности сертификата Оператора со стороны КриптоПро DSS необходимо поместить корневой сертификат издателя сертификата оператора DSS в специализированное хранилище `«<Имя_приложения_ЦИ> Client Authentication Issuers»`. Данная проверка возможна только после ее активации (активирована по умолчанию). Для активации проверки необходимо выполнить следующую команду:

```
Set-DssStsProperties –IsClientAuthenticationIssuersStoreEnabled 1
```

Список командлетов по настройке учетных записей Операторов КриптоПро DSS:

- Add-DssIdentityOperator
- Get-DssIdentityOperator
- Set-DssIdentityOperator
- Enable-DssIdentityOperator
- Disable-DssIdentityOperator
- Remove-DssIdentityOperator

Оператор

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 быть включен в одну и более групп. Оператор может управлять учётными записями и сертификатами Пользователей только в рамках своих 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.

Создание учётной записи Оператора осуществляется с помощью командлета Add-DssIdentityOperator, входящего в состав модуля `CryptoPro.DSS.PowerShell.STS`.

Контактная информация Оператора

Учетная запись Оператора может содержать контактную информацию. Это необходимо, например, для настройки оповещения указанной учетной записи (получение SMS- или Email-сообщений). Для этого в профиле Оператора должны быть указаны номер мобильного телефона и/или адрес электронной почты.

> **Внимание!**
>
> Контактную информацию можно задать только для Оператора. Для Оператора Аудита или Оператора-наблюдателя это недоступно.

Оператору можно назначить не более одного адреса или номера телефона, при этом их подтверждение не требуется.

Пример:

```
# Задание контактной информации при создании учетной записи Оператора

Add-DssIdentityOperator -Login <Логин Оператора> -Name <Отображаемое имя Оператора> -IssuerName realsts -Type
Operator -EmailAddress <Адрес эл. почты> -PhoneNumber <Номер телефона> -Certificate <Отпечаток сертификата
Оператора>

# Изменение контакной информации Оператора
Set-DssIdentityOperator -Login <Логин Оператора> -IssuerName realsts -ClearEmailAddress -ClearPhoneNumber

Set-DssIdentityOperator -Login <Логин Оператора> -IssuerName realsts -EmailAddress <Новый адрес эл. почты> -
PhoneNumber <Новый номер телефона>
```

> **Примечание**
>
> Оператор может просмотреть свою контактную информацию в личном кабинете. Редактировать контактную информацию через веб-интерфейс нельзя.

Оператор 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 DSS), 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.

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.

Создание учётной записи Оператора Аудита осуществляется с помощью командлета Add-DssIdentityOperator, с **обязательным** параметром `-type Audit`, входящего в состав модуля `CryptoPro.DSS.PowerShell.STS`.

Оператор-наблюдатель

Роль **Оператора-наблюдателя** позволяет исключительно просматривать информацию о Пользователях, поступающую с Сервиса Подписи и Центра Идентификации.

Оператор-наблюдатель может просматривать следующее:

- Список Пользователей СЭП «КриптоПро DSS»;
- Настройки аутентификации Пользователей;
- Просмотр средств аутентификации, зарегистрированных в ЦИ КриптоПро DSS;
- Просмотр сертификатов и/или запросов на сертификаты Пользователей СЭП «КриптоПро DSS»;
- Просмотр и печать событий аудита назначенных Оператору групп.

Роль Оператора-наблюдателя может использоваться также прикладными системами, которым необходим доступ к информации, указанной выше. Доступ возможен как через SOAP- и REST-интерфейсы, так и через Веб-интерфейс Пользователя — в этом случае у Оператора-наблюдателя будут отсутствовать некоторые элементы, отвечающие за изменение настроек аутентификации, сертификатов и проч.

Создание учётной записи Оператора-наблюдателя осуществляется с помощью командлета Add-DssIdentityOperator, с **обязательным** параметром `-type Readonly`.

Учетные записи Администраторов

Администратор СЭП «КриптоПро DSS» - это лицо, имеющее доступ к БД компонентов КриптоПро DSS и к управлению СЭП при помощи командлетов. 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.

Для управления учетными записями Администраторов используются командлеты вида `(Add/Get/Set/Remove)-Dss(Sts/SignSever/Analytics)Administrator` для DSS и `(Add/Get/Set/Remove)-MyDss(Internal/External)Administrator` для myDSS.

Группы

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. При этом Пользователи из разных экземпляров ЦИ (если было развернуто несколько ЦИ) могут быть объединены в одну группу. Назначенный для этой группы Оператор может управлять Пользователями независимо от того, к какому ЦИ они принадлежат.

Для управления группами используются командлеты вида `(New/Get/Set/Remove)-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 [Оператор] включён.

Поддержка CORS

CORS (Cross-origin resource sharing, совместное использование ресурсов между разными источниками) - механизм, использующий специальные HTTP заголовки, указывающие браузеру, что приложение, выполняемое в одном домене, имеет доступ к определённым ресурсам, расположенным на сервере из другого домена (под доменом или источником понимается совокупность URL-схемы, доменного имени и номера порта).

КриптоПро DSS позволяет ограничить перечень допустимых источников. Для этого предусмотрен специальный параметр командлетов `Set-DssProperties`, `Set-DssStsProperties`, `Set-VsProeprties`, `Set-LssProperties`: `-AllowedCorsOrigins`. В значении данного параметра можно указать через запятую список допустимых URL-адресов источников, с которых разрешено обращаться к соответствующим сервисам.

Пример 1

```
Set-DssProperties -AllowedCorsOrigins "https://test-cors.org,http://example.com"
```

URL-адрес источника должен удовлетворять следующим требованиям:

1. URL-адрес должен быть абсолютным (т.е. начинаться со схемы).
2. URL-адрес не должен заканчиватья на `/`.
3. URL-адрес на должен содержать относительный путь, строку запроса (query string) и фрагмент.

Пример 2

`https://test-cors.org` - правильный адрес.

`https://test-cors.org/`, `/test-cors.org`, `https://test-cors.org/path?query=string#fragment` - неправильные адреса.

По умолчанию значение для параметра `AllowedCorsOrigins` не задано. В этом случае разрешён любой источник. Указание пустой строки в значении параметра также отключает валидацию источников. Следует отметить, что разрешение любых источников не отключает поддержку CORS вообще: сервер продолжит формирование необходимых в рамках данного механизма HTTP-заголовков.

Текущее значение параметра можно посмотреть с помощью `Get-` командлетов: `Get-DssProperties`, `Get-DssStsProperties`, `Get-VsProeprties`, `Get-LssProperties`.

Пример

```
PinMode                           : Allow
TSPList                           : {testtsp, csptsp, qtsp}
SignatureTypeList                 : {GOST3410, CMS, CAdES, XMLDSig...}
ServiceCertificate                : 859D63834C7F61B81FF44D89382CD4081B20011B
ValidateCertificateBeforeSignature : False
ServiceType                       : Server
MonitoringTimeout                 : 10000
PdfSignatureSize                  : 100000
CadesUseOcspAuthorizedPolicy      : False
TokenTimeout                      : 600
RequireStrongConfirmation         : False
TransactionCacheMode              : DistributedCache
IsAdditionalCertStoreEnabled      : False
AdditionalCertStoreName           :
CadesUseProxy                     : False
OcspList                          :
ServiceIdentifier                 :
AllowedCorsOrigins                : http://www.test-cors.org
DisplayName                       : SignServer
```

Механизм **CORS** поддерживают все REST сервисы КриптоПро DSS:

- Сервис Подписи;
- Сервис Управления Пользователями;
- Сервис Подписи Lite;
- Сервис Проверки Подписи.

Настройка Центра Идентификации

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 интерфейса REST.

В этом разделе:

- Настройка экземпляра
- Объекты администрирования и командлеты
- Пример PowerShell-сценария

Работа с Центром Идентификации:

- Доверенные стороны
- Компоненты имени Пользователя
- Политика подтверждения операций
- Политика доступа к операциям
- Поддержка CORS

Создание и настройка экземпляра ЦИ

Данный раздел определяет последовательность действий при разворачивании и настройке экземпляра Центра Идентификации КриптоПро DSS.

- **Пример разворачивания**

Предварительные условия:

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

Базовая последовательность шагов по настройке (обязательные):

1. Создание экземпляра службы Центра Идентификации (командлет New-DssStsInstance). 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.

> Примечание
>
> Учетной записи, под которой работает пул приложения Центра Идентификации, необходимо выдать права на доступ **к закрытому ключу сервисного сертификата**.

3. Настройка Службы маркеров безопасности. При необходимости можно задать собственный сертификат подписи службы маркеров безопасности. По умолчанию сервисный сертификат ЦИ и сертификат подписи Службы маркеров безопасности совпадают, а сама Служба создается автоматически при создании экземпляра ЦИ.

4. Регистрация доверенных сторон.

Для полноценной работы компонентов КриптоПро DSS необходимо настроить отношения доверия между ними и Центром Идентификации:

> Внимание!
>
> Для выполнения данного пункта небходимо наличие экземпляров всех доверенных сторон и их сервисных сертификатов.

- регистрация доверенных сторон;
- Регистрация Центра Идентификации в качестве доверенного издателя маркеров безопасности - см. сценарий настройки остальных компонентов КриптоПро DSS.

> Примечание
>
> После внесения изменений в конфигурацию экземпляра необходимо перезапустить пул веб-приложения при помощи соответствующей команды.

Дополнительные действия по настройке (опциональные):

1. Ввод лицензии на методы аутентификации.

2. Настройка аутентификации. По умолчанию для нового Пользователя включены следующие методы аутентификации:

- По логину и паролю
- По сертификату

Администратор DSS может настроить технические требования к аутентификационным данным Пользователя (например,

длину и сложность пароля) и разрешить/запретить Пользователю менять эти настройки самостоятельно. При этом Пользователь может изменять *данные* аутентификации - например, сменить пароль или назначить другой сертификат для входа.

При этом назначать способы аутентификации Пользователю должен Оператор DSS.

3. Настройка профиля Пользователя. Администратор может настроить следующие параметры профиля Пользователя:

- Состав компонентов имени Пользователя (RDN) - имя, фамилия, должность, адрес, организация, ИНН и т.д.;
- Критичность наличия компонентов имени Пользователя;
- Значения по умолчанию для компонентов различительного имени Пользователя (например, страна, организация и т.п.).
- Возможность самостоятельного редактирования профиля Пользователем (включено по умолчанию).
- Требования к уникальности данных (например, номера телефона, адреса электронной почты, различительного имени Пользователя).

4. Настройка профиля Оператора. Администратор может зарегистрировать учётные данные Операторов DSS.

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

Для Оператора с полными правами может быть задана контактная информация для возможности отправлять ему уведомления.

5. Настройка оповещения Пользователей. Администратор DSS может настроить SMS- или Email-оповещение Пользователей о действиях, выполненных на Центре Идентификации.

Примечание

Оповещение Пользователей требует подключения ЦИ к SMS-шлюзу оператора сотовой связи или к почтовому серверу в соответствии со схемой размещения компонентов см. документ ЖТЯИ.00096-02 96 02 КриптоПро DSS. Общее описание) и в соответствии с требованиями к подключению к сетям общего пользования, описанными в Разделе 10 ЖТЯИ.00096-02 95 01 КриптоПро HSM. Правила пользования.

6. Настройка аудита. Администратор DSS может подключить Центр Идентификации к Сервису Аудита для ведения журнала аудита. Для этого потребуется включить отображение пункта меню "Аудит" в личном кабинете Пользователя или Оператора.

7. Кастомизация. Администратор DSS может кастомизировать веб-интерфейс Центра Идентификации: изменить цвета фона, текста, логотипы, тексты заголовков и т.п. при помощи набора командлетов.

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"
```

8. Настройка автоопределения формата документа.

9. Настройка журналирования экземпляра.

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.

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

1. Пользователь посредством веб-браузера (веб-клиента) запрашивает ресурсы (например, веб-страницу) приложения доверенной стороны (например, Веб-интерфейса Пользоваетеля);
2. Приложение доверенной стороны перенаправляет его на поставщика удостоверений (STS).
3. Пользователь предоставляет поставщику удостоверений свои учетные данные, например, имя Пользователя и пароль, билет Kerberos и т.д.
4. Поставщик удостоверений создает токен и отправляет его веб-клиенту.
5. Клиент отправляет доверенной стороне запрос вместе с полученным токеном, и доверенная сторона решает, соответствует ли токен условиям доступа и стоит ли удовлетворять запрос веб-клиента.
6. Если запрос веб-клиента удовлетворен, доверенная сторона предоставляет Пользователю свои ресурсы.

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

Регистрация доверенных сторон и управление зарегистрированными доверенными сторонами осуществляется с помощью

командлетов Add-DssRelyingPartyTrust, Set-DssRelyingPartyTrust, Enable-DssRelyingPartyTrust, Disable-DssRelyingPartyTrust, Remove-DssRelyingPartyTrust.

Регистрация доверенной стороны

Регистрация доверенной стороны на 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;
- Сервис Обработки Документов.

Регистрация доверенных сторон может осуществляться следующими способами:

Загрузка метаданных

Каждый из компонентов DSS публикует собственные метаданные по протоколу WS Federation Metadata.

Адреса публикации метаданных:

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`.

Сервис Обработки Документов

Метаданные отсутствуют.

По универсальному идентификатору ресурсов

В данном случае каждая доверенная сторона определяется идентификатором, который имеет следующий вид:

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

, где

- `apptype` – компонент DSS,
- `appname` – имя экземпляра компонента.

КОМПОНЕНТ	URI
Сервис Подписи	urn:cryptopro:dss:signserver:<appname>
Веб-интерфейс Пользователя	urn:cryptopro:dss:frontend:<appname>
Сервис Аудита	urn:cryptopro:dss:analytics:<appname>
Сервис Обработки Документов	urn:cryptopro:dss:documentstore:<appname>

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

Примеры регистрации доверенных сторон на ЦИ

Помимо выполнения рекомендаций данного раздела необходимо на каждой из зарегистрированных доверенных сторон зарегистрировать ЦИ DSS как доверенного поставщика маркеров безопасности. Данное действие выполняется при помощи командлета `Add-Dss...ClaimsPtoviderTrust`, где `...`:

- не добавляются для Сервиса Подписи;
- `Fe` - для Веб-интерфейса Пользователя;
- `Analytics` - для Сервиса Аудита
- `DocumentStore` - для Сервиса Обработки Документов.

Внимание!

Если сервисный сертификат какого-либо из компонента был изменен, необходима перерегистрация доверенной стороны.

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
```

При этом автоматически регистрируется сертификат аутентификации доверенной стороны. Если был изменен сервисный сертификат, полная перерегистрация метаданных необязательна (см. раздел про смену сертификатов).

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/
```

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
```

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
```

При этом автоматически регистрируется сертификат аутентификации доверенной стороны. Если был изменен сервисный сертификат, полная перерегистрация метаданных необязательна (см. раздел про смену сертификатов).

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"'
```

Регистрация Сервиса Обработки Документов

Для того, чтобы Сервис Обработки Документов предоставлял возможности загрузки, конвертации и выгрузки документов, отправленных на подпись/шифрование/расшифрование в КриптоПро DSS, его необходимо зарегистрировать в качестве доверенной стороны на Центре Идентификации.

СОД не поддерживает публикацию метаданных, поэтому добавление доверенной стороны возможно только вручную:

```
Add-DssRelyingPartyTrust -Name DocumentStore -Identities urn:cryptopro:dss:documentstore:
<DocumentStore_web_app>
```

Настройка компонентов имени Пользователя

Общие сведения

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 следующем 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 таблице ниже.

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
FriendlyName	String	Отображаемое имя компонента имени
MaxLength	int	Максимальная длина компонента имени
MinLength	int	Минимальная длина компонента имени
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 зарегистрированы следующие RDN:

КОМПОНЕНТ (ОТОБРАЖАЕМОЕ ИМЯ)	ИДЕНТИФИКАТОР СТРОКИ	MAX ДЛИНА	MIN ДЛИНА	ТИП ЗНАЧЕНИЯ	OID
Общее имя	CN	128	0	String	2.5.4.3
Имя Отчество	G	128	0	String	2.5.4.42
Фамилия	SN	40	0	String	2.5.4.4
Инициалы	I	5	0	String	2.5.4.43
Электронная почта	E	128	0	String	1.2.840.113549.1.9.1
ИНН	INN	12	12	Numeric	1.2.643.3.131.1.1

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
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
Адрес	Street	30	0	String	2.5.4.9
Организация	O	64	0	String	2.5.4.10
Подразделение	OU	64	0	String	2.5.4.11
Должность	T	64	0	String	2.5.4.12

Политики компонентов имени Пользователя

КриптоПро DSS позволяет настроить компоненты имени Пользователя на двух уровнях: глобальном (уровень настройки ЦИ) и уровне группы. 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.

> **Примечание**
>
> 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.

Политика подтверждения 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.

Примечание

Изменение настроек политики подтверждения операций для пользователей возможно только через Веб-интерфейс Пользователя или API DSS.

Политика подтверждения операций представляет собой набор следующих настроек:

ПАРАМЕТР	ТИП	ОПИСАНИЕ
Операции для подтверждения	-OpcActions <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.
AllowOverride	bool	Определяет, может ли политика быть переопределена на более низком уровне иерархии.

Примечание

В зависимости от того, политика какого уровня настраивается — уровня ЦИ или уровня группы — необходимо также соответственно использовать параметр `-IdpId` со значением `1`, ИЛИ параметр `-GroupId` со значением идентификатора настраиваемой группы.

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`, настройки политики уровнем ниже не имеют силы. Если все политики в иерархии имеют `AllowOverride = true`, параметры `AllowChangeByUser` и `AllowChangeByOperator` используются из политики группы, а настройка `OpcActions` применяется индивидуально для каждого Пользователя (настраивается в Веб-интерфейсе Пользователя).

Примечание

Перед изменением настроек политики подтверждения операций при помощи командлетов (уровень ЦИ DSS или

уровень группы), убедитесь, что на уровень выше не применялось значение `AllowOverride = false`.

Примеры:

Получение политик подтверждения операций по уровням:

```
# Получение политики ЦИ DSS:
Get-DssConfirmationPolicy -IdpId 1
# Если в выводе данной команды содержится AllowOverride = False,
# настройки уровня группы не имеют силы.

# Получение политики группы
Get-DssConfirmationPolicy -GroupId 1
# Если в выводе данной команды содержится AllowOverride = False,
# Пользователь не сможет изменить политику подтверждения операций в Веб-
# интерфейсе.
```

Примеры настроек политики подтверждения операций:

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

```
Set-DssConfirmationPolicy -IdpId 1 -AllOpcActions -AllowOverride 0
```

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

```
Set-DssConfirmationPolicy -IdpId 1 -NoneOpcActions -AllowOverride 0
```

Чтобы указать **набор операций, которым требуется подтверждение**, необходимо использовать параметр `-OpcActions`, указывая в его значении список операций, требующих подтверждения, следующим образом:

```
Set-DssConfirmationPolicy -IdpId 1 -OpcActions Issue, SignDocument
```

ИЛИ

```
Set-DssConfirmationPolicy -IdpId 1 –OpcActions 1, 2
```

В случае, если необходимо изменить политику группы, следует вместо параметра `-IdpId` указывать параметр `-GroupId`.

Полный список операций и их кодов приведен в таблице ниже.

НАИМЕНОВАНИЕ	КОД	ОПИСАНИЕ
Issue	1	
SignDocument	2	
SignDocuments	4	
DecryptDocument	8	
CreateRequest	16	
ChangePin	32	
RenewCertificate	64	

НАИМЕНОВАНИЕ	КОД	ОПИСАНИЕ
RevokeCertificate	128	
HoldCertificate	256	
UnholdCertificate	512	
DeleteCertificate	1024	
PrivateKeyAccess	2048	

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.

Примечание

Изменение настроек политики доступа к операциям для пользователей возможно только через Веб-интерфейс Пользователя или API DSS.

Политика доступа к операциям представляет собой набор следующих настроек:

ПАРАМЕТР	ТИП	ОПИСАНИЕ
Доступ к операциям	`-AllActionsAllowed` ИЛИ `-AllActionsDisallowed` ИЛИ `-DisallowedActions <DSSActions>`	Набор операций, к которым настраивается доступ.
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.

Примечание

В зависимости от того, политика какого уровня настраивается — уровня ЦИ или уровня группы — необходимо также соответственно использовать параметр `-IdpId` со значением `1`, ИЛИ параметр `-GroupId` со значением идентификатора настраиваемой группы.

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`, настройки политики уровнем ниже не имеют силы. Если все политики в иерархии имеют `AllowOverride` = `true`, параметры `AllowChangeByUser` и `AllowChangeByOperator` используются из политики группы, а настройка самого доступа к операциям применяется индивидуально для каждого Пользователя (настраивается в Веб-интерфейсе Пользователя).

Примечание

Перед изменением настроек политики доступа к операциям при помощи командлетов (уровень ЦИ DSS или уровень группы), убедитесь, что на уровень выше не применялось значение `AllowOverride` = `false`.

Примеры:

Получение политики доступа к операциям по уровням:

```
# Получение политики ЦИ DSS:
Get-DssAccessPolicy -IdpId 1
# Если в выводе данной команды содержится AllowOverride = False,
# настройки уровня группы не имеют силы.

# Получение политики группы
Get-DssAccessPolicy -GroupId 1
# Если в выводе данной команды содержится AllowOverride = False,
# Пользователь не сможет изменить политику доступа к операциям в Веб-
# интерфейсе.
```

Примеры настроек политики доступа к операциям:

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

```
Set-DssAccessPolicy -IdpId 1 -AllActionsAllowed -AllowOverride 0
```

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

```
Set-DssAccessPolicy -IdpId 1 -AllActionsDisallowed -AllowOverride 0
```

Чтобы указать набор операций, доступ к которым запрещен, необходимо использовать параметр `–DisallowedActions`, указывая в его значении список операций следующим образом:

```
Set-DssAccessPolicy -IdpId 1 -DisallowedActions Issue, SignDocument
```

ИЛИ

```
Set-DssAccessPolicy -IdpId 1 –DisallowedActions 1, 2
```

В случае, если необходимо изменить политику группы, следует вместо параметра `–IdpId` указывать параметр `–GroupId`.

Полный список операций и их кодов аналогичен списку на странице политики подтверждения операций.

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 -DisplayName STS -SiteName "Default Web Site" -SQLServerName “.\SQLEXPRESS”

# Добавление отпечатка сервисного сертификата Центра Идентификации
Set-DssStsProperties -DisplayName STS –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 -DisplayName STS -Login Admin -Name “Иванов Иван Иванович” -EmailAddress <Адрес
почты>  -PhoneNumber <Номер телефона> –IssuerName realsts –Certificate $cert
```

Пример добавления доверенной стороны:

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

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

# Включение проверки доверенных сторон (включена по умолчанию)
Set-DssStsProperties -AppliesToValidationRequired 1
```

Настройка Сервиса Подписи

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

В этом разделе:

Создание и настройка экземпляра Сервиса Подписи

Данный раздел определяет последовательность действий при разворачивании и настройке экземпляра Сервиса Подписи КриптоПро DSS.

- **Пример разворачивания**

Предварительные условия:

- Установленный SQL-Server;
- Установленная роль Сервер приложений (IIS);
- Настроенная привязка https на Сервере приложений (IIS);
- Установленный КриптоПро CSP (входит в комплект поставки);
- Установленный КриптоПро HSM Client;
- Установленный КриптоПро .NET (лицензия и дистрибутив входят в комплект поставки);
- Выпущенный и установленный сервисный сертификат Сервиса Подписи.

Базовая последовательность шагов по настройке (обязательные):

1. Создание экземпляра службы Сервиса Подписи (командлет New-DssSignServerInstance). На данном шаге будет создано веб-приложение на Сервере приложений IIS, развёрнуты базы данных, зарегистрированы журналы Windows.

```
New-DssSignServerInstance -SiteName "Default Web Site" -ApplicationName SignServer -SQLServerName
“.\SQLEXPRESS” –DisplayName SignServer
```

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

```
Set-DSSSignServerProperties -ServiceCertificate <thumbprint>
```

> **Примечание**
>
> Учетной записи, под которой работает пул приложения Сервиса Подписи, необходимо выдать права на доступ к закрытому ключу сервисного сертификата.

3. Ввод лицензии.

Пример ввода временной лицензии:

```
Add-DssLicense
```

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

Пример добавления HSM-провайдера с Мастер-ключом:

```
Add-DssCryptoProvider -DisplayName SignServer -TypeId GostWithMasterKey -ProviderType 80 -ProviderName
"Crypto-Pro GOST R 34.10-2012 HSM Svc CSP" -Exportable
```

5. Регистрация обработчика, реализующего функцию по созданию запроса на сертификат.

```
Add-DssEnrollment -DisplayName SignServer –Type EnrollOutOfBand –EnrollName <Имя обработчика> –RdnConfig
<Путь к файлу политики имен> -TemplatesConfig <Путь к файлу шаблонов сертификатов>
```

6. Настройка отношений доверия с Центром Идентификации. 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.

Данное действие выполняется при помощи командлета Add-DssClaimsProviderTrust.

- Регистрация Сервиса Подписи в качестве доверенной стороны на Центре Идентификации.

Данное действие выполняется при помощи командлета Add-DssRelyingPartyTrust.

Примечание

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

Пример настройки отношений доверия:

```
Add-DssRelyingPartyTrust -Name "SignServer" -MetadataUri
http://<signserver_host>/SignServer/FederationMetadata/2007-06/FederationMetadata.xml
Add-DssClaimsProviderTrust -IssuerName realsts -Thumbprint <Отпечаток сертификата Центра Идентификации>
```

Примечание

После внесения изменений в конфигурацию экземпляра необходимо перезапустить пул веб-приложения при помощи соответствующей команды.

Пример перезапуска:

```
# Перезапуск пула приложений Сервиса Подписи:
Restart-DssSignServerInstance -DisplayName <string>
```

Дополнительные действия по настройке (опциональные):

1. Настройка параметров подписи (Командлет Set-DssProperties). Администратор может ограничить набор форматов подписи, которые может создавать Сервис Подписи. По умолчанию доступны все форматы подписи (см. Общее Описание).

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.

2. Настройка оповещения Пользователя. Администратор DSS может настроить SMS- или Email-оповещение Пользователей о действиях, выполненных на Сервисе Подписи.

3. Настройка аудита. Администратор DSS может настроить сбор событий с Сервиса Подписи и их отправку на Сервис Аудита для ведения журнала событий. Для этого потребуется включить отображение пункта меню "Аудит" в личном кабинете Пользователя или Оператора.

4. 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.

5. Регистрация профилей подписи. Администратор DSS может создать правила для различных форматов подписи и

объединить данные правила в профиль. Профиль можно указать при подписи документов через API v2.

6. Включение режима асинхронной подписи. Администратор DSS может настроить и активировать асинхронную подпись. Асинхронная подпись упрощает взаимодействие с информационной системой, отправляющей в DSS запросы на подпись. При включенной асинхронной подписи DSS возвращает информационной системе результат работы, таким образом оповещая ее о завершении операции.

> **Внимание!**
>
> Асинхронная подпись возможна только для операций подписи с подтверждением при использовании APIv2.

Настройка производится следующим образом:

- Настройка асинхронной подписи (командлет Set-DssAsyncOperationSettings). Необходимо указать параметр `-ThreadCount <число>` - количество обработчиков асинхронной подписи. Рекомендуется рассчитывать, исходя из количества ядер процессора узла, где расположен Сервис Подписи, умноженного на 2;
- Включение асинхронной подписи (командлет Enable-DssAsyncOperationSettings).

Пример:

```
Set-DssAsyncOperationSettings -ThreadCount 4
Enable-DssAsyncOperationSettings -DisplayName <SignServer AppName>
```

7. Настройка журналирования экземпляра.

Профили подписи

Документы, отправляемые на подпись в КриптоПро DSS через API v2, могут быть подписаны с использованием профиля подписи. Профиль подписи - это набор правил подписи. Правило определяет, какой формат и прочие параметры подписи должны применяться к документам определенных форматов.

Настройка профиля подписи состоит из следующих этапов:

1. Регистрация правила (правил) подписи.
2. Создание профиля подписи и прикрепление к нему правил.
3. Создание операции подписи в соответствии с описанием работы REST-интерфейса Сервиса Подписи.

См. также:

- Командлеты администрирования профилей подписи
- Пример PowerShell-сценария

Регистрация правила подписи

Регистрация правила подписи выполняется при помощи командлета Add-DssProcessingRule. Командлет позволяет зарегистрировать форматы и параметры электронной подписи относительно расширений документов. Это означает, что при передаче на подпись документа по его расширению для него будет определен автоматически формат и параметры подписи.

Пример регистрации правил подписи:

```
Add-DssProcessingRule -Format MSOffice -DocumentsFormats @("docx", "doc")
Add-DssProcessingRule -Format CAdES -DocumentsFormats @('*') -Parameters @{IsDetached="true"; CADESType="T";
TSPAddress=" http://testca2012.cryptopro.ru/tsp/tsp.srf"}
Add-DssProcessingRule -Format CMS -DocumentsFormats @('txt')
```

Возможные варианты форматов подписи (параметр `-Format`):

- `XMLDSig` - подпись XML-документов,
- `GOST3410` - подпись ГОСТ Р 34.10–2001 и ГОСТ Р 34.10–2012 (Необработанная ЭП),
- `CAdES` - усовершенствованная подпись,
- `PDF` - подпись PDF-документов,
- `MSOffice` - подпись документов Microsoft Office,
- `CMS` - подпись формата CAdES-BES.

Список параметров подписи (Словарь `-Parameters`).

Создание профиля подписи и прикрепление к нему правил

Зарегистрированные правила подписи прикрепляются к определенному профилю подписи при помощи командлета New-DssProcessingTemplate. При этом потребуется указать идентификаторы правил. Получить идентификаторы правил подписи можно при помощи командлета Add-DssProcessingRule.

```
New-DssProcessingTemplate -ProcessingRulesIds @(14, 16) -Description <Описание профиля>
```

Профиль подписи будет зарегистрирован в БД с собственным идентификатором. Данный идентификатор необходимо указывать при создании операции подписи в параметре `ProcessingTemplateId` структуры DocumentSignature.

Получить значение идентификатора можно при помощи командлета Get-DssProcessingTemplate.

Другие случаи, когда используется данный идентификатор, описаны в документе ЖТЯИ.00096-02 97 01 КриптоПро DSS. Руководство разработчика.

Пример создания профиля подписи

```
Add-DssProcessingRule -Format MSOffice -DocumentsFormats @("docx", "doc")
Add-DssProcessingRule -Format CAdES -DocumentsFormats @('*') -Parameters @{IsDetached="true"; CADESType="T";
TSPAddress=" http://testca2012.cryptopro.ru/tsp/tsp.srf"}
New-DssProcessingTemplate -ProcessingRulesIds @(14, 16) -Description <Описание профиля>
```

Обработчики запросов на сертификат

Данный раздел определяет последовательность действий при регистрации в КриптоПро DSS обработчика запросов на сертификат, позволяющего Пользователю создавать запросы на сертификат в Веб-интерфейсе Пользователя и скачивать\распечатывать их для последующего обращения в Удостоверяющий Центр.

Регистрация обработчика запроса на сертификат

1. Регистрация обработчика

Регистрация обработчика запросов на сертификат производится при помощи командлета Add-DssEnrollment.

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

ПОЛЕ	ТИП	ОПИСАНИЕ
DisplayName	string	Имя экземпляра Сервиса Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Type	string	Тип УЦ. Для добавления обработчика только создания запроса на сертификат необходимо указать значение **EnrollOutOfBand**.
EnrollDisplayName	string	Отображаемое имя 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.
SNChangesEnabled	bool	Разрешить изменять имя субъекта в сертификате.
ValidationMode	string	Режим проверки сертификата ЭП перед использованием. Возможные значения: **ChainOffline** - для локально установленного CRL, **ChainOnline** - для локально установленного или загруженного по сети CRL ИЛИ при помощи OCSP-службы, **NoCheck** - не проверять.
CertificatePrintTemplate	string	Путь к шаблону печати сертификата. Встроенные в DSS шаблоны хранятся по умолчанию в папке `<C:\Program Files\Crypto Pro\DSS\SignServer\PrintTemplates>`.
RequestPrintTemplate	string	Путь к шаблону печати запроса на сертификат. Встроенные в DSS шаблоны хранятся по умолчанию в папке `<C:\Program Files\Crypto Pro\DSS\SignServer\PrintTemplates>`.
ExtensionsConfig	string	Путь к файлу с дополнительными расширениями для запроса на сертификат (см. п.4).
RdnConfig	string	Путь к файлу конфигурации компонентов имени Пользователя (см. п.3).
TemplatesConfig	string	Путь к файлу конфигурации шаблонов сертификатов Пользователей (см. п.2).

Полный **набор командлетов** для управления обработчиками запросов на сертификат.

2. Конфигурация шаблонов сертификатов

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

Примечание

Файлы должны быть сохранены в кодировке UTF-8.

```
[<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
```

3. Конфигурация компонентов имени Пользователя

Файлы конфигурации компонентов имени Пользователя представляют собой текстовые файлы, содержащие строки определенного формата.

Примечание

Файлы должны быть сохранены в кодировке UTF-8.

```
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'
```

4. Формат записи файла с дополнительными расширениями для запроса на сертификат

Файлы с дополнительными расширениями для запроса на сертификат представляют собой текстовые файлы, содержащие

строки определенного формата.

> **Примечание**
>
> Файлы должны быть сохранены в кодировке UTF-8.

и т.д., где

- `OID1`, `OID2`,... — идентификаторы расширений сертификата, которые попадут в запрос на сертификат;
- `Critical` — поле «Critical» расширения X.509-сертификата;
- `Value1`, `Value2`,... — значения расширений в нотации `ASN.1` , закодированные в base64.

Пример:

```
OID='1.2.643.100.111' Critical='true'
Value='DGrQn9CQ0JrQnCDCq9Ca0YDQuNC/0YLQvtCf0YDQviBIU03CuyDQstC10YDRgdC40Y8gMi4wICjQutC+0LzQv9C70LXQutGC0LDRht
C40Y8gMSkgKNC40YHQv9C+0LvQvdC10L3QuNC1IDEp'
```

Пример PowerShell-сценария для настройки компонента «Сервис Подписи»

Данный сценарий выполняет минимально необходимую настройку экземпляра компонента «Сервис 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 –DisplayName SignServer -ServiceCertificateThumbprint <Отпечаток сертификата компонента>

#Добавление HSM-провайдера с Мастер-ключом
Add-DssCryptoProvider -DisplayName SignServer -TypeId GostWithMasterKey -ProviderType 80 -ProviderName
"Crypto-Pro GOST R 34.10-2012 HSM Svc CSP" -Exportable

#Регистрация обработчика, отвечающего за генерацию запроса на сертификат
Add-DssEnrollment -DisplayName SignServer –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
Add-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 (двумя способами):

СПОСОБ 1:

```
#Задание служб штампов времени

$newTsp = New-Object -TypeName CryptoPro.DSS.Common.Service.TSPService
#Задание адреса
$newTsp.Url = " http://tsp.cryptopro.ru/tsp20/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/tsp20/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
```

СПОСОБ 2:

```
# Регистрация службы штампов времени при помощи специализированного командлета
Add-DssTspService -DisplayName SignServer -Name testTSP -Title "TSP-служба КРИПТО-ПРО" -Url "
http://tsp.cryptopro.ru/tsp20/tsp.srf"
```

Пример настройки конечных точек:

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

Пример включения журналирования:

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

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

# Включение журналирования
Enable-DssSignServerTracing -DisplayName SignServer
```

Настройка Веб-интерфейса Пользователя

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

В этом разделе:

- Настройка экземпляра
- Объекты администрирования и командлеты
- Пример PowerShell-сценария

См. также:

- Отображение документов

Создание и настройка экземпляра Веб-интерфейса Пользователя

Данный раздел определяет последовательность действий при разворачивании и настройке экземпляра Веб-интерфейса Пользователя КриптоПро DSS.

- **Пример разворачивания**

Предварительные условия:

- Установленная роль Сервер приложений (IIS);
- Настроенная привязка https на Сервере приложений (IIS);
- Установленный КриптоПро CSP (входит в комплект поставки);
- Выпущенный и установленный сервисный сертификат Веб-интерфейса Пользователя.

Базовая последовательность шагов по настройке (обязательные):

> **Примечание**
>
> После выполнения шагов, перечисленных в данном разделе, доступ к Веб-интерфейсу Пользователя осуществляется по умолчанию по следующим ссылкам:
>
> **Веб-интерфейс Сервиса Подписи:**
>
> ```
> https://<hostname>/Frontend
> ```
>
> **Личный кабинет Пользователя:**
>
> ```
> https://<hostname>/STS/Users
> ```

1. Создание экземпляра службы Веб-интерфейса Пользователя (командлет New-DssFeInstance). На данном шаге будет создано веб-приложение на Сервере приложений IIS, развёрнуты базы данных, зарегистрированы журналы Windows.

2. Настройка сервисного сертификата Веб-интерфейса Пользователя. На данном шаге экземпляру Сервиса Подписи назначается сервисный сертификат, который используется для аутентификации при межсервисном взаимодействии.

```
Set-DSSFEProperties -ServiceCertificate <thumbprint>
```

> **Примечание**
>
> Учетной записи, под которой работает пул приложения Веб-интерфейса Пользователя, необходимо выдать права на доступ к закрытому ключу сервисного сертификата.

3. Настройка URL-адресов компонентов DSS. На данном шаге задаются адреса компонентов DSS для межсервисного взаимодействия с Веб-интерфейсом Пользователя во время выполнения операций подписи и других операций.

Выполнение опциональных пунктов данной настройки (см. ниже) добавит на Веб-интерфейс Пользователя соответствующие кнопки (`Проверить подпись` и `Аудит`) в боковом меню.

Настройка осуществляется при помощи командлета Set-DssFEProperties:

- URL Центра Идентификации - параметр `-StsAddress`. Формат адреса: `https://<hostname>/<StsAppName>/Active.svc/service`.
- URL Сервиса Подписи - параметр `-SignServerAddress`. Формат адреса: `http://<hostname>/<SignServiceAppName>`.
- (опционально) URL Сервиса Проверки Подписи - параметр `-VsAddress`. Формат адреса: `http://<hostname>/<SVSAppName>/rest/api`.
- (опционально) URL Сервиса Аудита - параметр `-AnalyticsServiceAddress`. Формат адреса: `https://<hostname>/<AnalyticsServiceAppName>/analyticsservice.svc/issuedtoken/transport/nosc`.

- (опционально) URL Сервиса Обработки Документов - параметр `-DocumentStoreAddress`. Формат адреса: `https://<hostname>/<DocumentStoreAppName>`.

4. Настройка URL-адресов для доступа Пользователей СЭП.

На данном этапе настраиваются URL-адреса, по которым Веб-интерфейс Пользователя будет доступен Пользователям для аутентификации и работы с DSS с использованием протокола OpenID Connect 1.0.

Настройка осуществляется посредством ввода следующих команд:

```
# Настройка на Центре Идентификации доступа по OpenID Connect

Add-DssClient -Identifier cryptopro.dss.frontend.<FrontendAppName> -Name cryptopro.dss.frontend.
<FrontendAppName> -Description "<Frontend OAuth client description>" -AllowedFlow
AuthorizationCode,ClientCredentials,TokenExchange -RedirectUri
"https://<FEhostname>/<FrontendAppName>/Admins/Users/ExternalCallback","https://<FEhostname>/<FrontendAppName
>/Users/ExternalCallback" -GenerateSecret
```

```
# Настройка на Веб-интерфейсе доступа по OpenID Connect

$clientSecret = (Get-DssClientSecret -ClientId cryptopro.dss.frontend.<FrontendAppName>).Value

Set-DssFeOidcSettings -Issuer "https://<STShostname>/<StsAppName>" -Realm "https://<FEhostname>" -ClientId
cryptopro.dss.frontend.<FrontendAppName> -ClientSecret $clientSecret
```

Примечание

У Пользователей СЭП должен быть открыт доступ к указанным на данном шаге URL-адресам.

Примечание

Зарегистрированный `clientSecret` действителен в течение 1 года с момента его регистрации. После его истечения необходимо сгенерировать новый `clientSecret` для прежнего клиента:

```
Set-DssClient -ClientId cryptopro.dss.frontend.<FrontendAppName> -GenerateSecret

$clientSecret = (Get-DssClientSecret -ClientId cryptopro.dss.frontend.<FrontendAppName>).Value

Set-DssFeOidcSettings -ClientId cryptopro.dss.frontend.<FrontendAppName> -ClientSecret $clientSecret
```

5. Настройка отношений доверия с Центром Идентификации. На данном шаге устанавливается отношение доверия между Центром Идентификации и Веб-интерфейсом Пользователя.

Настройка выполняется в два шага:

- Регистрация на Веб-интерфейсе Пользователя Центра Идентификации в качестве доверенного издателя маркеров безопасности.

Данное действие выполняется при помощи командлета Add-DssFeClaimsProviderTrust.

- Регистрация Веб-интерфейса Пользователя в качестве доверенной стороны на Центре Идентификации.

Данное действие выполняется при помощи командлета Add-DssRelyingPartyTrust.

Примечание

К моменту выполнения шага 5 должен быть развёрнут экземпляр Центра Идентификации.

Примечание

После внесения изменений в конфигурацию экземпляра необходимо перезапустить пул веб-приложения при помощи

соответствующей команды.

Дополнительные действия по настройке (опциональные):

1. Кастомизация Веб-интерфейса Пользователя.

Администратор может изменить отображаемые на Веб-интерфейсе Пользователя логотипы, цвета интерфейса, цвета шрифтов, заголовки и т.п.

2. Настройка оповещения Пользователя.

Администратор DSS может настроить SMS- или Email-оповещение Пользователей о действиях, выполненных на Сервисе Подписи.

3. Визуализация документов.

Администратор может настроить отображение документов в Веб-интерфейсе при подписании и шифровании.

4. Настройка размера подписываемых документов.

Администратор может ограничить максимальный размер документа, который может быть подписан через Веб-интерфейс Пользователя. По умолчанию максимальный размер документа равен ~4Mb. Настройка размера документов осуществляется при помощи параметра `-MaxIISContentLength` командлета Set-DssFEProperties.

5. Интеграция с Сервисом Проверки Подписи.

Администратор может включить отображение дополнительных вкладок на Веб-интерфейсе Пользователя для проверки подписи и сертификата. Данная настройка описана в Шаге 3 Обязательных настроек (см. выше).

6. Интеграция с Сервисом Аудита.

Администратор может включить отображение журнала Сервиса Аудита на Веб-интерфейсе Пользователя. Данная настройка описана в сценарии настройки Сервиса Аудита.

7. Интеграция с Сервисом Обработки Документов.

Администратор может настроить преобразование документов, загружаемых через Веб-интерфейс Пользователя, на Сервисе Обработки Документов. Для этого необходимо указать адрес Сервиса Обработки Документов в параметре `-DocumentStoreAddress` командлета Set-DssFEProperties:

```
Set-DssFEProperties -DocumentStoreAddress <string>
```

Данное действие требует перезапуска пула приложений Веб-интерфейса Пользователя:

```
Restart-DssFEInstance -DisplayName <string>
```

Внимание!

В случае включения данной настройки, будут использованы плагины конвертации документов, настроенные для Сервиса Обработки Документов. При этом плагины, настроенные для Веб-интерфейса Пользователя и мобильного приложения более использоваться не будут.

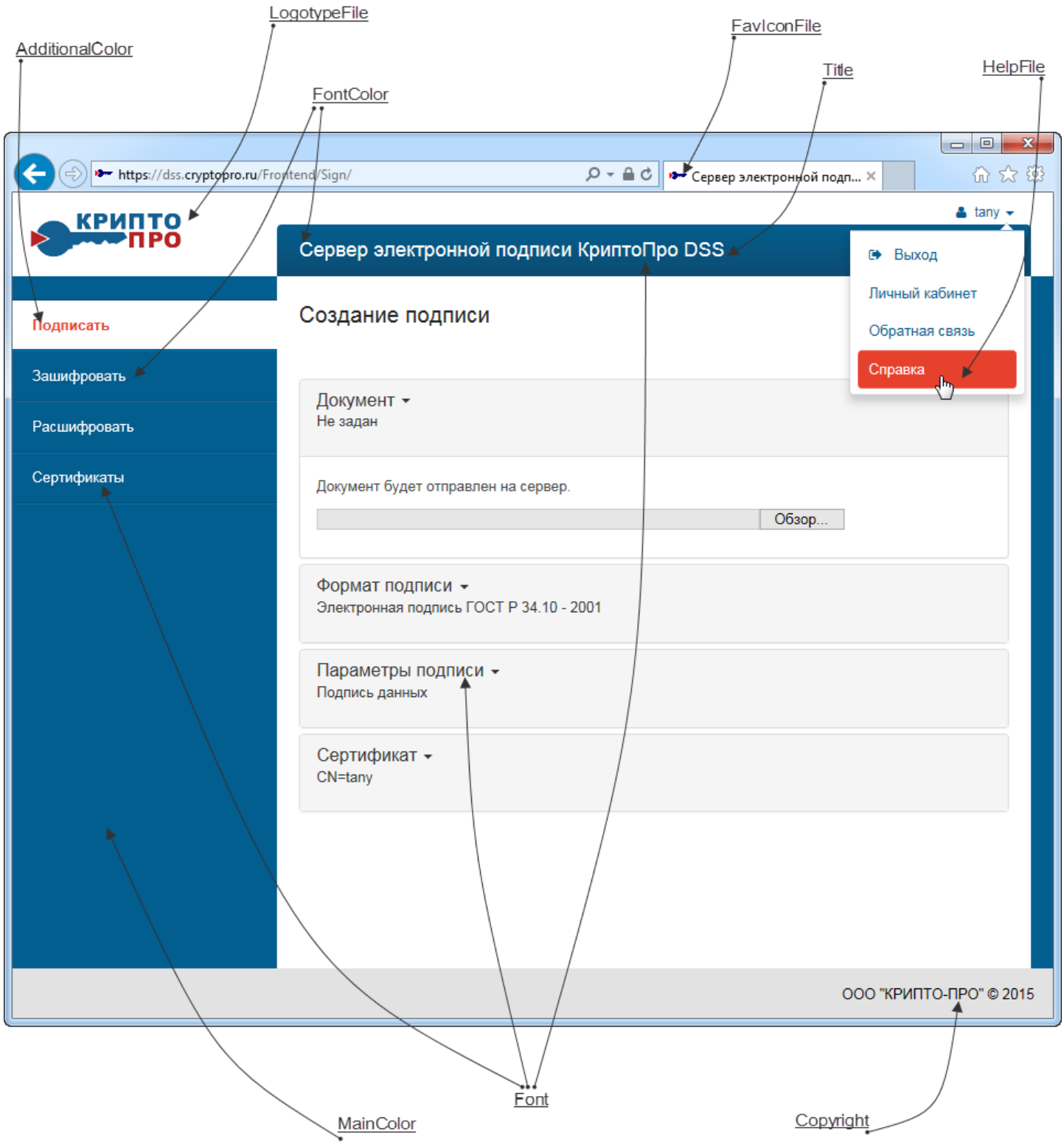
8. Настройка автоопределения формата документа.

9. Настройка журналирования экземпляра.

Кастомизация веб-интерфейса Пользователя

Администратор DSS может кастомизировать Веб-интерфейс Пользователя: изменить цвета фона, текста, логотипы, тексты заголовков и т.п. при помощи набора командлетов.

На рисунке ниже установлено соответствие элементов интерфейса и параметров командлетов кастомизации.



Пример скрипта для кастомизации веб-интерфейса 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"
```

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

Данный сценарий выполняет минимально необходимую настройку экземпляра компонента «Веб-интерфейс Пользователя».

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

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

# Настройка адресов Сервиса Подписи и Центра Идентификации:
Set-DSSFEProperties -DisplayName Frontend -SignServerAddress "http://<hostname>/SignServer" -StsAddress
"https://<hostname>/STS/Active.svc/service"

# Регистрация на Веб-интерфейсе Пользователя Центра Идентификации в качестве доверенного издателя маркеров
безопасности:
Add-DssFEClaimsProviderTrust -DisplayName Frontend -IssuerName realsts -Thumbprint <Отпечаток сертификата
Центра Идентификации>



# Настройка URL-адресов для доступа Пользователей СЭП

# Настройка на Центре Идентификации доступа по OpenID Connect
Add-DssClient -DisplayName STS -Identifier cryptopro.dss.frontend.<FrontendAppName> -Name
cryptopro.dss.frontend.<FrontendAppName> -Description "<Frontend OAuth client description>" -AllowedFlow
AuthorizationCode,ClientCredentials,TokenExchange -RedirectUri
"https://<FEhostname>/<FrontendAppName>/Admins/Users/ExternalCallback","https://<FEhostname>/<FrontendAppName
>/Users/ExternalCallback" -GenerateSecret

# Настройка на Веб-интерфейсе доступа по OpenID Connect
$clientSecret = (Get-DssClientSecret -ClientId cryptopro.dss.frontend.<FrontendAppName>).Value
Set-DssFeOidcSettings -Issuer "https://<STShostname>/<StsAppName>" -Realm "https://<FEhostname>/<FEAppName>"
-ClientId cryptopro.dss.frontend.<FrontendAppName> -ClientSecret $clientSecret
```

Регистрация Веб-интерфейса Пользователя в качестве доверенной стороны на Центре Идентификации:

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

Пример кастомизации Веб-интерфейса 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"
```

Настройка Сервиса Аудита

Компонент КриптоПро DSS Сервис Аудита предназначен для сбора событий с других компонентов СЭП и формирования отчетности в веб-версии и печатном виде.

В этом разделе:

- Настройка экземпляра
- Объекты администрирования и командлеты
- Пример PowerShell-сценария

См. также:

- Настройка аудита компонентов КриптоПро DSS

Создание и настройка экземпляра Сервиса Аудита

Данный раздел определяет последовательность действий при разворачивании и настройке экземпляра Сервиса Аудита КриптоПро DSS.

- **Пример разворачивания**
- **Включение аудита компонентов**

Предварительные условия:

- Установленный SQL-Server;
- Установленная роль Сервер приложений (IIS);
- Настроенная привязка https на Сервере приложений (IIS);
- Выпущенный и установленный сервисный сертификат Сервиса Аудита.
- (Если планируется обеспечение целостности записей аудита) Установленный КриптоПро CSP (входит в комплект поставки) ();

Базовая последовательность шагов по настройке (обязательные):

1. Создание экземпляра службы Сервиса Аудита (командлет New-DssAnalyticsServiceInstance).

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

2. Настройка сервисного сертификата Сервиса Аудита.

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

```
Set-DSSAnalyticsServiceProperties -ServiceCertificate <thumbprint>
```

> **Примечание**
>
> Учетной записи, под которой работает пул приложения Сервиса Аудита, необходимо выдать права на доступ к закрытому ключу сервисного сертификата.

3. Настройка конечной точки Сервиса Аудита для отображения записей аудита на веб-интерфейсе.

На данном шаге требуется задать параметр `-AnalyticsServiceUri` командлета Set-DssAnalyticsServiceProperties.

Адрес конечной точки в общем виде выглядит следующим образом:

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

, где

`hostname` - имя узла, на котором разворачивается Сервиса Аудита; `AnalyticsAppName` - имя веб-приложения Сервиса Аудита.

4. Настройка адреса ЦИ, куда Сервис Аудита обращается для аутентификации.

На данном шаге требуется задать параметр `-StsAddress` командлета Set-DssAnalyticsServiceProperties.

Адрес ЦИ в общем виде выглядит следующим образом:

```
https://<hostname>/<STSAppName>/Active.svc/service
```

, где

`hostname` - имя узла, на котором разворачивается Сервиса Аудита; `AnalyticsAppName` - имя веб-приложения Сервиса Аудита.

5. Настройка контроля целостности записей аудита.

6. Настройка отношений доверия с Центром Идентификации.

На данном шаге устанавливается отношение доверия между Центром Идентификации и Сервисом Аудита, необходимое для корректной работы Сервиса.

Настройка выполняется в два шага:

- Регистрация на Сервисе Аудита Центра Идентификации в качестве доверенного издателя маркеров безопасности.

Данное действие выполняется при помощи командлета Add-DssAnalyticsClaimsProviderTrust.

- Регистрация Сервиса Аудита в качестве доверенной стороны на Центре Идентификации.

Данное действие выполняется при помощи командлета Add-DssRelyingPartyTrust. Примеры регистрации доверенных сторон приведены также в соответствующем разделе.

Примечание

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

7. Настройка URL-адресов для доступа Пользователей и Операторов СЭП.

На данном этапе настраиваются URL-адреса, по которым веб-интерфейс Сервиса Аудита будет доступен Пользователям и Операторам для аутентификации и работы с DSS с использованием протокола WS-Federation. Настраиваемые URL-адреса имеют определенный формат, описанный ниже.

Настройка URL-адресов производится при помощи командлета Set-DssAnalyticsWSFederationSettings:

- URL Центра Идентификации - в параметре `-Issuer`. Формат адреса: `https://<hostname>/<StsAppName>/sts/issue/`, где `<hostname>` - имя узла, на котором развернут Центр Идентификации, `StsAppName` - имя веб-приложения Центра Идентификации.
- URL Веб-интерфейса Пользователя - в параметре `Realm`. Формат адреса: `https://<hostname>/<AnalyticsAppName>/Audit`, где `<hostname>` - имя узла, на котором развернут Сервис Аудита, `AnalyticsAppName` - имя веб-приложения Сервиса Аудита.
- URL-адрес доверенного Центра Идентификации - в параметре `HomeRealm`. По умолчанию не заполняется, зарезервирован для дальнейшего использования.
- Требование защищенного соединения (флаг) в параметре `RequireHttps`. По умолчанию равен 0.

Примечание

У Пользователей и Операторов СЭП должен быть доступ к указанным на данном шаге URL-адресам.

8. Настройка отображения пункта меню "Аудит" на веб-интерфейсе ЦИ и Веб-интерфейсе Пользователя.

- В личном кабинете Пользователя (на веб-интерфейсе ЦИ) - при помощи параметра `-AnalyticsServiceAddress` командлета Set-DssStsProperties.
- На Веб-интерфейсе Пользователя - при помощи параметра `-AnalyticsServiceAddress` командлета Set-DssFEProperties.

Значение параметра `-AnalyticsServiceAddress` в общем виде выглядит следующим образом:

Для Центра Идентификации:

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

Для Веб-интерфейса Пользователя:

```
https://<hostname>/<AnalyticsAppName>
```

> **Примечание**
>
> После внесения изменений в конфигурацию экземпляра необходимо перезапустить пул веб-приложения при помощи соответствующей команды.

9. Включение аудита компонентов

Дополнительные действия по настройке (опциональные):

1. Настройка плагинов формирования отчетов.

2. Настройка шаблонов печатных форм.

3. Настройка журналирования экземпляра.

4. Кастомизация. Администратор DSS может кастомизировать веб-интерфейс Сервиса Аудита: изменить цвета фона, текста, логотипы, тексты заголовков и т.п. при помощи набора командлетов.

Плагины формирования отчетов

В Сервисе Аудита КриптоПро DSS доступна расширенная настройка различных отчетов. Эту возможность реализуют плагины формирования отчетов, настраиваемые при помощи специализированного набора командлетов.

В зависимости от типов отчетов, представленных в таблице ниже, к плагину нужно подключить соответствующий класс отчета. Все предопределенные типы отчетов содержатся в сборке `CryptoPro.DSS.AnalyticsService.ReportPlugins.dll`. Имя сборки указывается в параметре `-Assembly`.

ТИП ОТЧЕТА	КЛАСС ОТЧЕТА	ОПИСАНИЕ
Отчеты о сертификатах	CryptoPro.DSS.AnalyticsService.ReportPlugins.CertificateReports.CreatedCertificateReport	Отчет о созданных сертификатах
	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.UnheldCertificatesReport	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 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 `paramNamei`, `paramValuei` – название и значение параметра соответственно. Каждый параметр и его значение помещаются в двойные кавычки.

В таблице ниже указаны параметры плагинов формирования отчета, которые настраиваются при добавлении плагинов разных типов.

ПАРАМЕТР	ТИП	ОПИСАНИЕ
Отчеты о сертификатах		
AuditConnectionString	string	Строка подключения к БД Сервиса Аудита
InstanceName	string	Уникальный идентификатор экземпляра Сервиса Подписи, по данным которого строится отчет. **ВНИМАНИЕ:** идентификатор имеет формат ***<SiteId>/<ApplicationName>***, где значения *SiteId* и ApplicationName можно получить в выводе командлета **Get-DssAnalyticsServiceInstance**.
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 об ЭП		
AuditConnectionString	string	Строка подключения к БД Сервиса Аудита
InstanceName	string	Уникальный идентификатор экземпляра Сервиса Подписи, по данным которого строится отчет. **ВНИМАНИЕ:** идентификатор имеет формат ***<SiteId>/<ApplicationName>***, где значения *SiteId* и *ApplicationName* можно получить в выводе командлета **Get-DssAnalyticsServiceInstance**.
Xslt	string	Путь к файлу с XSLT-преобразованием
ReportName	string	Отображаемое имя отчета
Delimiter	string	Символ разделения элементов при экспорте отчета в CSV-формат
StsConnectionString	string	Строка подключения к БД Центра Идентификации
Отчеты о Пользователях		
StsConnectionString	string	Строка подключения к БД Центра Идентификации
RealmName	string	Идентификатор экземпляра ЦИ, которому принадлежат Пользователи. **ВНИМАНИЕ:** идентификатор равен значению параметра *IssuerName*, который можно получить в выводе командлета **Get-DssIdentityProvider.**
RdnList	string	Список объектных идентификаторов 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	Идентификатор экземпляра ЦИ, по данным которого строится отчет. **ВНИМАНИЕ:** идентификатор равен значению параметра ***<SiteId>/<ApplicationName>***, где значения *SiteId* и *ApplicationName* можно получить в выводе командлета **Get-DssStsInstance**.
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	Идентификатор экземпляра ЦИ, по данным которого строится отчет.
Xslt	string	**ВНИМАНИЕ:** идентификатор равен значению параметра ***<SiteId>/<ApplicationName>***, где значения SiteId и *ApplicationName* можно получить в выводе командлета **Get-DssStsInstance**.
ReportName	string	Путь к файлу с XSLT-преобразованием
Delimiter	string	Отображаемое имя отчета

Примечание

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 -DisplayName <DisplayName> -FileExtension csr -Assembly
CryptoPro.DSS.AnalyticsService.ReportPlugins.dll -Classname
CryptoPro.DSS.AnalyticsService.ReportPlugins.SignatureReports.CreatedSignaturesReport -Parameters
@{"AuditConnectionString" = "<AuditServiceDbConnection>"; "InstanceName"="<SiteId/ApplicationName>";
"ReportName"="Количество созданных подписей";"StsConnectionString"="<StsDbConnection>";}
```

Плагин отчета по количеству созданных сертификатов:

```
Add-DssAnalyticsReportPlugin -DisplayName <DisplayName> -FileExtension ccr -Assembly
CryptoPro.DSS.AnalyticsService.ReportPlugins.dll -Classname
CryptoPro.DSS.AnalyticsService.ReportPlugins.CertificatesReport. CreatedCertificateReport -Parameters
@{"AuditConnectionString" = "<AuditServiceDbConnection>"; "InstanceName"="<SiteId/ApplicationName>";
"ReportName"="Количество созданных сертификатов";}
```

Плагин отчета по количеству созданных Пользователей:

```
Add-DssAnalyticsReportPlugin -DisplayName <DisplayName> -FileExtension cur -Assembly
CryptoPro.DSS.AnalyticsService.ReportPlugins.dll -Classname
CryptoPro.DSS.AnalyticsService.ReportPlugins.UserReports.CreatedUsersReport -Parameters
@{"StsConnectionString" = "<StsDbConnection>"; "ReportName"="Количество созданных пользователей";
"RealmName"="<STS Realm Name>";"RdnList"="2.5.4.3"}
```

Плагин отчета по количеству пользователей MyDSS:

```
Add-DssAnalyticsReportPlugin -DisplayName <DisplayName> -FileExtension mur -Assembly
CryptoPro.DSS.AnalyticsService.ReportPlugins.dll -Classname
CryptoPro.DSS.AnalyticsService.ReportPlugins.MyDss.MyDssUserReport -Parameters @{"AuditConnectionString" = "
<AuditServiceDbConnection>";  "InstanceName"="<SiteId/ApplicationName>"; "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.CloudCspReport.CloudCspReport -Parameters
@{"AuditConnectionString" = "<AuditServiceDbConnection>"; "InstanceName"="<SiteId/ApplicationName>";
"ReportName"="Отчет о пользователях Cloud CSP";}
```

Генерация печатных форм

Для активации возможности создания печатной формы списка записей аудита необходимо зарегистрировать нужные форматы и соответствующие плагины с помощью специализированного набора командлетов. 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"}
```

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 настройки экземпляра Сервиса Аудита.

Регистрация криптопровайдеров на Сервисе Аудита осуществляется при помощи набора командлетов.

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

- Зарегистрировать криптопровайдер подписи записей аудита при помощи командлета Add-DssAnalyticsCryptoProvider.
- Задать имя узла, для которого зарегистрирован криптопровайдер подписи записей аудита при помощи командлета Set-DssAnalyticsCryptoProvider, параметр `-NodeId`.
- Настроить при помощи командлета Set-DssAnalyticsServiceProperties следующие параметры Сервиса Аудита: `-SignatureTimerInterval` (частоту создания подписи блока событий) и `-SignatureBlockLength` (размер подписываемого блока (сегмента) событий).

Пример:

```
### Добавление криптопровайдера
Add-DssAnalyticsCryptoProvider -DisplayName <Имя экземпляра Сервиса Аудита> -TypeId AuditIntegrity -
ProviderName "Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider"  -ProviderType 80

### Нацеливание криптопровайдера на определенный узел Сервиса Аудита
Set-DssAnalyticsCryptoProvider -ID <Идентификатор криптопровайдера> -NodeId $env:COMPUTERNAME -DisplayName
<Имя экземпляра Сервиса Аудита>

### Настройка параметров контроля целостности
Set-DssAnalyticsServiceProperties -SignatureTimerInterval 1 -SignatureBlockLength 10 -DisplayName <Имя
экземпляра Сервиса Аудита>
```

> **Примечание**
>
> Параметр `-NodeId` должен быть настроен вне зависимости от использования Сервиса Аудита самостоятельно или в кластере. Данный параметр может содержать только имя узла, получить которое можно из переменной среды `$env:COMPUTERNAME`.

После выполнения описанных действий Сервис Аудита начнет формирование блоков записей аудита заданного размера, которые впоследствии будут подписаны при помощи криптопровайдера, зарегистрированного на Сервисе Аудита. Вся информация о блоке и подписи затем помещается в БД Сервиса Аудита и может быть просмотрена позднее.

Ключи подписи событий аудита

Ключи электронной подписи, используемые при подписи событий аудита, имеют ограниченный срок действия. Поэтому после окончания действия данного ключа контроль целостности на данном экземпляре Сервиса Аудита осуществляться не будет. Необходимо создать и настроить новый экземпляр Сервиса Аудита, в то время как старый экземпляр можно заархивировать, чтобы работать с записями аудита в дальнейшем.

Настройка контроля целостности записей аудита в кластере

Контроль целостности записей аудита при работе нескольких экземпляров Сервиса Аудита требует наличия отдельного ключа подписи для каждого экземпляра. Если экземпляры Сервиса Аудита раположены в кластере, для каждого узла кластера должен быть зарегистрирован собственный криптопровайдер при помощи командлета Add-DssAnalyticsCryptoProvider.

Для нацеливания криптопровайдера на определенный узел Сервиса Аудита необходимо ввести строковый идентификатор в параметр `-NodeId` командлета Set-DssAnalyticsCryptoProvider. Идентификатор представляет собой значение

`$env:computername` **для каждого узла в кластере**.

Настройка контроля целостности также должна выполняться для каждого узла в кластере.

Таким образом, настройка контроля целостности записей аудита в кластере сводится к выполнению описанных выше действий для каждого узла кластера. При этом все указанные действия могут быть выполнены на одном узле.

Проверка целостности аудита

Проверка целостности аудита осуществляется при помощи утилиты `auditverify.exe`.

Утилита имеет следующие режимы работы:

- Проверка целостности сегмента (параметр `-m` со значением `Segment`), ограниченного индексами `s` и `e` записей журнала целостности;
- Проверка целостности записей (параметр `-m` со значением `Full`), созданных не позднее чем за `d` дней до текущей (последней) записи журнала целостности.

Все параметры утилиты:

- `-m`: режим работы утилиты. Может принимать значения `Full` или `Segment`;
- `-s`: Индекс начала сегмента при работе в режиме проверки целостности сегмента;
- `-e`: Индекс конца сегмента при работе в режиме проверки целостности сегмента;
- `-d`: Количество дней, за которое следует проверять записи аудита, начиная от текущей даты;
- `-v`: Параметр, наличие которого указывает, следует ли проверять подпись каждой записи журнала Аудита;

Примеры вызова утилиты в различных режимах:

```
# Проверка целостности сегмента:
-m Segment -s 30 -e 60 [-v]

# Проверка целостности всех записей за 30 дней:
-m Full -d 30 [-v] или
```

Утилита подключается напрямую к БД Аудита, строка подключения указывается в `app.config` утилиты в секции `AppSettings`.

Архивирование аудита

> **Примечание**
>
> Скорость увеличения размера БД Сервиса Аудита зависит от текущих **настроек аудита**, что необходимо учитывать при планировании архивирования. Приблизительные размеры записей:
>
> - 1 запись ~ 2 Кбайт.
> - 1 000 000 записей ~ 1 Гбайт.
> - Аудит (Аутентификация Пользователя + Подпись документа + Подтверждение операции) ~ 5-10 событий.

Если аппаратные возможности сервера, на котором расположена БД Сервиса Аудита, превышены (к примеру, закончилось место на диске), следует прибегнуть к архивации аудита. Для этого необходимо выполнить следующие действия.

- Создать и настроить новый экземпляр Сервиса Аудита. **ВАЖНО:** Для каждого компонента DSS потребуется зарегистрировать еще по одному плагину аудита. При этом начнется запись событий аудита сразу в две БД.
- Убедившись в работоспособности нового сервиса, вывести старый из эксплуатации.
  - Архивировать БД старого Сервиса Аудита любыми доступными средствами и перенести (при необходимости) в другое место для хранения.
  - (необязательно) Удалить старый экземпляр Сервиса Аудита. Старый экземпляр Сервиса Аудита можно не удалять и использовать в дальнейшем для обращения к архивным сведениям. В этом случае достаточно остановить соответствующее Сервису веб-приложение.

Пример PowerShell-сценария для настройки компонента «Сервис Аудита»

Данный сценарий выполняет минимально необходимую настройку экземпляра компонента «Сервис Аудита».

```
#ВВОД ИСПОЛЬЗУЕМЫХ ПЕРЕМЕННЫХ

$hostname = "<Адрес узла Сервиса Аудита>"
$stsHostname = "Адрес узла Центра Идентификации"

$auditDisplayName = "AnalyticsService"
$feDisplayName = "Frontend"
$ssAppName = "SignServer"

$stsAppName = "STS"
$auditAppName = "AnalyticsService"

$auditDbName = "AnalyticsServiceDB"

$auditCertThumb = "<Отпечаток сертификата Сервиса Аудита>"
$stsCertThumb = "<Отпечаток сертификата Центра Идентификации>"

$provName = "Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider"
$provType = 80


# Добавление нового экземпляра Сервиса Аудита
New-DssAnalyticsServiceInstance -SiteName "Default Web Site" –DisplayName $auditDisplayName -ApplicationName
$auditAppName -SqlServerName "DSS-SDK\DSSSDKSQL" -DBName $auditDbName


# Добавление отпечатка сервисного сертификата Сервиса Аудита
Set-DssAnalyticsServiceProperties –DisplayName $auditDisplayName -ServiceCertificate $auditCertThumb


# Настройка конечной точки Сервиса Аудита для отображения записей аудита на веб-интерфейсе
Set-DssAnalyticsServiceProperties –DisplayName $auditDisplayName -AnalyticsServiceUri
"https://$hostname/$auditAppName/AnalyticsService.svc/issuedtoken/transport/nosc"


# Настройка адреса ЦИ, куда Сервис Аудита обращается для аутентификации
Set-DssAnalyticsServiceProperties –DisplayName $auditDisplayName -StsAddress
"https://$stsHostname/$stsAppName/Active.svc/service"


# Настройка URL-адресов для доступа Пользователей и Операторов СЭП
Set-DssAnalyticsWSFederationSettings –DisplayName $auditDisplayName -Issuer
"https://$stsHostname/$stsAppName/sts/issue/" -Realm https://$hostname/$auditAppName/Audit


# Настройка контроля целостности записей аудита
Add-DssAnalyticsCryptoProvider -DisplayName $auditAppName -ProviderName $provName -ProviderType $provType -
TypeId AuditIntegrity -Description "контроль целостности аудита"
Set-DssAnalyticsServiceProperties -DisplayName $auditAppName -SignatureTimerInterval 60 -SignatureBlockLength
10 -ProviderMonitoringInterval 10000


# НАСТРОЙКА ОТНОШЕНИЙ ДОВЕРИЯ

# Регистрация на Сервисе Аудита Центра Идентификации в качестве доверенного издателя маркеров безопасности
Add-DssAnalyticsClaimsProviderTrust –DisplayName $auditDisplayName -IssuerName realsts -Thumbprint
$stsCertThumb
```

```
# Регистрация Сервиса Аудита в качестве доверенной стороны на Центре Идентификации
Add-DssRelyingPartyTrust -DisplayName $stsAppName -Name $auditDisplayName –MetadataUri
https://$hostname/$auditAppName/federationmetadata/2007-06/federationmetadata.xml


# НАСТРОЙКА ОТОБРАЖЕНИЯ ПУНКТА МЕНЮ "АУДИТ"

# На Центре Идентификации
Set-DssStsProperties –DisplayName $stsAppName –AnalyticsServiceAddress
https://$hostname/$auditAppName/analyticsservice.svc/issuedtoken/transport/nosc

# На Веб-интерфейсе Пользователя
Set-DssFEProperties –DisplayName $feDisplayName –AnalyticsServiceAddress https://$hostname/$auditAppName
```

Настройка аудита компонентов

Данный сценарий демонстрирует пример настройки аудита Сервиса Подписи и Центра Идентификации. Подробнее сценарий настройки аудита компонентов описан в соответствующем разделе.

```
# Настройка аудита Центра Идентификации
New-DssStsAudit -DisplayName $stsAppName -UseRestApi 1 -AuditServiceAddress
http://$hostname/$auditAppName/api/writer

# Настройка аудита Сервиса Подписи
New-DssSignServerAudit -DisplayName $ssAppName -UseRestApi 1 -AuditServiceAddress
http://$hostname/$auditAppName/api/writer
```

Аудит компонентов КриптоПро DSS

Настройка аудита доступна для следующих компонентов КриптоПро DSS:

- Центр Идентификации;
- Сервис Подписи;
- Сервис Обработки Документов.

В этом разделе:

Настройка аудита компонентов DSS

Аудит компонентов КриптоПро DSS производится при помощи службы `AuditWriter`, которая автоматически создается при разворачивании экземпляра Сервиса Аудита. Настройка данной службы доступна для следующих компонентов КриптоПро DSS:

- Центр Идентификации;
- Сервис Подписи;
- Сервис Обработки Документов.

Для того, чтобы начать записывать в БД Сервиса Аудита события аудита выбранного компонента, необходимо включить для него аудит и зарегистрировать соответствующие плагины конвертации событий аудита и модули оповещения (доставки) этих событий в БД Сервиса Аудита. Данные действия выполняются при помощи следующих командлетов:

- New-DssStsAudit - для Центра Идентификации;
- New-DssSignServerAudit - для Сервиса Подписи;
- New-DssDocumentStoreAudit - для Сервиса Обработки Документов.

> **Примечание**
>
> Все параметры описываемых в данном разделе командлетов `New-Dss...Audit` одинаковы для каждого из компонентов. Поэтому пример разворачивания приводится для одного из них.

- **Пример настройки аудита**

Предварительные условия:

- Установленные и настроенные компоненты КриптоПро DSS, для которых требуется выполнять аудит (список доступных к аудиту компонентов см. выше).
- Установленный и настроенный в соответствии со сценарием настройки экземпляр Сервиса Аудита.

Базовая последовательность шагов по настройке (обязательные)

1. Включение аудита для экземпляра компонента КриптоПро DSS, регистрация необходимых плагинов и модулей оповещения (выполняется в одно действие).

Данный шаг производится для каждого из компонентов, которым требуется аудит, при помощи командлета (например) New-DssStsAudit. При этом необходимо указать следующие параметры:

- `-DisplayName` - имя экземпляра компонента, для которого настраивается аудит.
- `-AuditServiceAddress` - URL-адрес службы `AuditWriter` Сервиса Аудита. Формат адреса: `http://<hostname>/<analyticsAppName>/AuditWriter.svc)`.
- `-Settings` - параметры регистрируемого модуля оповещения. Формат словаря:
  `@{"<Имя параметра 1>"="<Значение параметра 1>"; "<Имя параметра 2>"="<Значение параметра 2>"; ...; "<Имя параметра N>"="<Значение параметра N>"}`
  .

Параметр `-Settings` является опциональным. Однако рекомендуется настроить путь для резервирования канала записи сообщений аудита при помощи настройки `FolderPath`:

```
-Settings @{"FolderPath"="<Путь к файлу>\"}
```

Данная настройка позволяет сохранить недоставленные события аудита в файл, откуда их потом можно импортировать в БД Сервиса Аудита.

Пример настройки аудита

Данный сценарий включает аудит Сервиса Подписи КриптоПро DSS с настроенным резервированием канала записи

сообщения аудита.

```
New-DssSignServerAudit -AuditServiceAddress http://hostname/Analytics/AuditWriter.svc -Settings
@{"FolderPath"="C:\tmp\"}
```

Дополнительные действия по настройке (опциональные)

1. Включение/отключение блокирующего аудита.

Данная настройка выполняется при при помощи параметра `-UseBlockingAudit <1/0>` командлета (например) New-DssStsAudit или командлета (например) Set-DssStsAudit.

> **Примечание**
>
> Включение блокирующего аудита создает новый словарь настроек модуля оповещения (см. п. 2). После переключения службы в режим блокирующего аудита необходимо убедиться, что настройки были перенесены. Для вывода всех настроек, записанных в `-Settings` можно выполнить следующую команду:
>
> `(Get-Dss**Audit -DisplayName <name>).Settings | fl`

> **Внимание!**
>
> Настройка `FolderPath` (т.е. резервирование записей аудита) при включенном блокирующем аудите игнорируется. Резервирование не будет производиться.

2. Изменение параметров модуля оповещения службы аудита компонента.

Параметры модуля оповещения службы аудита компонента можно изменить при помощи словаря `-Settings` командлета (например) Set-DssStsAudit. Полный список доступных настроек:

- `MinQueueSize` – приемлемый размер очереди сообщений. При превышении 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 в мс. По умолчанию параметр равен `500`.
- `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. По умолчанию включен.
- `FolderPath` – путь к папке, в которой будет создан файл с недоставленными записями аудита.

3. Использование REST API для записи событий аудита.

Данную настройку можно выполнить ТОЛЬКО при создании нового аудита компонента (командлет New-DssStsAudit). В этом случае параметр `-AuditServiceAddress` должен быть следующим:

```
-AuditServiceAddress https://host/appname/api/writer
```

Если для какого-либо компонента DSS уже существует настроенный аудит, необходимо удалить его при помощи командлета Remove-DssStsAudit и зарегистрировать заново с данной настройкой.

Резервирование канала записи событий аудита

В силу того, что события аудита генерируются и записываются на различных компонентах независимо друг от друга, для обеспечения непрерывной записи событий необходимо наличие постоянной связи по сети между источниками событий и Службой Записи событий аудита (`AuditWriter.svc`). Ситуации, в которых служба записи событий аудита может быть недоступной, приводят к потере записей аудита. Для предотвращения подобного КриптоПро DSS обладает функцией резервирования канала записи сообщений аудита путем записи недоставленных событий в файл на жестком диске с последующей возможностью импорта этих записей в БД Сервиса Аудита.

Настройка экспорта недоставленных сообщений аудита

Активация резервного канала записи утерянных сообщений аудита на жесткий диск осуществляется путем задания параметра `-FolderName` модуля оповещения типа «Аудит». Данный параметр можно задать в командлете `New-DssXXXAudit` (XXX = `SignServer`, `STS` или `DocumentStore`) среди параметров модуля оповещения или же добавить параметр к уже существующему модулю путем вызова командлета `Set-DssXXXAudit` (XXX = `SignServer`, `STS` или `DocumentStore`). Данный параметр задает путь к папке, в которой будет создан файл с недоставленными записями аудита. Формат имени файла имеет следующий вид:

```
{product}_{instanceName}_Messages(0).cdm
```

, где

- `product` — это тип экземпляра компонента КриптоПро DSS (`SignServer`, `STS` или `DocumentStore`);
- `instanceName` — имя экземпляра компонента КриптоПро DSS, с которого записываются сообщения аудита.

Пример добавления параметра:

```
# Получение ID модуля оповещения при помощи командлета Get-DssSignServerNotifier

Get-DssSignServerNotifier

ID              : 5
Type            : Audit
Settings        : {[Enabled, True], [FolderName, C:\tmp], [ThreadCount, 1]}
IsEnabled       : True
TransportPlugin : CryptoPro.DSS.PowerShell.Common.Objects.Plugin
MessagePlugin   : CryptoPro.DSS.PowerShell.Common.Objects.Plugin

# Назначение параметра -FolderPath

Set-DssSignServerNotifier -NotifierID 5 -Settings @{"FolderPath"="C:\tmp\"}
```

> **Примечание**
>
> Аналогичным образом резервирование может быть включено для модуля оповещения при его создании:
>
> ```
> New-DssSignServerAudit -AuditServiceAddress http://host.name/Analytics/AuditWriter.svc -Settings
> @{"FolderPath"="C:\tmp\"}
> ```

Настройка импорта недоставленных сообщений аудита

По восстановлении связи с компонентом Сервис Аудита и/или его БД. Утерянные и недоставленные сообщения могут быть импортированы в БД из файла, куда велось резервирование, при помощи следующей команды:

```
Import-SignServerAuditRecords -FilePath <путь>
```

При этом производится проверка каждого события на возможные дубликаты. Таким образом попадание одного и того же события в БД дважды исключено.

Блокирующий аудит

Сервис Аудита КриптоПро DSS обладает возможностью записи сообщений в режиме блокирующего аудита. Под термином «блокирующий аудит» понимается режим работы КриптоПро DSS, при котором невозможность з аписи сообщения аудита в БД по тем или иным причинам приводит к завершению выполняемой операции с ошибкой. Данный режим полезен для тех сценариев, в которых журналирование операций является критичным при их выполнении. Данный режим подразумевает, что в случае штатной работы всех компонентов информация о любой завершившейся успехом операции может быть найдена в БД Сервиса Аудита.

Режим блокирующего аудита может быть включен как при первоначальной конфигурации аудита на компоненте, так и при конфигурации уже существующих экземпляров. Для активации блокирующего аудита при первоначальной конфигурации необходимо выставить параметр `-UseBlockingAudit` командлета `New-DssXXXAudit` (XXX = `SignServer`, `STS` или `DocumentStore`) в значение `1`. Для модификации режима уже существующей конфигурации аудита необходимо использовать командлет `Set-DssXXXAudit` (XXX = `SignServer`, `STS` или `DocumentStore`) с параметром `–UseBlockingAudit`, выставленным в значение `1`. При передаче данного параметра Powershell считывает текущую конфигурацию аудита, осуществляет перерегистрацию типа модуля оповещения на запрошенную и задает ему параметры, полученные из зачитанной конфигурации.

Пример настройки блокирующего аудита:

```
New-DssSignServerAudit -AuditServiceAddress http://hostname/Analytics/AuditWriter.svc -Settings
@{"FolderName"="C:\tmp"} -UseBlockingAudit 1
```

Примечание

Включение блокирующего аудита создает новый словарь настроек модуля оповещения. После переключения службы в режим блокирующего аудита необходимо убедиться, что настройки были перенесены. Для вывода всех настроек, записанных в `-Settings` можно выполнить следующую команду:

```
(Get-Dss**Audit -DisplayName <name>).Settings | fl
```

Внимание!

Настройка `FolderPath` (т.е. резервирование записей аудита) при включенном блокирующем аудите игнорируется. Резервирование не будет производиться.

События аудита для Сервиса Подписи

Для всех событий Сервиса Подписи в аудит заносятся следующие сведения о пользователе:

ПАРАМЕТР	ОПИСАНИЕ
GlobalUid	Идентификатор пользователя
DelegatedGlobalUid	Идентификатор пользователя. Используется если операция выполнялась Оператором DSS
UserID	Идентификатор пользователя
DelegatedUserID	Идентификатор пользователя. Используется если операция выполнялась Оператором DSS
Login	Логин пользователя
DelegateUserLogin	Логин пользователя. Используется если операция выполнялась Оператором DSS.
DssRole	Роль пользователя
Realm	Домен пользователя
Phone	Номер телефона пользователя
Email	Адрес электронной почты
AccessTokenID	Идентификатор токена аутентификации

Для операций, выполняемых с подтверждением, в аудит заносятся следующие сведения:

ПАРАМЕТР	ОПИСАНИЕ
SsOperationID	Идентификатор операции
SsOperationNotAfter	Время истечения операции
SsOperationNotBefore	Время создания операции
SsOperationState	Состояние операции

События создания подтверждаемой операции на Сервисе Подписи через API V2 (Программный интерфейс DSS 2ой версии):

КОД СОБЫТИЯ	ИМЯ СОБЫТИЯ	ПАРАМЕТРЫ СОБЫТИЯ	ОПИСАНИЕ

КОД СОБЫТИЯ	ИМЯ СОБЫТИЯ	ПАРАМЕТРЫ СОБЫТИЯ	ОПИСАНИЕ
SignDocumentOperationCreated	248	`Сведения о пользователе` (см. выше) `Сведения об операции` (см. выше) `SignatureType` - Тип подписи `CertificateID` - ID сертификата `CertFriendlyName` - Отображаемое имя сертификата `Thumbprint` - Отпечаток сертификата `SsDocInfo` - Сведения о подписываемых документах	Запрос подписи документа (-ов) на сервисе подписи через V2
SignDocumentOperationCreateFailed	249	`Сведения о пользователе` (см. выше) `ErrorMsg` - Описание ошибки	
CertificateRequestOperationCreated	250	`Сведения о пользователе` (см. выше) `Сведения об операции` (см. выше) `RequestSubject` - Имя субъекта `CAName` - Отображаемое имя УЦ `CertTemplateName` - Отображаемое имя шаблона сертификата `CertTemplateOid` - Идентификатор шаблона сертификата `EkuString` - Использование ключа `CAId` - Идентификатор модуля УЦ `GroupId` - Идентификатор криптопровайдера	Запрос создания сертификата на сервисе подписи через V2
CertificateRequestOperationCreateFailed	251	`Сведения о пользователе` (см. выше) `ErrorMsg` - Описание ошибки	

КОД СОБЫТИЯ	ИМЯ СОБЫТИЯ	ПАРАМЕТРЫ СОБЫТИЯ	ОПИСАНИЕ
DecryptOperationCreated	252	`Сведения о пользователе` (см. выше) `Сведения об операции` (см. выше) `SignatureType` - Тип шифрования `CertificateID` - ID сертификата `CertFriendlyName` - Отображаемое имя сертификата `Thumbprint` - Отпечаток сертификата `SsDocInfo` - сведения о подписываемых документах	Запрос расшифрования док-та (-ов) на сервисе подписи через V2
DecryptOperationCreateFailed	253	`Сведения о пользователе` (см. выше) `ErrorMsg` - Описание ошибки	
ChangeCertificatePinOperationCreated	254	`Сведения о пользователе` (см. выше) `Сведения об операции` (см. выше) `CertificateID` - ID сертификата `CertFriendlyName` - Отображаемое имя сертификата `Thumbprint` - Отпечаток сертификата	Запрос смены ПИН-кода на 3К сертификата на сервисе подписи через V2
ChangeCertificatePinOperationCreateFailed	255	`Сведения о пользователе` (см. выше) `ErrorMsg` - Описание ошибки	

КОД СОБЫТИЯ	ИМЯ СОБЫТИЯ	ПАРАМЕТРЫ СОБЫТИЯ	ОПИСАНИЕ
ChangeCertificateStatusOperationCreated	256	`Сведения о пользователе` (см. выше) `Сведения об операции` (см. выше) `CertificateID` - ID сертификата `CertFriendlyName` - Отображаемое имя сертификата `Thumbprint` - Отпечаток сертификата `RevocationReason` - Причина отзыва `HoldTime` - Время приостановления действия `CAId` - Идентификатор модуля УЦ CAName - Отображаемое имя УЦ	Запрос смены свойств сертификата на сервисе подписи через V2: * отзыв/приостановление/восстановление Запрос смены ПИН-кода на ЗК сертификата на сервисе подписи через V2 * Дружественное имяЗапрос смены ПИН-кода на ЗК сертификата на сервисе подписи через V2 * Запрос смены ПИН-кода на ЗК сертификата на сервисе подписи через V2 * Сертификат по умолчанию
ChangeCertificateStatusOperationCreateFailed	257	`Сведения о пользователе` (см. выше) `ErrorMsg` - Описание ошибки	
PrivateKeyAccessOperationCreated	258	`Сведения о пользователе` (см. выше) `Сведения об операции` (см. выше) `CertificateID` - ID сертификата `CertFriendlyName` - Отображаемое имя сертификата `Thumbprint` - Отпечаток сертификата	Запрос доступа к ЗК сертификата (для Cloud CSP) на сервисе подписи через V2
PrivateKeyAccessOperationCreateFailed	259	`Сведения о пользователе` (см. выше) `ErrorMsg` - Описание ошибки	

События аудита для Центра Идентификации

Группы событий:

- Создание учетной записи пользователя
- Аутентификация пользователя пользователя
- События myDSS
- События myDSS Client

Аутентификация пользователя

КОД СОБЫТИЯ	ИМЯ СОБЫТИЯ	ПАРАМЕТРЫ СОБЫТИЯ	ОПИСАНИЕ
130	AuthenticationCompleted		Пользователь аутентифицирован
92	SecondaryAuthLogin		Запрошено подтверждение входа пользователя
129	OperationConfirmed		Операция подтверждена
131	OperationDeclined		Ошибка при подтверждении операции

Создание учетной записи пользователя

КОД СОБЫТИЯ	ИМЯ СОБЫТИЯ	ПАРАМЕТРЫ СОБЫТИЯ	ОПИСАНИЕ
2	UserCreatedByAdmin		Оператор создал учетную запись пользователю
223	AuthMethodAssigned		Пользователю назначены аутентификационные данные
84	AuthenticationSchemeChanged	AuthnMethodUri - метод аудтентификации IsAuthnMethodAssigned - метода аутентификации назначен/отключен	Метод аутентификации назначен
85	AuthenticationSchemeChangeFail		Ошибка назначения метода аутентификации

События myDSS

КОД СОБЫТИЯ	ИМЯ СОБЫТИЯ	ПАРАМЕТРЫ СОБЫТИЯ	ОПИСАНИЕ
294	MyDssKeyUpdates		Обновление ключа аутентификации myDSS 1.0

События myDSS Client

КОД СОБЫТИЯ	ИМЯ СОБЫТИЯ	ПАРАМЕТРЫ СОБЫТИЯ	ОПИСАНИЕ
227	AnonDeviceRegistered		Регистрация анонимного устройства myDSS
228	AnonDeviceRegisteredFailed		Ошибка регистрация анонимного устройства myDSS
229	KInitRequested		Запрос создания KInit для myDSS

КОД СОБЫТИЯ	ИМЯ СОБЫТИЯ	ПАРАМЕТРЫ СОБЫТИЯ	ОПИСАНИЕ
230	RegisterByKInit		Регистрация устройства myDSS по KInit
231	RegisterByKInitFailed		Ошибка регистрации устройства myDSS по KInit
232	DeviceConfirmed		Подтверждение устройства myDSS
233	DeviceConfirmedFailed		Ошибка подтверждение устройства myDSS
234	AssignMyDssSdkDevice		Назначение устройства myDSS пользователю
235	AssignMyDssSdkDeviceFailed		Ошибка назначения устройства myDSS пользователю
236	DeleteKInit		Удаления KInit для myDSS
237	DeleteKInitFailed		Ошибка при удалении KInit для myDSS
238	DeviceVerified		Подтверждение УЗ myDSS
239	DeviceVerifiedFailed		Ошибка Подтверждение УЗ myDSS
240	AddNewDeviceRequest		Запрос добавления нового устройства myDSS
241	AddNewDeviceRequestFailed		Ошибка добавления нового устройства myDSS
242	ApproveNewDeviceRequest		Запрос одобрения нового устройства myDSS
243	ApproveNewDeviceRequestFailed		Ошибка одобрения нового устройства myDSS
244	RejectNewDeviceRequest		Запрос отклонения нового устройства myDSS
245	RejectNewDeviceRequestFailed		Ошибка отклонения нового устройства myDSS
246	VerifyDeviceByCertificate		Подтверждение устройства myDSS по сертификату
247	VerifyDeviceByCertificateFailed		Ошибка подтверждение устройства myDSS по сертификату
295	MyDssSdkVerifyHmac		Проверка кода подтверждения myDSS Client
296	MyDssSdkVerifyHmacFailed		Ошибка проверка кода подтверждения myDSS Client"

События аудита для Центра Идентификации

Группы событий:

- События подписи покумента
- События myDSS Client
- События аутентификации

События подписи покумента

КОД СОБЫТИЯ	ИМЯ СОБЫТИЯ	ПАРАМЕТРЫ СОБЫТИЯ	ОПИСАНИЕ
130	AuthenticationCompleted		Аутентификация пользователя
297	DocumentUploaded		Документ загружен
248	SignDocumentOperationCreated		Создание операции подписи на Сервисе Подписи
93	SecondaryAuthSign		Запрошено подтверждение операции на мобильном устройстве
295	MyDssSdkVerifyHmac		Операция подтверждена через мобильное приложение
129	OperationConfirmed		Операция подтверждена
268	SignDocumentOperationExecuted		Документы подписаны

Если операция была отклонена пользователем, то событие 129 заменяется событием 131. Соответственно событие 268 не наступит.

КОД СОБЫТИЯ	ИМЯ СОБЫТИЯ	ПАРАМЕТРЫ СОБЫТИЯ	ОПИСАНИЕ
131	OperationDeclined		Операция отклонена

Аутентификация пользователя

КОД СОБЫТИЯ	ИМЯ СОБЫТИЯ	ПАРАМЕТРЫ СОБЫТИЯ	ОПИСАНИЕ
130	AuthenticationCompleted		Пользователь аутентифицирован
92	SecondaryAuthLogin		Запрошено подтверждение входа пользователя
129	OperationConfirmed		Операция подтверждена
131	OperationDeclined		Ошибка при подтверждении операции

События myDSS Client

КОД СОБЫТИЯ	ИМЯ СОБЫТИЯ	ПАРАМЕТРЫ СОБЫТИЯ	ОПИСАНИЕ
227	AnonDeviceRegistered		Регистрация анонимного устройства myDSS
228	AnonDeviceRegisteredFailed		Ошибка регистрация анонимного устройства myDSS

КОД СОБЫТИЯ	ИМЯ СОБЫТИЯ	ПАРАМЕТРЫ СОБЫТИЯ	ОПИСАНИЕ
229	KInitRequested		Запрос создания KInit для myDSS
230	RegisterByKInit		Регистрация устройства myDSS по KInit
231	RegisterByKInitFailed		Ошибка регистрации устройства myDSS по KInit
232	DeviceConfirmed		Подтверждение устройства myDSS
233	DeviceConfirmedFailed		Ошибка подтверждение устройства myDSS
234	AssignMyDssSdkDevice		Назначение устройства myDSS пользователю
235	AssignMyDssSdkDeviceFailed		Ошибка назначения устройства myDSS пользователю
236	DeleteKInit		Удаления KInit для myDSS
237	DeleteKInitFailed		Ошибка при удалении KInit для myDSS
238	DeviceVerified		Подтверждение УЗ myDSS
239	DeviceVerifiedFailed		Ошибка Подтверждение УЗ myDSS
240	AddNewDeviceRequest		Запрос добавления нового устройства myDSS
241	AddNewDeviceRequestFailed		Ошибка добавления нового устройства myDSS
242	ApproveNewDeviceRequest		Запрос одобрения нового устройства myDSS
243	ApproveNewDeviceRequestFailed		Ошибка одобрения нового устройства myDSS
244	RejectNewDeviceRequest		Запрос отклонения нового устройства myDSS
245	RejectNewDeviceRequestFailed		Ошибка отклонения нового устройства myDSS
246	VerifyDeviceByCertificate		Подтверждение устройства myDSS по сертификату
247	VerifyDeviceByCertificateFailed		Ошибка подтверждение устройства myDSS по сертификату
295	MyDssSdkVerifyHmac		Проверка кода подтверждения myDSS Client
296	MyDssSdkVerifyHmacFailed		Ошибка проверка кода подтверждения myDSS Client"

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.

В этом разделе:

Модуль аутентификации 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:

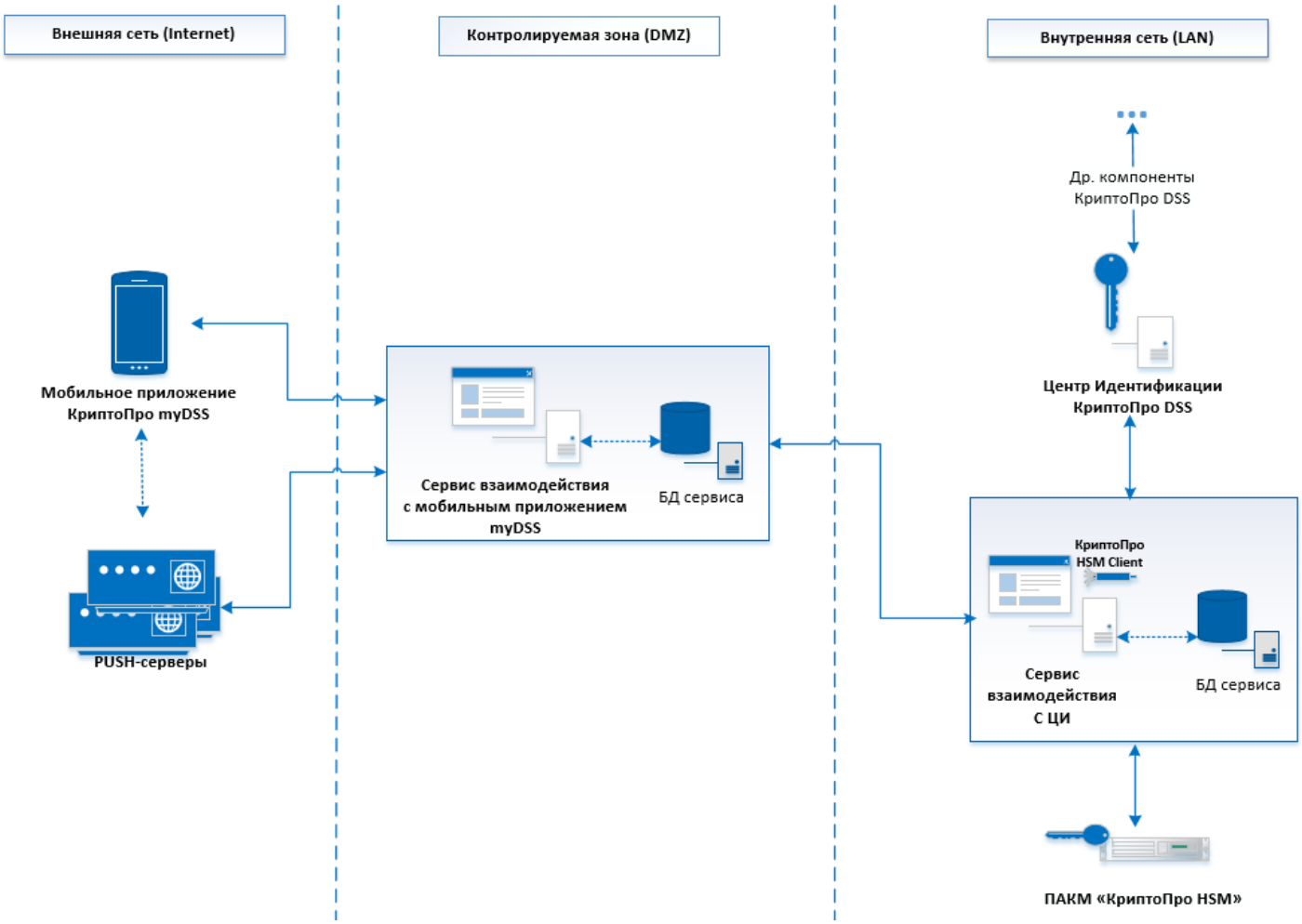
- регистрацию устройств пользователей для отправки PUSH-уведомлений;
- отправку PUSH-уведомлений;
- предоставление информации о операциях, необходимых для подтверждения пользователем;
- прием и проверку кодов подтверждения при помощи Сервиса взаимодействия с ЦИ.

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 КриптоПро, приведена на рисунке ниже.


Внешняя сеть (Internet)
Контролируемая зона (DMZ)
Внутренняя сеть (LAN)
Др. компоненты КриптоПро DSS
Мобильное приложение КриптоПро myDSS
Центр Идентификации КриптоПро DSS
Сервис взаимодействия с мобильным приложением myDSS
БД сервиса
КриптоПро HSM Client
Сервис взаимодействия С ЦИ
БД сервиса
PUSH-серверы
ПАКМ «КриптоПро HSM»

Создание и настройка экземпляров myDSS

Данный раздел определяет последовательность действий при разворачивании и настройке экземпляров модуля аутентификации myDSS.

- **Пример разворачивания**
- **Ввод лицензии**

Предварительные условия:

- Установленный SQL-Server;
- Установленная роль Сервер приложений (IIS);
- Настроенная привязка https на Сервере приложений (IIS);
- Доступность адресов PUSH-серверов с сервера, где будет разворачиваться экземпляр Сервиса взаимодействия с мобильным приложением myDSS.
- Наличие ключей доступа к PUSH-серверам (если необходимо).
- Установленный и настроенный экземпляр Центра Идентификации.

> Примечание
>
> **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`.

> Примечание
>
> Для отправки PUSH-уведомлений на устройства Apple требуется **сертификат с клиентской аутентификацией** на Apple Push Notification Service. Получить данный сертификат можно по запросу на `dsssupport@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 `dsssupport@cryptopro.ru`.

Базовая последовательность шагов по настройке (обязательные):

1. Создание экземпляра Сервиса взаимодействия с ЦИ (командлет New-MyDssServerInternalInstance).

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 (командлет New-MyDssServerExternalInstance).

На данном шаге экземпляру Сервиса взаимодействия с мобильным приложением myDSS назначается сервисный сертификат, который используется для аутентификации при межсервисном взаимодействии.

> Примечание
>
> Необходимо переключить в режим автоматического запуска службу **КриптоПро myDSS (External Service)**.

3. Регистрация криптопровайдеров.

На данном шаге в экземпляре Сервиса взаимодействия с ЦИ регистрируется криптопровайдер, который используется для выработки векторов аутентификации Пользователей.

> Примечание
>
> Зарегистрированное имя криптопровайдера 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`

4. Настройка Сервиса взаимодействия с ЦИ.

На данном шаге выполняется настройка экземпляра Сервиса взаимодействия с ЦИ. Настройка осуществляется при помощи командлета Set-MyDssServerInternalProperties. Необходимо выполнить следующие действия:

- Задание адреса сервиса рассылки PUSH-уведомлений - при помощи параметра `InteractionPushServiceAddress`.
- Задание адреса сервиса, с которым связывается мобильное приложение - при помощи параметра `InteractionServiceAddress`.

Примечание

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.

5a. Задание на ЦИ КриптоПро DSS адреса Сервиса взаимодействия с ЦИ - при помощи командлета Set-DssMobileAuthProperties.

Пример минимально необходимой настройки данного адреса:

```
Set-DssMobileAuthProperties -DisplayName <Имя экземпляра ЦИ> -ServiceAddress
"http://localhost/MyDssServerInternal/service.svc"
```

4b. Задание на ЦИ КриптоПро DSSадреса ЦИ, куда возвращается результат подтверждения операций из мобильного приложения.

```
Set-DssMobileAuthProperties -DisplayName <Имя экземпляра ЦИ> -CallbackUriPrefix
"https://<hostname>/<STSappname>"
```

5. Настройка Сервиса взаимодействия с мобильным приложением myDSS.

На данном шаге выполняется настройка экземпляра Сервиса взаимодействия с мобильным приложением myDSS. Необходимо выполнить следующие действия:

- Задание адреса Сервиса взаимодействия с ЦИ.

Настройка осуществляется при помощи параметра `-ServiceAddress` командлета Set-MyDssInteractionServiceProperties.

- Настройка взаимодействия с серверами рассылки PUSH-уведомлений (Apple Push Notification Service и Firebase Cloud Messaging Server).

Настройка осуществляется при помощи указания всех необходимых параметров командлета Set-MyDssPushServiceProperties.

Примечание

После внесения изменений в конфигурацию экземпляра необходимо перезапустить пул веб-приложения при помощи соответствующей команды. Также может потребоваться ручной перезапуск службы `КриптоПро myDSS (External Service)`.

6. Настройка плагина для отправки оповещений

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 плагин и модуль оповещения.

Пример PowerShell-сценария для настройки компонента myDSS

Данный сценарий выполняет минимально необходимую настройку экземпляра компонента myDSS.

```
# Создание экземпляра Сервиса взаимодействия с ЦИ
New-MyDssServerInternalInstance -SiteName "Default Web Site" -SQLServerName "<sqlservername>" -DisplayName
MyDssServerInternal

# Создание экземпляра Сервиса взаимодействия с мобильным приложением myDSS
New-MyDssServerExternalInstance -SiteName "Default Web Site" -SQLServerName "<sqlservername>" -DisplayName
MyDssServerExternal


#Настройка экземпляра Сервиса взаимодействия с ЦИ

# Добавление криптопровайдера
Add-MyDssServerInternalCryptoProviders -DisplayName MyDssServerInternal -TypeId GostWithMasterKey -
ProviderType 80 -ProviderName "Crypto-Pro GOST R 34.10-2012 HSM Svc CSP"

#Задание адреса сервиса рассылки PUSH-уведомлений
Set-MyDssServerInternalProperties -DisplayName MyDssServerInternal -InteractionPushServiceAddress
"http://<hostname>/MyDssServerExternal/InteractionPushService.svc"

#Задание адреса Сервиса взаимодействия с мобильным приложением myDSS
Set-MyDssServerInternalProperties -DisplayName MyDssServerInternal -InteractionServiceAddress
"http://<hostname>/MyDssServerExternal/InteractionService.svc"

#Задание на ЦИ КриптоПро DSS адреса Сервиса взаимодействия с ЦИ и адреса ЦИ, куда возвращается результат
подтверждения операций из мобильного приложения
Set-DssMobileAuthProperties -DisplayName <Имя экземпляра ЦИ> -ServiceAddress
"http://<hostname>/MyDssServerInternal/service.svc" -CallbackUriPrefix "https://<hostname>/<STSappname>"



# Настройка Сервиса взаимодействия с мобильным приложением myDSS
Set-MyDssInteractionServiceProperties -DisplayName MyDssServerExternal -ServiceAddress
"http://<hostname>/MyDssServerInternal/Service.svc"

# Настройка взаимодействия с серверами рассылки PUSH-уведомлений (Apple Push Notification Service и Firebase
Cloud Messaging Server).
Set-MyDssPushServiceProperties -DisplayName MyDssServerExternal -ApnClientCertPassword P@SSW0RD -
ApnClientCertPath C:\apn2019.pfx -GoogleServerKey "eyJ0eXAiOiJKV...5Wti-H8CeXycwB6A"
```

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 плагин и модуль оповещения.

```
#Настройка транспортного плагина
$plugin = Add-DssStsPlugin -PluginTypeName
"CryptoPro.DSS.Identity.Authentication.Notification.HttpTransportPlugin,CryptoPro.DSS.Identity.Authentication
.Notification" -PluginType AuthenticationResult -Settings @{}

#Добавление модуля оповещения
Add-DssStsNotifier -TransportPluginID $plugin.ID -NotifierType AuthenticationResultCallback -Settings @{}
```

ID плагинов присваиваются автоматически после их добавления.

Сервис Обработки Документов

Сервис Обработки Документов (СОД) предоставляет возможность работы с документами, отправленными на подпись или шифрование/расшифрование в КриптоПро DSS. Сервис Обработки Документов выполняет следующие задачи:

- конвертация документов в различные форматы для отображения в мобильном приложении myDSS;
    - конвертация документов для отображения полного текста документа;
    - преобразование документов для отображения краткой информации о документе или его печатной формы.

Внимание!

Пользователь всегда может просмотреть полный текст документа, если краткой информации недостаточно.

- загрузка и хранение документов в БД Сервиса Обработки Документов;
- выгрузка подписанных (зашифрованных, расшифрованных) документов из БД Сервиса Обработки Документов.

В этом разделе:

Принцип работы Сервиса Обработки Документов

Взаимодействие с Сервисом Обработки Документов возможно при помощи его программного интерфейса. В общем виде схемы взаимодействия выглядят следующим образом:

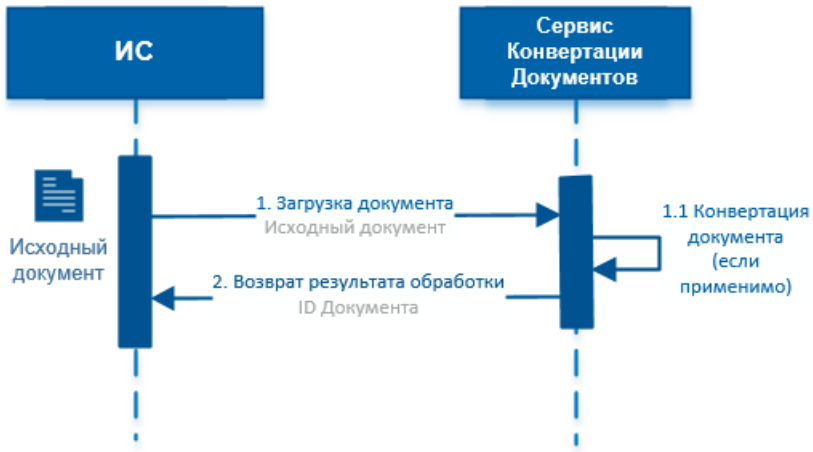
Загрузка документа

Вызывающая система отправляет в Сервис Обработки Документов некоторый документ, подлежащий подписи и/или шифрованию/расшифрованию. СОД выполняет конвертацию данного документа (если настроено). После этого производится запись документа в БД СОД и идентификатор документа возвращается вызывающей системе.

Примечание

Исходный документ, конвертированные и/или подписанные версии одного и того же документа с точки зрения СОД являются различными документами. Однако идентификатор в БД СОД присваивается только исходному документу, а его конвертированные и/или подписанные версии связываются с ним и доступны по запросу вызывающей системы.

Срок хранения документа в БД СОД может быть настроен отдельно (см. дополнительные шаги настройки в сценарии настройки экземпляра СОД).



Подпись документа с подтверждением операции в мобильном приложении myDSS

1. Вызывающая система отправляет в DSS запрос на подпись некоторого документа. Запрос содержит идентификатор документа, подлежащего подписи.

   1.1. DSS создает транзакцию подписи и выполняет другие необходимые действия в системе.

   1.2. В мобильное приложение myDSS отправляется PUSH-уведомление с требованием подтверждения операции.

   1.3. Пользователь при помощи мобильного приложения myDSS запрашивает список операций, требующих подтверждения.

   1.4. DSS направляет к СОД запрос, содержащий идентификатор подписываемого документа.

   1.4.1. СОД формирует краткую информацию о документе (snippet).

   1.5. СОД отправляет snippet в DSS.

> **Примечание**
>
> Пользователь может запросить также полный текст документа. Механизм получения данного документа аналогичен получению краткой информации о документе, но без генерации snippet.

1.6. DSS возвращает мобильному приложению myDSS список операций, требующих подтверждения, и краткую информацию о документе.

1.6.1. Пользователь просматривает краткую информацию о документе (и полный текст документа), подтверждает операцию.

1.7. Мобильное приложение отправляет сведения для подтверждения операции в DSS.

1.8. DSS запрашивает в СОД исходный документ для подписи по его идентификатору.

1.9. СОД отправляет исходный документ в DSS.

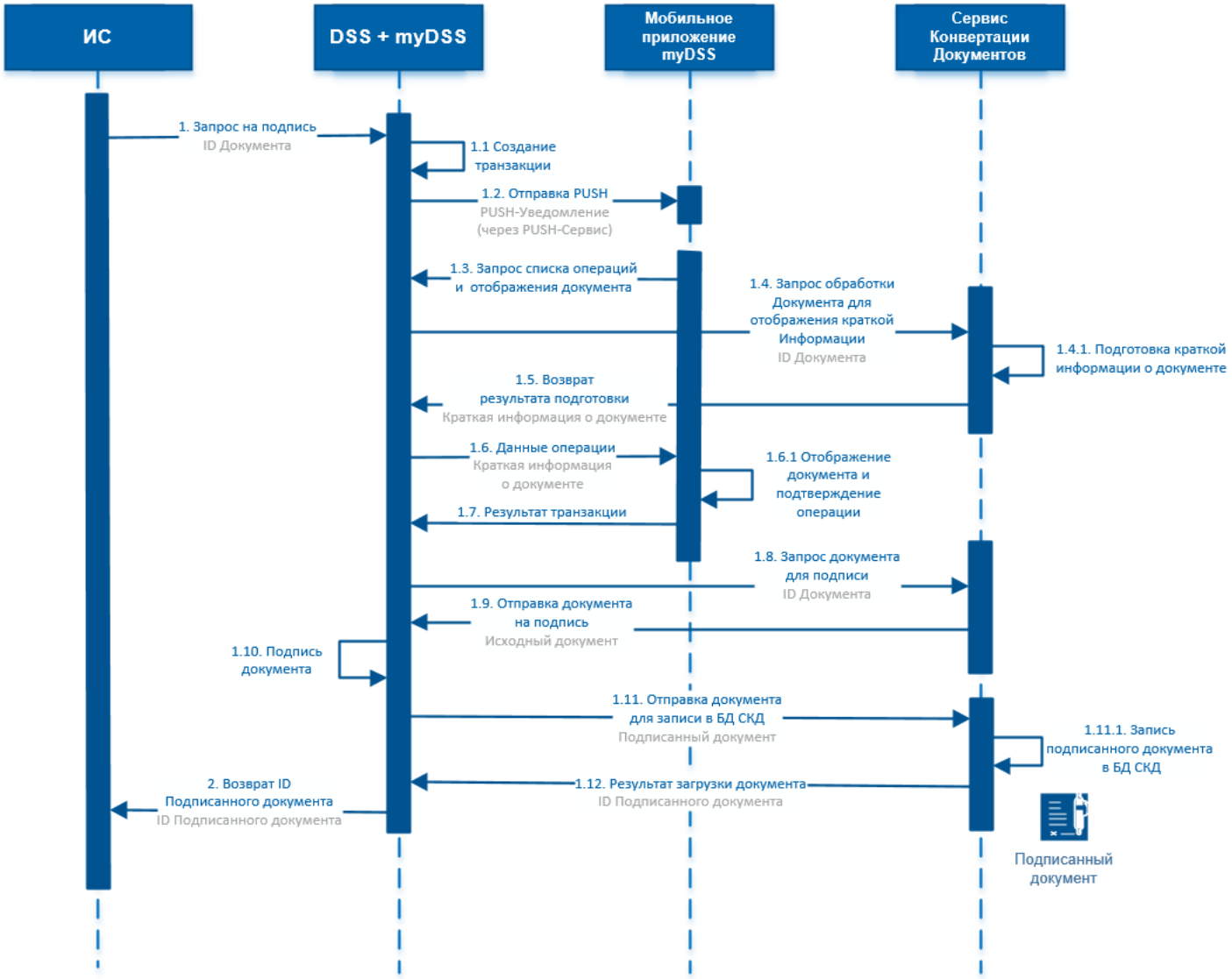
1.10. DSS подписывает исходный документ.

1.11. DSS загружает подписанный документ в СОД.

1.11.1. СОД помещает подписанный документ в БД.

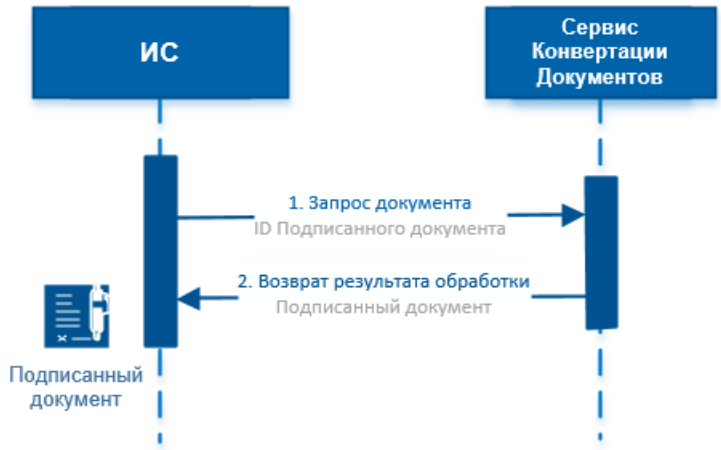
1.12. СОД возвращает идентификатор подписанного документа в DSS.

1. DSS возвращает идентификатор подписанного документа в вызывающую систему.



Выгрузка документа

Вызывающая система отправляет в СОД запрос на получение документа, содержащий идентификатор необходимого документа, полученного ранее. СОД возвращает указанный документ.



Создание и настройка экземпляра Сервиса Обработки Документов

Данный раздел определяет последовательность действий при разворачивании и настройке экземпляра Сервиса Обработки Документов КриптоПро DSS.

- **Пример разворачивания**

Предварительные условия:

- Установленный SQL-Server;
- Установленная роль Сервер приложений (IIS);
- Настроенная привязка https на Сервере приложений (IIS);
- Выпущенный и установленный сервисный сертификат Сервиса Обработки Документов.
- Установленный КриптоПро CSP (входит в комплект поставки).

Базовая последовательность шагов по настройке (обязательные):

0. Настройка потокового доступа к документам (FILESTREAM).

Для ускорения обработки документов на сервере, где разворачивается БД СОД, может быть настроен потоковый доступ к документам (FILESTREAM).

> **Примечание**
>
> По умолчанию FILESTREAM не используется. Все обрабатываемые документы записываются непосредственно в БД СОД, где и происходит их обработка.

Инструкция по настройке FILESTREAM приведена в соответствующем разделе.

1. Создание экземпляра Сервиса Обработки Документов (командлет New-DssDocumentStoreInstance). На данном шаге будет создано веб-приложение на Сервере приложений IIS, развёрнуты базы данных, зарегистрированы журналы Windows.

> **Внимание!**
>
> Одновременно с созданием экземпляра СОД *по умолчанию* будут зарегистрированы следующие плагины преобразования документов для отображения в мобильном приложении myDSS:
>
> - для отображения полного текста **PDF-документа** - `DSS.DocumentConverter.PdfStub.dll`. Для изменения параметров данного плагина, либо добавления плагинов для преобразования документов других форматов см. соответствующий раздел.
> - для отображения краткой информации о документе **любого формата** - шаблон, позволяющий отобразить имя подписываемого документа `DSS.DocumentConverter.Preview.dll`. Для изменения параметров шаблона см. соответствующий раздел.

2. Настройка сервисного сертификата Сервиса Обработки Документов.

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

```
Set-DSSDocumentStoreProperties -ServiceCertificate <thumbprint>
```

> **Примечание**
>
> Учетной записи, под которой работает пул приложения Сервиса Обработки Документов, необходимо выдать права на доступ к закрытому ключу сервисного сертификата.

3. Настройка отношений доверия с Центром Идентификации. На данном шаге устанавливается отношение доверия между

Центром Идентификации и Сервисом Обработки Документов.

Настройка выполняется в два шага:

- Регистрация Центра Идентификации в качестве доверенного издателя маркеров безопасности на Сервисе Обработки Документов.

Данное действие выполняется при помощи командлета Add-DssDocumentStoreClaimsProviderTrust.

- Регистрация Сервиса Обработки Документов в качестве доверенной стороны на Центре Идентификации.

Данное действие выполняется при помощи командлета Add-DssRelyingPartyTrust.

> **Примечание**
>
> К моменту выполнения шага 2 должен быть развёрнут экземпляр Центра Идентификации.

> **Примечание**
>
> Если Сервис Обработки Документов разворачивается на отдельной машине, необходимо добавить на ней сервисный сертификат Центра Идентификации в хранилище `Trusted People`.

4. Настройка адреса Сервиса Обработки Документов на Сервисе Подписи.

Данная настройка необходима для взаимодействия СОД и Сервиса Подписи в процессе подписи, шифрования и расшифрования документов, хранящихся в СОД. Для регистрации СОД на Сервисе Подписи необходимо выполнить следующую команду:

```
Set-DssProperties -DocumentStoreAddress http://<hostname>/documentstore
```

> **Примечание**
>
> После внесения изменений в конфигурацию экземпляра необходимо перезапустить пул веб-приложения при помощи соответствующей команды.

Дополнительные действия по настройке (опциональные):

1. Настройка конвертации документов.

- конвертация документов для отображения полного текста документа.

Администратор может настроить отображение *полного текста документа* при подтверждении операций в мобильном приложении myDSS при помощи специальных плагинов.

Пример регистрации плагина конвертации документов MS Office Word в PDF:

```
Add-DssDocumentStoreConverterPlugin -FileExtension pdf -Assembly "C:\Program Files\Crypto
Pro\DSS\Plugins\Converters\DSS.DocumentConverter.Word.dll"
```

- преобразование документов для отображения краткой информации о документе.

Администратор может дополнительно настроить формат отображения *краткой информации о документе* и (при необходимости) печатной формы документа в мобильном приложении myDSS.

2. Настройка запрета передачи внешних шаблонов документов.

При загрузке документа в СОД, вместе с ним может быть передан шаблон конвертации для отображения краткой информации о документе. Если передача внешних шаблонов включена и шаблон был передан при загрузке документа - конвертация будет происходить по этому шаблону. Передача шаблона с документом приведет к ошибке загрузки всего документа, если данная настройка выключена.

Для запрета внешних шаблонов необходимо выполнить следующую команду:

```
Set-DssDocumentStoreProperties -AllowExternalTemplates 0
```

По умолчанию передача внешних шаблонов разрешена.

3. Настройка срока хранения документов.

Документы, отправляемые в СОД при помощи программного интерфейса, могут иметь различные сроки хранения:

- *Временные* (временного хранения) - загружены с флагом `IsTemporary`, показывающим, что данный документ загружен только на короткое время (например, для подписи) и далее будет удален. Администратор может настроить срок хранения временных документов *в минутах* при помощи параметра `-TempDocumentStorageTime` командлета Set-DssDocumentStoreProperties. По умолчанию срок хранения временных документов равен 1 суткам (1440 минут).
- *Долговременные* (долговременного хранения) - хранятся в пределах срока (*в днях*), установленного Администратором при помощи параметра `-DocumentStorageTime` командлета Set-DssDocumentStoreProperties. По умолчанию срок равен 30 дням.

Удаление документов производится при помощи мониторинга с заданным интервалом. Если на момент осуществления мониторинга в БД СОД присутствуют документы с истекшим сроком хранения, они будут удалены. Администратор может настроить период мониторинга в *минутах* при помощи параметра `-DefaultMonitoringPeriod` командлета Set-DssDocumentStoreProperties. По умолчанию период мониторинга равен 5 минутам.

4. Настройка размера загружаемых документов.

Администратор может настроить максимальный размер документов, загружаемых на СОД, при помощи параметра `-MaxMessageSize` командлета Set-DssDocumentStoreProperties. По умолчанию максимальный размер загружаемого файла составляет около 2 ГБ.

5. Ограничение размера хранилища для Пользователя.

Администратор может ввести ограничение на общий объем документов, загруженных Пользователем, параметра `-DefaultMemoryLimitPerUser` командлета Set-DssDocumentStoreProperties. По умолчанию максимальный объем документов, загружаемых одним Пользователем, составляет около 4 ГБ.

6. Настройка аудита. Администратор DSS может настроить сбор событий с Сервиса Обработки Документов и их отправку на Сервис Аудита для ведения журнала событий.

7. Настройка автоопределения формата документа.

Настройка потокового доступа к документам (FILESTREAM)

Для настройки потокового доступа СОД к документам (FILESTREAM) необходимо выполнить следующую последовательность действий, описанных в данном разделе:

1. Включить поддержку FILESTREAM в диспетчере конфигурации MS SQL Server.

2. Переключить имеющийся экземпляр СОД в режим работы с FILESTREAM, либо создать новый экземпляр с соответствующим флагом.

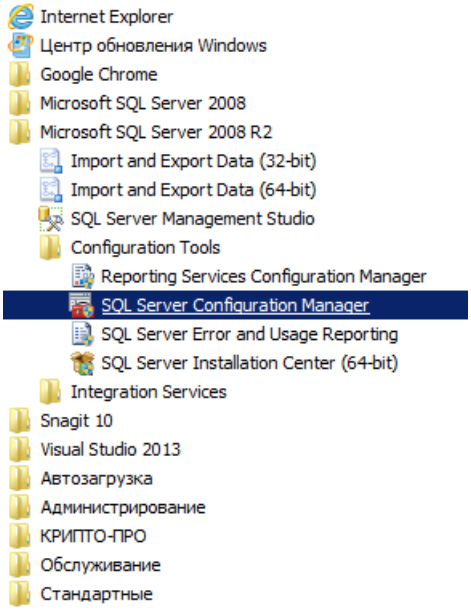
Включение FILESTREAM (БД расположена на одном сервере с экземпляром СОД)

FILESTREAM не включается автоматически при установке или обновлении SQL Server. FILESTREAM необходимо включить с помощью Диспетчера конфигурации SQL Server и среды SQL Server Management Studio.

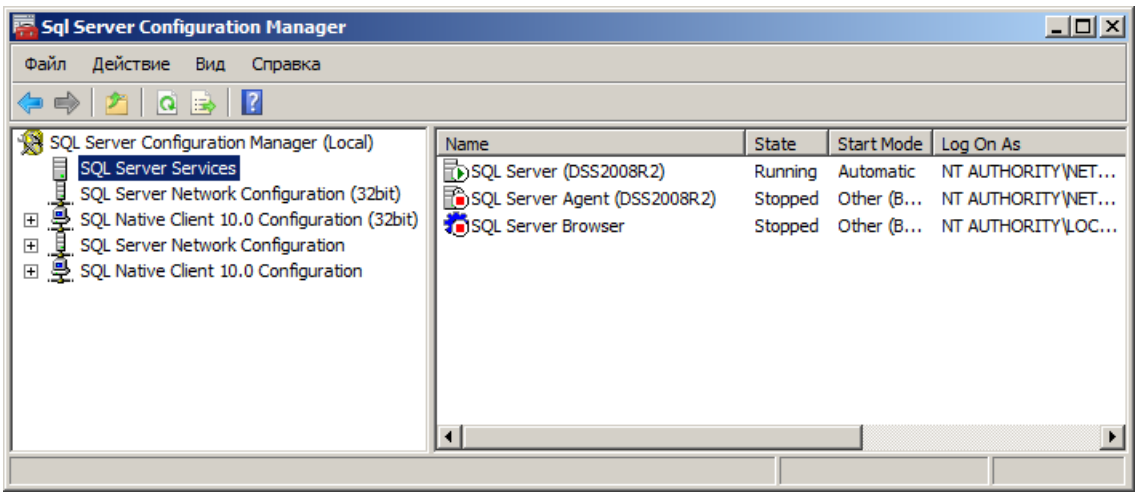
В данном разделе приведена последовательность действий по включению FILESTREAM в соответствии с **Инструкцией по включению FILESTREAM на официальном сайте Microsoft**.

Действия в Диспетчере конфигурации SQL Server

В меню Пуск выберите пункт `Все программы -> Microsoft SQL Server \<version> -> Средства настройки` и выберите пункт Диспетчер конфигурации SQL Server.



В списке служб щелкните правой кнопкой мыши "Службы SQL Server" и выберите "Открыть".



В открывшейся оснастке Диспетчера конфигурации SQL Server найдите экземпляр SQL Server, в котором нужно включить FILESTREAM.

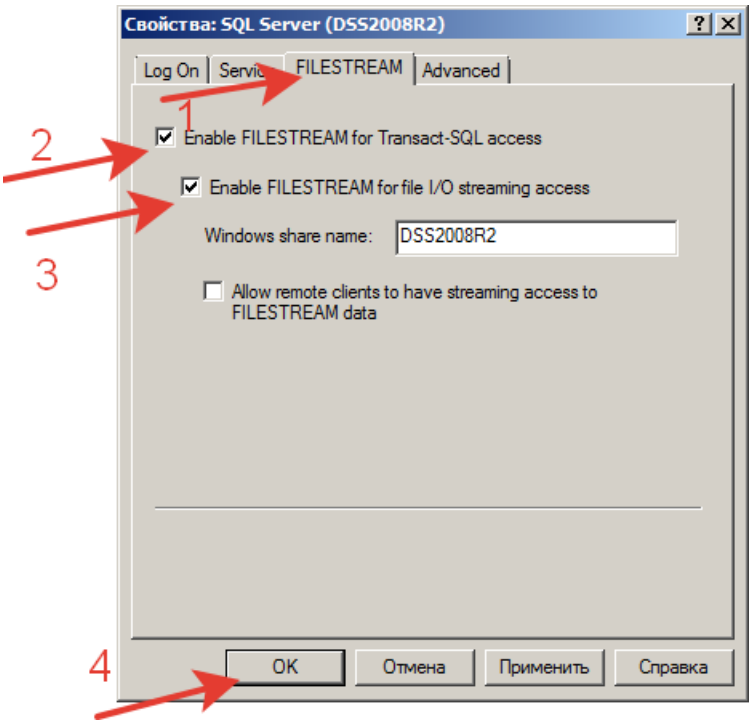
Щелкните правой кнопкой мыши экземпляр и выберите пункт "Свойства".

В диалоговом окне "Свойства: SQL Server" перейдите на вкладку `FILESTREAM` (1).

Установите флажок `Enable FILESTREAM for Transact-SQL access` (Разрешить FILESTREAM при доступе через Transact-SQL) (2).

Установите флажок `Enable FILESTREAM for file I/O streaming access` (Разрешить FILESTREAM при потоковом доступе ввода-вывода) Введите имя общего ресурса Windows в поле `Windows share name`. (3).

Нажмите кнопку OK (4) для сохранения настроек и окончания редактирования свойств FILESTREAM.



Примечание

Отмечать флажок "Allow remote clients to have streaming access to FILESTREAM data" (Разрешить удаленным клиентам потоковый доступ к данным FILESTREAM) необходимо только в том случае, если SQL Server развёрнут на отдельном сервере (см. Включение FILESTREAM при использовании БД на удаленном сервере).

Действия в SQL Server Management Studio

В среде SQL Server Management Studio нажмите кнопку **Создать запрос**, чтобы открыть редактор запросов. В редакторе запросов введите следующий код Transact-SQL:

```
EXEC sp_configure filestream_access_level, 2
RECONFIGURE
```

Нажмите кнопку **Выполнить**.

Перезапустите службу `SQL Server`.

Включение FILESTREAM (БД расположена на удаленном сервере)

Выполните все действия, описанные в предыдущем пункте. Помимо этого, выполните следующее:

1. Установите флажок "Allow remote clients to have streaming access to FILESTREAM data (Разрешить удаленным клиентам потоковый доступ к данным FILESTREAM) в меню свойств SQL Server на вкладке FILESTREAM.

Настройка экземпляра СОД для работы с FILESTREAM

Примечание

Действия, описанные в данном разделе, должны выполняться **ПОСЛЕ** настройки FILESTREAM.

Настройка поддержки Сервисом Обработки Документов включенного ранее FILESTREAM состоит из следующих этапов:

1. Включение FILESTREAM на экземпляре СОД.

Даже если FILESTREAM уже настроен, необходимо настроить экземпляр СОД для работы с ним. Существует две ситуации:

- **Создается новый экземпляр СОД.**

В данном случае при создании экземпляра СОД в командлете New-DssDocumentStoreInstance необходимо установить флаг `-CreateFileStreamDb` в положение `1`. По умолчанию данный флаг не будет взведен, и FILESTREAM не будет использоваться, даже если он был включен ранее.

- **Экземпляр СОД уже создан (и используется).**

В данном случае необходимо переключить экземпляр в режим работы с FILESTREAM при помощи командлета SwitchDssDocumentStoreInstance.

Пример:

```
Switch-DssDocumentStoreInstance -SQLServerName win-srv -ApplicationName DocumentStore -DisplayName
DocumentStore -UseFileStream 1 -DBName DocumentStoreFs
```

Внимание!

Данное действие создает **новый экземпляр** БД СОД, предназначенный для работы с FILESTREAM. При этом:

- Старый экземпляр БД сохраняется вместе со всем содержимым.
- Все настройки старого экземпляра БД будут перенесены на новый.
- Файлы из БД старого экземпляра **НЕ переносятся**.
- С момента взведения флага СОД продолжает работу **ТОЛЬКО** с новым экземпляром БД.

2. Установка флага `SmallFile` в поле `AdditionalDocumentInfo` структуры `PostDocumentInput` при выполнении REST-запроса на загрузку документа в СОД.

Если выполнены все предыдущие пункты данного раздела, запись документов все еще производится полностью в БД, т.к. флаг `SmallFile` в поле `AdditionalDocumentInfo` структуры `PostDocumentInput` по умолчанию не установлен или установлен в значение `true`, а значит все загружаемые в СОД документы считаются "маленькими".

Для начала записи с использованием FILESTREAM установите для загружаемых в СОД документов, считаемых "большими", флаг `SmallFile` в значение `false`.

Примечание

Критерии установки флага `SmallFile` в значение `true` или `false` могут быть различными. Рекомендуется считать "маленькими" (`SmallFile` = `true`) документы размером до 10 Мбайт.

Внимание!

Если FILESTREAM не настроен или настроен некорректно, флаг `SmallFile` = `false` будет записан в состояние `true`, а загружаемый документ будет записан в БД без использования FILESTREAM.

Конвертация документов в различные форматы для отображения в мобильном приложении myDSS

Сервис Обработки Документов предоставляет возможность преобразования (в т.ч. конвертации) документов в различные форматы для отображения в мобильном приложении myDSS. Преобразование документов производится для выполнения следующих задач:

- конвертация документов для отображения полного текста документа;
- преобразование документов для отображения краткой информации о документе или его печатной формы.

При этом принцип работы при преобразовании документов следующий.

1. При возникновении необходимости преобразования (в т.ч. конвертации) документа на основе его формата (например, `docx`) будет выбран соответствующий конвертер (плагин для визуализации документа заданного формата). По умолчанию в КриптоПро DSS НЕ зарегистрированы плагины такого типа. Их необходимо зарегистрировать согласно инструкции в соответствующем разделе.

2. Отображение краткой формы документа в мобильном приложении myDSS позволяет сформировать удобную для просмотра и подтверждения операций версию подписываемого документа. При этом в КриптоПро DSS используется соответствующий формату документа плагин. Если плагин не зарегистрирован, будет использован плагин по умолчанию, отображающий только имя подписываемого документа.

3. Для генерации краткой информации о документе используется шаблон. При этом шаблон может быть задан как в настройках плагина (по умолчанию или уже настроен), так и передан при загрузке документа в полях структуры `AdditionalDocumentInfo` (см. раздел Отображение краткой информации о документе). При этом приоритет имеет внешний шаблон.

Внимание!

По умолчанию передача внешних шаблонов разрешена. Для запрета внешних шаблонов необходимо выполнить следующую команду:

```
Set-DssDocumentStoreProperties -AllowExternalTemplates 0
```

Логика действий при этом следующая:

- Если плагин под формат **найден**:
  - Если внешний шаблон **передан**:
    - Если **разрешено** использование внешних шаблонов, краткая информация о документе будет сгенерирована и отображена в мобильном приложении по переданному внешнему шаблону.
    - Если **запрещено** использование внешних шаблонов - система выдаст ошибку.
  - Если внешний шаблон **НЕ передан**, выполняется поиск шаблона в выбранном плагине:
    - Если шаблон **найден**, краткая информация о документе будет сгенерирована и отображена в мобильном приложении по этому шаблону.
    - Если шаблон **НЕ найден** - система выдаст ошибку.
- Если плагин под формат **НЕ найден**, используется плагин по умолчанию:
  - Если внешний шаблон **передан**:
    - Если **разрешено** использование внешних шаблонов, краткая информация о документе будет сгенерирована и отображена в мобильном приложении по переданному внешнему шаблону.
    - Если **запрещено** использование внешних шаблонов - система выдаст ошибку.
  - Если внешний шаблон **НЕ передан**, выполняется поиск шаблона в плагине по умолчанию:

- Если шаблон **найден**, краткая информация о документе будет сгенерирована и отображена в мобильном приложении по этому шаблону.
- Если шаблон **НЕ найден** - система выдаст ошибку.

4. Отображение печатной формы документа также требует настроенного плагина и шаблона. Если таковых настроек не производилось, будут использованы плагин (и шаблон) по умолчанию. Логика выбора плагина и шаблона аналогична п. 3.

Отображение полного текста документа из Сервиса Обработки Документов в мобильном приложении myDSS

Мобильное приложение myDSS имеет возможность отображать документ при подтверждении операции с этим документом. Настройка соответствующих плагинов преобразования документов осуществляется при помощи специализированного набора командлетов.

Сервис Обработки Документов предоставляет Пользователям возможность визуализации документов в мобильном предложении myDSS перед созданием подписи. Поддерживается просмотр документов следующих форматов: `PDF`, `XML`, `ODT`.

Также могут быть обработаны документы 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>\DocumentStore` 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.


MTS RUS
18:46
88 %
ОПЕРАЦИЯ 1 из 1
Данные операции
КРИПТОПРО
ПОДТВЕРДИТЬ
ОТКАЗАТЬСЯ

Пример:

```
Add-DssDocumentStoreConverterPlugin -FileExtension pdf -Assembly DSS.DocumentConverter.PdfStub.dll

Add-DssDocumentStoreConverterPlugin -FileExtension doc -Assembly DSS.DocumentConverter.Word.dll

Add-DssDocumentStoreConverterPlugin -FileExtension dot -Assembly DSS.DocumentConverter.Word.dll

Add-DssDocumentStoreConverterPlugin -FileExtension docm -Assembly DSS.DocumentConverter.Word.dll

Add-DssDocumentStoreConverterPlugin -FileExtension dotm -Assembly DSS.DocumentConverter.Word.dll

Add-DssDocumentStoreConverterPlugin -FileExtension docx -Assembly DSS.DocumentConverter.Word.dll

Add-DssDocumentStoreConverterPlugin -FileExtension dotx -Assembly DSS.DocumentConverter.Word.dll

Add-DssDocumentStoreConverterPlugin -FileExtension FlatOpc -Assembly DSS.DocumentConverter.Word.dll

Add-DssDocumentStoreConverterPlugin -FileExtension FlatOpcMacroEnabled -Assembly
DSS.DocumentConverter.Word.dll

Add-DssDocumentStoreConverterPlugin -FileExtension FlatOpcTemplate -Assembly DSS.DocumentConverter.Word.dll

Add-DssDocumentStoreConverterPlugin –FileExtension FlatOpcTemplateMacroEnabled -Assembly
DSS.DocumentConverter.Word.dll

Add-DssDocumentStoreConverterPlugin -FileExtension xml -Assembly DSS.DocumentConverter.Word.dll

Add-DssDocumentStoreConverterPlugin -FileExtension odt -Assembly DSS.DocumentConverter.Word.dll

Add-DssDocumentStoreConverterPlugin -FileExtension ott -Assembly DSS.DocumentConverter.Word.dll

Add-DssDocumentStoreConverterPlugin -FileExtension ooxml -Assembly DSS.DocumentConverter.Word.dll

Add-DssDocumentStoreConverterPlugin -FileExtension WordML -Assembly DSS.DocumentConverter.Word.dll

Add-DssDocumentStoreConverterPlugin -FileExtension rtf -Assembly DSS.DocumentConverter.Word.dll

Add-DssDocumentStoreConverterPlugin -FileExtension html -Assembly DSS.DocumentConverter.Word.dll

Add-DssDocumentStoreConverterPlugin -FileExtension xhtml -Assembly DSS.DocumentConverter.Word.dll

Add-DssDocumentStoreConverterPlugin -FileExtension mhtml -Assembly DSS.DocumentConverter.Word.dll

Add-DssDocumentStoreConverterPlugin -FileExtension txt -Assembly DSS.DocumentConverter.Word.dll

Add-DssDocumentStoreConverterPlugin -FileExtension png -Assembly DSS.DocumentConverter.Image.dll

Add-DssDocumentStoreConverterPlugin -FileExtension jpg -Assembly DSS.DocumentConverter.Image.dll

Add-DssDocumentStoreConverterPlugin -FileExtension bmp -Assembly DSS.DocumentConverter.Image.dll

Add-DssDocumentStoreConverterPlugin -FileExtension jpeg -Assembly DSS.DocumentConverter.Image.dll

Add-DssDocumentStoreConverterPlugin -FileExtension tiff -Assembly DSS.DocumentConverter.Image.dll
```

Просмотр настроек плагина:

```
Get-DssDocumentStoreConverterPlugin | where { $_.Extension -eq "xml" }  | select -ExpandProperty Converters |
Format-List
```

Изменение настроек плагина:

```
Set-DssDocumentStoreConverterPlugin -FileExtension xml -Assembly DSS.DocumentConverter.Word.dll -ClassName
CryptoPro.DSS.DocumentConverter.Word.WordConverter -Parameters @{ "encoding" = "UTF-8"}
```

Внимание!

При возникновении ошибки во время изменения настроек плагин удаляется из списка. Необходимо добавить его заново командой Add-DssDocumentStoreConverterPlugin.

Пример настройки кодировки

Примечание

Плагин `DSS.DocumentConverter.Word.dll` может неверно определить кодировку в документах типа `xml`, `txt`. В этом случае её необходимо задать вручную через параметр encoding. Имена кодировок приведены на сайте IANA. Чаще всего используются значения: `UTF-8`, `UTF-7`, `UTF-16BE`, `UTF-16LE`, `UTF-16`, `US-ASCII`.

При добавлении плагина:

```
Add-DssStsConverterPlugin -FileExtension xml -Assembly DSS.DocumentConverter.Word.dll -Parameters @{
"encoding" = "UTF-8"}
```

При изменении настроек:

```
Set-DssStsConverterPlugin -FileExtension xml -Assembly DSS.DocumentConverter.Word.dll -ClassName
CryptoPro.DSS.DocumentConverter.Word.WordConverter -Parameters @{ "encoding" = "UTF-8"}
```

Отображение краткой информации о документе

Сервис Обработки Документов предоставляет возможности по конвертации документов с целью отображения в мобильном приложении myDSS наиболее релевантной информации из метаданных документа и/или его содержания.

Отображение краткой информации о документе

По умолчанию после создания экземпляра СОД в КриптоПро DSS автоматически регистрируется плагин, выводящий в мобильном приложении myDSS *имя файла*, действие с которым требует подтверждения. Плагин применяется к документам всех форматов, для которых не зарегистрировано собственного плагина.

Если необходимо выводить другую информацию о документе, можно настроить имеющийся HTML-шаблон по умолчанию, по которому СОД преобразовывает документ. Данное действие производится при помощи командлета Set-DssDocumentStoreConverterPlugin.

Шаблон плагина по умолчанию выглядит следующим образом:

```
<div><body><p>{0:Name}.</p></p></body></div>
```

Настройка плагина по умолчанию в общем виде выглядит следующим образом:

```
Set-DssDocumentStoreConverterPlugin -FileExtension preview_@default_html -Parameters @{snippetTemplate="
<Пользовательский HTML-шаблон>"}
```

, где в значение параметра `-Parameters` должен быть помещен пользовательский HTML-шаблон формата `@{snippetTemplate="<Пользовательский HTML-шаблон>"}`.

Примечание

При необходимости шаблон может содержать `CSS`.

Как видно из примера выше, шаблон представляет собой HTML-документ с подстановочными параметрами. Подстановочное поле имеет формат {0:<Имя параметра>}. В шаблоне **ДОЛЖНЫ** использоваться только подстановочные поля, поддерживаемые зарегистрированным плагином. К примеру, шаблон по умолчанию может использовать только подстановочные параметры, соответствующие полям структуры DocumentInfo.

Примечание

Для обращения к значению подстановочного параметра из поля `AdditionalInfo` структуры DocumentInfo необходимо воспользоваться форматом {0: AdditionalInfo.NAME}, где `NAME` - имя ключа в словаре `AdditionalInfo`.

Для расширенного использования подстановочных параметров внутри шаблона может использоваться структура `CDATA`. Структура `CDATA` должна находиться внутри тэга HTML-шаблона `<div></div>` и иметь следующий формат:

```
<![CDATA[{""<Ключ 1 - Имя подстановочного параметра>"":{""<Ключ 2 - Содержимое подстановочного параметра>"":""
<Значение, соответствующее Ключу 2>""}}]]>
```

Таким образом, подстановочный параметр, поддерживаемый зарегистрированным плагином, является ключом (Ключ 1) словаря подстановочных параметров. А парой к этому ключу (значением данного параметра) является еще один словарь, где ключом (Ключ 2) является значение подстановочного параметра. Для этого значения может присутствовать пользовательское содержимое, которое при конвертации будет подставлено в краткую информацию о документе.

Пример:

```
Set-DssDocumentStoreConverterPlugin -FileExtension preview_@default_html -Parameters @{snippetTemplate="<div>
<body><h1>DefaultTemplate</h1><p>{0:Name}</p><p>{0:FileType}</p></body><![CDATA[{""FileType"":{""txt"":""Это
текстовый документ""}}]]></div>"}
```

Для файла в формате qwe и именем `Договор.txt` результат будет выведен документ следующего вида:

```
DefaultTemplate
Договор.txt
Это текстовый документ
```

Отображение печатной формы документа

Отображение печатной формы документа в мобильном приложении myDSS также позволяет сформировать удобную для просмотра и подтверждения операций версию подписываемого документа. Данная форма является дополнительной, и не может быть настроена без отображения краткой информации о документе и полного его текста.

Порядок настройки отображения печатной формы документа полностью аналогичен настройке отображения краткой информации, за исключением того, что в словаре параметров `Parameters` ключом является `documentTemplate`.

Добавление HTML-шаблона из файла

Плагины отображения краткой и информации о документе позволяют получить HTML-шаблон из файла. Для этого в словаре параметров `-Parameters` должен использоваться ключ `snippetTemplatePath` или `documentTemplatePath` для отображения краткой информации о документе или его печатной формы соответственно. Значение ключа должно содержать полный путь к файлу с HTML-шаблоном.

Пример:

```
Set-DssDocumentStoreConverterPlugin -FileExtension preview_test_html -Parameters
@{snippetTemplatePath="C:\templates\template.txt"}
```

Пример PowerShell-сценария для настройки компонента «Сервис Обработки Документов»

Данный сценарий выполняет минимально необходимую настройку экземпляра компонента «Сервис Обработки Документов».

```
# Создание нового экземпляра Сервиса Обработки Документов:
New-DssDocumentStoreInstance -SQLServerName <sqlservername> -DisplayName DocumentStore -SiteName "Default Web
Site"

# Настройка сервисного сертификата
Set-DSSDocumentStoreProperties -ServiceCertificate <thumbprint>

# Настройка отношений доверия с Центром Идентификации:

   # Регистрация на Сервисе Обработки Документов Центра Идентификации в качестве доверенного издателя
маркеров безопасности.
Add-DssDocumentStoreClaimsProviderTrust -IssuerName realsts -Thumbprint <Thumbprint>

   # Регистрация Сервиса Обработки Документов в качестве доверенной стороны на Центре Идентификации.
Add-DssRelyingPartyTrust -Name DocumentStore -Identities urn:cryptopro:dss:documentstore:DocumentStore

# Настройка адреса Сервиса Обработки Документов на Сервисе Подписи:
Set-DssProperties -DocumentStoreAddress http://<hostname>/documentstore
```

Запрет внешних шаблонов документов:

```
Set-DssDocumentStoreProperties -AllowExternalTemplates 0
```

Работа с документами

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);
- на веб-интерфейсе Центра Идентификации (используются для отображения документа в мобильном приложении myDSS);
- Отображение документов в формате DTBS.

Для всех загружаемых в КриптоПро DSS документов могут быть настроены ограничения размеров документов и автоопределение формата документов.

Также в КриптоПро DSS могут быть реализованы пользовательские преобразования XML-документов при создании электронной подписи формата `XMLDSIG`.

См. также:

- Сервис Обработки Документов

Отображение документов перед подписью на Веб-интерфейсе Пользователя

Веб-интерфейс Пользователя предоставляет Пользователям возможность визуализации документов перед созданием подписи. Поддерживается просмотр документов следующих форматов: `PDF`, `XML`, `ODT`.

Также могут быть обработаны документы 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 набора специализированных командлетов.

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:

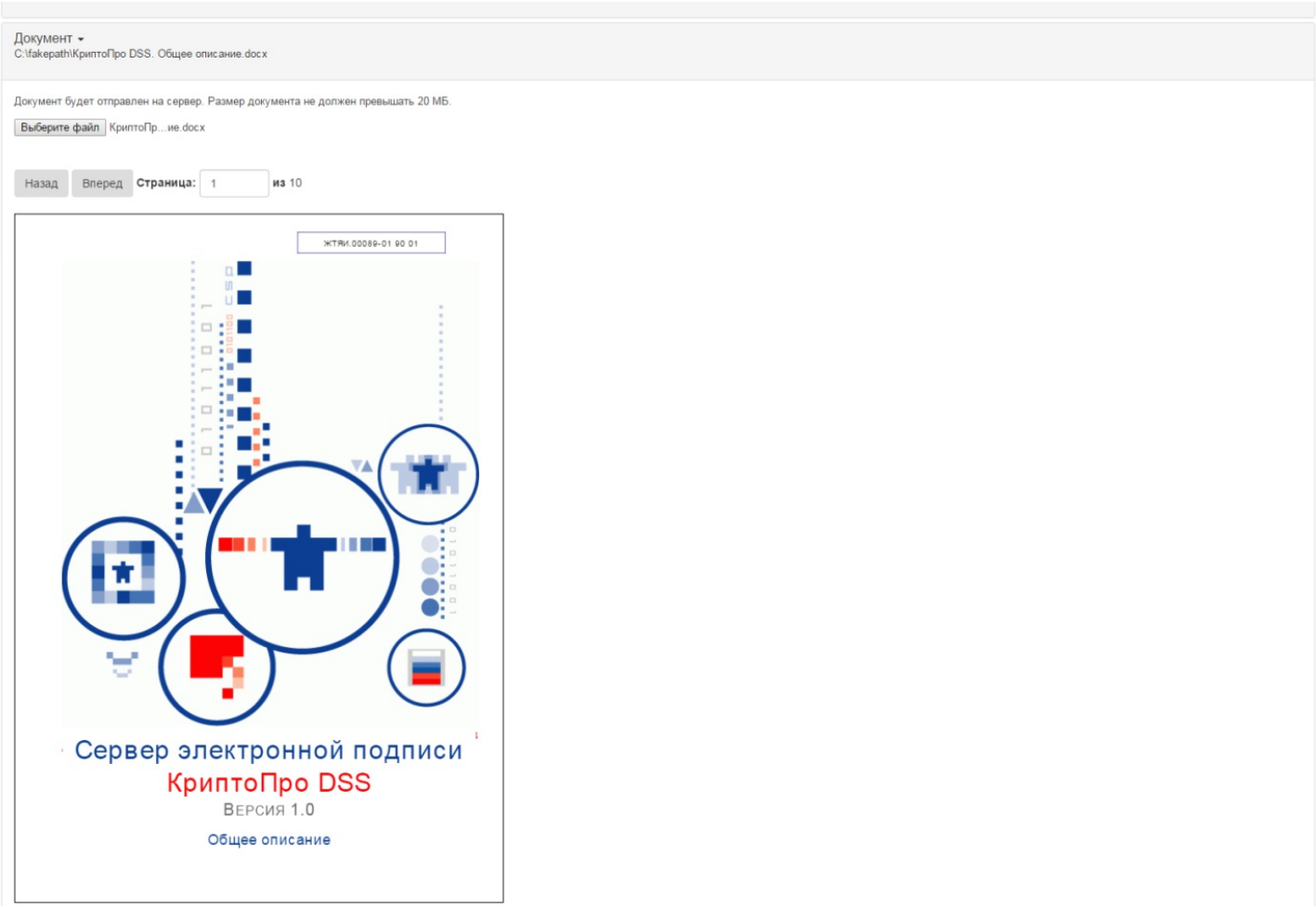
Данный сценарий регистрирует форматы документов, для которых возможен просмотр с помощью установленных плагинов.

```
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
```

Внимание!

При возникновении ошибки во время изменения настроек плагин удаляется из списка. Необходимо добавить его заново командой Add-Dss***ConverterPlugin.

Если просмотр загруженного документа поддерживается установленными плагинами и выполнена регистрация в конфигурационном файле, то документ отображается во вкладке «Загрузка документа».



Для поддержки отображения документов особых форматов необходимо реализовать и зарегистрировать соответствующий плагин, отвечающий описанным в Руководстве разработчика требованиям.

Пример настройки кодировки

> **Примечание**
>
> Плагин `DSS.DocumentConverter.Word.dll` может неверно определить кодировку в документах типа `xml`, `txt`. В этом случае её необходимо задать вручную через параметр encoding. Имена кодировок приведены на сайте IANA. Чаще всего используются значения: `UTF-8`, `UTF-7`, `UTF-16BE`, `UTF-16LE`, `UTF-16`, `US-ASCII`.

При добавлении плагина:

```
Add-DssStsConverterPlugin -FileExtension xml -Assembly DSS.DocumentConverter.Word.dll -Parameters @{
"encoding" = "UTF-8"}
```

При изменении настроек:

```
Set-DssStsConverterPlugin -FileExtension xml -Assembly DSS.DocumentConverter.Word.dll -ClassName
CryptoPro.DSS.DocumentConverter.Word.WordConverter -Parameters @{ "encoding" = "UTF-8"}
```

Отображение документов в мобильном приложении myDSS

Мобильное приложение myDSS имеет возможность отображать документ при подтверждении операции с этим документом. Настройка соответствующих плагинов преобразования документов осуществляется при помощи специализированного набора командлетов.

Центр Идентификации предоставляет Пользователям возможность визуализации документов в мобильном предложении myDSS перед созданием подписи. Поддерживается просмотр документов следующих форматов: `PDF`, `XML`, `ODT`.

Также могут быть обработаны документы 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.


MTS RUS
18:46
88 %
ОПЕРАЦИЯ 1 из 1
Данные операции
КРИПТОПРО
ПОДТВЕРДИТЬ
ОТКАЗАТЬСЯ

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
```

Просмотр настроек плагина:

```
Get-DssStsConverterPlugin | where { $_.Extension -eq "xml" }  | select -ExpandProperty Converters | Format-
List
```

Изменение настроек плагина:

```
Set-DssStsConverterPlugin -FileExtension xml -Assembly DSS.DocumentConverter.Word.dll -ClassName
CryptoPro.DSS.DocumentConverter.Word.WordConverter -Parameters @{ "encoding" = "UTF-8"}
```

Внимание!

При возникновении ошибки во время изменения настроек плагин удаляется из списка. Необходимо добавить его заново командой Add-Dss***ConverterPlugin.

Настройка кодировки

> **Примечание**
>
> Плагин `DSS.DocumentConverter.Word.dll` может неверно определить кодировку в документах типа `xml`, `txt`. В этом случае её необходимо задать вручную через параметр encoding. Имена кодировок приведены на сайте IANA. Чаще всего используются значения: `UTF-8`, `UTF-7`, `UTF-16BE`, `UTF-16LE`, `UTF-16`, `US-ASCII`.

Пример настройки кодировки аналогичен настройке при отображении документов на Веб-интерфейсе Пользователя.

Плагин для визуализации больших документов

Данный плагин обеспечивает визуализацию документов, которые в силу своего размера не могут быть визуализированы другими способами.

Для документов, превышающих максимально возможный для визуализации размер, плагин формирует xml-"выжимку" документа, включающую в себя:

- имя документа;
- размер документа;
- хэш документа в кодировке Base64.

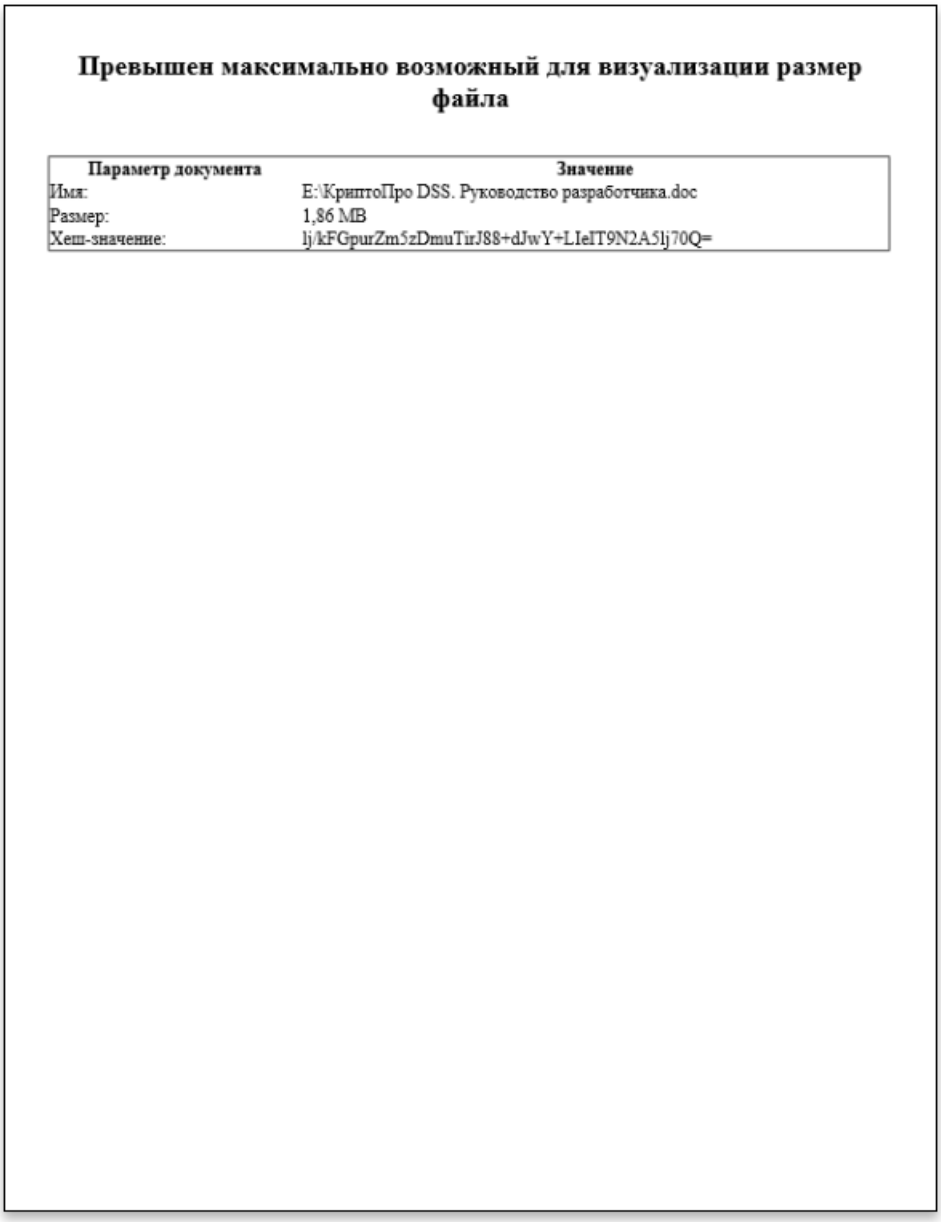
Далее, при помощи XSLT-преобразования данный xml транформируется в HTML-документ, который в свою очередь и визуализируется.

Пример xml-"выжимки" представлен ниже:

```
<LargeDocPreview>
  <FileName>fileName.doc</FileName>
  <Size>1,86</Size>
  <HashVal>/kf ... </HashVal>
</LargeDocPreview>
```

Пример XSTL-преобразования, используемого в плагине по умолчанию доступен по ссылке:

В случае, если плагин настроен правильно, большие файлы будут визуализироваться следующим образом:



Превышен максимально возможный для визуализации размер файла

Параметр документа	Значение
Имя:	E:\КриптоПро DSS. Руководство разработчика.doc
Размер:	1,86 MB
Хеш-значение:	lj/kFGpurZm5zDmuTirJ88+dJwY+LIeIT9N2A5lj70Q=

Регистрация плагина

Для регистрации плагина необходимо выполнить следующую команду:

```
Add-DssStsConverterPlugin -FileExtension %FileExtension% -Assembly
DSS.DocumentConverter.LargeDocPreprocessor.dll -Classname
DSS.DocumentConverter.LargeDocPreprocessor.LargeDocPreprocessor -Parameters @{"MinimalDocSize"="1"} -Priority
1
```

Параметры плагина включают в себя:

- `MinimalDocSize` - минимальный пороговый размер файлов (в мегабайтах) для которых будет осуществляться преобразование (все файлы с меньшим размером игнорируются);
- `Xslt` - путь к файлу с пользовательским XSLT-преобразованием (для ситуаций, когда преобразование по умолчанию не подходит).

Примечание

Параметр `MaxIisContentLength` Веб-интерфейса ограничивает максимальный размер файла, который может быть обработан сервисом. Конфигурацию плагина следует осуществлять с учетом значения данного параметра.

Примечание

Мобильное приложение myDSS при помощи данного конвертера позволяет отображать документы размером не более 17 МБ.

Построение цепочки плагинов визуализации

Система плагинов Центра Идентификации позволяет формировать из них цепочку. Это дает возможность сконфигурировать плагины визуализации таким образом, чтобы документы размером ниже порогового значения обрабатывались одним плагином, а документы выше - другим.

Для того, чтобы Центр Идентификации построил из плагинов цепочку, они должны быть зарегистрированы для одного и того же расширения, при этом порядок отработки плагинов в цепочке зависит от параметра Priority, задаваемого при регистрации плагина.

Плагины с меньшим Priority выполняют преобразование в цепочке раньше. Далее приведен пример регистрации плагинов, который позволит обрабатывать документы с расширением .doc любого размера.

```
Add-DssStsConverterPlugin -FileExtension doc -Assembly DSS.DocumentConverter.LargeDocPreprocessor.dll -
Classname DSS.DocumentConverter.LargeDocPreprocessor.LargeDocPreprocessor -Parameters @{"MinimalDocSize"="10"}
-Priority 1
Add-DssStsConverterPlugin -FileExtension doc -Assembly DSS.DocumentConverter.Word.dll -Classname
CryptoPro.DSS.DocumentConverter.Word.WordConverter -Priority 2
```

В данном примере регистрируется плагин для больших файлов с минимальным размеров в 10МБ и `Priority` 1, а также плагин визуализации документов Word. При передаче документа .doc в мобильное приложение будет происходить следующее:

- Если документ превышает размер в 17 МБ, он не будет визуализирован;
- Документ попадает в плагин визуализации больших документов (плагин с приоритетом `1`);
    - Если размер документа превышает пороговое значение (10 МБ в данном примерер), он будет визуализирован плагином больших документов в специальном виде (см. скриншот выше);
    - Если размер документа меньше порогового значения, документ передается следующему плагину цепочки без изменений;
- Документ попадает в плагин визуализации документов Word (плагин с приоритетом `2`) и для него формируется традиционная отображаемая форма.

Отображение документа в формате DTBS

КриптоПро DSS предоставляет Пользователям возможность отображения специально подготовленных документов на Веб-интерфейсе Пользователя перед созданием подписи или шифрованием документа.

DTBS-документ представляет собой XML-документ, сформированный в соответствии со следующей схемой:

```
<?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>
```

Отображение DTBS-документов возможно также в мобильном приложении myDSS, если на Центре Идентификации настроены соответствующие плагины. Плагин, позволяющий отобразить эту информацию, находится в директории `<Путь установки>\DSS\Plugins\Converters` и называется `DSS.DocumentConverter.Dtbs.dll`.

Работа с плагином производится при помощи специальных командлетов. При добавлении плагина необходимо также задать настройки, перечисленные в таблице ниже. Эти настройки задаются внутри параметра `Parameters` типа `Hashtable`:

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

, где `paramNamei`, `paramValuei` – название и значение параметра соответственно.

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.
PageSetup.PaperSize	Размеры отображаемого документа. Данный параметр позволяет выбрать стандартные размеры по обозначению формата из таблицы ниже. Для ввода пользовательских параметров используется значение **Custom**.
PageSetup.Gutter	Расстояние между строками.
xslt	Путь к файлу с XSLT-преобразованием. Опциональный параметр.

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″
Custom	При выборе данного размера необходимо самостоятельно задать размеры страницы при помощи параметров из таблицы выше.

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"}
```

Примечание

Расширение, указанное в параметре `-FileExtension` при регистрации плагина, и расширение файла отображаемого документа должны совпадать.

Пример содержимого документа, 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>
```

Отображение документа:

Создание подписи

Документ ▾

Документ был загружен с внешнего сайта.

d4a9aa2f-6933-4a82-b508-854dd8c9c878

```
Наименование платежа: Новое платёжное поручение №85,
Счёт получателя: 575019630,
Счёт отправителя: 1696919449.
```

Настройка ограничений размеров 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 таблице ниже.

КОМПОНЕНТ	КОМАНДЛЕТ
Сервис Подписи	Set-DssEndpointGlobalSettings с параметром `MaxMessageSize`.
Центр Идентификации	Set-DssStsEndpointGlobalSettings с параметром `MaxMessageSize`.
Веб-интерфейс Пользователя	Set-DssFeProperties с параметром `MaxIISContentLength`.
myDSS External Interaction Server	Set-MyDssServerInteractionPushServiceEndpointGlobalSettings и Set-MyDssServerInteractionServiceEndpointGlobalSettings с параметром `MaxMessageSize`.
myDSS Internal Interaction Server	Set-MyDssServerInternalEndpointGlobalSettings с параметром `MaxMessageSize`.
mDAG	Set-MdagEndpointGlobalSettings с параметром `MaxMessageSize`.

Значение параметра `MaxMessageSize` задается в байтах и по умолчанию равно 5 Мбайт (2147482624 байт).

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 таблице выше, но с параметрами `MaxRecieveTimeOut` и `MaxSendTimeOut`. Эти параметры позволяют настроить время получения и отправки сообщения сервером.

> **Примечание**
>
> 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

# Настройка ограничения на mDAG
Set-MdagEndpointGlobalSettings -MaxMessageSize 2147482624
```

Настройка автоопределения формата документов

В КриптоПро DSS существует возможность настроить автоопределение формата документа, передаваемого информационной системой в DSS посредством REST-интерфейса. Это позволяет упростить процесс создания подписи в случаях, когда информационная система по тем или иным причинам не имеет возможности передать в запросе на подпись документа его формат.

Список командлетов, при помощи которых настраивается автоопределение формата передаваемого документа, приведен в таблице ниже.

КОМПОНЕНТ	КОМАНДЛЕТ
Центр Идентификации	Add-DssStsConverterAutoDetectProperties, Enable-DssStsConverterAutoDetectProperties.
Веб-интерфейс Пользователя	Add-DssFeConverterAutoDetectProperties, Enable-DssFeConverterAutoDetectProperties.
Сервис Обработки Документов	Add-DssDocumentStoreConverterAutoDetectProperties, Enable-DssDocumentStoreConverterAutoDetectProperties.

Настройка производится следующим образом:

- Добавление формата документа и его сигнатуры (параметры `-FileExtension <string>` и `-Signature <int>`);
- Включение автоопределения формата документов.

> **Примечание**
>
> Параметр `-Signature` должен содержать **HEX-значение** первых байтов документа, определяющих его формат.

Пример настройки для СОД:

```
Add-DssDocumentStoreConverterAutoDetectProperties -FileExtension docx -Signature <значение в HEX> -
DisplayName <DocumentStore AppName>
Enable-DssDocumentStoreConverterAutoDetectProperties -DisplayName <DocumentStore AppName>
```

Преобразование XML-документов

Сервис Подписи обеспечивает поддержку пользовательских XML-преобразований при формировании подписи формата `XMLDSig`. Данная возможность обеспечивается путем регистрации на Сервисе Подписи плагина XML-преобразования.

Регистрация плагина осуществляется при помощи командлетов среды Windows Powershell. Для регистрации необходима следующая информация:

- имя сборки, содержащей класс с реализацией XML-преобразования;
- имя класса, реализующего XML-преобразование (опционально);
- список идентификаторов данного преобразования.

После получения требуемой информации необходимо выполнить командлет Add-DssSignServerTransformPlugin, который позволит зарегистрировать плагин системы. Далее представлены примеры регистрации пользовательских преобразований, которые идут в составе дистрибутива КриптоПро DSS.

Примеры:

Добавление XML-преобразования для Фонда Социального страхования (ФСС) РФ (Нормативный документ доступен по ссылке):

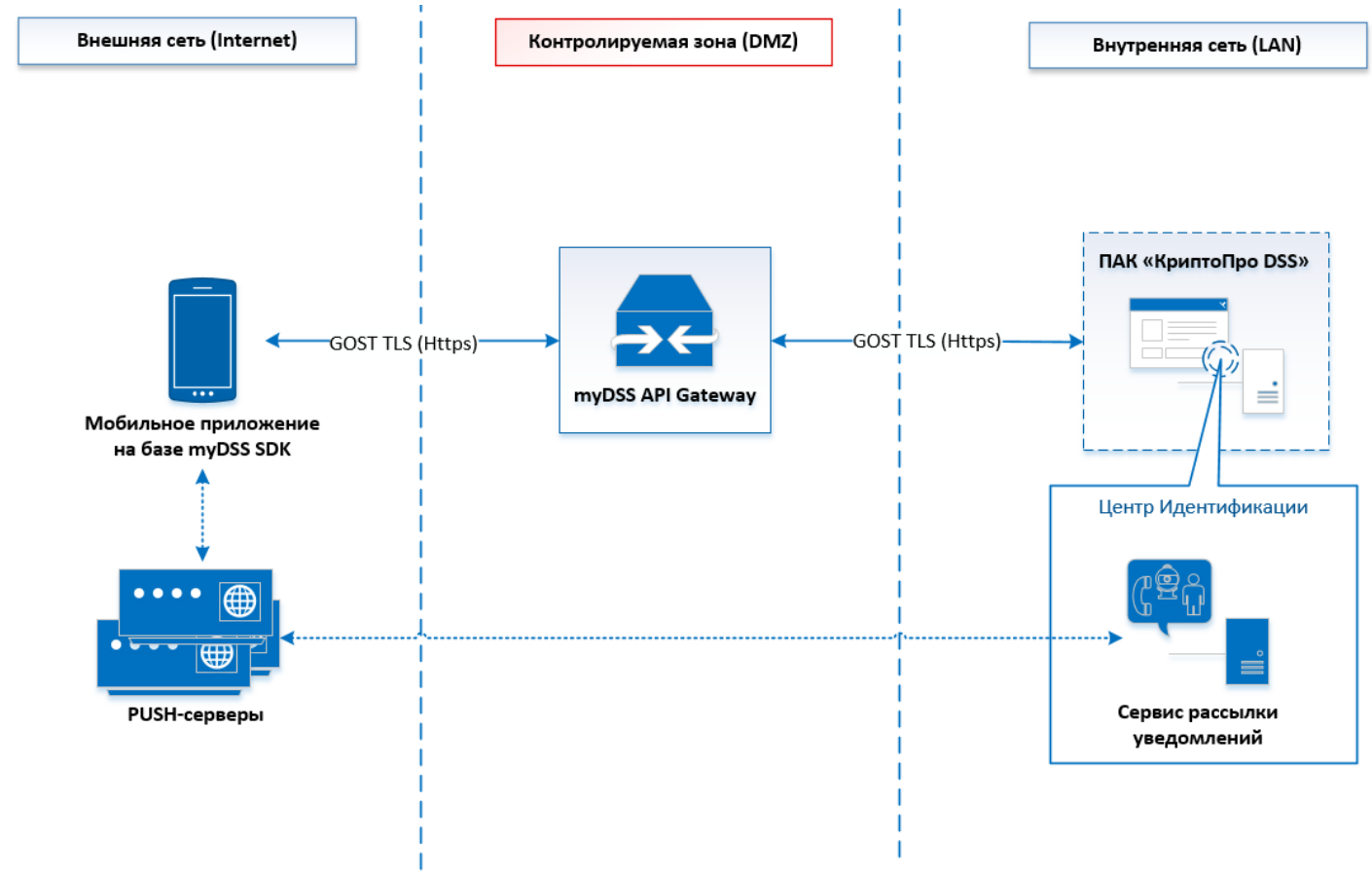
```
Add-DssSignServerTransformPlugin -Assembly CryptoPro.DSS.Xml.Transforms.dll -Classname
CryptoPro.DSS.Xml.Transforms.XmlFssTransform -Identifiers "urn:xml-dsig:transformation:v1.1"
```

Добавление XML-преобразования XPath Filter 2.0 (Нормативный документ доступен по ссылке):

```
Add-DssSignServerTransformPlugin -Assembly CryptoPro.DSS.Xml.Transforms.dll -Classname
CryptoPro.DSS.Xml.Transforms.Filter2SubstractTransform-Identifiers "http://www.w3.org/2002/06/xmldsig-
filter2"
```

Настройка Сервиса взаимодействия с DSS SDK (myDssApiGateway, mDAG)

Сервис взаимодействия с DSS SDK (myDssApiGateway, mDAG) предоставляет доступ к компонентам DSS при взаимодействии с ними через DSS SDK. При этом схема взаимодействия DSS SDK и DSS выглядит следующим образом:



В этом разделе:

- Настройка экземпляра
- Объекты администрирования и командлеты
- Пример PowerShell-сценария

Создание и настройка экземпляра Сервиса взаимодействия с DSS SDK (myDssApiGateway, mDAG)

Данный раздел определяет последовательность действий при разворачивании и настройке экземпляра Сервиса взаимодействия с DSS SDK (mDAG).

- **Пример разворачивания**

Предварительные условия:

- Установленная роль Сервер приложений (IIS);
- Настроенная привязка https* на Сервере приложений (IIS);
- Установленный КриптоПро CSP (входит в комплект поставки);

> Внимание!
>
> Веб-сервер, на котором разворачивается mDAG, должен использовать сертификат, соответствующий ГОСТ Р 34.10-2012.

> Примечание
>
> Экземпляр mDAG можно полноценно настроить, когда развернуты и настроены экземпляры остальных компонентов DSS.

Базовая последовательность шагов по настройке (обязательные):

1. Создание экземпляра службы mDAG (командлет New-MdagInstance).

На данном шаге будет создано веб-приложение на Сервере приложений IIS.

Пример:

```
New-MdagInstance -SiteName "Default Web Site" -DisplayName apigateway
```

2. Настройка доступа к DSS через mDAG.

На данном шаге производится настройка доступа к DSS через mDAG с использованием протокола OpenID Connect 1.0.

Настройка осуществляется посредством ввода следующих команд:

```
# Настройка на Центре Идентификации доступа по OpenID Connect

Add-DssClient -Identifier cryptopro.dss.mydss.<apigateway App Name> -Name "<myDSS API Gateway>" -Description
"<myDSS API Gateway OAuth client description>" -AllowedFlow MyDssAssertion,ClientCredentials -GenerateSecret
```

```
# Настройка на mDAG доступа по OpenID Connect

$clientSecret = (Get-DssClientSecret -ClientId cryptopro.dss.mydss.<apigateway App Name>).Value

Set-MdagProperties -ClientId cryptopro.dss.mydss.<apigateway App Name> -ClientSecret $clientSecret
```

> Примечание
>
> Зарегистрированный `clientSecret` действителен в течение 1 года с момента его регистрации. После его истечения необходимо сгенерировать новый `clientSecret` для прежнего клиента:

```
Set-DssClient -ClientId cryptopro.dss.mydss.<apigateway App Name> -GenerateSecret

$clientSecret = (Get-DssClientSecret -ClientId cryptopro.dss.mydss.<apigateway App Name>).Value

Set-DssFeOidcSettings -ClientId cryptopro.dss.mydss.<apigateway App Name> -ClientSecret $clientSecret
```

3. Регистрация криптопровайдера для mDAG.

На данном шаге в экземпляре Центра Идентификации регистрируется криптопровайдер, который используется работы mDAG с закрытыми ключами Пользователей.

Пример регистрации криптопровайдера для КриптоПро CSP (для работы в тестовом режиме):

```
Add-DssCryptoProviderProfile -DisplayName \<STSAppName> -Type MyDss -PrimaryProviderName "Crypto-Pro GOST R
34.10-2012 Cryptographic Service Provider" -PrimaryProviderType 80 -Name "CryptoProfile for DSS SDK"
```

4. Настройка параметров взаимодействия с myDSS.

На данном шаге производится настройка параметров взаимодействия с myDSS. Полное описание параметров приведено в описании командлета Set-DssMyDssProperties. Для обеспечения базовой работоспособности mDAG необходимо следующее:

- задать на ЦИ адрес mDAG;
- задать режим работы SDK - `Strong` для создания УКЭП, `Weak` для УНЭП;
- настроить требование проверять уникальность отпечатка устройства Пользователя `-DeviceFingerprintRequired` - `$true` или `$false`.

```
Set-DssMyDssProperties -MyDssServiceUrl https://<hostname>/<mDAG App Name> -MyDssKeyProtectionType Strong -
DeviceFingerprintRequired $true
```

> **Примечание**
>
> Режим работы SDK `Weak` (параметр `-MyDssKeyProtectionType`) может использоваться только для создания усиленной неквалифицированной электронной подписи.

Дополнительно для сценария инициализации мобильного устройства при помощи QR-кода с начальным вектором аутентификации (см. раздел 5.3 документа "ЖТЯИ.00096-02 96 02 КриптоПро DSS. Общее описание") можно настроить защиту начального вектора аутентификации при помощи кода активации, передаваемого в SMS- или Email-сообщении. Для этого необходимо выполнить следующие настройки:

```
# Для Пользователя
Set-DssMyDssProperties -KeyInfoDivideByUserRequired 1

# Для Оператора
Set-DssMyDssProperties -KeyInfoDivideRequired 1

# Установка длины кода активации 8 символов
Set-DssMyDssProperties -SecondKeyPartLength 8
```

5. Включение метода аутентификации.

На данном шаге производится включение метода аутентификации myDSS при помощи командлета Enable-DssAuthenticationMethod.

```
Enable-DssAuthenticationMethod -Uri "http://dss.cryptopro.ru/identity/authenticationmethod/mydss"

или

Enable-DssAuthenticationMethod -Id 16
```

6. Интеграция с компонентами DSS.

На данном шаге производится интеграция mDAG с другими компонентами DSS. Для этого Администратор должен настроить адреса всех необходимых сервисов при помощи командлета Set-MdagProperties.

```
# Интеграция с Центром Идентификации:
Set-MdagProperties -IdpBaseAddress <http://<hostname>/Sts App Name>

# Интеграция с Сервисом Подписи
Set-MdagProperties -SignServerBaseAddress <http://<hostname>/SignServer App Name>

# Интеграция с Сервисом Аудита
Set-MdagProperties -AnalyticsBaseAddress <http://<hostname>/Analytics App Name>

# Интеграция с Сервисом Обработки Документов
Set-MdagProperties -DocumentStoreBaseAddress <http://<hostname>/DocumentStore App Name>
```

7. Подключение Сервиса Обработки Операций.

На данном шаге производится подключение Сервиса Обработки Операций к Сервису Подписи и Центру Идентификации.

```
# Подключение Сервиса Обработки Операций
Connect-DssOperationStore -ConnectionInfo <$connInfo> -DisplayName <SignServer AppName>
Connect-DssStsOperationStore -ConnectionInfo <$connInfo> -DisplayName <STS AppName>
```

В параметр `-ConnectionInfo` можно поместить переменную, в которой находится результат заполнения структуры `SQLConnectionInfo`, используемой при разворачивании БД компонентов DSS.

Пример:

```
$connInfo = New-DssSqlConnectionInfo -ServerName .\SQLServer -DatabaseName <OperationServiceDbName>
```

Внимание!

В параметре `-ConnectionInfo` должны быть параметры подключения к одной и той же ранее созданной БД Сервиса Обработки Операций. Подробнее развертывание БД описано в соответствующем разделе.

Примечание

После внесения изменений в конфигурацию экземпляров необходимо перезапустить пулы их веб-приложения при помощи соответствующих команд.

Пример перезапуска:

```
# Перезапуск пула приложений mDAG:
Restart-MdagInstance -DisplayName <string>

# Перезапуск пула приложений Центра Идентификации:
Restart-DssStsInstance -DisplayName <string>
```

Дополнительные действия по настройке (опциональные):

Администратор DSS может настроить для mDAG ограничение размера получаемых сервером сообщений при помощи параметра `-MaxMessageSize` командлета Set-MdagEndpointGlobalSettings. Значение задается в байтах и по умолчанию равно 5 Мбайт (2147482624 байт).

```
Set-MdagEndpointGlobalSettings -MaxMessageSize 2147482624
```

Пример PowerShell-сценария для настройки компонента «Сервис взаимодействия с DSS SDK (myDssApiGateway, mDAG)»

Данный сценарий выполняет минимально необходимую настройку экземпляра компонента «Сервис взаимодействия с DSS SDK (myDssApiGateway, mDAG)».

```
# Создание нового экземпляра mDAG:
New-MdagInstance -SiteName "Default Web Site" -DisplayName apigateway


# Настройка на Центре Идентификации доступа по OpenID Connect
Add-DssClient -Identifier cryptopro.dss.mydss.<apigateway App Name> -Name "<myDSS API Gateway>" -Description
"<myDSS API Gateway OAuth client description>" -AllowedFlow MyDssAssertion,ClientCredentials -GenerateSecret

# Настройка на mDAG доступа по OpenID Connect
$clientSecret = (Get-DssClientSecret -ClientId cryptopro.dss.mydss.<apigateway App Name>).Value
Set-MdagProperties -ClientId cryptopro.dss.mydss.<apigateway App Name> -ClientSecret $clientSecret

# Регистрация криптопровайдера
Add-DssCryptoProviderProfile -DisplayName \<STSAppName> -Type MyDss -PrimaryProviderName "Crypto-Pro GOST R
34.10-2012 Cryptographic Service Provider" -PrimaryProviderType 80 -Name "CryptoProfile for DSS SDK"


# Настройка взаимодействия mDAG с myDSS:
Set-DssMyDssProperties -MyDssServiceUrl https://<hostname>/<mDAG App Name> -MyDssKeyProtectionType Strong -
DeviceFingerprintRequired $true


# Включение метода аутентификации:
Enable-DssAuthenticationMethod -Uri "http://dss.cryptopro.ru/identity/authenticationmethod/mydss"
ИЛИ
Enable-DssAuthenticationMethod -Id 16


# Интеграция с Центром Идентификации:
Set-MdagProperties -IdpBaseAddress <http://<hostname>/Sts App Name>

# Интеграция с Сервисом Подписи
Set-MdagProperties -SignServerBaseAddress <http://<hostname>/SignServer App Name>

# Интеграция с Сервисом Аудита
Set-MdagProperties -AnalyticsBaseAddress <http://<hostname>/Analytics App Name>

# Интеграция с Сервисом Обработки Документов
Set-MdagProperties -DocumentStoreBaseAddress <http://<hostname>/DocumentStore App Name>


# Подключение Сервиса Обработки Операций

$connInfo = New-DssSqlConnectionInfo -ServerName .\SQLServer -DatabaseName <OperationServiceDbName>

Connect-DssOperationStore -ConnectionInfo <$connInfo> -DisplayName <SignServer AppName>
Connect-DssStsOperationStore -ConnectionInfo <$connInfo> -DisplayName <STS AppName>



# Перезапуск пула приложений mDAG:
Restart-MdagInstance -DisplayName <string>

# Перезапуск пула приложений Центра Идентификации:
Restart-DssStsInstance -DisplayName <string>
```

Дополнительные настройки

```
# Смена Client Secret:
Set-DssClient -ClientId cryptopro.dss.mydss.<apigateway App Name> -GenerateSecret
$clientSecret = (Get-DssClientSecret -ClientId cryptopro.dss.mydss.<apigateway App Name>).Value
Set-DssFeOidcSettings -ClientId cryptopro.dss.mydss.<apigateway App Name> -ClientSecret $clientSecret


# Настройка ограничения размера получаемых сообщений на веб-сервере:
Set-MdagEndpointGlobalSettings -MaxMessageSize 2147482624
```

Аутентификация в КриптоПро DSS

КриптоПро DSS поддерживает несколько методов аутентификации Пользователей DSS. Все методы аутентификации делятся на следующие группы:

- Первичная аутентификация.
  - Аутентификация по логину и паролю
  - Аутентификация по сертификату
- Подтверждение операций.
  - Подтверждение операций при помощи мобильного приложения myDSS
  - Подтверждение операций при помощи апплета на SIM-карте
- Вторичная аутентификация.

Первичная аутентификация используется при входе в Веб-интерфейс Пользователя и личный кабинет Пользователя на веб-интерфейсе Центре Идентификации.

Подтверждение операций может использоваться как при входе в указанные веб-интерфейсы, так и во время выполнения других операций, требующих доступа к закрытому ключу Пользователя (например, подписи документа).

Вторичная аутентификация в КриптоПро DSS является **вспомогательной** и может дополнять первичную в качестве дополнительной меры безопасности. При этом вторичная аутентификация не ослабляет требований первичной.

> **Примечание**
>
> При настройке вторичной аутентификации необходимо обратить особое внимание на регистрацию Сервиса Подписи в качестве доверенной стороны на Центре Идентификации при помощи параметра `-BackChannelUrl` командлета Add-DssRelyingPartyTrust.

Список доступных методов аутентификации приводится в выводе командлета Get-DssAuthenticationMethod. Включение/отключение метода аутентификации по идентификатору производится при помощи параметра `-Uri` командлетов Enable-DssAuthenticationMethod и Disable-DssAuthenticationMethod. Все неиспользуемые методы аутентификации должны быть отключены.

> **Внимание!**
>
> Идентификаторы методов аутентификации, описанных в данном разделе, приведены в начале каждого подраздела.

Пример включения метода аутентификации по логину и паролю:

```
Enable-DssAuthenticationMethod -Uri http://dss.cryptopro.ru/identity/authenticationmethod/password
```

Аутентификация по логину и 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-DssPasswordPolicy:

ПАРАМЕТР	ОПИСАНИЕ
`PasswordType`	Тип паролей, генерируемых сервером: Парольные фразы (`Phrase`); Символьные пароли (`Symbolic`).
`PasswordSource`	Источник паролей: Только Пользователь задаёт пароль (`ClientOnly`); Пароль генерируется только на стороне сервера (`ServerOnly`); Смешанный режим (`ClientAndServer`).
`PasswordComplexity`	Сложность символьных паролей: Цифры и буквы нижнегшо регистра (`Weak`); Цифры и буквы разного регистра (`Fair`); Все вышеперчисленное, включая спецсимволы (`Strong)`.
`PasswordLength`	Длина символьных паролей.
`PasswordPhraseComplexity`	Сложность парольной фразы: Из трех слов (`Common`); Из четырех слов(`Strong`).
`InvalidPasswordAttempts`	Количество попыток ввода пароля.
`PasswordLifetime`	Срок действия пароля Пользователя.
`ChangePasswordAfterReset`	Требование смены пароля Пользователя при первом входе.

Параметр `PasswordType` определяет тип паролей, генерируемых ТОЛЬКО 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:

- сбрасывает пароль для существующей учётной записи Пользователя.
- создаёт учётную запись Пользователя и назначает аутентификацию по логину и паролю;

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 чувствительна 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, спецсимволы. 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.

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 различительное имя Пользователя может быть автоматически заполнено правильными значениями из сертификата Пользователя.

Примечание

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`.

Для проверки подлинности сертификата веб-сервером необходимо добавить корневой сертификат издателя сертификата в хранилище «Доверенные корневые центры сертификации» локального компьютера.

(Необязательно) Для проверки подлинности сертификата со стороны КриптоПро DSS необходимо поместить корневой сертификат издателя сертификата в специализированное хранилище `<Имя_веб-приложения_ЦИ> Client Authentication Issuers`. Данная проверка возможна только после ее активации. Для активации проверки необходимо выполнить следующую команду:

```
Set-DssStsProperties –IsClientAuthenticationIssuersStoreEnabled 1
```

Аутентификация при помощи мобильного приложения myDSS

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 96 02 КриптоПро DSS. Общее Описание).

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 96 02 КриптоПро DSS. Общее Описание).

Настройка аутентификации при помощи мобильного приложения myDSS

Идентификатор:

```
http://dss.cryptopro.ru/identity/authenticationmethod/mobile
```

Предварительные условия для настройки аутентификации с использованием myDSS:

- Развернутые и настроенные основные компоненты КриптоПро DSS.
- КриптоПро HSM Client.
- Развернутые и настроенные экземпляры модуля аутентификации myDSS.
- Включенный метод аутентификации mobile

Для настройки аутентификации при помощи мобильного приложения myDSS необходимо выполнить следующие действия:

Настройка оповещения интегрируемой системы

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 зарегистрировать сооветствующие плагины (транспортный и форматирования) и модуль оповещения.

Управление модулями оповещения интегрируемой системы производится через набор командлетов, используемых для управления модулями оповещения DSS.

Для включения оповещения интегрируемой системы необходимо выполнить действия, описанные в таблице ниже.

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	@{}
Описание	Пустой словарь. Данный плагин не имеет настраиваемых параметров.
Пример	
Add-DssStsPlugin -PluginTypeName "CryptoPro.DSS.Identity.Authentication.Notification.AuthenticationResultFormatter,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,CryptoPro.DSS.Identity.Authentication.Notification" -PluginType AuthenticationResult -Settings @{}	

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	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 @{}	

Пример

Ниже приводится полная последовательность вызовов командлетов PowerShell для регистрации модуля.

```
#Настройка транспортного плагина
Add-DssStsPlugin -PluginTypeName
"CryptoPro.DSS.Identity.Authentication.Notification.HttpTransportPlugin,CryptoPro.DSS.Identity.Authentication.Noti
fication" -PluginType AuthenticationResult -Settings @{}

#Настройка плагина форматирования
Add-DssStsPlugin -PluginTypeName
"CryptoPro.DSS.Identity.Authentication.Notification.AuthenticationResultFormatter,CryptoPro.DSS.Identity.Authentic
ation.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.
```

Аутентификация при помощи 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.
- Включенный метод аутентификации simauth.

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.

2. Настройка подключения к OTA-платформе.

3. Регистрация партии SIM-карт и профиля криптопровайдера (набора Мастер-ключей).

На данном шаге необходимо выполнить следующее:

- Создать новый модуль. Модуль — это профиль криптоповайдера (набор Мастер-ключей) и другие параметры, необходимые для создания файла персонализации.
- Сгенерировать 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).

> **Примечание**
>
> Для каждого нового файла персонализации (партии SIM-карт) требуется создание нового профиля криптопровайдера (набора Мастер-ключей).

Набор расширенных параметров модуля может быть переиспользован для создания файла персонализации. Новый профиль криптопровайдера может быть назначен существующему модулю без регистрации нового. Изменение параметров существующего модуля (включая назначение нового профиля криптопровайдера) также описано в данном разделе.

Зарегистрированные модули и партии SIM-карт можно просмотреть в DSS при помощи PowerShell.

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.

Для включения оповещения интегрируемой системы необходимо выполнить действия, описанные в таблице ниже.

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	Название типа плагина 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.Notification" -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.

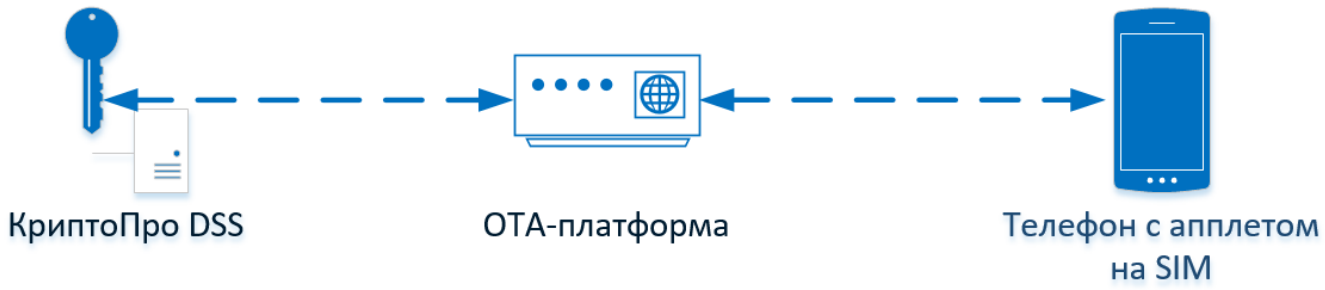
```
#Добавление плагина формирования сообщений
Add-DssStsPlugin -PluginTypeName
"CryptoPro.DSS.SimAuth.Notification.SimAuthFormatterPlugin,DSS.SimAuth.Notification" -PluginType Formatter –
Settings @{}

#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
```

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.

Взаимодействие КриптоПро DSS с апплетом на SIM-карте организовано в соответствии со схемой, приведённой на рисунке ниже.



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 таблице ниже.

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.Notification" -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.Notification" -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.

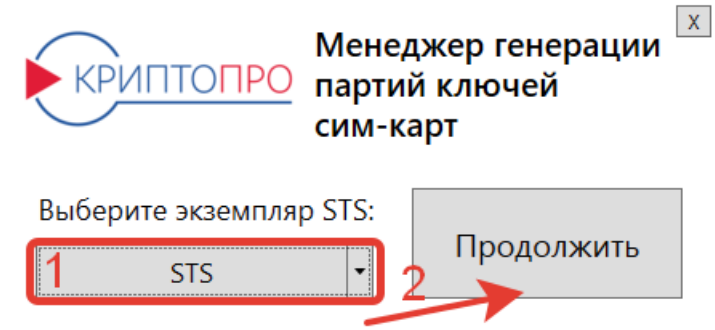
```
#Добавление плагина формирования сообщений
Add-DssStsPlugin -PluginTypeName
"CryptoPro.DSS.SimAuth.Notification.OtaFormatterPlugin,DSS.SimAuth.Notification" -PluginType Formatter –
Settings @{ "UseQuatedValue" = "true" }

#Добавление транспортного плагина
Add-DssStsPlugin –PluginTypeName
"CryptoPro.DSS.SimAuth.Notification.OtaTransportPlugin,DSS.SimAuth.Notification" -PluginType Ota –Settings @{
"Address" = "http://<otaAddress>" }

#Добавление модуля оповещения
Add-DssStsNotifier –TransportPluginId 1 –FormatterPluginId 2 –NotifierType Ota
```

Регистрация партии SIM-карт и профиля криптопровайдера

Создание нового модуля

Запустите от имени администратора утилиту `SimAuthKeysManager.exe`, находящуюся в расположении `C:\Program Files\Crypto Pro\DSS\STS\bin SimAuthKeysManager.exe`.

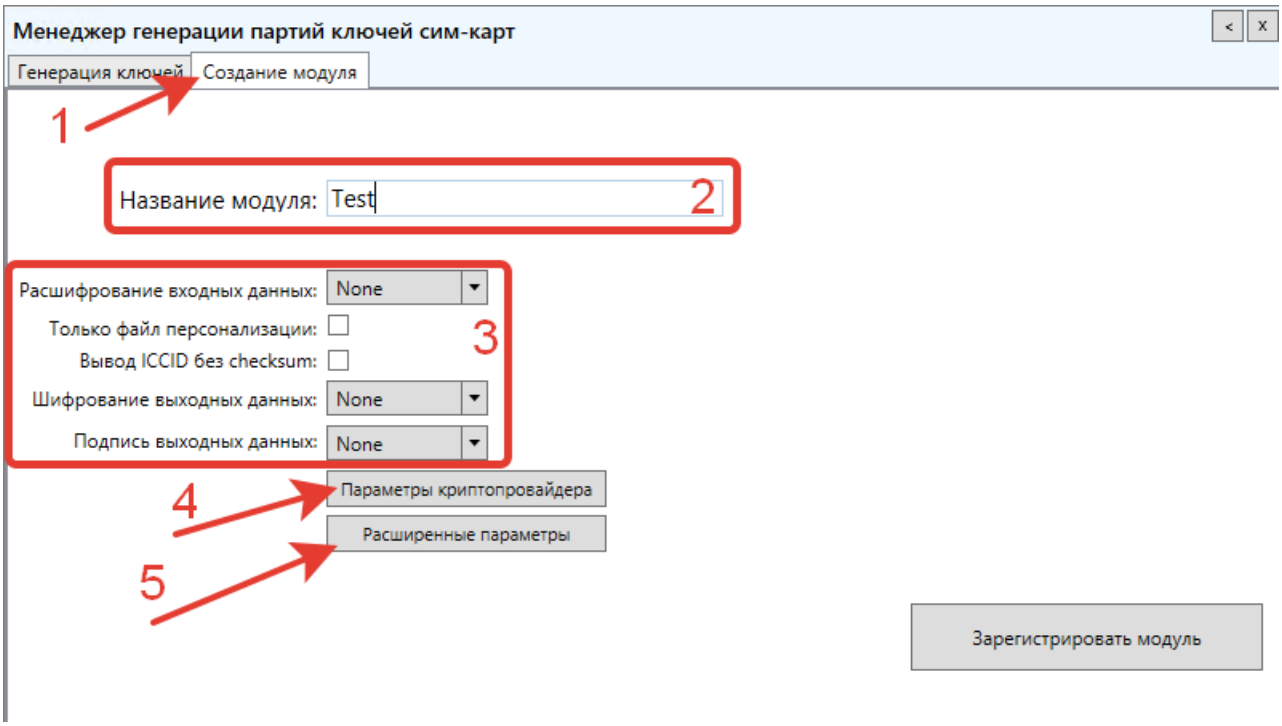
В приветственном окне менеджера генерации партий ключей SIM-карт выберите из выпадающего списка экземпляр Центра Идентификации, на котором будет зарегистрирована партия SIM-карт (1). Нажмите кнопку «Продолжить» (2).



В открывшемся окне перейдите на вкладку «Создание модуля» (1). Введите название модуля в поле «Название модуля» (2). Под модулем в данном случае принято считать набор настроек для формирования файла персонализации партии SIM-карт.

Описание и рекомендации по установке параметров, входящих в блок (3), представлены в таблице ниже.

Шаги (4) и (5) описаны в разделах "Параметры криптопровайдера" и "Расширенные параметры" соответственно.



Параметры модуля

ПАРАМЕТР	ОПИСАНИЕ
Расшифрование входных данных	Изменять не требуется.
Только файл персонализации	Установка данного чекбокса означает, что сгенерированная партия SIM-карт **НЕ БУДЕТ** записана в БД ЦИ DSS. Будет создан только файл персонализации. Используется для повторной генерации одного и того же файла персонализации.
Вывод ICCID без checksum	Изменять не требуется.

ПАРАМЕТР	ОПИСАНИЕ
Шифрование выходных данных	Используется для безопасной передачи файла персонализации производителю SIM-карт. **Возможные значения:** `None` — Без шифрования; `Pgp` — Используется PGP-шифрование. При выборе необходимо в появившемся поле заполнить путь к файлу с открытым ключом получателя. `Cms` — используется CMS-шифрование. При выборе необходимо в появившемся поле заполнить путь к файлу с сертификатом получателя.
Подпись выходных данных	Изменять не требуется.

Параметры криптопровайдера

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 может быть также осуществлено при помощи соответствующих командлетов, однако рекомендуется использовать инструкцию, описанную в настоящем разделе.

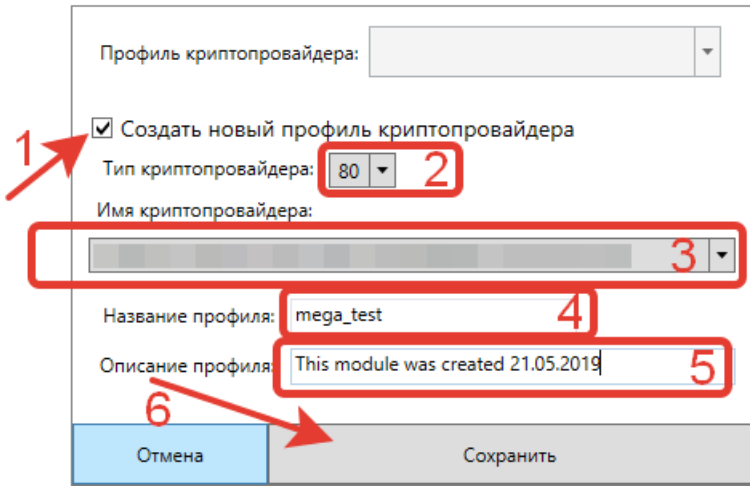
Нажмите на кнопку «Параметры криптопровайдера». В открывшемся окне заполните необходимые поля в соответствии с таблицей ниже.

> **Примечание**
>
> Для каждой новой партии SIM-карт требуется создание нового профиля криптопровайдера.

Параметры криптопровайдера

ПАРАМЕТР	ОПИСАНИЕ
Профиль криптопровайдера	Не заполняется, если требуется создание новой партии SIM-карт.
Создать новый профиль криптопровайдера (1)	Чекбокс должен быть установлен, если требуется создание новой партии SIM-карт.
Тип криптопровайдера (2)	80
Имя криптопровайдера (3)	Crypto-Pro GOST R 34.10-2012 HSM Svc CSP
Название профиля (4)	На усмотрение администратора.
Описание профиля (5)	На усмотрение администратора. Рекомендуется записывать дату создания профиля.

После заполнения всех необходимых полей убедитесь, что кнопка «Сохранить» активна, и нажмите ее (6).



Расширенные параметры

Нажмите на кнопку «Расширенные параметры». В открывшемся окне заполните необходимые поля В СООТВЕТСТВИИ с таблицей "Расширенные параметры". (**ВНИМАНИЕ!** Таблица НЕ описывает параметры, а устанавливает их значения, необходимые для настройки аутентификации).

Примечание

Следующие параметры влияют на список и/или значения параметров «Параметры»:

- Тип профиля генерации ключей (Все значения и описание параметров для профилей Sim3 и M2M см. таблицу "Дополнительные настройки профиля криптопровайдера");
- Профиль генерации ключей (Все значения в зависимости от выбранного шаблона файла персонализации и описание параметров см. таблицу "Шаблоны файла персонализации").

Расширенные параметры

ПАРАМЕТР	ОПИСАНИЕ
Тип профиля генерации ключей	Sim3
Профиль генерации ключей	**Возможные значения:**
	Sim3BasicFixPassword — для партии SIM-карт будет установлен фиксированный код активации.
	Sim3BasicRandomPassword8 — для партии SIM-карт будет установлен случайный код активации* (см. параметр RandomPasswordLength).
	Sim3LegacyFixPassword — фиксированный код активации для обеспечения совместимости с Windows Server 2008 R2
	Sim3LegacyRandomPassword8 — случайный код активации для обеспечения совместимости с Windows Server 2008 R2
Обработчик входных данных	Изменять не требуется.
Генератор ключей	Изменять не требуется.
Обработчик выходных данных	Изменять не требуется.

Параметры	**BlobType** — Изменять не требуется
	BlobVersion — Изменять не требуется
	UseKeyVersion — Изменять не требуется
	PRF — Изменять не требуется
	PasswordFormat — Формат вывода кода активации в файле персонализации: **Numeric** – десятичный, **Hex** - шестнадцатеричный
	IsRandomPassword — Изменять не требуется
	RandomPasswordLength — Длина кода активации (если выбран профиль генерации ключей **Sim3BasicRandomPassword8**. По умолчанию равна 8.
	FixedPassword — Значение фиксированного кода активации
	UseMoKey — Изменять не требуется
	UseMask — Изменять не требуется
	SsdCnt — Счетчик числа использования SSD-ключей. **ДОЛЖЕН** быть равным **0**.
	Header — Заголовок файла персонализации. Изменять не требуется

Дополнительные настройки профиля криптопровайдера (набора Мастер-ключей)

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.

ПАРАМЕТР	ОПИСАНИЕ	ЗНАЧЕНИЕ ПАРАМЕТРА
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.
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.

Шаблоны файла персонализации

ШАБЛОН	ПАРАМЕТР	ЗНАЧЕНИЕ	ОПИСАНИЕ
	BlobType	17	Тип блоба для передачи DCKA-ключа.
	BlobVersion	2	Версия блоба для передачи DCKA-ключа.
	UseKeyVersion	True	Использовать версию при генерации ключей.

BasicFixPassword	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.

После заполнения всех параметров щелкните двойным щелчком по пустой последней строке в столбце «Название» таблицы «Параметры».

Впишите в новое поле в столбце «Название» значение `SsdProfile` (1). **ВНИМАНИЕ! **Поле чувствительно к регистру букв.

Заполните значение для `SsdProfile` (2). Значение данного поля регистрируется на OTA-платформе.

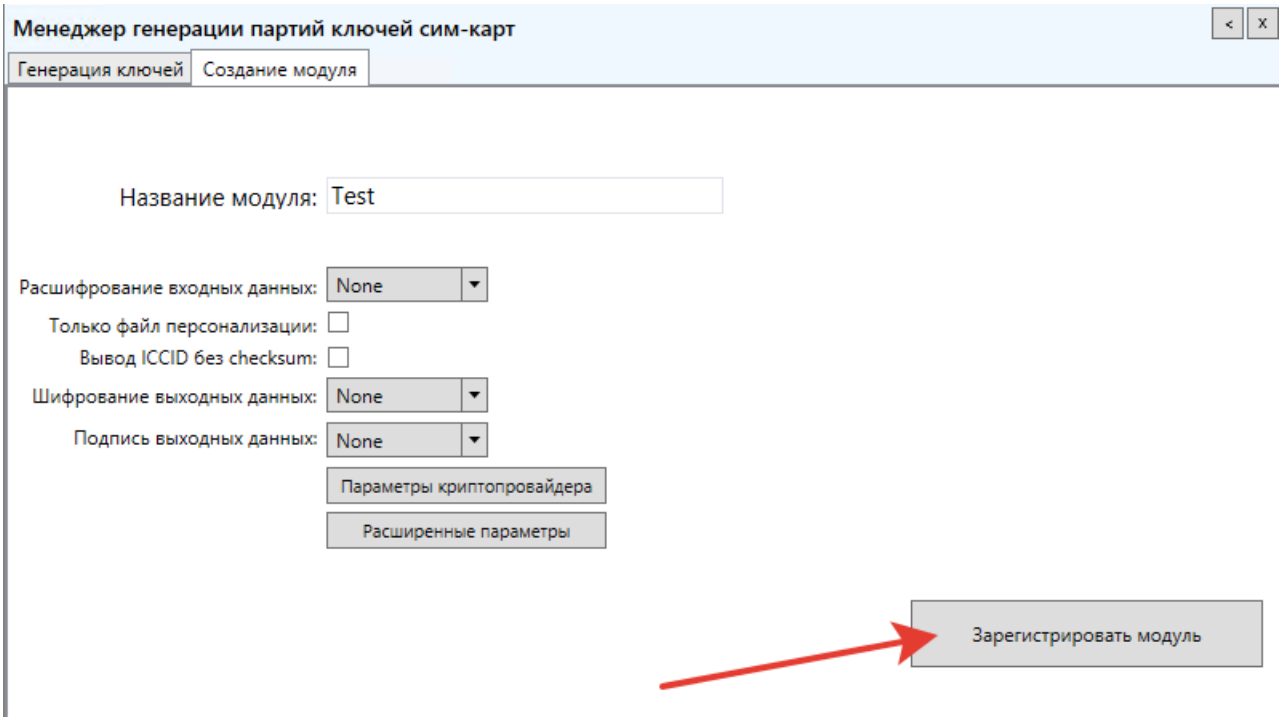
Параметры:

Название	Значение
BlobType	17
BlobVersion	4
UseKeyVersion	true
PRF	AESCMAC
PasswordFormat	numeric
IsRandomPassword	true
RandomPasswordLength	8
UseMoKey	false
UseMask	true
SsdCnt	-1
[illegible]	[illegible]
SsdProfile	1 2

После установки всех параметров, перечисленных в данном разделе, нажмите кнопку «Сохранить».

Регистрация модуля

После выполнения всех действий, описанных ранее, нажмите кнопку «Зарегистрировать модуль» на вкладке «Создание модуля» Менеджера генерации партий ключей SIM-карт.



Генерация файла персонализации

Перейдите на вкладку «Генерация ключей» (1) Менеджера генерации партий ключей SIM-карт, если автоматический переход на нее не произошел после выполнения предыдущего раздела.

Выберите из списка модулей необходимый зарегистрированный модуль (2).

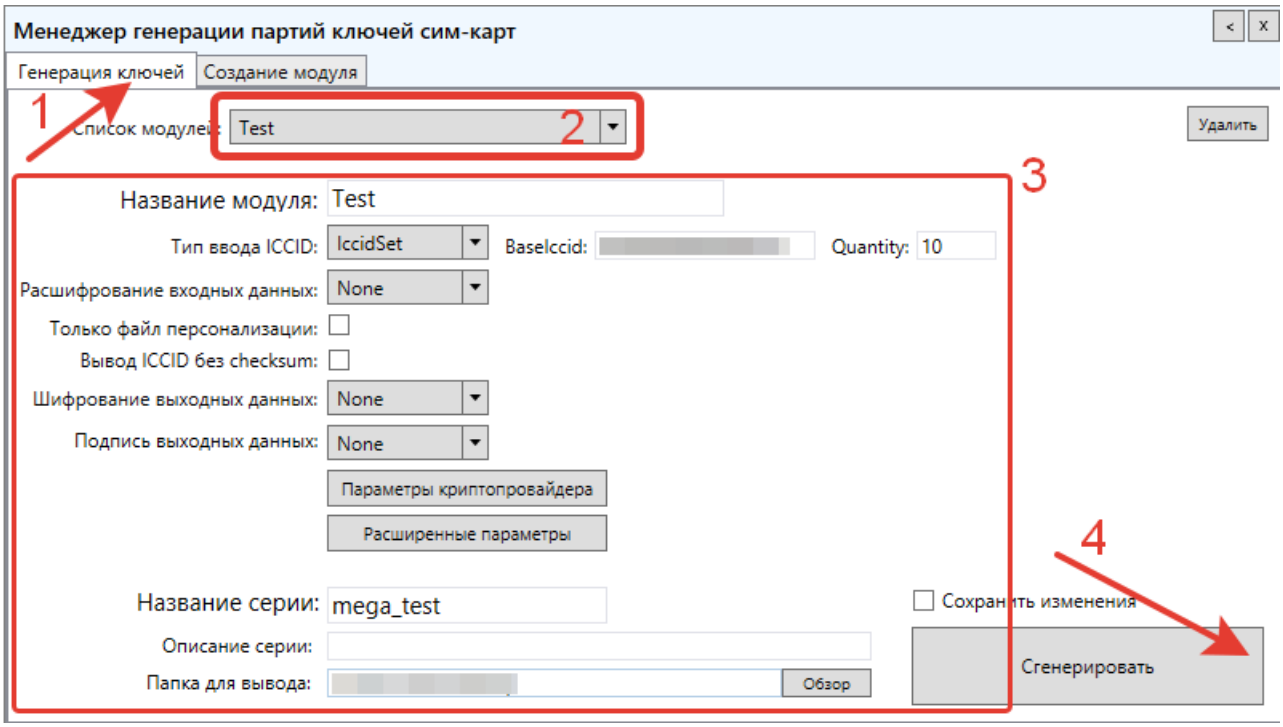
Заполните необходимые поля (3) в соответствии с таблицей ниже.

Генерация ключей

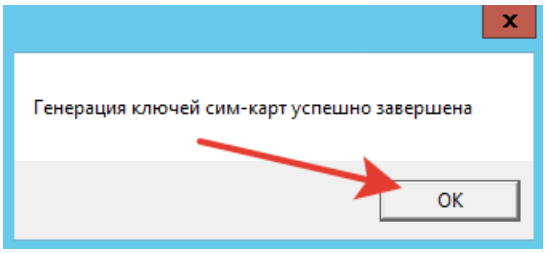
ПАРАМЕТР	ОПИСАНИЕ
Название модуля	Имя зарегистрированного модуля можно изменить перед генерацией ключей.

ПАРАМЕТР	ОПИСАНИЕ
Тип ввода ICCID	IccidSet
BaseIccid	Значение базового ICCID.
Quantity	Количество SIM-карт в партии.
Расшифрование входных данных	Изменять не требуется.
Только файл персонализации	Установка данного чекбокса означает, что сгенерированная партия SIM-карт **НЕ БУДЕТ** записана в БД ЦИ DSS. Будет создан только файл персонализации. Используется для повторной генерации одного и того же файла персонализации.
Вывод ICCID без checksum	Изменять не требуется.
Шифрование выходных данных	Используется для безопасной передачи файла персонализации производителю SIM-карт. **Возможные значения:** `None` — Без шифрования; `Pgp` — Используется PGP-шифрование. При выборе необходимо в появившемся поле заполнить путь к файлу с открытым ключом получателя. `Cms` — используется CMS-шифрование. При выборе необходимо в появившемся поле заполнить путь к файлу с сертификатом получателя.
Подпись выходных данных	Изменять не требуется.
Параметры криптопровайдера	**ИЗМЕНЯТЬ НЕ РЕКОМЕНДУЕТСЯ**. Позволяет изменить используемый модулем профиль криптопровайдера или добавить новый.
Расширенные параметры	**ИЗМЕНЯТЬ НЕ РЕКОМЕНДУЕТСЯ**. Позволяет изменить некоторые параметры, настроенные в разделе "Расширенные параметры".
Название серии	На усмотрение администратора.
Описание серии	На усмотрение администратора. Необязательный параметр.
Папка для вывода	На усмотрение администратора.
Сохранить изменения	Установка данного чекбокса означает, что все изменения, внесенные в данной форме, сохранятся в модуле и изменят настройки, внесенные в разделе "Создание нового модуля". Если чекбокс не установлен, изменения, внесенные в данной форме, применятся только один раз при генерации партии SIM-карт.

После установки всех необходимых параметров нажмите кнопку «Сгенерировать» (4).



В случае успешной генерации партии SIM-карт появится сообщение «Генерация ключей сим-карт успешно завершена». Для завершения генерации ключей нажмите кнопку «OK».



Выйдите из Менеджера генерации партий ключей SIM-карт, нажав красный крестик.

Изменение параметров существующего модуля

Каждое создание файла персонализации новой партии SIM-карт (и регистрации его в DSS) требует создания нового профиля криптопровайдера (набора Мастер-ключей). Для удобства использования не требуется каждый раз создавать новый модуль.

Процедура, описанная в данном разделе, позволяет изменить параметры существующего модуля без повторного заполнения расширенных параметров.

Аналогично разделу "Генерация файла персонализации", перейдите на вкладку «Генерация ключей» (1) Менеджера генерации партий ключей SIM-карт.

Выберите из списка модулей необходимый зарегистрированный ранее модуль (2).

Заполните необходимые поля (3) в соответствии с таблицей "Генерация ключей" в разделе "Генерация файла персонализации".

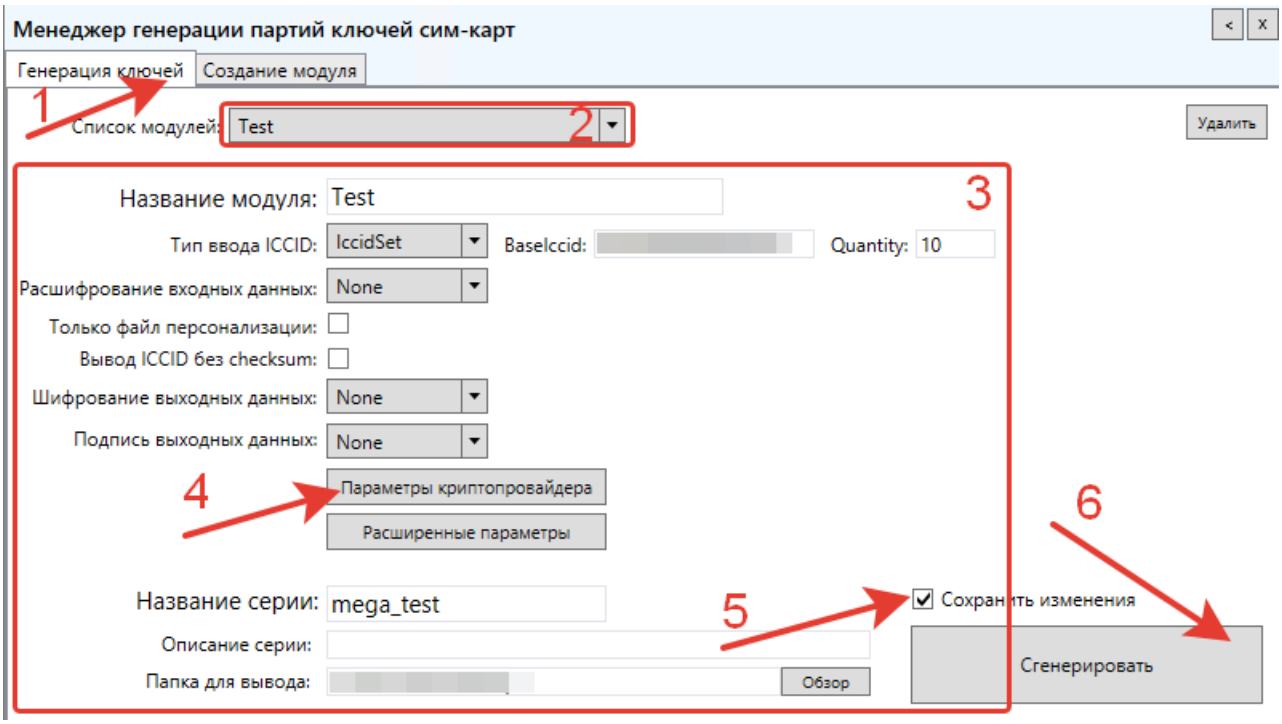
Примечание

Укажите НОВЫЕ значения полей «Название серии» и «Описание серии».

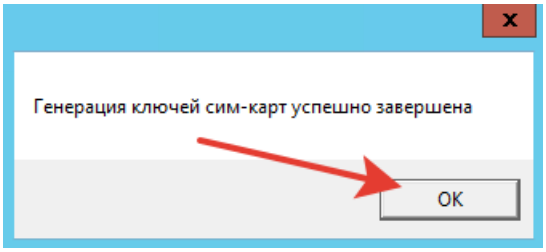
Нажмите на кнопку «Параметры криптопровайдера» (4), чтобы назначить модулю новый профиль криптопровайдера (набор Мастер-ключей). В открывшемся окне выполните все действия аналогично разделу "Параметры криптопровайдера" данного документа.

Установите чекбокс «Сохранить изменения» (5), чтобы перезаписать старые настройки модуля текущими (например, если изменяли расширенные параметры). Если чекбокс не установлен, изменения, внесенные в данной форме, применятся только один раз при генерации партии SIM-карт.

После установки всех необходимых параметров нажмите кнопку «Сгенерировать» (6).



В случае успешной генерации файла персонализации (партии SIM-карт) появится сообщение «Генерация ключей сим-карт успешно завершена». Для завершения нажмите кнопку «OK».



Выйдите из Менеджера генерации партий ключей SIM-карт, нажав красный крестик.

Командлеты для настройки 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`.

Командлеты для настройки профиля криптопровайдера

- Add-DssSimAuthCryptoProviderProfile
- Get-DssSimAuthCryptoProviderProfile
- Remove-DssSimAuthCryptoProviderProfile

Командлеты для настройки криптопровайдеров

Командлеты для настройки криптопровайдеров входят в набор командлетов объекта администрирования "Криптопровайдеры".

Командлеты для просмотра сведений о зарегистрированных SIM-картах

- Get-DssTokenProfile

Используется для вывода на консоль сведений о зарегистрированных в DSS партиях SIM-карт. При этом в столбец `Vendor`

помещается значение поля «Название серии», в столбец `Model` — значение поля «Описание серии».

- Remove-DssTokenProfile

Используется для удаления зарегистрированных в DSS партий SIM-карт.

- Get-DssAuthenticationToken

Используется для вывода на консоль сведений о SIM-картах, содержащихся в партии.

Аутентификация с использованием одноразовых паролей

Дополнительные способы аутентификации

При использовании аутентификации только по логину и паролю или аутентификации по сертификату возможно назначить дополнительные способы аутентификации:

- аутентификация с использованием одноразового пароля, доставляемого через SMS-сообщение (OTP-via-SMS).

При использовании данного метода для подтверждения входа и операций у Пользователя дополнительно будет запрашиваться ввод одноразового пароля, доставляемого в SMS-сообщении на телефон Пользователя.

- аутентификация с использованием одноразового пароля, доставляемого через EMAIL (OTP-via-EMAIL).

При использовании данного метода для подтверждения входа и операций дополнительно у Пользователя будет запрашиваться ввод одноразового пароля, доставляемого по электронной почте.

> **Примечание**
>
> Дополнительные способы аутентификации в КриптоПро DSS являются вспомогательными и не ослабляют требований первичной аутентификации.

Общие настройки одноразовых паролей

К управлению одноразовыми паролями относится следующий набор параметров, задаваемых через командлет Set-DssPasswordPolicy:

- `-InvalidOtpAttempts`,
- `-TransactionTimeOut`,
- `-OtpComplexity`,
- `-OtpLength`

и командлет Set-DssStsProperties:

- `-OtpConfirmationTimeOut`,
- `-MinOtpConfirmationTimeOut`.

`OtpComplexity` и `OtpLength` определяют сложность и длину одноразовых паролей, передаваемых через SMS или Email. По умолчанию создаются одноразовые 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`. Также данный параметр устанавливает таймаут до повторной операции с подтверждением, если предыдущее подтверждение Пользователь отменил самостоятельно. 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 и операции с подтверждением без ограничений.

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.

Настройка аутентификации с использование 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.

> **Примечание**
>
> Данный вид вспомогательной аутентификации требует подключения к SMS-шлюзу оператора сотовой связи в соответствии со схемой размещения компонентов (см раздел 6.3 ЖТЯИ.00096-02 96 02 КриптоПро DSS. Общее описание) и в соответствии с требованиями к подключению к сетям общего пользования, описанными в разделе 10 ЖТЯИ.00096-02 95 01 КриптоПро HSM. 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.

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 параметры `-PhoneConfirmation` и `-PhoneConfirmationByOperator` позволяют включить или отключить подтверждение номера телефона.

Пример:

```
Set-DssStsProperties -PhoneConfirmation $true
```

ИЛИ

```
Set-DssStsProperties -PhoneConfirmationByOperator $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 потребуется, если параметр `-PhoneConfirmationByOperator` = True.

Настройка аутентификации с использование одноразовых Email-паролей

При использовании данного метода для подтверждения входа и операций дополнительно у Пользователя будет запрашиваться ввод одноразового пароля, доставляемого по электронной почте.

> **Примечание**
>
> Данный вид вспомогательной аутентификации требует подключения к почтовому серверу в соответствии со схемой размещения компонентов (см раздел 6.3 ЖТЯИ.00096-02 96 02 КриптоПро DSS. Общее описание) и в соответствии с требованиями к подключению к сетям общего пользования, описанными в разделе 10 ЖТЯИ.00096-02 95 01 КриптоПро HSM. 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.

Для успешной аутентификации в профиле Пользователя должен быть задан адрес электронной почты.

Настройка оповещения

СЭП «КриптоПро DSS» позволяет настроить оповещение Пользователей и Операторов о различных событиях системы. Также события могут заноситься в журнал Сервиса Аудита.

> **Примечание**
>
> 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.00096-02 96 02 КриптоПро DSS. Общее описание) и в соответствии с требованиями к подключению к сетям общего пользования, описанными в разделе 10 документа ЖТЯИ.00096-02 95 01 КриптоПро HSM. Правила пользования.

В этом разделе:

Принцип работы системы оповещения

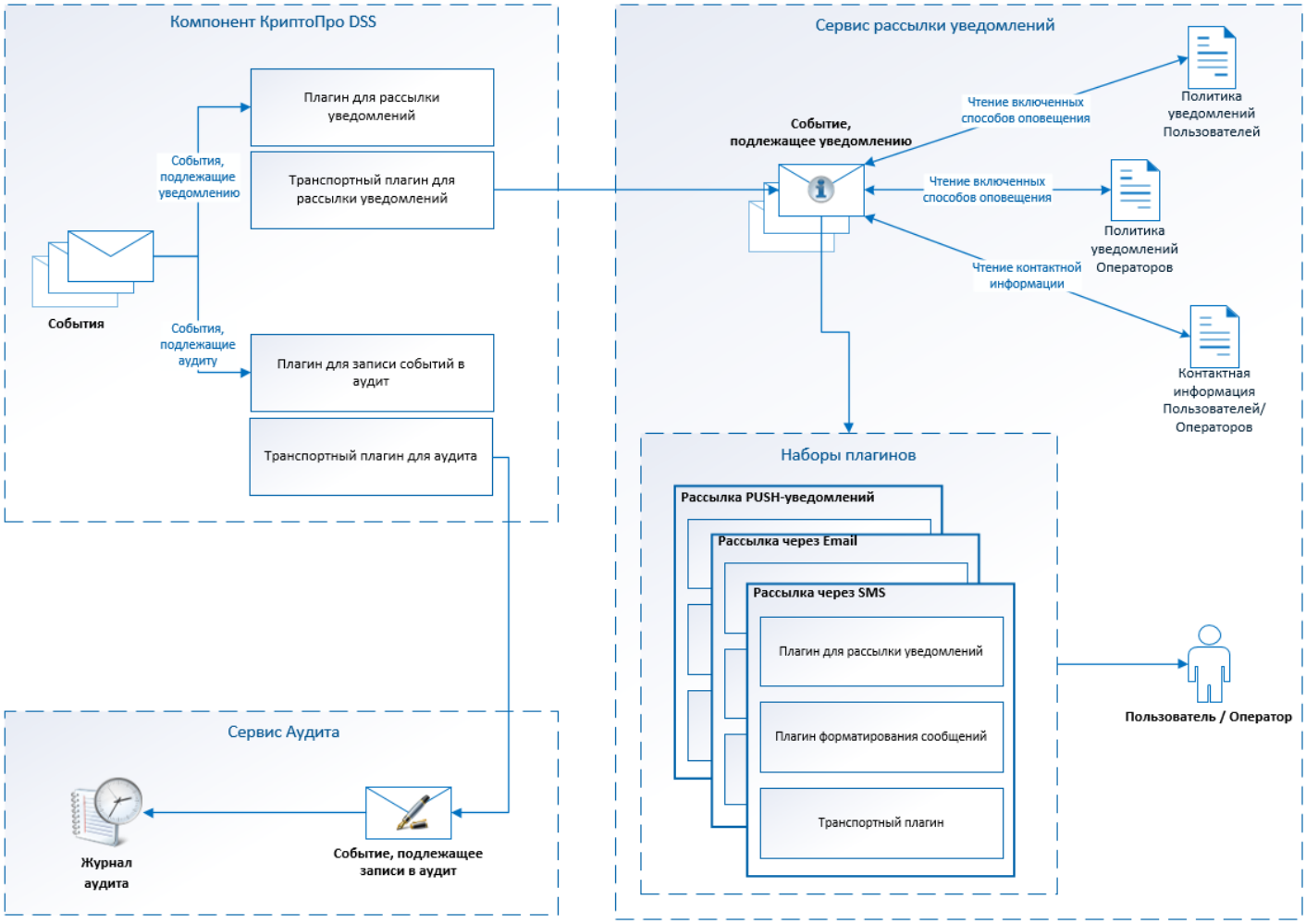
Система оповещения КриптоПро DSS позволяет уведомлять различными способами Пользователей и Операторов о событиях, происходящих на следующих компонентах:

- Центр Идентификации;
- Сервис Подписи;
- Сервис Обработки Документов;
- модуль аутентификации myDSS (PUSH-уведомления для подтверждения операций).

При этом используется разделение событий на два основных потока:

- события, подлежащие уведомлению, отправляются на Сервис рассылки уведомлений (`Notification Service`), откуда могут быть доставлены Пользователям и Операторам в соответствии с политиками оповещения;
- события, подлежащие записи в журнал аудита, отправляются на Сервис Аудита.

Некоторые события могут отправляться как в аудит, так и на Сервис рассылки уведомлений.



Настройка оповещения Пользователей и/или Операторов

Пользователи и Операторы КриптоПро DSS могут быть оповещены о событиях Центра Идентификации, Сервиса Подписи и myDSS посредством SMS-сообщений, электронной почты и PUSH-уведомлений (в мобильном приложении myDSS при использовании данного метода аутентификации).

Примечание

События Сервиса Обработки Документов предназначены исключительно для записи в журнал аудита. Оповещение указанными выше способами об этих событиях не производится.

Настройка оповещения Пользователей и/или Операторов о событиях КриптоПро DSS производится следующим образом.

1. Регистрация плагинов для доставки событий на Сервис рассылки уведомлений.

Все события КриптоПро DSS, предназначенные для отправки Пользователям и Операторам, должны быть переданы в Сервис рассылки уведомлений. Сервис рассылки уведомлений является частью Центра Идентификации и разворачивается автоматически при создании экземпляра. Для передачи событий на Сервис рассылки уведомлений необходимо зарегистрировать **на том компоненте, с которого собираются события**, следующие плагины:

Для событий Центра Идентификации:

- `Add-DssStsPlugin` - регистрация транспортного плагина.
- `Add-DssStsNotifier` - регистрация модуля рассылки уведомлений.

```
$hostname = <hostname>
$STSappName = "STS"

# Регистрация транспортного плагина
$plugin = Add-DssStsPlugin –PluginTypeName
"DSS.Notification.Transport.NotificationTransportPlugin,DSS.Notification.Transport" -PluginType
NotificationService -Settings @{ServiceAddress="https://$hostname/$STSappName/"}

# Регистрация модуля оповещения
Add-DssStsNotifier -TransportPluginID $plugin.ID -NotifierType NotificationService
```

Для событий Сервиса Подписи:

- `Add-DssSignServerPlugin` - регистрация транспортного плагина.
- `Add-DssSignServerNotifier` - регистрация модуля рассылки уведомлений.
- Транспортный плагин - командлет `Add-DssSignServerPlugin`.

```
$hostname = <hostname>
$STSappName = "STS"

$plugin = Add-DssSignServerPlugin –PluginTypeName
"DSS.Notification.Transport.NotificationTransportPlugin,DSS.Notification.Transport" -PluginType
NotificationService -Settings @{ServiceAddress="https://$hostname/$STSappName/"}

Add-DssSignServerNotifier -TransportPluginID $plugin.ID -NotifierType NotificationService
```

Для событий DSS SDK:

Используются собственные командлеты.

Для событий Сервиса Обработки Документов:

События Сервиса Обработки Документов предназначены только для записи в журнал аудита.

`Дополнительные настройки плагинов для доставки событий на Сервис рассылки уведомлений`

Плагины для доставки событий на Сервис рассылки уведомлений имеют также дополнительные параметры. Полный список доступных настроек:

Транспортный плагин (командлет Add(Set)-Dss...Plugin):

- `ServiceAddress` - адрес Сервиса рассылки уведомлений в формате "http(s)://<Sts hostname>/<StsAppName>/".
- `UseMutualTlsFlag` - флаг ('True' или 'False'), включающий использование конечной точки `notifications/cert` на Сервисе рассылки уведомлений. Использование данной конечной точки позволяет подключаться к ней по протоколу TLS, используя сервисный сертификат компонента, на котором регистрируется транспортный плагин.

Плагин рассылки уведомлений (командлет Add(Set)-Dss...Notifier):

- `MinQueueSize` – приемлемый размер очереди сообщений. При превышении 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 в мс. По умолчанию параметр равен `500`.
- `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. По умолчанию включен.

2. Настройка политик оповещения Пользователей и/или Операторов.

Политики оповещения

События, отправленные с компонентов DSS при помощи настроенных ранее плагинов, доставляются на Сервис рассылки уведомлений. Здесь происходит получение информации о доступных способах доставки (Email, SMS, PUSH), а также контактной информации из профиля Пользователя или Оператора, которому должно быть доставлено уведомление. Для получения данной информации необходимо настроить политику оповещения для Пользователей и Операторов.

Политика оповещения Пользователей

Политика оповещения Пользователей состоит из трех уровней:

- глобального,
- уровня группы,
- уровня Пользователя (настройка доступна только через веб- и REST-интерфейсы).

Политика оповещения Пользователей заполняется при помощи командлета Set-DssNotificationPolicy и представляет собой набор следующих настроек:

ПАРАМЕТР	ТИП	ОПИСАНИЕ
Type	`User`	Определяет, для кого настраивается политика.
Notifiers	`SMS, Email, PUSH` (1 или несколько через запятую)	Список назначений для отправки уведомлений о событиях, указанных в параметре `Notifiers`.
GroupID	int	Идентификатор группы, если необходимо настроить политику уровня группы.
NotificationEvents	`AllNotificationEvents` ИЛИ `Notifiers {}` (пустой список) ИЛИ `Notifiers` (1 или несколько через запятую)	Набор событий, о которых необходимо оповещать.
AllowChangeByOperator	bool	Определяет, может ли Оператор изменять политику оповещения Пользователя в веб-интерфейсе.
AllowChangeByUser	bool	Определяет, может ли Пользователь изменять политику оповещения в веб-интерфейсе.
AllowOverride	bool	Определяет, может ли политика быть переопределена на более низком уровне иерархии.

Примечание

В зависимости от того, политика какого уровня настраивается — глобального уровня или уровня группы — необходимо также соответственно использовать параметр `-GroupId` со значением идентификатора настраиваемой группы. Для заполнения глобальной политики специальный параметр указывать не требуется.

Если в иерархии политик есть политика с `AllowOverride` = `false`, настройки политики уровнем ниже не имеют силы. Если все политики в иерархии имеют `AllowOverride` = `true`, параметры `AllowChangeByUser` и `AllowChangeByOperator` используются из политики группы, а настройка самого оповещения применяется индивидуально для каждого Пользователя (настраивается в Веб-интерфейсе Пользователя).

Примечание

Перед изменением настроек политики оповещения при помощи командлетов (глобальный уровень или уровень группы), убедитесь, что на уровень выше не применялось значение `AllowOverride` = `false`.

Политика оповещения Операторов

Политика оповещения Операторов состоит из двух уровней:

- глобального,
- уровня Оператора (настройка доступна только через веб- и REST-интерфейсы).

Политика оповещения Пользователей заполняется при помощи командлета Set-DssNotificationPolicy и представляет собой набор следующих настроек:

ПАРАМЕТР	ТИП	ОПИСАНИЕ
Type	`Operator`	Определяет, для кого настраивается политика.
Notifiers	`SMS, Email` (1 или оба через запятую)	Список назначений для отправки уведомлений о событиях, указанных в параметре `Notifiers`.
NotificationEvents	`AllNotificationEvents` ИЛИ `{}` (пустой список) ИЛИ `Notifiers` (1 или несколько через запятую)	Набор событий, о которых необходимо оповещать.
AllowChangeByOperator	bool	Определяет, может ли Оператор изменять политику оповещения в веб-интерфейсе.
AllowOverride	bool	Определяет, может ли политика быть переопределена на более низком уровне иерархии.

Если в глобальной политике имеется значение `AllowOverride` = `false`, настройки политики уровня Оператора на веб-интерфейсе будут недоступны. Если глобальная политика `AllowOverride` = `true`, параметр `AllowChangeByOperator` применяется индивидуально для каждого Оператора (настраивается в его личном кабинете на веб-интерфейсе или при помощи REST API).

Примеры:

Примечание

Примеры составлены для случая, когда редактируется политика оповещения Пользователей. Для редактирования политики оповещения Операторов следует указывать параметр `-Type Operator` и **НЕ использовать** параметр `-GroupId <ID группы>`.

Получение политики оповещения Пользователей по уровням:

```
# Получение глобальной политики:
Get-DssNotificationPolicy -Type User
# Если в выводе данной команды содержится AllowOverride = False,
# настройки уровня группы не имеют силы.

# Получение политики группы Пользователей
Get-DssNotificationPolicy -Type User -GroupId 1
# Если в выводе данной команды содержится AllowOverride = False,
# Пользователь не сможет изменить политику доступа к операциям в Веб-
# интерфейсе.

# Просмотр списка событий с указанием настроенных способов доставки для каждого события:
(Get-DssNotificationPolicy -Type User ).EventNotifiers
```

Настройка политики оповещения Пользователей:

```
# Оповещать Пользователей о всех событиях:
Set-DssNotificationPolicy -Type User -AllNotificationEvents -Notifiers SMS,Email -AllowOverride 0

# НЕ оповещать Пользователей ни о каких событиях:
Set-DssNotificationPolicy -Type User -AllNotificationEvents -Notifiers @() -AllowOverride 0

# Указать набор событий, о которых необходимо оповещать Пользователей:
Set-DssNotificationPolicy -Type User -NotificationEvents CertificateCreated,DeviceConfirmed -Notifiers
SMS,Email

ИЛИ

Set-DssNotificationPolicy -Type User -NotificationEvents 1, 2 -Notifiers SMS,Email

# Выбор способа доставки для всех событий SMS и Email:
Set-DssNotificationPolicy –Type User -AllNotificationEvents -Notifiers SMS,Email
```

Примечание

В случае, если необходимо изменить политику группы, следует добавлять параметр `-GroupId <ID группы>`.

Примечание

Если для какого-либо события уже был задан параметр `-Notifiers`, следующее его заполнение для данного события перезапишет все указанные способы доставки. Т.е. при изменении данного параметра каждый раз нужно указывать все необходимые способы доставки.

Отключение оповещения обо всех событиях

Для того чтобы отключить оповещение обо всех событиях необходимо в параметре `Notifier` передать пустой список типов оповещения.

Примечание

Отключение оповещения обо всех событиях необходимо выполнить перед настройкой оповещение **только** о выделенных событиях.

```
Set-DssNotificationPolicy -Type User -AllNotificationEvents -GroupId 1 -Notifier @()
```

Полный список событий и их кодов.

3. Задание контактной информации Пользователей и/или Операторов.

Наличие контактной информации Пользователей и/или Операторов необходимо для корректной работы системы оповещения. В зависимости от выбранного способа оповещения (Email, SMS) в профиле Пользователя или Оператора

должны быть указаны соответствующие номера телефонов или адрес электронной почты. Заполнение контактной информации возможно следующими способами:

- **Для Пользователей** - посредством REST API или непосредственно Пользователем в Личном кабинете на веб-интерфейсе.
- **Для Операторов** - при помощи специализированных командлетов.

4. Регистрация набора плагинов для определенного способа рассылки.

Как только для события получены способы доставки и контактная информация, производится его отправка. Для отправки должны быть зарегистрированы следующие плагины:

- **Плагин форматирования сообщений** - командлеты `Add-DssStsPlugin`, `Add-DssStsPlugin` с параметром `-PluginType Formatter` `-PluginTypeName "<имя класса>,<имя сборки>"`
- **Транспортный плагин** - командлеты `Add-DssStsPlugin`, `Add-DssStsPlugin` с параметром `-PluginType Email` или `-PluginType Sms` в зависимости от выбранного способа доставки;
- **Плагин рассылки уведомлений** - командлет `Add-DssInternalNotifier` с параметрами `-NotifierType Email` или `-NotifierType Sms` в зависимости от выбранного способа доставки, `-TransportPluginID <ID транспортного плагина>`, `-FormatterPluginID <ID плагина формирования сообщений>`.

Пример настройки оповещения Пользователей по Email

Пример настройки уведомлений по SMS

Для описанных способов оповещения установлены шаблоны сообщений. Администратор может их изменять при помощи специализированных командлетов.

Настройка PUSH-уведомлений и их шаблонов

5. Включение/отключение оповещения

После выполнения всех перечисленных выше действий оповещение будет настроено и включено автоматически. Для отключения оповещения можно использовать следующие способы:

- Убрать контактную информацию Пользователя/Оператора, с которой связаны настройки оповещения.
- Запретить отправку уведомлений в политике оповещения.
- Отключить плагин рассылки уведомлений (см. п.4) при помощи командлета Disable-DssInternalNotifier. Включить плагин возможно при помощи командлета Enable-DssInternalNotifier.

Настройка записи событий в аудит

Плагины, необходимые для отправки и записи сообщений в журнал аудита, регистрируются при помощи командлетов вида `New-Dss...Audit`.

Настройка оповещения

СЭП «КриптоПро DSS» позволяет настроить оповещение Пользователей и Операторов о различных событиях системы. Также события могут заноситься в журнал Сервиса Аудита.

> **Примечание**
>
> 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.00096-02 96 02 КриптоПро DSS. Общее описание) и в соответствии с требованиями к подключению к сетям общего пользования, описанными в разделе 10 документа ЖТЯИ.00096-02 95 01 КриптоПро HSM. Правила пользования.

В этом разделе:

Принцип работы системы оповещения

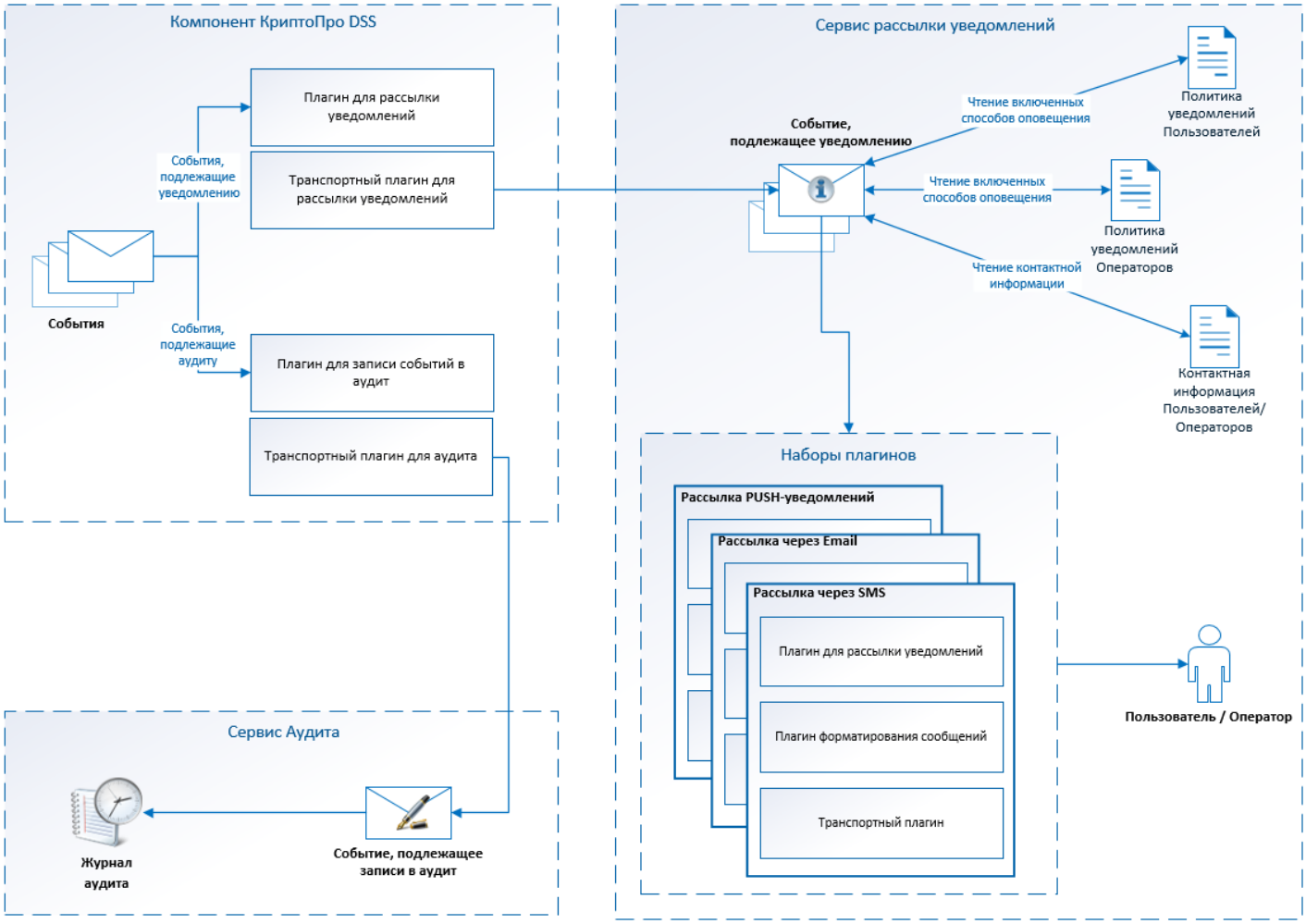
Система оповещения КриптоПро DSS позволяет уведомлять различными способами Пользователей и Операторов о событиях, происходящих на следующих компонентах:

- Центр Идентификации;
- Сервис Подписи;
- Сервис Обработки Документов;
- модуль аутентификации myDSS (PUSH-уведомления для подтверждения операций).

При этом используется разделение событий на два основных потока:

- события, подлежащие уведомлению, отправляются на Сервис рассылки уведомлений (`Notification Service`), откуда могут быть доставлены Пользователям и Операторам в соответствии с политиками оповещения;
- события, подлежащие записи в журнал аудита, отправляются на Сервис Аудита.

Некоторые события могут отправляться как в аудит, так и на Сервис рассылки уведомлений.



Настройка оповещения Пользователей и/или Операторов

Пользователи и Операторы КриптоПро DSS могут быть оповещены о событиях Центра Идентификации, Сервиса Подписи и myDSS посредством SMS-сообщений, электронной почты и PUSH-уведомлений (в мобильном приложении myDSS при использовании данного метода аутентификации).

Примечание

События Сервиса Обработки Документов предназначены исключительно для записи в журнал аудита. Оповещение указанными выше способами об этих событиях не производится.

Настройка оповещения Пользователей и/или Операторов о событиях КриптоПро DSS производится следующим образом.

1. Регистрация плагинов для доставки событий на Сервис рассылки уведомлений.

Все события КриптоПро DSS, предназначенные для отправки Пользователям и Операторам, должны быть переданы в Сервис рассылки уведомлений. Сервис рассылки уведомлений является частью Центра Идентификации и разворачивается автоматически при создании экземпляра. Для передачи событий на Сервис рассылки уведомлений необходимо зарегистрировать **на том компоненте, с которого собираются события**, следующие плагины:

Для событий Центра Идентификации:

- `Add-DssStsPlugin` - регистрация транспортного плагина.
- `Add-DssStsNotifier` - регистрация модуля рассылки уведомлений.

```
$hostname = <hostname>
$STSappName = "STS"

# Регистрация транспортного плагина
$plugin = Add-DssStsPlugin –PluginTypeName
"DSS.Notification.Transport.NotificationTransportPlugin,DSS.Notification.Transport" -PluginType
NotificationService -Settings @{ServiceAddress="https://$hostname/$STSappName/"}

# Регистрация модуля оповещения
Add-DssStsNotifier -TransportPluginID $plugin.ID -NotifierType NotificationService
```

Для событий Сервиса Подписи:

- `Add-DssSignServerPlugin` - регистрация транспортного плагина.
- `Add-DssSignServerNotifier` - регистрация модуля рассылки уведомлений.
- Транспортный плагин - командлет `Add-DssSignServerPlugin`.

```
$hostname = <hostname>
$STSappName = "STS"

$plugin = Add-DssSignServerPlugin –PluginTypeName
"DSS.Notification.Transport.NotificationTransportPlugin,DSS.Notification.Transport" -PluginType
NotificationService -Settings @{ServiceAddress="https://$hostname/$STSappName/"}

Add-DssSignServerNotifier -TransportPluginID $plugin.ID -NotifierType NotificationService
```

Для событий DSS SDK:

Используются собственные командлеты.

Для событий Сервиса Обработки Документов:

События Сервиса Обработки Документов предназначены только для записи в журнал аудита.

Дополнительные настройки плагинов для доставки событий на Сервис рассылки уведомлений

Плагины для доставки событий на Сервис рассылки уведомлений имеют также дополнительные параметры. Полный список доступных настроек:

Транспортный плагин (командлет Add(Set)-Dss...Plugin):

- `ServiceAddress` - адрес Сервиса рассылки уведомлений в формате "http(s)://<Sts hostname>/<StsAppName>/".
- `UseMutualTlsFlag` - флаг ('True' или 'False'), включающий использование конечной точки `notifications/cert` на Сервисе рассылки уведомлений. Использование данной конечной точки позволяет подключаться к ней по протоколу TLS, используя сервисный сертификат компонента, на котором регистрируется транспортный плагин.

Плагин рассылки уведомлений (командлет Add(Set)-Dss...Notifier):

- `MinQueueSize` – приемлемый размер очереди сообщений. При превышении 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 в мс. По умолчанию параметр равен `500`.
- `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. По умолчанию включен.

2. Настройка политик оповещения Пользователей и/или Операторов.

Политики оповещения

События, отправленные с компонентов DSS при помощи настроенных ранее плагинов, доставляются на Сервис рассылки уведомлений. Здесь происходит получение информации о доступных способах доставки (Email, SMS, PUSH), а также контактной информации из профиля Пользователя или Оператора, которому должно быть доставлено уведомление. Для получения данной информации необходимо настроить политику оповещения для Пользователей и Операторов.

Политика оповещения Пользователей

Политика оповещения Пользователей состоит из трех уровней:

- глобального,
- уровня группы,
- уровня Пользователя (настройка доступна только через веб- и REST-интерфейсы).

Политика оповещения Пользователей заполняется при помощи командлета Set-DssNotificationPolicy и представляет собой набор следующих настроек:

ПАРАМЕТР	ТИП	ОПИСАНИЕ
Type	`User`	Определяет, для кого настраивается политика.
Notifiers	`SMS, Email, PUSH` (1 или несколько через запятую)	Список назначений для отправки уведомлений о событиях, указанных в параметре `Notifiers`.
GroupID	int	Идентификатор группы, если необходимо настроить политику уровня группы.
NotificationEvents	`AllNotificationEvents` ИЛИ `Notifiers {}` (пустой список) ИЛИ `Notifiers` (1 или несколько через запятую)	Набор событий, о которых необходимо оповещать.
AllowChangeByOperator	bool	Определяет, может ли Оператор изменять политику оповещения Пользователя в веб-интерфейсе.
AllowChangeByUser	bool	Определяет, может ли Пользователь изменять политику оповещения в веб-интерфейсе.
AllowOverride	bool	Определяет, может ли политика быть переопределена на более низком уровне иерархии.

Примечание

В зависимости от того, политика какого уровня настраивается — глобального уровня или уровня группы — необходимо также соответственно использовать параметр `-GroupId` со значением идентификатора настраиваемой группы. Для заполнения глобальной политики специальный параметр указывать не требуется.

Если в иерархии политик есть политика с `AllowOverride` = `false`, настройки политики уровнем ниже не имеют силы. Если все политики в иерархии имеют `AllowOverride` = `true`, параметры `AllowChangeByUser` и `AllowChangeByOperator` используются из политики группы, а настройка самого оповещения применяется индивидуально для каждого Пользователя (настраивается в Веб-интерфейсе Пользователя).

Примечание

Перед изменением настроек политики оповещения при помощи командлетов (глобальный уровень или уровень группы), убедитесь, что на уровень выше не применялось значение `AllowOverride` = `false`.

Политика оповещения Операторов

Политика оповещения Операторов состоит из двух уровней:

- глобального,
- уровня Оператора (настройка доступна только через веб- и REST-интерфейсы).

Политика оповещения Пользователей заполняется при помощи командлета Set-DssNotificationPolicy и представляет собой набор следующих настроек:

ПАРАМЕТР	ТИП	ОПИСАНИЕ
Type	`Operator`	Определяет, для кого настраивается политика.
Notifiers	`SMS, Email` (1 или оба через запятую)	Список назначений для отправки уведомлений о событиях, указанных в параметре `Notifiers`.
NotificationEvents	`AllNotificationEvents` ИЛИ `{}` (пустой список) ИЛИ `Notifiers` (1 или несколько через запятую)	Набор событий, о которых необходимо оповещать.
AllowChangeByOperator	bool	Определяет, может ли Оператор изменять политику оповещения в веб-интерфейсе.
AllowOverride	bool	Определяет, может ли политика быть переопределена на более низком уровне иерархии.

Если в глобальной политике имеется значение `AllowOverride` = `false`, настройки политики уровня Оператора на веб-интерфейсе будут недоступны. Если глобальная политика `AllowOverride` = `true`, параметр `AllowChangeByOperator` применяется индивидуально для каждого Оператора (настраивается в его личном кабинете на веб-интерфейсе или при помощи REST API).

Примеры:

Примечание

Примеры составлены для случая, когда редактируется политика оповещения Пользователей. Для редактирования политики оповещения Операторов следует указывать параметр `-Type Operator` и **НЕ использовать** параметр `-GroupId <ID группы>`.

Получение политики оповещения Пользователей по уровням:

```
# Получение глобальной политики:
Get-DssNotificationPolicy -Type User
# Если в выводе данной команды содержится AllowOverride = False,
# настройки уровня группы не имеют силы.

# Получение политики группы Пользователей
Get-DssNotificationPolicy -Type User -GroupId 1
# Если в выводе данной команды содержится AllowOverride = False,
# Пользователь не сможет изменить политику доступа к операциям в Веб-
# интерфейсе.

# Просмотр списка событий с указанием настроенных способов доставки для каждого события:
(Get-DssNotificationPolicy -Type User ).EventNotifiers
```

Настройка политики оповещения Пользователей:

```
# Оповещать Пользователей о всех событиях:
Set-DssNotificationPolicy -Type User -AllNotificationEvents -Notifiers SMS,Email -AllowOverride 0

# НЕ оповещать Пользователей ни о каких событиях:
Set-DssNotificationPolicy -Type User -AllNotificationEvents -Notifiers @() -AllowOverride 0

# Указать набор событий, о которых необходимо оповещать Пользователей:
Set-DssNotificationPolicy -Type User -NotificationEvents CertificateCreated,DeviceConfirmed -Notifiers
SMS,Email

ИЛИ

Set-DssNotificationPolicy -Type User -NotificationEvents 1, 2 -Notifiers SMS,Email

# Выбор способа доставки для всех событий SMS и Email:
Set-DssNotificationPolicy –Type User -AllNotificationEvents -Notifiers SMS,Email
```

Примечание

В случае, если необходимо изменить политику группы, следует добавлять параметр `-GroupId <ID группы>`.

Примечание

Если для какого-либо события уже был задан параметр `-Notifiers`, следующее его заполнение для данного события перезапишет все указанные способы доставки. Т.е. при изменении данного параметра каждый раз нужно указывать все необходимые способы доставки.

Отключение оповещения обо всех событиях

Для того чтобы отключить оповещение обо всех событиях необходимо в параметре `Notifier` передать пустой список типов оповещения.

Примечание

Отключение оповещения обо всех событиях необходимо выполнить перед настройкой оповещение **только** о выделенных событиях.

```
Set-DssNotificationPolicy -Type User -AllNotificationEvents -GroupId 1 -Notifier @()
```

Полный список событий и их кодов.

3. Задание контактной информации Пользователей и/или Операторов.

Наличие контактной информации Пользователей и/или Операторов необходимо для корректной работы системы оповещения. В зависимости от выбранного способа оповещения (Email, SMS) в профиле Пользователя или Оператора

должны быть указаны соответствующие номера телефонов или адрес электронной почты. Заполнение контактной информации возможно следующими способами:

- **Для Пользователей** - посредством REST API или непосредственно Пользователем в Личном кабинете на веб-интерфейсе.
- **Для Операторов** - при помощи специализированных командлетов.

4. Регистрация набора плагинов для определенного способа рассылки.

Как только для события получены способы доставки и контактная информация, производится его отправка. Для отправки должны быть зарегистрированы следующие плагины:

- **Плагин форматирования сообщений** - командлеты `Add-DssStsPlugin`, `Add-DssStsPlugin` с параметром `-PluginType Formatter` `-PluginTypeName "<имя класса>,<имя сборки>"`
- **Транспортный плагин** - командлеты `Add-DssStsPlugin`, `Add-DssStsPlugin` с параметром `-PluginType Email` или `-PluginType Sms` в зависимости от выбранного способа доставки;
- **Плагин рассылки уведомлений** - командлет `Add-DssInternalNotifier` с параметрами `-NotifierType Email` или `-NotifierType Sms` в зависимости от выбранного способа доставки, `-TransportPluginID <ID транспортного плагина>`, `-FormatterPluginID <ID плагина формирования сообщений>`.

Пример настройки оповещения Пользователей по Email

Пример настройки уведомлений по SMS

Для описанных способов оповещения установлены шаблоны сообщений. Администратор может их изменять при помощи специализированных командлетов.

Настройка PUSH-уведомлений и их шаблонов

5. Включение/отключение оповещения

После выполнения всех перечисленных выше действий оповещение будет настроено и включено автоматически. Для отключения оповещения можно использовать следующие способы:

- Убрать контактную информацию Пользователя/Оператора, с которой связаны настройки оповещения.
- Запретить отправку уведомлений в политике оповещения.
- Отключить плагин рассылки уведомлений (см. п.4) при помощи командлета Disable-DssInternalNotifier. Включить плагин возможно при помощи командлета Enable-DssInternalNotifier.

Настройка записи событий в аудит

Плагины, необходимые для отправки и записи сообщений в журнал аудита, регистрируются при помощи командлетов вида `New-Dss...Audit`.

Настройка оповещения по Email

При формировании Email-сообщения используется специальный траспортный плагин – его задача состоит в создании текста сообщения на основе информации о выполняемом действии, подписываемом документе, одноразовом пароле и т.п. Для настройки плагина используются командлеты `Add-DssStsPlugin` и `Set-DssStsPlugin`.

Внимание!

В профиле Пользователя/Оператора должна быть заполнена соответствующая контактная информация (Email).

Транспортный Email-плагин представляет собой сборку .NET (см. Руководство разработчика). В состав СЭП «КриптоПро DSS» входят следующие плагины:

- `DSS.EmailService.SmtpPlugin.dll`

Все транспортные плагины для рассылки Email-сообщений устанавливаются в папку `<"Путь установки">\DSS\Plugins\Email`. Перед использованием плагина Администратор должен зарегистрировать плагин, как это описано в сценарии настройки системы оповещения.

Параметры плагина `DSS.EmailService.SmtpPlugin`

НАИМЕНОВАНИЕ ПАРАМЕТРА	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ	ОБЯЗАТЕЛЬНЫЙ
Host	Адрес SMTP-сервера		Да
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	false	Нет
Timeout	Время истечения ожидания при отправке сообщения в милисекундах.	30 секунд	Нет

Тип плагина, указываемый при регистрации в командлете `Add-DssStsPlugin` в параметре `-PluginTypeName "CryptoPro.DSS.EmailService.SmtpPlugin.SmtpPlugin,DSS.EmailService.SmtpPlugin"`.

Пример настройки оповещения по Email

```
# Регистрация транспортного плагина 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” }

# Регистрирация плагина для формирования сообщений
Add-DssStsPlugin -PluginTypeName “CryptoPro.DSS.MessageFormatter.EmailFormatter,DSS.MessageFormatter” -
PluginType Formatter –Settings @{}

# Регистрирация компонента для отправки Email сообщений.
# Идентификаторы транспортного плагина и плагина для формирования сообщений
# можно посмотреть в выводе командлет Get-DssStsPlugin
Add-DssInternalNotifier -TransportPluginID <Transport_Plugin_ID> -FormatterPluginID <Formatter_Plugin_ID> -
NotifierType Email
```

Настройка оповещения по SMS

Для отправки оповещений КриптоПро DSS использует специальные SMS-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, как это описано в сценарии настройки системы оповещения.

Внимание!

В профиле Пользователя/Оператора должна быть заполнена соответствующая контактная информация (Email).

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`.

Параметры, задаваемые при регистрации, перечислены в таблице ниже.

НАИМЕНОВАНИЕ ПАРАМЕТРА	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ	ОБЯЗАТЕЛЬНЫЙ
WorkingDirectory	Путь к папке для сохранения файлов с текстом SMS сообщений.	`<Путь установки>\DSS\<StsAppName>\fakesms`	Нет

Тип плагина, указываемый при регистрации в командлете `Add-DssStsPlugin` в параметре `-PluginTypeName "CryptoPro.DSS.SmsService.StubPlugin.SmsStub,DSS.SmsService.StubPlugin"`.

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 таблице ниже.

Примечание

Названия параметров регистрозависимы.

НАИМЕНОВАНИЕ ПАРАМЕТРА	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ	ОБЯЗАТЕЛЬНЫЙ
login	Логин для доступа к услуге.	Нет	Да
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-DssStsPlugin` в параметре `-PluginTypeName "CryptoPro.DSS.SmsService.DevinoSms.DevinoSmsPlugin,DevinoSmsPlugin"`.

Плагин DSS.SmsService.MtsSms

Данный плагин предназначен для работы со службой рассылки SMS http://mcommunicator.ru. Параметры, задаваемые при регистрации, перечислены в таблице ниже.

НАИМЕНОВАНИЕ ПАРАМЕТРА	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ	ОБЯЗАТЕЛЬНЫЙ
login	Логин для доступа к услуге (представляет из себя номер телефона в формате `7XXXXXXXXXX`).	Нет	Да

НАИМЕНОВАНИЕ ПАРАМЕТРА	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ	ОБЯЗАТЕЛЬНЫЙ
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 MD5функции 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
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-DssStsPlugin` в параметре `-PluginTypeName "CryptoPro.DSS.SmsService.MtsSms.MtsSmsPlugin,DSS.SmsService.MtsSms"`.

Плагин DSS.SmsService.SmppPlugin

Данный плагин предназначен для работы со службой рассылки SMS по протоколу SMPP. Параметры, задаваемые при регистрации, перечислены в таблице ниже.

НАИМЕНОВАНИЕ ПАРАМЕТРА	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ	ОБЯЗАТЕЛЬНЫЙ
ServiceAddress	Адрес сервера SMPP.	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-DssStsPlugin` в параметре `-PluginTypeName "CryptoPro.DSS.SmsService.SmppPlugin.SmppPlugin,DSS.SmsService.SmppPlugin"`.

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 регистрации и настройки плагина используется командлет `Add-DssStsPlugin`.

Параметры, задаваемые при регистрации, перечислены в таблице ниже.

НАИМЕНОВАНИЕ 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-DssStsPlugin` в параметре `-PluginTypeName "CryptoPro.DSS.MessageFormatter.SMSFormatter,DSS.DSS.MessageFormatter"`.

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-DSSStsPlugin -PluginTypeName "CryptoPro.DSS.SmsService.StubPlugin.SmsStub,DSS.SmsService.StubPlugin" -PluginType SMS -
Settings @{"WorkingDirectory" = $SMSBaseDir}

Write-Host "Добавление плагина для форматирования СМС-сообщений"
Add-DSSStsPlugin -PluginTypeName "CryptoPro.DSS.MessageFormatter.SMSFormatter,DSS.MessageFormatter" -PluginType Formatter -
Settings @{Header="КриптоПро DSS."}

Write-Host "Добавление модуля оповещения для отправки СМС-сообщений"
Add-DSSInternalNotifier -TransportPluginID 1 -FormatterPluginID 2 -NotifierType SMS -Settings
@{"MinQueueSize"="0";"MaxQueueSize"="10000";"TimerInterval"="500";"TTL"="1";"MessageWindow"="50";"ThreadCount"="1";"Enabled"="tru
e"}
```

Настройка PUSH-уведомлений

PUSH-уведомления, настройка которых описана в данном разделе, позволяют оповещать Пользователей о событиях КриптоПро DSS в мобильном приложении DSS SDK.

Внимание!

Для настройки PUSH-уведомлений для экземпляра ЦИ должен быть настроен и включен метод аутентификации при помощи мобильного приложения DSS SDK. При этом включение метода для Пользователей не требуется.

Внимание!

Получать PUSH-уведомления Пользователь может только на привязанное к его учетной записи мобильное устройство.

Внимание!

Операторы DSS **НЕ могут** получать PUSH-уведомления (даже для событий, у которых в параметре `UsageType` есть назначение `Operator`. Операторам доступно только редактирование настроек PUSH-уведомлений Пользователей в веб-интерфейсе при наличии соответствующих настроек политики оповещения.

Настройка PUSH-уведомлений производится в несколько этапов:

- Настройка набора плагинов для рассылки PUSH-уведомлений
- Включение PUSH-уведомлений путем редактирования политики оповещения
- Инициализация (привязка к учетной записи) устройства Пользователя
- (Опционально) Настройка шаблонов PUSH-уведомлений

Пример настройки PUSH-уведомлений

1. Настройка набора плагинов

Настройка набора плагинов для рассылки PUSH-уведомлений производится при помощи единого командлета Add-MyDssSystem. При этом в DSS автоматически создается система PUSH-уведомлений и регистрируются следующие плагины:

- плагин форматирования сообщений (`pushFmtPluginType = "CryptoPro.DSS.PushService.NotificationEx.PushFormatterPlugin,DSS.PushService.NotificationEx"`);
- транспортный плагин (`pushPluginType = "CryptoPro.DSS.PushService.NotificationEx.PushPlugin,DSS.PushService.NotificationEx"`);
- плагин рассылки уведомлений (`pushNotifierType = "CryptoPro.DSS.PushService.NotificationEx.PushNotifier,DSS.PushService.NotificationEx"`).

```
Add-MyDssSystem -Name <Отображаемое имя системы> -ApnClientCertPath "<Путь к файлу с сертификатом APN>" -
ApnClientCertPassword <Пароль APN> -CollapseKey <string> -MyDssAddress https://<hostname>/<mydssAppName> -
GoogleServiceKey <Идентификатор FCM>
```

Примечание

Для отправки PUSH-уведомлений на устройства Apple требуется **сертификат с клиентской аутентификацией** (`-ApnClientCertPath` и `-ApnClientCertPassword`) на Apple Push Notification Service. Получить данный сертификат можно по запросу на `dsssupport@cryptopro.ru`.

Для отправки PUSH-уведомлений на устройства Android требуется получить **ключ доступа** к Firebase Cloud Messaging Server (-GoogleServiceKey). Получить данный ключ можно по запросу на `dsssupport@cryptopro.ru`.

Изменение настроек зарегистрированных плагинов возможно при помощи командлета Set-MyDssSystem. Для указания

системы, в которую вносятся изменения, требуется заполнить параметр `SystemId`. Получить значение данного параметра для всех зарегистрированных систем можно в выводе командлета Get-MyDssSystem без параметров.

2. Включение PUSH-уведомлений

Включить оповещение Пользователей посредством PUSH-уведомлений можно, добавив в политику оповещения Пользователей в параметр `Notifiers` значение `PUSH`.

> **Примечание**
>
> Если для какого-либо события уже был задан параметр `-Notifiers`, следующее его заполнение для данного события перезапишет все указанные способы доставки. Т.е. при изменении данного параметра каждый раз нужно указывать все необходимые способы доставки.

3. Инициализация (привязка к учетной записи) устройства Пользователя

Получать PUSH-уведомления Пользователь может только на привязанное к его учетной записи мобильное устройство. Сценарии привязки (инициализации) мобильного устройства Пользователя описаны в соответствующем разделе.

4. (Опционально) Настройка шаблонов PUSH-уведомлений

Администратор может создать собственные шаблоны PUSH-уведомлений, доставляемых Пользователям, для каждой системы, созданной на шаге 1.

Если собственные шаблоны не заданы, используются шаблоны по умолчанию. Удалять или изменять шаблоны по умолчанию невозможно.

Чтобы добавить собственный шаблон PUSH-уведомления, необходимо выполнить следующие действия:

1. Выбрать событие, для которого нужно добавить шаблон PUSH-уведомления и получить его идентификатор `EventID`.
2. Выбрать систему из ранее зарегистрированных, для которой настраиваются PUSH-уведомления, при помощи командлета Get-MyDssSystem и получить ее идентификатор `SystemId`.
3. Добавить шаблон для выбранного события и выбранной системы, используя `EventID` выбранного события и `SystemId` выбранной системы соответственно:

```
Add-DssPushFormatterTemplate -EventID <ID события> -MyDssSystemId "<ID системы>" -Text "<У Вас новое
уведомление {0:Date}>" -Payload '{"Date" : "{0:Date}", "MyDssPushAddress" : "{0:MyDssPushAddress}"}' "
```

> **Примечание**
>
> В параметре `-Text` можно использовать только подстановочные параметры, указанные в обычных шаблонах сообщений для данного события (командлет `Get-DssFormatterTemplate -EventID <ID выбранного события>`).
>
> Параметр `-Payload` содержит набор параметров, которые будут переданы в приложение, работающее с DSS SDK. Зарезервирован для дальнейшего использования.

Чтобы просмотреть все шаблоны PUSH-уведомлений, зарегистрированных в данной системе, можно использовать командлет Get-DssPushFormatterTemplate.

5. Примеры

```
# Регистрация системы PUSH-уведомлений и набора плагинов
Add-MyDssSystem -Name <Отображаемое имя системы> -ApnClientCertPath "<Путь к файлу с сертификатом APN>" -
ApnClientCertPassword <Пароль APN> -CollapseKey <string> -MyDssAddress https://<hostname>/<mydssAppName> -
GoogleServiceKey <Идентификатор FCM>

# Настройка политики оповещения Пользователей для PUSH-уведомлений:
Set-DssNotificationPolicy –Type User -NotificationEvents CertificateCreated,DeviceConfirmed -Notifiers PUSH

# (Опционально) Добавление нового шаблона PUSH-уведомления для события
Add-DssPushFormatterTemplate -EventID <ID события> -MyDssSystemId "<ID системы>" -Text "<У Вас новое
уведомление {0:Date}>" -Payload '{"Date" : "{0:Date}", "MyDssPushAddress" : "{0:MyDssPushAddress}"}' "
```

Политики оповещения

События, отправленные с компонентов DSS при помощи настроенных ранее плагинов, доставляются на Сервис рассылки уведомлений. Здесь происходит получение информации о доступных способах доставки (Email, SMS, PUSH), а также контактной информации из профиля Пользователя или Оператора, которому должно быть доставлено уведомление. Для получения данной информации необходимо настроить политику оповещения для Пользователей и Операторов.

Политика оповещения Пользователей

Политика оповещения Пользователей состоит из трех уровней:

- глобального,
- уровня группы,
- уровня Пользователя (настройка доступна только через веб- и REST-интерфейсы).

Политика оповещения Пользователей заполняется при помощи командлета Set-DssNotificationPolicy и представляет собой набор следующих настроек:

ПАРАМЕТР	ТИП	ОПИСАНИЕ
Type	`User`	Определяет, для кого настраивается политика.
Notifiers	`SMS, Email, PUSH` (1 или несколько через запятую)	Список назначений для отправки уведомлений о событиях, указанных в параметре `Notifiers`.
GroupID	int	Идентификатор группы, если необходимо настроить политику уровня группы.
NotificationEvents	`AllNotificationEvents` ИЛИ `Notifiers {}` (пустой список) ИЛИ `Notifiers` (1 или несколько через запятую)	Набор событий, о которых необходимо оповещать.
AllowChangeByOperator	bool	Определяет, может ли Оператор изменять политику оповещения Пользователя в веб-интерфейсе.
AllowChangeByUser	bool	Определяет, может ли Пользователь изменять политику оповещения в веб-интерфейсе.
AllowOverride	bool	Определяет, может ли политика быть переопределена на более низком уровне иерархии.

Примечание

В зависимости от того, политика какого уровня настраивается — глобального уровня или уровня группы — необходимо также соответственно использовать параметр `-GroupId` со значением идентификатора настраиваемой группы. Для заполнения глобальной политики специальный параметр указывать не требуется.

Если в иерархии политик есть политика с `AllowOverride` = `false`, настройки политики уровнем ниже не имеют силы. Если все политики в иерархии имеют `AllowOverride` = `true`, параметры `AllowChangeByUser` и `AllowChangeByOperator` используются из политики группы, а настройка самого оповещения применяется индивидуально для каждого Пользователя (настраивается в Веб-интерфейсе Пользователя).

Примечание

Перед изменением настроек политики оповещения при помощи командлетов (глобальный уровень или уровень группы), убедитесь, что на уровень выше не применялось значение `AllowOverride` = `false`.

Политика оповещения Операторов

Политика оповещения Операторов состоит из двух уровней:

- глобального,
- уровня Оператора (настройка доступна только через веб- и REST-интерфейсы).

Политика оповещения Пользователей заполняется при помощи командлета Set-DssNotificationPolicy и представляет собой набор следующих настроек:

ПАРАМЕТР	ТИП	ОПИСАНИЕ
Type	`Operator`	Определяет, для кого настраивается политика.
Notifiers	`SMS, Email` (1 или оба через запятую)	Список назначений для отправки уведомлений о событиях, указанных в параметре `Notifiers`.
NotificationEvents	`AllNotificationEvents` ИЛИ `{}` (пустой список) ИЛИ `Notifiers` (1 или несколько через запятую)	Набор событий, о которых необходимо оповещать.
AllowChangeByOperator	bool	Определяет, может ли Оператор изменять политику оповещения в веб-интерфейсе.
AllowOverride	bool	Определяет, может ли политика быть переопределена на более низком уровне иерархии.

Если в глобальной политике имеется значение `AllowOverride` = `false`, настройки политики уровня Оператора на веб-интерфейсе будут недоступны. Если глобальная политика `AllowOverride` = `true`, параметр `AllowChangeByOperator` применяется индивидуально для каждого Оператора (настраивается в его личном кабинете на веб-интерфейсе или при помощи REST API).

Примеры:

Примечание

Примеры составлены для случая, когда редактируется политика оповещения Пользователей. Для редактирования политики оповещения Операторов следует указывать параметр `-Type Operator` и **НЕ использовать** параметр `-GroupId <ID группы>`.

Получение политики оповещения Пользователей по уровням:

```
# Получение глобальной политики:
Get-DssNotificationPolicy -Type User
# Если в выводе данной команды содержится AllowOverride = False,
# настройки уровня группы не имеют силы.

# Получение политики группы Пользователей
Get-DssNotificationPolicy -Type User -GroupId 1
# Если в выводе данной команды содержится AllowOverride = False,
# Пользователь не сможет изменить политику доступа к операциям в Веб-
# интерфейсе.

# Просмотр списка событий с указанием настроенных способов доставки для каждого события:
(Get-DssNotificationPolicy -Type User ).EventNotifiers
```

Настройка политики оповещения Пользователей:

```
# Оповещать Пользователей о всех событиях:
Set-DssNotificationPolicy -Type User -AllNotificationEvents -Notifiers SMS,Email -AllowOverride 0

# НЕ оповещать Пользователей ни о каких событиях:
Set-DssNotificationPolicy -Type User -AllNotificationEvents -Notifiers @() -AllowOverride 0

# Указать набор событий, о которых необходимо оповещать Пользователей:
Set-DssNotificationPolicy -Type User -NotificationEvents CertificateCreated,DeviceConfirmed -Notifiers
SMS,Email

ИЛИ

Set-DssNotificationPolicy -Type User -NotificationEvents 1, 2 -Notifiers SMS,Email

# Выбор способа доставки для всех событий SMS и Email:
Set-DssNotificationPolicy –Type User -AllNotificationEvents -Notifiers SMS,Email
```

Примечание

В случае, если необходимо изменить политику группы, следует добавлять параметр `-GroupId <ID группы>`.

Примечание

Если для какого-либо события уже был задан параметр `-Notifiers`, следующее его заполнение для данного события перезапишет все указанные способы доставки. Т.е. при изменении данного параметра каждый раз нужно указывать все необходимые способы доставки.

Отключение оповещения обо всех событиях

Для того чтобы отключить оповещение обо всех событиях необходимо в параметре `Notifier` передать пустой список типов оповещения.

Примечание

Отключение оповещения обо всех событиях необходимо выполнить перед настройкой оповещение **только** о выделенных событиях.

```
Set-DssNotificationPolicy -Type User -AllNotificationEvents -GroupId 1 -Notifier @()
```

Полный список событий и их кодов.

Шаблоны сообщений при оповещении Пользователей и Операторов

События КриптоПро DSS могут иметь один или несколько текстовых шаблонов с подстановочными параметрами для отправки Пользователям и Операторам DSS посредством электронной почты, SMS-сообщений и PUSH-уведомлений. Список событий предопределен и не может быть изменен.

> **Примечание**
>
> Все командлеты, приведенные в данном разделе, должны выполняться на Центре Идентификации DSS.

Изменение шаблона сообщения для события

1. Поиск шаблона, который необходимо изменить.

Поиск шаблона, текст которого необходимо изменить, осуществляется в следующей последовательности:

- Выбор события, за которым закреплен изменяемый шаблон.
- Выбор шаблона сообщения из прикрепленных к событию шаблонов.

Получить список всех событий и соответствующих им идентификаторов шаблонов можно в соответствующем разделе документации или с помощью следующего командлета:

```
Get-DssEvent
```

Выберите из списка событие, у которого есть шаблоны сообщений. На это указывает наличие идентификаторов шаблонов в столбце `MessageTemplates`.

Чтобы просмотреть все шаблоны, закрепленные за выбранным событием, необходимо выполнить следующую команду:

```
Get-DssFormatterTemplate -EventTypes <Выбранное событие>

# ИЛИ

Get-DssFormatterTemplate -EventID <ID выбранного события>
```

2. Изменение текста шаблона сообщения.

> **Примечание**
>
> Количество шаблонов, прикрепленных к событию, изменять нельзя, но возможно изменить их текст.

После выбора шаблона, текст которого необходимо изменить, потребуется запомнить его идентификатор, либо передать его по конвейеру в следующий командлет. Изменение текста шаблона сообщения производится при помощи следующей команды:

```
Set-DssFormatterTemplate -TemplateID <ID шаблона сообщения> -Template "<Новый текст шаблона сообщения>"
```

> **Внимание!**
>
> В текстах шаблонов по умолчанию используются подстановочные параметры вида `{0:<Параметр>}`. При необходимости их можно не указывать, однако нельзя добавлять другие подстановочные параметры, которых не было в шаблоне по умолчанию.

События КриптоПро DSS

Внимание!

Список событий КриптоПро DSS может изменяться. Получить список всех событий и соответствующих им идентификаторов шаблонов можно с помощью следующего командлета:

```
Get-DssEvent
```

Все события делятся по типу использования (столбец `UsageType`):

1. `Internal` – для отправки системных оповещений DSS.
2. `User` – отправляются Пользователям.
3. `Operator` – отправляются Операторам (действия Оператора и Пользователей из его группы).
4. `AuditOnly` – отправляются только в журнал аудита.
5. `Custom` – для отправки системных оповещений DSS.

Столбец `MessageTemplates` содержит идентификаторы шаблонов сообщений, закрепленные за данным событием. Количество шаблонов изменять нельзя, но возможно изменить их текст.

ID	EVENTTYPE	USAGETYPE	MESSAGETEMPLATES
--	---------	---------	----------------
1	UserCreated	User Operator	-1, 2, 3, 4, 444
2	UserCreatedByAdmin	User Operator	-5, 6, 7, 8, 445
3	UserCreateFail	Operator	-9, 10
4	UserAccountChanged	User Operator	-11, 12, 13, 14, 446
5	UserAccountChangeFail	User Operator	-15, 16, 17, 18, 447
6	UserPasswordChanged	User Operator	-19, 20, 21, 22, 448
7	UserPasswordChangeFail	User Operator	-23, 24, 25, 26, 449
8	UserPhoneChangeFail	User Operator	-27, 28, 29, 30, 450
9	UserPasswordReset	User Operator	-31, 32, 33, 34, 451
10	UserDeleted	Operator	-35, 36, 37, 452
11	UserDeleteFail	User Operator	-38, 39, 40, 41, 453
12	AdminCreated	Operator	-42, 43
13	AdminCreateFail	Operator	-44, 45
14	AdminDeleted	Operator	-46, 47
15	AdminDeleteFail	Operator	-48, 49

16	AdminAccountChanged	Operator	-50, 51
17	AdminAccountChangeFail	Operator	-52, 53
18	UserEnterConfirmation	User	-54, 55, 454
19	UserPhoneConfirmation	User Operator	-56, 57, 58, 59, 455
20	CertificateCreated	User Operator	-76, 77, 78, 79, 460
21	RequestCreated	User Operator	-60, 61, 62, 63, 456
22	RequestCreateFail	User Operator	-64, 65, 66, 67, 457
23	RequestDeleted	User Operator	-68, 69, 70, 71, 458
24	RequestDeletedAll	User Operator	-72, 73, 74, 75, 459
25	CertRequestsRequested	AuditOnly	-
26	CertRequestRequested	AuditOnly	-
27	CertificatesRequested	AuditOnly	-
28	CertificateRequested	AuditOnly	-
29	RevokeRequestsRequested	AuditOnly	-
30	CertRequestContentRequested	AuditOnly	-
31	CertificateContentRequested	AuditOnly	-
32	RevokeRequestContentRequested	AuditOnly	-
33	ServicePolicyRequested	AuditOnly	-
34	DocumentSignSuccess	User Operator	-80, 81, 82, 83, 461
35	DocumentSignFail	User Operator	-84, 85, 86, 87, 462
36	DocumentEncrypted	User Operator	-88, 89, 90, 91, 463
37	DocumentEncryptionFail	User Operator	-92, 93, 94, 95, 464
38	DocumentDecrypted	User Operator	-96, 97, 98, 99, 465
39	DocumentDecryptionFail	User Operator	-100, 101, 102, 103, 466
40	CertRequestAccepted	User Operator	-104, 105, 106, 107, 467
41	CertRequestDeclined	User Operator	-108, 109, 110, 111, 468

42	RegRequestAccepted	User Operator	-112, 113, 114, 115, 469
43	RegRequestDeclined	User Operator	-116, 117, 118, 119, 470
44	RevokeRequestAccepted	User Operator	-120, 121, 122, 123, 471
45	RevokeRequestDeclined	User Operator	-124, 125, 126, 127, 472
46	CertificateDeleted	User Operator	-128, 129, 130, 131, 473
47	CertificateDeletedAll	User Operator	-132, 133, 134, 135, 474
48	CertificateRevoke	User Operator	-136, 137, 138, 139, 475
49	CertificateHold	User Operator	-140, 141, 142, 143, 476
50	CertificateUnhold	User Operator	-144, 145, 146, 147, 477
51	CertificatePinChanged	User Operator	-148, 149, 150, 151, 478
52	CertificatePinChangeFail	User Operator	-152, 153, 154, 155, 479
53	CertificateSetDefault	User Operator	-156, 157, 158, 159, 480
54	CertificateSetDefaultFail	User Operator	-160, 161, 162, 163, 481
55	CertificateResetDefault	User Operator	-164, 165, 166, 167, 482
56	CertificateResetDefaultFail	User Operator	-168, 169, 170, 171, 483
57	OTP	Internal	-172, 173, 268, 282, 296, 310, 324, 338, 352, 366, 484
58	CertificateInstalled	User Operator	-174, 175, 176, 177, 485
61	UserAccountStateChanged	User Operator	-178, 179, 180, 181, 486
62	UserAuthenticationPassed	User Operator	-182, 183, 184, 185, 487
63	UserAuthenticationFailed	User Operator	-186, 187, 188, 189, 488
64	SmsVerificationPassed	Internal	-
65	SmsVerificationFailed	Internal	-
66	UserPhoneChanged	User Operator	-190, 191, 192, 193, 489
67	UserPhoneConfirmationFail	User Operator	-194, 195, 196, 197, 490
68	UserPhoneConfirmationOtp	Internal	-198, 491
69	SimAuthSuccess	Internal	-

76	OtaNotification	Custom	-199, 200, 201, 492
77	UserEmailConfirmationOtp	Internal	-202
78	UserEmailChanged	User Operator	-203, 204, 205, 206, 493
79	UserEmailConfirmationFail	User Operator	-207, 208, 209, 210, 494
80	UserEmailChangeFail	User Operator	-211, 212, 213, 214, 495
81	UserMobileAuthSecretKeyInfo	Internal	-215, 216, 496
84	AuthenticationSchemeChanged	AuditOnly	-217
85	AuthenticationSchemeChangeFail	AuditOnly	-
86	AddExternalLogin	User Operator	-218, 219, 220, 221, 497
87	AddExternalLoginFail	User Operator	-222, 223, 224, 225, 498
88	RemoveExternalLogin	User Operator	-226, 227, 228, 229, 499
89	RemoveExternalLoginFail	User Operator	-230, 231, 232, 233, 500
90	EnhanceSignature	User Operator	-234, 235, 236, 237, 501
91	EnhanceSignatureFail	User Operator	-238, 239, 240, 241, 502
92	SecondaryAuthLogin	Internal	-242, 255, 269, 283, 297, 311, 325, 339, 353, 367, 503
93	SecondaryAuthSign	Internal	-243, 256, 270, 284, 298, 312, 326, 340, 354, 368, 504
94	SecondaryAuthSignDocs	Internal	-244, 257, 271, 285, 299, 313, 327, 341, 355, 369, 505
95	SecondaryAuthDecrypt	Internal	-245, 258, 272, 286, 300, 314, 328, 342, 356, 370, 506
96	SecondaryAuthCreateRequest	Internal	-246, 259, 273, 287, 301, 315, 329, 343, 357, 371, 507
97	SecondaryAuthChangePin	Internal	-247, 260, 274, 288, 302, 316, 330, 344, 358, 372, 508
98	SecondaryAuthRenewCert	Internal	-248, 261, 275, 289, 303, 317, 331, 345, 359, 373, 509
99	SecondaryAuthRevokeCert	Internal	-249, 262, 276, 290, 304, 318, 332, 346, 360, 374, 510
100	SecondaryAuthHoldCert	Internal	-250, 263, 277, 291, 305, 319, 333, 347, 361, 375, 511
101	SecondaryAuthUnholdCert	Internal	-251, 264, 278, 292, 306, 320, 334, 348, 362, 376, 512
102	SecondaryAuthDeleteCert	Internal	-252, 265, 279, 293, 307, 321, 335, 349, 363, 377, 513
103	SecondaryAuthDeleteCerts	Internal	-253, 266, 280, 294, 308, 322, 336, 350, 364, 378, 514

104	SecondaryAuthPrivateKeyAccess	Internal	-254, 267, 281, 295, 309, 323, 337, 351, 365, 379, 515
105	CertificateSetFriendlyName	User Operator	-380, 381, 382, 383, 516
106	CertificateSetFriendlyNameFail	User Operator	-384, 385, 386, 387, 517
107	GlonassUserActivated	Internal	-
108	GlonassUserActivationFail	Internal	-
109	GlonassUserDeactivated	Internal	-
110	GlonassUserDeactivationFail	Internal	-
111	GlonassUserReactivated	Internal	-
112	GlonassUserReactivationFail	Internal	-
113	GlonassCertificateCreated	Internal	-
114	GlonassCertificateCreationFail	Internal	-
117	UserAirKeyAuthSecretKeyInfo	Internal	-388, 389, 518
118	AuthenticationResultCallback	Custom	-
119	ScopeConfirmation	Internal	-
120	TestMessage	Internal	-390, 391, 519
121	UserMobileAuthSendQrCodeByEmail	Internal	-392
122	SimAuthAppletActivated	Internal	-
129	OperationConfirmed	AuditOnly	-
130	AuthenticationCompleted	AuditOnly	-
131	OperationDeclined	Internal	-
132	SimAuthCallbackAuthentication	Custom	-
133	SimAuthCallbackChangePin	Custom	-
134	SimAuthCallbackChangeKey	Custom	-
135	SimAuthCallbackGetStatus	Custom	-
136	SimAuthCallbackActivation	Custom	-
143	CertificateRevocationFail	User Operator	-393, 394, 395, 396, 520

146	CertificateHoldFail	User Operator	-397, 398, 399, 400, 521
149	CertificateUnholdFail	User Operator	-401, 402, 403, 404, 522
152	CertificateDeleteFail	User Operator	-405, 406, 407, 408, 523
160	TransactionTokenCreated	AuditOnly	-
161	TransactionTokenCreationFail	AuditOnly	-
162	SamlAuthMethodDeleteFail	AuditOnly	-
163	SamlAuthMethodDeleted	AuditOnly	-
164	SamlAuthMethodAssignationFail	AuditOnly	-
165	SamlAuthMethodAssigned	AuditOnly	-
166	OtpSmsAuthMethodDeleteFail	AuditOnly	-
167	OtpSmsAuthMethodDeleted	AuditOnly	-
168	OtpSmsAuthMethodAssignationFail	AuditOnly	-
169	OtpSmsAuthMethodAssigned	AuditOnly	-
170	OAthAuthMethodDeleteFail	AuditOnly	-
171	OAthAuthMethodDeleted	AuditOnly	-
172	OAthAuthMethodAssignationFail	AuditOnly	-
173	OAthAuthMethodAssigned	AuditOnly	-
174	OtpEmailAuthMethodDeleteFail	AuditOnly	-
175	OtpEmailAuthMethodDeleted	AuditOnly	-
176	OtpEmailAuthMethodAssignationFail	AuditOnly	-
177	OtpEmailAuthMethodAssigned	AuditOnly	-
178	SimAuthMethodDeleteFail	AuditOnly	-
179	SimAuthMethodDeleted	AuditOnly	-
180	SimAuthMethodAssignationFail	AuditOnly	-
181	SimAuthMethodAssigned	AuditOnly	-
182	MobileAuthMethodDeleteFail	AuditOnly	-

183	MobileAuthMethodDeleted	AuditOnly	-
184	MobileAuthMethodAssignationFail	AuditOnly	-
185	MobileAuthMethodAssigned	AuditOnly	-
186	MtmoAuthMethodDeleteFail	AuditOnly	-
187	MtmoAuthMethodDeleted	AuditOnly	-
188	MtmoAuthMethodAssignationFail	AuditOnly	-
189	MtmoAuthMethodAssigned	AuditOnly	-
190	MoAuthMethodDeleteFail	AuditOnly	-
191	MoAuthMethodDeleted	AuditOnly	-
192	MoAuthMethodAssignationFail	AuditOnly	-
193	MoAuthMethodAssigned	AuditOnly	-
194	AirkeyAuthMethodDeleteFail	AuditOnly	-
195	AirkeyAuthMethodDeleted	AuditOnly	-
196	AirkeyAuthMethodAssignationFail	AuditOnly	-
197	AirkeyAuthMethodAssigned	AuditOnly	-
198	MyDssAuthMethodDeleteFail	AuditOnly	-
199	MyDssAuthMethodDeleted	AuditOnly	-
200	MyDssAuthMethodAssignationFail	AuditOnly	-
201	MyDssAuthMethodAssigned	AuditOnly	-
203	IdOnlyAuthMethodDeleteFail	AuditOnly	-
204	IdOnlyAuthMethodDeleted	AuditOnly	-
205	IdOnlyAuthMethodAssignationFail	AuditOnly	-
206	IdOnlyAuthMethodAssigned	AuditOnly	-
207	CertificateAuthMethodDeleteFail	AuditOnly	-
208	CertificateAuthMethodDeleted	AuditOnly	-
209	CertificateAuthMethodAssignationFail	AuditOnly	-

210	CertificateAuthMethodAssigned	AuditOnly	-
211	PasswordAuthMethodDeleteFail	AuditOnly	-
212	PasswordAuthMethodDeleted	AuditOnly	-
213	PasswordAuthMethodAssignationFail	AuditOnly	-
214	PasswordAuthMethodAssigned	AuditOnly	-
215	CloudCspUsed	AuditOnly	-
216	InstanceConfigurationChanged	AuditOnly	-
217	UserTfaFailed	AuditOnly	-
218	SecondaryAuthGenKey	Internal	-409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 524
219	CryptGenKeySuccess	User Operator	-420, 421, 422, 423, 525
220	CryptGenKeyFail	User Operator	-424, 425, 426, 427, 526
223	AuthMethodAssigned	User Operator	-428, 429, 430, 431, 527
224	AuthMethodAssignationFail	User Operator	-432, 433, 434, 435, 528
225	AuthMethodRemoved	User Operator	-436, 437, 438, 439, 529
226	AuthMethodRemovalFail	User Operator	-440, 441, 442, 443, 530
227	AnonDeviceRegistered	AuditOnly	-
228	AnonDeviceRegisteredFailed	AuditOnly	-
229	KInitRequested	AuditOnly	-
230	RegisterByKInit	AuditOnly	-
231	RegisterByKInitFailed	AuditOnly	-
232	DeviceConfirmed	AuditOnly	-
233	DeviceConfirmedFailed	AuditOnly	-
234	AssignMyDssSdkDevice	AuditOnly	-
235	AssignMyDssSdkDeviceFailed	AuditOnly	-
236	DeleteKInit	AuditOnly	-
237	DeleteKInitFailed	AuditOnly	-

238	DeviceVerified	AuditOnly	-
239	DeviceVerifiedFailed	AuditOnly	-
240	AddNewDeviceRequest	AuditOnly	-
241	AddNewDeviceRequestFailed	AuditOnly	-
242	ApproveNewDeviceRequest	AuditOnly	-
243	ApproveNewDeviceRequestFailed	AuditOnly	-
244	RejectNewDeviceRequest	AuditOnly	-
245	RejectNewDeviceRequestFailed	AuditOnly	-
246	VerifyDeviceByCertificate	AuditOnly	-
247	VerifyDeviceByCertificateFailed	AuditOnly	-
297	DocumentUploaded	AuditOnly	-
298	DocumentUploadFail	AuditOnly	-
299	DocumentPatched	AuditOnly	-
300	DocumentPatchFailed	AuditOnly	-
301	DocumentConvertationRetreived	AuditOnly	-
302	DocumentConvertationRetreiveFail	AuditOnly	-
303	DocumentConvertedFail	AuditOnly	-
304	DocumentDeleted	AuditOnly	-
305	DocumentContentRetreived	AuditOnly	-
306	DocumentContentRetreivedFail	AuditOnly	-

Управление сервисными сертификатами

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.

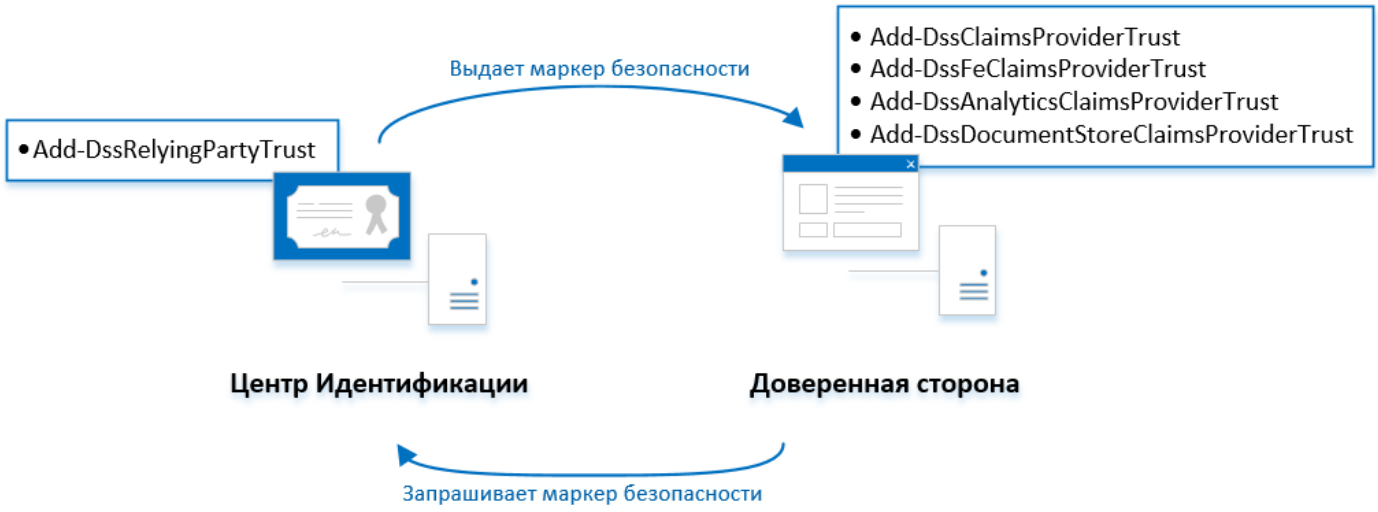
В связи с этим каждому из компонентов КриптоПро DSS требуется сервисный сертификат.

На рисунке ниже изображена настройка сервисных сертификатов в компонентах КриптоПро DSS. Рисунок иллюстрирует следующие требования к настройке и взаимодействию компонентов КриптоПро DSS:

1. Каждому компоненту КриптоПро DSS назначается сервисный сертификат. Назначение сервисных сертификатов осуществляется с помощью командлетов вида `Set-...Properties`.
2. Между Центром Идентификации и остальными компонентами КриптоПро DSS необходимо установить отношения доверия. Установка отношений доверия осуществляется путём регистрации сервисного сертификата ЦИ в компонентах КриптоПро DSS (используются командлеты вида `Add-...RelyingPartyTrust`).
3. Центр Идентификации должен быть зарегистрирован на остальных компонентах КриптоПро DSS как доверенный издатель маркеров безопасности (используются командлеты вида `Add-...ClaimsProviderTrust`, см. сценарии настройки компонентов).
4. Для некоторых компонентов (Сервис Аудита, Веб-интерфейс Пользователя) должны быть настроены требования аутентификации доверенной стороны.

Внимание!

Если регистрация доверенной стороны производилась через метаданные, аутентификация доверенной стороны была настроена автоматически. Смена аутентификационных данных доверенной стороны описана в соответствующем разделе.



Также в этом разделе:

- Требования к сервисным сертификатам
- Пример создания самоподписанного сертификата
- Назначение прав доступа к закрытому ключу сертификата
- Примеры назначения и смены сервисных сертификатов

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» должно быть задано следующее значение:

```
Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
```

Требований к содержимому поля «Субъект» нет. В значении компонента 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.

> **Примечание**
>
> После получения сертификата его следует установить в хранилище Личные локального компьютера с привязкой 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. Имена учетных записей компонентов КриптоПро DSS приведены в таблице ниже.

КОМПОНЕНТ	ИМЯ УЧЁТНОЙ ЗАПИСИ
Веб-интерфейс Пользователя	IIS AppPool\CryptoProDSS-1-Frontend
Сервис Подписи	IIS AppPool\CryptoProDSS-1-SignServer
Центр Идентификации	IIS AppPool\CryptoProDSS-1-STS
Сервис Аудита	IIS AppPool\CryptoProDSS-1-AnalyticsService
Сервис Обработки Документов	IIS AppPool\CryptoProDSS-1-DocumentStore

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. Справку по формату файлов с шаблоном запроса на сертификат можно посмотреть по ссылке. 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
```

> **Примечание**
>
> 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`.

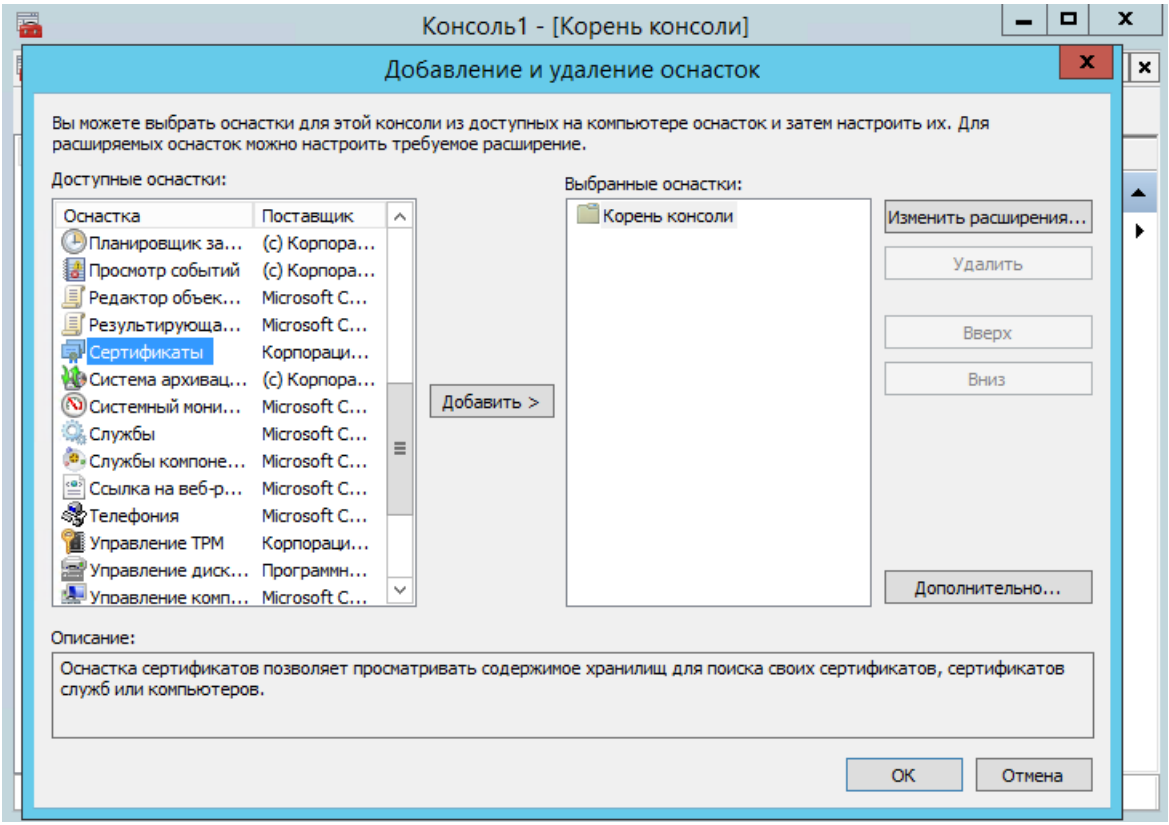
6. Для использования данного сертификата необходимо будет выдать права на закрытый ключ.

Назначение прав доступа к закрытому ключу сертификата

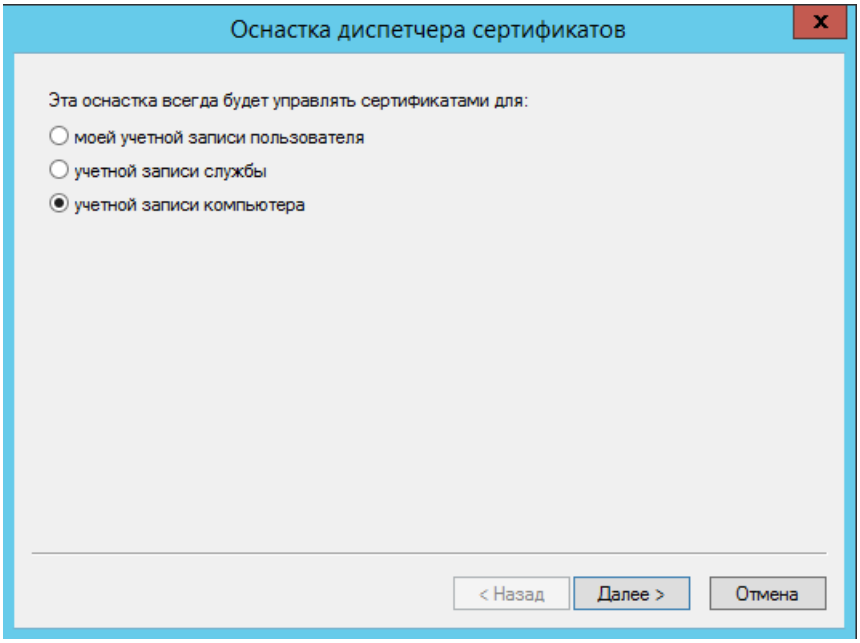
Примечание

Данное действие необходимо выполнять после развертывания экземпляров служб.

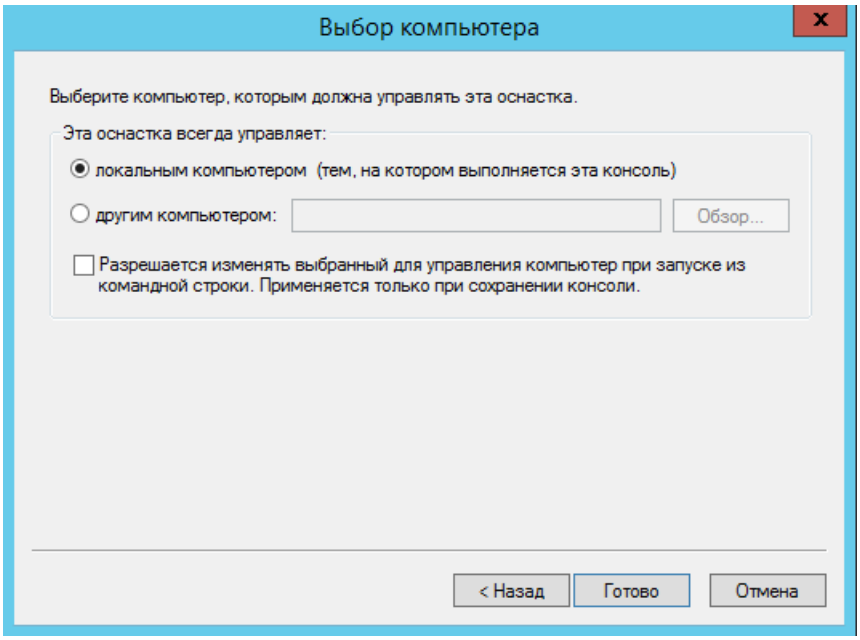
Назначить права доступа к закрытому ключу можно в оснастке «Сертификаты». Для запуска оснастки выполните следующие шаги: *Пуск – Выполнить – mmc*. В открывшейся консоли управления выберите: *Файл – Добавить или удалить оснастку*. В открывшемся окне выберите оснастку «Сертификаты» и нажмите кнопку «Добавить».



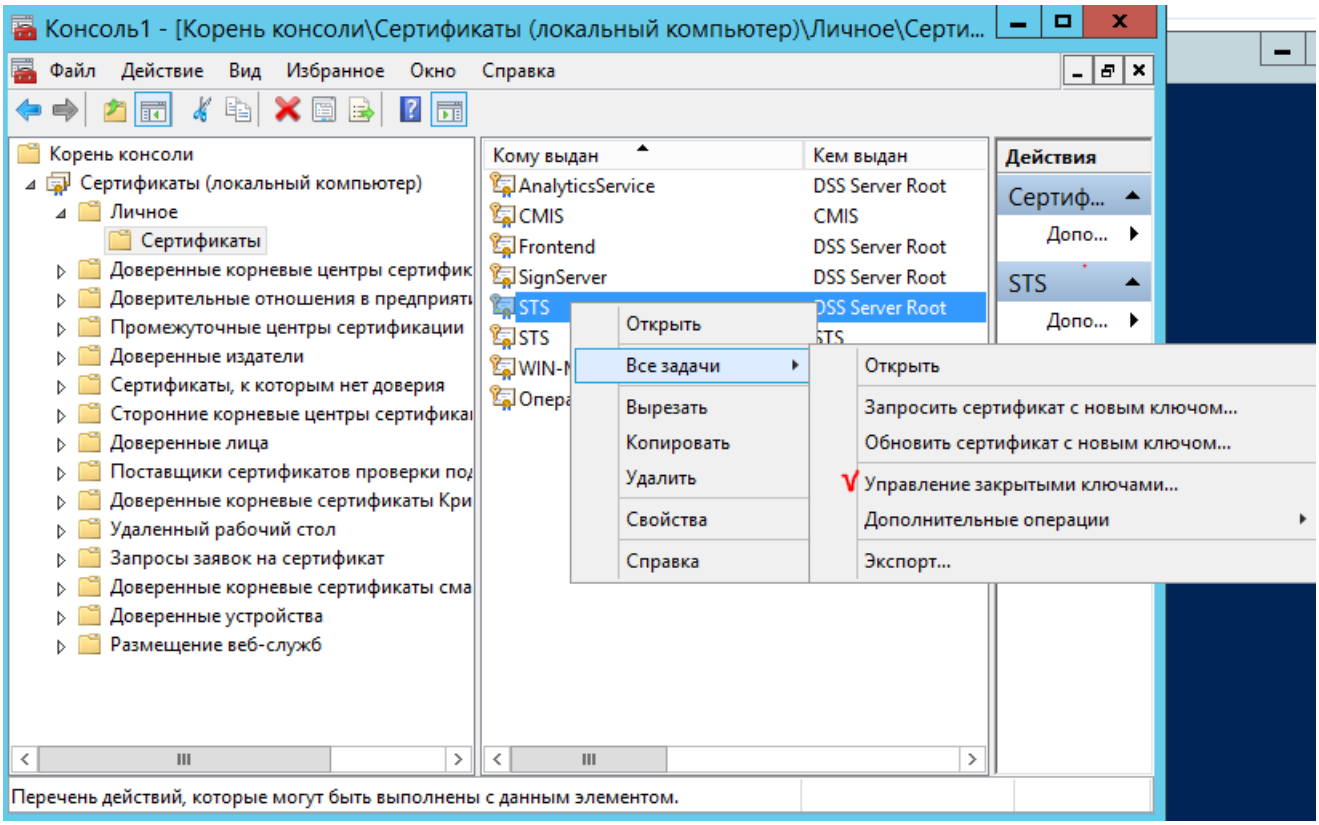
Далее в диалоге «Оснастка диспетчера сертификатов» выберите пункт «Учетной записи компьютера» и нажмите «Далее».



В качестве компьютера, которым будет управлять данная оснастка, необходимо указать локальный компьютер.

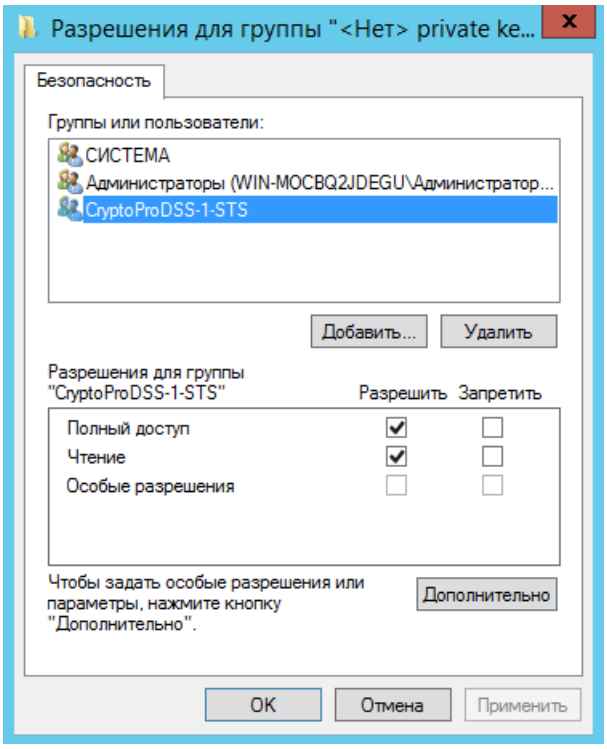


Далее в разделе *Сертификаты (локальный компьютер) – Личное – Сертификаты* выберите нужный сертификат. Нажмите правой кнопкой мыши по выбранному сертификату и выберите: *Все действия – Управление закрытыми ключами*.



В открывшемся окне 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*.


Разрешения для группы "<Нет> private ke...
Безопасность
Группы или пользователи:
СИСТЕМА
Администраторы (WIN-MOCBQ2JDEGU\Администратор...
CryptoProDSS-1-STS
Добавить...
Удалить
Разрешения для группы "CryptoProDSS-1-STS"
Разрешить
Запретить
Полный доступ
Чтение
Особые разрешения
Чтобы задать особые разрешения или параметры, нажмите кнопку "Дополнительно".
Дополнительно
OK
Отмена
Применить

Примеры назначения и смены сервисных сертификатов

> Внимание!
>
> Смена сервисного сертификата влечет за собой изменения в настройке отношений доверия между компонентами. (см. примеры ниже).

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.
- Смена сертификата в настройках отношений доверия на компонентах DSS (Сервис Подписи, Веб-интерфейс Пользователя, Сервис Аудита).

Ниже приводится пример Powershell-сценария, демонстрирующий смену сертификата Центра Идентификации.

Пример:

```
# Назначение и/или смена сервисного сертификата Центра Идентификации
Set-DssStsProperties –ServiceCertificate <thumbprint>

# (!) Примечание
# Пулу приложений Центра Идентификации необходимо выдать права на доступ к закрытому
# ключу нового сервисного сертификата

# (!) Примечание
# После изменения настроек сертификатов необходимо перезапустить пул приложения при
# помощи команды Restart-DssStsInstance

# Смена сертификата в настройках отношений доверия на Сервисе Подписи
Set-DSSClaimsProviderTrust -IssuerName realsts –NewThumbprint <thumbprint>

# Смена сертификата в настройках отношений доверия на Веб-интерфейсе Пользователя
Set-DSSFeClaimsProviderTrust -IssuerName realsts –NewThumbprint <thumbprint>

# Смена сертификата в настройках отношений доверия на Сервисе Аудита
Set-DssAnalyticsClaimsProviderTrust -IssuerName realsts –NewThumbprint <thumbprint>

# Смена сертификата в настройках отношений доверия на Сервисе Обработки Документов
Set-DssDocumentStoreClaimsProviderTrust -IssuerName realsts –NewThumbprint <thumbprint>

# (!) Примечание
# Значение параметра IssuerName можно посмотреть в выводе командлетов:
# Get-DSSClaimsProviderTrust
# Get-DSSFeClaimsProviderTrust
# Get-DSSAnalyticsClaimsProviderTrust
# Get-DSSDocumentStoreClaimsProviderTrust
# Имя издателя маркеров безопасности будет выведено в столбце «Имя»

# (!) Примечание
# После изменения настроек сертификатов необходимо перезапустить пул приложения при
# помощи команды Restart-Dss(...,Fe,Analytics,DocumentStore)Instance
```

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.

Ниже приводится пример Powershell-сценария, демонстрирующий смену сертификата Сервиса Подписи.

Пример:

```
# Назначение и/или смена 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
# После изменения настроек сертификатов необходимо перезапустить пул приложения при
# помощи команды Restart-DssSignServerInstance

# Смена сервисного 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

# (!) Примечание
# После изменения настроек сертификатов необходимо перезапустить пул приложения при
# помощи команды Restart-DssStsInstance.
```

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 и/или смена сервисного сертификата Веб-интерфейса Пользователя
Set-DSSFEProperties -ServiceCertificate <thumbprint>

# (!) Примечание
# Пулу приложений Веб-интерфейса Пользователя необходимо выдать
# права на доступ к закрытому ключу нового сервисного сертификата

# (!) Примечание
# После изменения настроек сертификатов необходимо перезапустить пул приложения при
# помощи команды Restart-DssFeInstance.

# Смена сервисного сертификата доверенной стороны на Центре Идентификации
Set-DssRelyingPartyTrust -Id <frontend_ID> –MetadataUri https://<hostname>/<AppName>/FederationMetadata/2007-
06/FederationMetadata.xml

# ИЛИ
# если необходимо сменить только сертификат аутентификации Веб-интерфейса Пользователя

Set-DssRelyingPartyTrust -Id <frontend_ID> -AuthenticationCertificate <thumbprint>

# 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

# (!) Примечание
# После изменения настроек сертификатов необходимо перезапустить пул приложения при
# помощи команды Restart-DssStsInstance.
```

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 и/или смена сервисного сертификата Сервиса Аудита
Set-DSSAnalyticsServiceProperties -ServiceCertificateThumbprint <thumbprint>

# (!) Примечание
# Пулу приложений Сервиса Аудита необходимо выдать
# права на доступ к закрытому нового сервисного сертификата

# (!) Примечание
# После изменения настроек сертификатов необходимо перезапустить пул приложения при
# помощи команды Restart-DssAnalyticsInstance.

# Смена сервисного 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

# (!) Примечание
# После изменения настроек сертификатов необходимо перезапустить пул приложения при
# помощи команды Restart-DssStsInstance.
```

Пример назначения и смены сертификата Сервиса Обработки Документов

Назначение и/или смена сервисного сертификата Сервиса Обработки Документов происходит в два этапа:

- Назначение и/или смена сервисного сертификата Сервиса Обработки Документов.
- Назначение и/или смена сертификата доверенной стороны на Центре Идентификации.

Ниже приводится пример Powershell-сценария, демонстрирующий смену сертификата Сервиса Обработки Документов.

Пример:

```
# Назначение и/или смена сервисного сертификата Сервиса Обработки Документов
Set-DSSDocumentStoreProperties -ServiceCertificate <thumbprint>

# (!) Примечание
# Пулу приложений Сервиса Обработки Документов необходимо выдать
# права на доступ к закрытому ключу нового сервисного сертификата

# (!) Примечание
# После изменения настроек сертификатов необходимо перезапустить пул приложения при
# помощи команды Restart-DssDocumentStoreInstance.

# Смена сервисного сертификата доверенной стороны на Центре Идентификации
Set-DssRelyingPartyTrust -Id <documentstore_ID> -AuthenticationCertificate <thumbprint>

# (!) Примечание
# После изменения настроек сертификатов необходимо перезапустить пул приложения при
# помощи команды Restart-DssStsInstance.
```

Диагностика

Раздел содержит информацию, необходимую для сбора сведений о работе КриптоПро DSS и устранения возможных незначительных неполадок.

Для получения оперативной технической поддержки необходимо приобрести сертификат технической поддержки по продукту КриптоПро DSS (см. Форма заказов) и зарегистрировать его на Портале технической поддержки.

В этом разделе:

- Перезапуск пулов приложений
- Устранение неполадок
- Импорт и экспорт конфигурации экземпляров
- Журналы Windows
- Журналирование
- Коды состояния HTTP, используемые в службах IIS

См. также:

- КриптоПро Центр Мониторинга

Перезапуск пулов приложений

После изменения конфигурации одного или нескольких экземпляров компонентов КриптоПро DSS требуется перезапуск его пула приложений. Если необходимо перезапустить несколько пулов, можно использовать следующую команду для перезапуска всего веб-сервера:

```
iisreset
```

Для удобства может быть перезапущен пул приложения только одного компонента. Для этого используются командлеты вида `Restart-*Instance`.

Синтаксис:

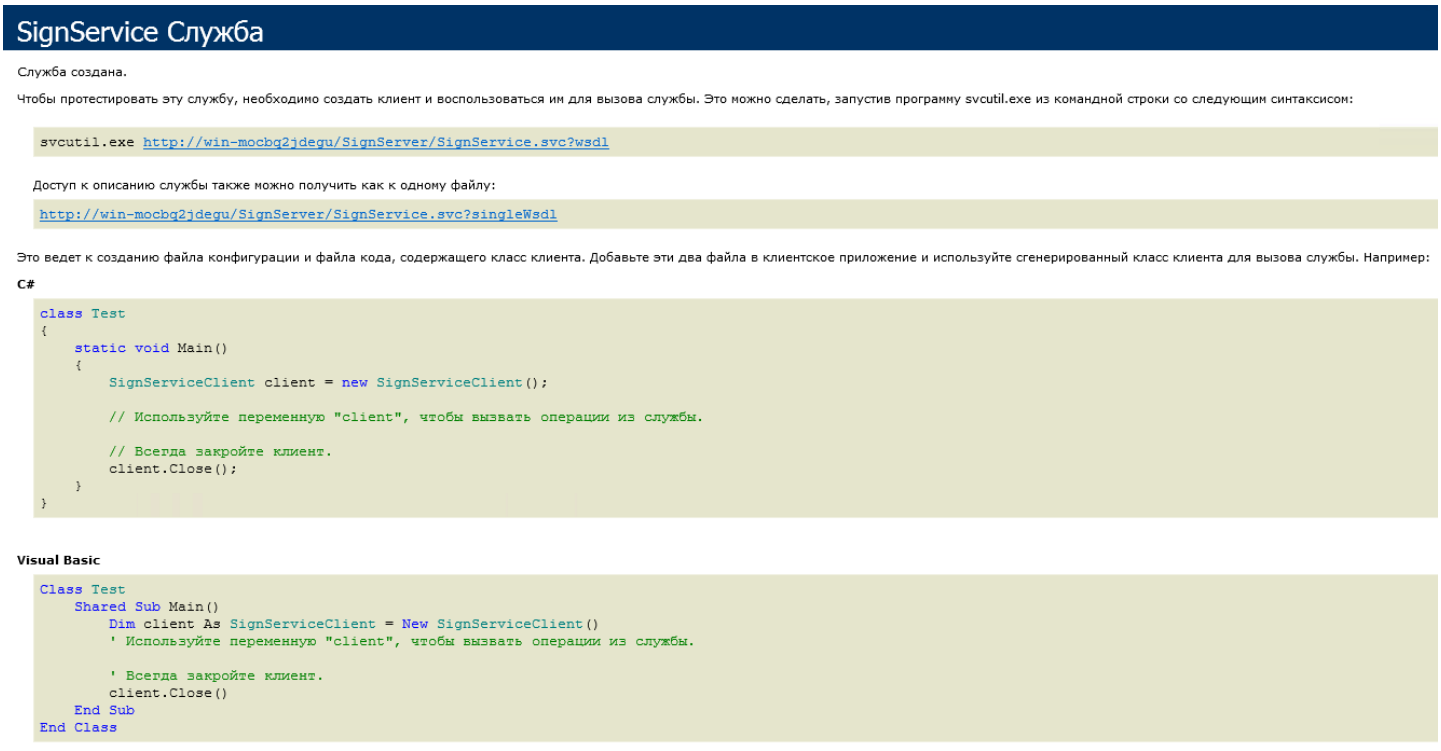
```
# Перезапуск пула приложений Сервиса Подписи:
Restart-DssSignServerInstance -DisplayName <string>

# Перезапуск пула приложений Центра Идентификации:
Restart-DssStsInstance -DisplayName <string>

# Перезапуск пула приложений Веб-интерфейса Пользователя:
Restart-DssFEInstance -DisplayName <string>

# Перезапуск пула приложений Сервиса Аудита:
Restart-DssAnalyticsServiceInstance -DisplayName <string>

# Перезапуск пула приложений mDAG:
Restart-MdagInstance -DisplayName <string>

# Перезапуск пула приложений Сервиса Обработки Документов:
Restart-DssDocumentStoreInstance -DisplayName <string>

# Перезапуск пула приложений Сервиса взаимодействия с мобильным приложением myDSS:
Restart-MyDssServerExternalInstance -DisplayName <string>

# Перезапуск пула приложений Сервиса взаимодействия с ЦИ:
Restart-MyDssServerInternalInstance -DisplayName <string>
```

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 таблице ниже.

КОМПОНЕНТ	СЛУЖБА	СТРАНИЦА ЗАПУСКА
Центр Идентификации	Служба выпуска маркеров безопасности	http://<host_name>/STS/active.svc
	Служба управления Пользователями	http://<hostname>/STS/usermanagement.svc
Сервис Подписи	Служба Сервиса Подписи	http://<hostname>//signserver/signservice.svc
Сервис Аудита	Служба обработки событий аудита	http://<hostname>/AnalyticsService/analyticsservice.svc
	Служба записей событий аудита	http://<hostname>/AnalyticsService/AuditWriter.svc
myDSS	Служба взаимодействия с ЦИ	http://<hostname>//MyDssServerInternal/service.svc
	Служба взаимодействия с мобильным приложением myDSS	http://<hostname>//MyDssServerExternal/InteractionService.svc

В случае правильной настройки компонента служба успешно запустится, и будет выведена веб-страница примерно следующего содержания:



SignService Служба

Служба создана.

Чтобы протестировать эту службу, необходимо создать клиент и воспользоваться им для вызова службы. Это можно сделать, запустив программу svcutil.exe из командной строки со следующим синтаксисом:

```
svcutil.exe http://win-mocbq2jdegu/SignServer/SignService.svc?wsdl
```

Доступ к описанию службы также можно получить как к одному файлу:

```
http://win-mocbq2jdegu/SignServer/SignService.svc?singleWsdl
```

Это ведет к созданию файла конфигурации и файла кода, содержащего класс клиента. Добавьте эти два файла в клиентское приложение и используйте сгенерированный класс клиента для вызова службы. Например:

C#

```
class Test
{
    static void Main()
    {
        SignServiceClient client = new SignServiceClient();

        // Используйте переменную "client", чтобы вызвать операции из службы.

        // Всегда закройте клиент.
        client.Close();
    }
}
```

Visual Basic

```
Class Test
    Shared Sub Main()
        Dim client As SignServiceClient = New SignServiceClient()
        ' Используйте переменную "client", чтобы вызвать операции из службы.

        ' Всегда закройте клиент.
        client.Close()
    End Sub
End Class
```

Если страница успешного запуска службы не появляется, необходимо обратиться к журналам Windows, где регистрируются ошибки запуска служб и другие системные события.

Импорт и экспорт конфигурации экземпляров

КриптоПро DSS позволяет экспортировать настройки экземпляров в файл, а также импортировать их из файла. Экспорт и импорт конфигурации экземпляров предназначен для переноса настроек с тестового СЭП на основной.

> **Примечание**
>
> Импорт и экспорт конфигурации экземпляров **НЕ** предназначен для резервирования настроек.

Импорт и экспорт конфигурации экземпляров доступен для экземпляров Сервиса Подписи, Центра Идентификации и Сервиса Аудита при помощи командлетов, приведенных в таблице ниже:

КОМПОНЕНТ DSS	КОМАНДЛЕТЫ
Центр Идентификации	Import-DssStsConfiguration, Export-DssStsConfiguration
Сервис Подписи	Import-DssSignServerConfiguration, Export-DssSignServerConfiguration
Сервис Аудита	Import-DssAnalyticsConfiguration, Export-DssAnalyticsConfiguration

Для каждого из перечисленных экземпляров к экспорту и импорту доступны различные типы конфигурации (наборы настроек), представленные в таблицах ниже.

> **Примечание**
>
> Импорт конфигурации экземпляров в некоторых случаях несовместим с уже имеющимися настройками экземпляра. В этом случае в таблице ниже в столбце «Возможность импорта на преднастроенный экземпляр» стоит знак «-» с указанием причины несоместимости.

Описание наборов настроек экземпляра Центра Идентификации

НАБОР НАСТРОЕК	ОПИСАНИЕ	ВОЗМОЖНОСТЬ ИМПОРТА НА ПРЕДНАСТРОЕННЫЙ ЭКЗЕМПЛЯР
IdentityConfiguration	Общие настройки экземпляра, настройки различительных имен Пользователей, области использования маркеров безопасности.	-, если есть зарегистрированные пользователи
IdentityProviders	Зарезервировано для дальнейшего использования.	-, если есть зарегистрированные пользователи
AuthnMethods	Настройки методов аутентификации.	-, если есть зарегистрированные пользователи
CryptoProviders	Настройки криптопровайдеров.	+
RelyingParties	Настройки доверенных сторон.	+
OauthClients	Настройки Oauth-клиентов.	+
Notifiers	Настройки модулей оповещения.	+
Events	Настройки событий и шаблонов событий.	+

Описание наборов настроек экземпляра Сервиса Подписи

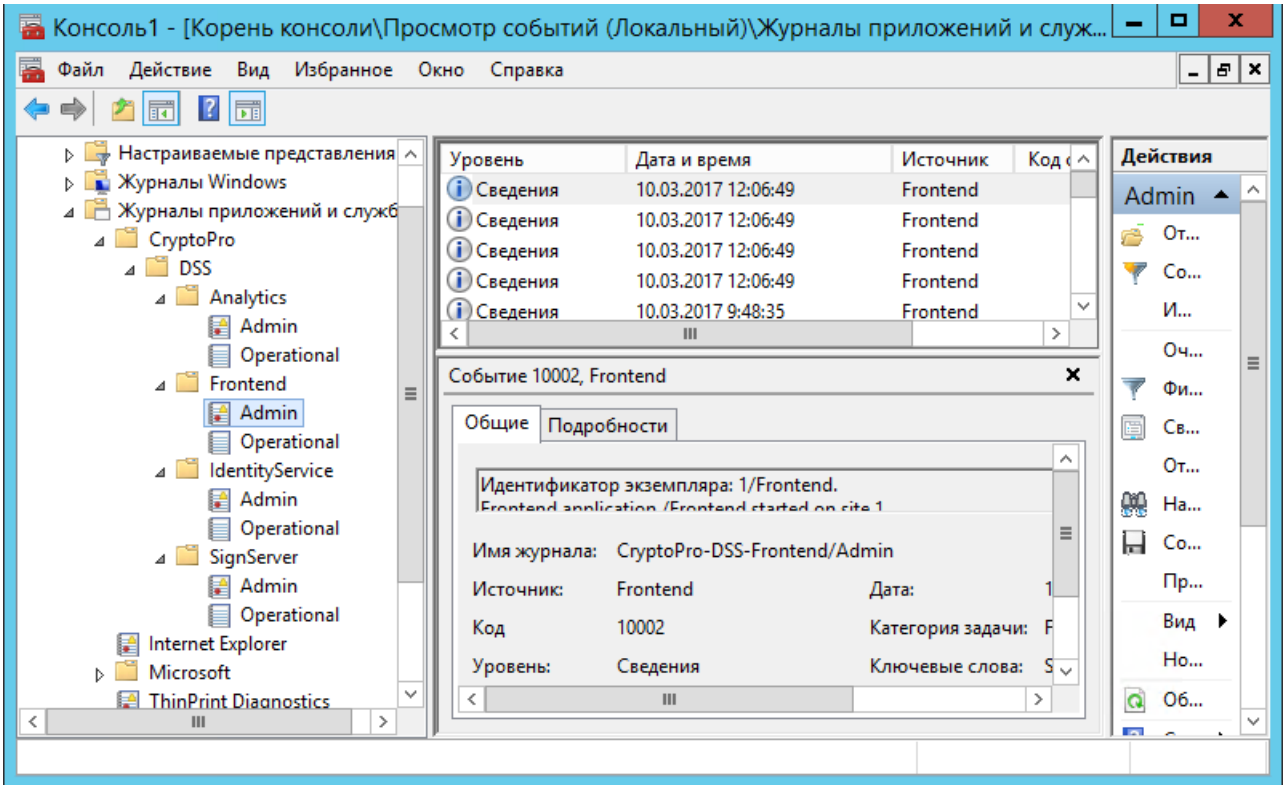
НАБОР НАСТРОЕК	ОПИСАНИЕ	ВОЗМОЖНОСТЬ ИМПОРТА НА ПРЕДНАСТРОЕННЫЙ ЭКЗЕМПЛЯР
Configuration	Общие настройки экземпляра.	+
CryptoProviders	Настройки криптопровайдеров.	-, если есть выпущенные сертификаты
Enrolls	Настройки обработчиков для генерации запросов на сертификат.	-, если есть выпущенные сертификаты
Notifiers	Настройки модулей оповещения.	+
Events	Настройки событий и шаблонов событий.	+

Описание наборов настроек экземпляра Сервиса Аудита

НАБОР НАСТРОЕК	ОПИСАНИЕ	ВОЗМОЖНОСТЬ ИМПОРТА НА ПРЕДНАСТРОЕННЫЙ ЭКЗЕМПЛЯР
Configuration	Общие настройки экземпляра.	+
CryptoProviders	Настройки криптопровайдеров.	+

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 (см. рисунок ниже). 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`.



Коды событий журналов КриптоПро DSS

Каждый компонент КриптоПро DSS использует для записи событий собственный журнал. Каждый журнал имеет два канала для записи:

- `Admins` - используется для записи административных событий.
- `Operational` - используется для записи отладочной информации о работе и состоянии соответствующего компонента.

Список компонентов DSS и соответствующие журналы событий

В таблице приведён список журналов и соответствующие им компоненты DSS.

НАЗВАНИЕ ЖУНАЛА	НАЗВАНИЕ КОМПОНЕНТА
Analytics	Сервис Аудита
Frontend	Веб-интерфейс Пользователя
Health Monitor	Центр Мониторинга
IdentityService	Центр Идентификации
MyDssServer	Модуль аутентификации myDSS

НАЗВАНИЕ ЖУНАЛА	НАЗВАНИЕ КОМПОНЕНТА
SignServer	Сервис Подписи

Журнал Центра Идентификации

В данном разделе приведено описание событий журнала Центра Идентификации.

КОД	НАЗВАНИЕ	УРОВЕНЬ	КАНАЛ	ОПИСАНИЕ	ПАРАМЕТРЫ	ФОРМАТ
65001	LexerNoViableAltException	Ошибка	Admins	Ошибка лексического разбора правила преобразования утверждения	---	:---
65002	ParserSyntaxError	Ошибка	Admins	Ошибка синтаксического разбора правила преобразования утверждения	---	:---
65101	IssuerDisabled	Информация	Admins	Издатель маркеров отключен	---	:---
65102	IssuerSigningKeyLoaded	Информация	Admins	Ключ проверки подписи издателя маркеров загружен	---	:---
65103	IssuerSigningKeyMissing	Ошибка	Admins	Ключ проверки подписи издателя маркеров не найден в хранилище	---	:---
65104	IssuerSigningKeyResolved	Подробно	Operational	Ключ проверки подписи доверенного издателя найден	---	:---
65105	IssuerSigningKeyUnResolved	Ошибка	Admins	Ключ проверки подписи доверенного издателя не найден	---	:---
65106	IssuerSigningTokenResolved	Подробно	Operational	Маркер безопасности доверенного издателя найден	---	:---

КОД	НАЗВАНИЕ	УРОВЕНЬ	КАНАЛ	ОПИСАНИЕ	ПАРАМЕТРЫ	ФОРМАТ
65107	IssuerSigningTokenUnResolved	Ошибка	Admins	Маркер безопасности доверенного издателя не найден	---	:---
65108	IssuerNameResolved	Подробно	Operational	Имя доверенного издателя найдено	---	:---
65109	IssuerNameUnResolved	Ошибка	Admins	Имя доверенного издателя не найдено	---	:---
65110	IssuerSigningTokensDownloadSucceeded	Подробно	Operational	Ключи проверки маркеров стороннего ЦИ успешно загружены	---	:---
65111	IssuerSigningTokensDownloadFailed	Ошибка	Admins	Произошла ошибка при загрузке ключей проверки маркеров стороннего ЦИ	---	:---
65112	IssuerSigningTokensImportFailed	Ошибка	Admins	Произошла ошибка при загрузке ключа проверки маркеров стороннего ЦИ	---	:---

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 в зависимости от компонента для которого выполняется настройка. Все модули содержат однотипный набор команд для настройки журналирования. Наборы командлетов в зависимости от компонента DSS приведены ниже:

- Сервис Подписи
- Центр Идентификации
- Сервис Аудита
- Веб-интерфейс Пользователя

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).

> **Примечание**
>
> Здесь XXX – имя компонента для которого настаивается оповещение: `SignServer` - для Сервиса Подписи, `FE` (Frontend) - для Веб-интерфейса Пользователя, `AnalyticsService` - для Сервиса Аудита, `UMS` (User Management Service) или `STS` (Security Token Service) - для Центра Идентификации.

Коды состояния HTTP, используемые в службах IIS

В этом разделе описываются коды состояния HTTP, используемые в службах IIS 7.0 и более поздних версиях.

> **Примечание**
>
> В данном разделе указаны не все коды состояния HTTP, приведенные в спецификации HTTP. В ней указаны только некоторые коды состояния HTTP, которые могут быть отправлены службами IIS 7.0 и более поздними версиями. Например, пользовательский фильтр ISAPI или HTTP-модуль могут задать собственный код состояния HTTP.

`3xx` — перенаправление

Эти коды состояния HTTP указывают, что для выполнения запроса браузер клиента должен выполнить дополнительные действия. например запросить другую страницу на сервере или Также клиентский браузер может повторить запрос, используя прокси-сервер.

В службах IIS 7.0 и более поздних версиях используются следующие статусные коды перенаправления HTTP:

- `301` — Перемещено навсегда.
- `302` — объект перемещен.
- `304` — объект не изменялся.
- `307` — временное перенаправление.

`4xx` — ошибка клиента

Эти коды состояния HTTP указывают, что произошла ошибка и возник сбой в работе браузера клиента. Например, браузер мог запросить страницу, которой не существует, или не предоставил правильные данные для проверки подлинности.

В службах IIS 7.0 и более поздних версиях используются указанные ниже коды ошибок клиента HTTP:

- `400` — неверный запрос. Серверу не удалось обработать запрос из-за синтаксических ошибок. Клиент не должен повторять запрос без изменений.

В IIS 7.0 и более поздних версиях определены следующие коды состояния HTTP, указывающие более точную причину ошибки `400`:

```
* 400.1 – Недопустимый заголовок назначения.
* 400.2 – Недопустимый заголовок глубины.
* 400.3 – Недопустимый заголовок "Если".
* 400.4 – Недопустимый заголовок перезаписи.
* 400.5 – Недопустимый заголовок передачи.
* 400.6 – Недопустимое тело запроса.
* 400.7 – Недопустимая длина содержимого.
* 400.8 – Недопустимое время ожидания.
* 400.9 – Недопустимая метка блокировки.
```

- `401` — Доступ запрещен.

В IIS 7.0 и более поздних версиях определены некоторые коды состояния HTTP, указывающие более точную причину ошибки `401`. Они отображаются на экране браузера, но не регистрируются в журнале служб IIS.

```
* 401.1 – Ошибка входа.
* 401.2 – вход не выполнен из-за настройки сервера.
* 401.3 – доступ запрещен списком управления доступом к ресурсу.
* 401.4 – доступ запрещен фильтром.
* 401.5 – авторизация не выполнена из-за приложения ISAPI/CGI.
* 401.501 – доступ запрещен: Слишком много запросов от одного IP-клиента; ограничение динамического IP-
адреса, достигнут лимит одновременных запросов.
* 401.502 – Запрещено: Слишком много запросов от одного IP-клиента; ограничение динамического IP-адреса,
достигнут максимальный лимит запросов.
* 401.503 – Доступ запрещен: IP-адрес включен в запрещающий список с ограничениями IP-адресов
* 401.504 – Доступ запрещен: имя узла включено в запрещающий список с ограничениями IP-адресов
```

- `403` — запрет.

В IIS 7.0 и более поздних версиях определены следующие коды состояния HTTP, указывающие более точную причину ошибки `403`:

```
* 403.1 – доступ на выполнение запрещен.
* 403.2 – доступ на чтение запрещен.
* 403.3 – доступ на запись запрещен.
* 403.4 – требуется SSL.
* 403.5 – требуется SSL 128.
* 403.6 – IP-адрес отклонен.
* 403.7 – требуется сертификат клиента.
* 403.8 – отказ в доступе к узлу.
* 403.9 – Запрещено: слишком много клиентов пытается подключиться к веб-серверу.
* 403.10 – Запрещено: веб-сервер настроен на запрет доступа на выполнение.
* 403.11 – Запрещено: пароль был изменен.
* 403.12 – Отказ доступа от программы сопоставления.
* 403.13 – сертификат клиента отозван.
* 403.14 – вывод каталогов запрещен.
* 403.15 – Запрещено: превышен лимит доступа клиентов на веб-сервере.
* 403.16 – Сертификат клиента поврежден или не является надежным.
* 403.17 – Срок действия сертификата клиента истек, либо сертификат еще не вступил в силу.
* 403.18 – Запрос указанного URL-адреса не может быть выполнен в текущем пуле приложений.
* 403.19 – Невозможно выполнять приложения CGI для этого клиента в данном пуле приложений.
* 403.20 – Запрещено: ошибка входа с паспортом.
* 403.21 – Запрещено: доступ к источнику запрещен.
* 403.22 – Запрещено: неограниченная глубина запрещена.
* 403.501 – Запрещено: Слишком много запросов от одного IP-клиента; ограничение динамического IP-адреса,
достигнут лимит одновременных запросов.
* 403.502 – Запрещено: Слишком много запросов от одного IP-клиента; ограничение динамического IP-адреса,
достигнут максимальный лимит запросов.
* 403.503 – Запрещено: IP-адрес включен в запрещенный список с ограничениями IP-адресов
* 403.504 – Запрещено: имя узла включено в запрещенный список с ограничениями IP-адресов
```

- `404` — объект не найден.

В IIS 7.0 и более поздних версиях определены следующие коды состояния HTTP, указывающие более точную причину ошибки `404`:

```
* 404,0 – объект не найден.
* 404.1 – Сайт не найден.
* 404.2 – Ограничение ISAPI или CGI.
* 404.3 – Ограничение типа MIME.
* 404.4 – Обработчик не настроен.
* 404.5 – Запрещено конфигурацией фильтров.
* 404.6 – Команда отклонена.
* 404.7 – Расширение имени файла отклонено.
* 404.8 – Скрытое пространство имен.
* 404.9 – Атрибут файла скрыт.
* 404.10 – Превышена допустимая длина заголовка запроса.
* 404.11 – Запрос содержит двойную escape-последовательность.
* 404.12 – Запрос содержит символы старшего разряда.
* 404.13 – Превышен лимит длины содержимого.
* 404.14 – Превышена допустимая длина URL-адреса запроса.
* 404.15 – Строка запроса слишком длинная.
* 404.16 – Запрос DAV отправлен статическому обработчику файла.
* 404.17 – Динамическое содержимое сопоставлено со статическим обработчиком файлов с помощью сопоставления
MIME с подстановочными знаками.
* 404.18 – Запрещенная последовательность строк запроса.
* 404.19 – Запрещено правилом фильтрации.
* 404.20 – Слишком много сегментов URL
* 404.501 – Не найдено: Слишком много запросов от одного IP-клиента; ограничение динамического IP-адреса,
достигнут лимит одновременных запросов.
* 404.502 – Не найдено: Слишком много запросов от одного IP-клиента; ограничение динамического IP-адреса,
достигнут максимальный лимит запросов.
* 404.503 – Не найдено: IP-адрес включен в запрещенный список с ограничениями IP-адресов
* 404.504 – Не найдено: имя узла включено в запрещенный список с ограничениями IP-адресов
```

- `405` — Недопустимый метод.
- `406` — Браузером клиента не принимается тип MIME запрашиваемой страницы.
- `408` — Превышено время ожидания для запроса.
- `412` — Необходимое условие не выполнено.

`5xx` — Ошибка сервера

Эти коды состояния HTTP указывают, что сервер не может выполнить запрос из-за ошибки.

В службах IIS 7.0 и более поздних версиях используются следующие коды ошибок сервера HTTP:

- `500` — внутренняя ошибка сервера.

В IIS 7.0 и более поздних версиях определены следующие коды состояния HTTP, указывающие более точную причину ошибки `500`:

```
* 500.0 – Ошибка модуля или ISAPI.
* 500.11 – Приложение на веб-сервере закрывается.
* 500.12 – Приложение на веб-сервере перезапускается.
* 500.13 – веб-сервер перегружен.
* 500.15 – Прямые запросы для Global.asax запрещены.
* 500.19 – Недопустимые данные конфигурации.
* 500.21 – Модуль не распознан.
* 500.22 – Конфигурация ASP.NET httpModules не применяется в режиме управляемого конвейера.
* 500.23 – Конфигурация ASP.NET httpHandlers не применяется в режиме управляемого конвейера.
* 500.24 –Конфигурация олицетворения ASP.NET не применяется в режиме управляемого конвейера.
* 500.50 – При обработке уведомления RQ_BEGIN_REQUEST произошла ошибка перезаписи. Возникла ошибка
конфигурации или выполнения правила для входящего подключения.
```

Примечание

Здесь конфигурация распределенных правил считывается как для входящих, так и для исходящих правил.

```
* 500.51 – При обработке уведомления GL_PRE_BEGIN_REQUEST произошла ошибка перезаписи. Возникла ошибка
глобальной конфигурации или выполнения глобального правила.
```

Примечание

Здесь читается конфигурация глобальных правил.

```
* 500.52 – При обработке уведомления RQ_SEND_RESPONSE произошла ошибка перезаписи. Возникла ошибка при
выполнении правила для исходящего подключения.
* 500.53 – При обработке уведомления RQ_RELEASE_REQUEST_STATE произошла ошибка перезаписи. Возникла ошибка
при выполнении правила для исходящего подключения. Настроено выполнение правила до обновления выходного кэша
пользователя.
* 500.100 – Внутренняя ошибка ASP.
* 501 – значения, указанные в заголовке, определяют нереализованную конфигурацию.
```

- `502` — веб-сервером в качестве шлюза или прокси-сервера получен недопустимый ответ.

В IIS 7.0 и более поздних версиях определены следующие коды состояния HTTP, указывающие более точную причину ошибки `502`:

```
* 502.1 – истекло время ожидания приложения CGI.
* 502.2 – Недопустимый шлюз: преждевременный выход.
* 502.3 – Недопустимый шлюз: ошибка перенаправленного подключения (ARR).
* 502.4 – Недопустимый шлюз: нет сервера (ARR).
```

- `503` — Служба недоступна.

В IIS 7.0 и более поздних версиях определены следующие коды состояния HTTP, указывающие более точную причину ошибки `503`:

```
* 503.0 – Пул приложений недоступен.
* 503.2 – Исчерпан предел одновременных запросов.
* 503.3 – Очередь ASP.NET переполнена
* 503.4 – очередь FastCGI переполнена
```

Файлы под контролем целостности

В КриптоПро DSS должны быть охвачены контролем целостности следующие файлы:

Сервис Подписи

```
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DbMigrator.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.Common.Clients.Rest.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.Common.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.Common.Enrollment.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.Common.Notification.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.Common.Web.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.DocumentStore.Client.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.Operations.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.Operations.EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.Operations.EntityFramework.Migration.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.PowerShell.Common.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.PowerShell.SignServer.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.SignatureServer.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\DSS.SignatureServer.Data.CommonMigration.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\DSS.SignatureServer.Data.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\DSS.SignatureServer.Data.Migration.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\DSS.SignatureServer.Diagnostics.CryptoPro-DSS-
SignServer.etwManifest.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\DSS.SignatureServer.Diagnostics.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\DSS.SignatureServer.Host.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\DSS.SignatureServer.Managers.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\DSS.SignatureServer.Services.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\EntityFramework.SqlServer.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\itextsharp.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.Common.Clients.Rest.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.Common.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.Common.Enrollment.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.Common.Notification.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.Common.Web.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.DocumentStore.Client.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.Operations.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.Operations.EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.Operations.EntityFramework.Migration.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.PowerShell.Common.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.SignatureServer.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.SignatureServer.Web.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\DSS.SignatureServer.Data.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\DSS.SignatureServer.Diagnostics.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\DSS.SignatureServer.Managers.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\EntityFramework.SqlServer.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\itextsharp.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\LightInject.WebApi.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\Microsoft.Owin.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\Microsoft.Owin.Host.SystemWeb.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\Microsoft.Owin.Security.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\Microsoft.Owin.Security.Jwt.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\Microsoft.Owin.Security.OAuth.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\Owin.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\System.IdentityModel.Tokens.Jwt.dll
```

```
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\System.Net.Http.Formatting.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\System.Web.Cors.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\System.Web.Http.Cors.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\System.Web.Http.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\System.Web.Http.Owin.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\System.Web.Http.Tracing.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\web.config
C:\Program Files\Crypto Pro\DSS\SignServer\Web.config
```

Центр Идентификации

```
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\csc.exe.config
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\Microsoft.Build.Tasks.CodeAnalysis.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\Microsoft.CodeAnalysis.CSharp.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\Microsoft.CodeAnalysis.CSharp.Scripting.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\Microsoft.CodeAnalysis.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\Microsoft.CodeAnalysis.Scripting.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\Microsoft.DiaSymReader.Native.amd64.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\Microsoft.DiaSymReader.Native.x86.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.AppContext.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Collections.Immutable.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Console.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Diagnostics.FileVersionInfo.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Diagnostics.StackTrace.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.IO.Compression.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.IO.FileSystem.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.IO.FileSystem.Primitives.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.IO.Pipes.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Reflection.Metadata.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Security.AccessControl.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Security.Claims.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Security.Cryptography.Algorithms.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Security.Cryptography.Encoding.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Security.Cryptography.Primitives.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Security.Cryptography.X509Certificates.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Security.Principal.Windows.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Text.Encoding.CodePages.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.ValueTuple.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Xml.ReaderWriter.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Xml.XmlDocument.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Xml.XPath.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Xml.XPath.XDocument.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\VBCSCompiler.exe.config
C:\Program Files\Crypto Pro\DSS\STS\bin\ru\Microsoft.AspNet.Identity.Core.resources.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\x64\libsass.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\AjaxMin.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Antlr3.Runtime.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Antlr4.Runtime.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Base3264-UrlEncoder.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\BouncyCastle.Crypto.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\BundleTransformer.Core.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\BundleTransformer.MicrosoftAjax.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\BundleTransformer.SassAndScss.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DbMigrator.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Analytics.Web.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Common.Clients.Rest.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Common.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Common.Notification.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Common.OpenIdConnect.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Common.Web.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.DocumentStore.Client.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Identity.Diagnostics.CryptoPro-DSS-
IdentityService.etwManifest.dll
```

```
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Identity.Diagnostics.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Identity.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Identity.EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Identity.EntityFramework.Migration.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Identity.Host.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Identity.Services.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Identity.Web.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Operations.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Operations.EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Operations.EntityFramework.Migration.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.PowerShell.Common.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.PowerShell.STS.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\EntityFramework.SqlServer.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\LibSassHost.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\LightInject.Web.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\LinqKit.EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.AspNet.Identity.Core.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.AspNet.Identity.EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.AspNet.Identity.Owin.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.AspNet.SignalR.Core.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.AspNet.SignalR.SqlServer.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.AspNet.SignalR.SystemWeb.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.CodeDom.Providers.DotNetCompilerPlatform.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.IdentityModel.Protocol.Extensions.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.Owin.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.Owin.Host.SystemWeb.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.Owin.Security.Cookies.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.Owin.Security.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.Owin.Security.Jwt.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.Owin.Security.OAuth.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.Owin.Security.WsFederation.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.Web.Infrastructure.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Owin.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.IdentityModel.Tokens.Jwt.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Net.Http.Formatting.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.Cors.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.Helpers.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.Http.Cors.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.Http.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.Http.Owin.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.Http.WebHost.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.Mvc.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.Optimization.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.Razor.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.WebPages.Deployment.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.WebPages.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.WebPages.Razor.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\WebGrease.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\zxing.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\zxing.presentation.dll
C:\Program Files\Crypto Pro\DSS\STS\Web.config
```

Веб-интерфейс Пользователя

```
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\x64\libsass.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\AjaxMin.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\Antlr3.Runtime.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\BundleTransformer.Core.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\BundleTransformer.MicrosoftAjax.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\BundleTransformer.SassAndScss.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\CryptoPro.DSS.Common.dll
```

```
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\CryptoPro.DSS.Common.Notification.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\CryptoPro.DSS.Common.OpenIdConnect.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\CryptoPro.DSS.Common.Web.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\DSS.Web.Frontend.Admins.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\LibSassHost.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\LightInject.Web.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\Microsoft.IdentityModel.Protocol.Extensions.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\Microsoft.Owin.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\Microsoft.Owin.Host.SystemWeb.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\Microsoft.Owin.Security.Cookies.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\Microsoft.Owin.Security.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\Microsoft.Owin.Security.Jwt.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\Microsoft.Owin.Security.OAuth.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\Microsoft.Web.Infrastructure.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\Owin.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\System.IdentityModel.Tokens.Jwt.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\System.Net.Http.Formatting.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\System.Web.Helpers.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\System.Web.Http.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\System.Web.Http.Owin.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\System.Web.Mvc.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\System.Web.Optimization.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\System.Web.Razor.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\System.Web.WebPages.Deployment.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\System.Web.WebPages.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\System.Web.WebPages.Razor.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\WebGrease.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\Views\Web.config
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\Web.config
C:\Program Files\Crypto Pro\DSS\Frontend\bin\x64\libsass.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\AjaxMin.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\Antlr3.Runtime.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\BundleTransformer.Core.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\BundleTransformer.MicrosoftAjax.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\BundleTransformer.SassAndScss.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.Analytics.Client.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.Analytics.Web.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.Cmis.Client.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.Cmis.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.Common.Clients.Rest.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.Common.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.Common.Notification.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.Common.OpenIdConnect.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.Common.Web.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.DocumentStore.Client.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.PowerShell.Common.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.PowerShell.Frontend.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.SignatureServer.Clients.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.SignatureServer.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.VerificationService.Web.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.VerificationService.WebApi.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\DSS.Web.Frontend.Diagnostics.CryptoPro-DSS-
Frontend.etwManifest.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\DSS.Web.Frontend.Diagnostics.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\DSS.Web.Frontend.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\LibSassHost.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\LightInject.Web.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\Microsoft.IdentityModel.Protocol.Extensions.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\Microsoft.Owin.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\Microsoft.Owin.Host.SystemWeb.dll
```

```
C:\Program Files\Crypto Pro\DSS\Frontend\bin\Microsoft.Owin.Security.Cookies.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\Microsoft.Owin.Security.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\Microsoft.Owin.Security.Jwt.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\Microsoft.Owin.Security.OAuth.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\Microsoft.Web.Infrastructure.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\Owin.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\System.IdentityModel.Tokens.Jwt.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\System.Net.Http.Formatting.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\System.Web.Helpers.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\System.Web.Http.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\System.Web.Http.Owin.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\System.Web.Mvc.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\System.Web.Optimization.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\System.Web.Razor.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\System.Web.WebPages.Deployment.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\System.Web.WebPages.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\System.Web.WebPages.Razor.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\WebGrease.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Views\Web.config
C:\Program Files\Crypto Pro\DSS\Frontend\Web.config
```

Сервис Аудита

```
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\x64\libsass.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\AjaxMin.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\Antlr3.Runtime.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\BundleTransformer.Core.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\BundleTransformer.MicrosoftAjax.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\BundleTransformer.SassAndScss.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DbMigrator.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Analytics.Data.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Analytics.Data.Migration.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Analytics.Diagnostics.CryptoPro-DSS-
Analytics.etwManifest.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Analytics.Diagnostics.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Analytics.Host.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Analytics.Services.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Analytics.Web.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Analytics.WebApi.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Common.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Common.Notification.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Common.Web.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Identity.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Identity.EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.PowerShell.Analytics.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.PowerShell.Common.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\EntityFramework.SqlServer.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\LibSassHost.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\LightInject.Web.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\LightInject.WebApi.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\Microsoft.AspNet.Identity.Core.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\Microsoft.AspNet.Identity.EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\Microsoft.Owin.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\Microsoft.Owin.Host.SystemWeb.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\Microsoft.Owin.Security.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\Microsoft.Owin.Security.Jwt.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\Microsoft.Owin.Security.OAuth.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\Microsoft.Web.Infrastructure.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\Owin.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\System.IdentityModel.Tokens.Jwt.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\System.Net.Http.Formatting.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\System.Web.Helpers.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\System.Web.Http.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\System.Web.Http.Owin.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\System.Web.Mvc.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\System.Web.Optimization.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\System.Web.Razor.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\System.Web.WebPages.Deployment.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\System.Web.WebPages.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\System.Web.WebPages.Razor.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\WebGrease.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\Web.config
```

Сервис Обработки Документов

```
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\csc.exe.config
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\Microsoft.Build.Tasks.CodeAnalysis.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\Microsoft.CodeAnalysis.CSharp.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\Microsoft.CodeAnalysis.CSharp.Scripting.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\Microsoft.CodeAnalysis.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\Microsoft.CodeAnalysis.Scripting.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\Microsoft.DiaSymReader.Native.amd64.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\Microsoft.DiaSymReader.Native.x86.dll
```

```
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.AppContext.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Collections.Immutable.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Console.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Diagnostics.FileVersionInfo.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Diagnostics.StackTrace.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.IO.Compression.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.IO.FileSystem.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.IO.FileSystem.Primitives.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.IO.Pipes.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Reflection.Metadata.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Security.AccessControl.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Security.Claims.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Security.Cryptography.Algorithms.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Security.Cryptography.Encoding.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Security.Cryptography.Primitives.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Security.Cryptography.X509Certificates.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Security.Principal.Windows.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Text.Encoding.CodePages.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.ValueTuple.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Xml.ReaderWriter.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Xml.XmlDocument.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Xml.XPath.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Xml.XPath.XDocument.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\VBCSCompiler.exe.config
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DbMigrator.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.Common.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.Common.Notification.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.DocumentStore.Data.Migration.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.DocumentStore.Data.Migration.NoFileStream.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.DocumentStore.Diagnostics.CryptoPro-DSS-
DocumentStore.etwManifest.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.DocumentStore.Diagnostics.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.DocumentStore.EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.DocumentStore.WebApi.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.PowerShell.Common.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.PowerShell.DocumentStore.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\EntityFramework.SqlServer.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\itextsharp.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\LightInject.WebApi.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Microsoft.CodeDom.Providers.DotNetCompilerPlatform.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Microsoft.Owin.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Microsoft.Owin.Host.SystemWeb.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Microsoft.Owin.Security.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Microsoft.Owin.Security.Jwt.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Microsoft.Owin.Security.OAuth.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Owin.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\System.IdentityModel.Tokens.Jwt.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\System.Net.Http.Formatting.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\System.Web.Http.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\System.Web.Http.Owin.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\System.Web.Http.Tracing.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\System.Web.Http.WebHost.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\Web.config
```

Сервис Взаимодействия с мобильным приложением (DSS SDK)

```
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\ru\Microsoft.AspNet.Identity.Core.resources.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Analytics.Client.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Common.Clients.Rest.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Common.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Common.Enrollment.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Common.Notification.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.DocumentStore.Client.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.DocumentStore.Client.dll.config
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Identity.Clients.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Identity.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.MyDss.ApiGateway.Diagnostics.CryptoPro-DSS-
MyDssApiGateway.etwManifest.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.MyDss.ApiGateway.Diagnostics.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.MyDss.ApiGateway.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.MyDss.ApiGateway.dll.config
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Operations.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Powershell.Common.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Powershell.MyDssApiGateway.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.SignatureServer.Clients.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.SignatureServer.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\LightInject.WebApi.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Microsoft.AspNet.Identity.Core.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Microsoft.AspNet.WebApi.Versioning.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Microsoft.Owin.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Microsoft.Owin.Host.SystemWeb.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Microsoft.Owin.Security.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Microsoft.SqlServer.ConnectionInfo.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Microsoft.SqlServer.Dmf.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Microsoft.SqlServer.Management.Sdk.Sfc.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Microsoft.SqlServer.ServiceBrokerEnum.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Microsoft.SqlServer.Smo.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Microsoft.SqlServer.SqlEnum.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Owin.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\System.Net.Http.Formatting.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\System.Web.Cors.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\System.Web.Http.Cors.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\System.Web.Http.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\System.Web.Http.Owin.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\Web.config
```

myDSS Server (myDSS 1.0)

```
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DbMigrator.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.Common.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.Common.Notification.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.Common.Web.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.MyDssServer.Cache.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.MyDssServer.Common.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.MyDssServer.Diagnostics.CryptoPro-DSS-
MyDssServer.etwManifest.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.MyDssServer.Diagnostics.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.MyDssServer.ExternalData.Migration.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.MyDssServer.ExternalServiceManagers.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.MyDssServer.InteractionPushService.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.MyDssServer.InteractionService.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.MyDssServer.Utility.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.PowerShell.Common.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.PowerShell.MyDssServerExternal.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\EntityFramework.SqlServer.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\Web.config
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DbMigrator.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.Common.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.Common.Notification.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.Common.Web.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.MyDssServer.Cache.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.MyDssServer.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.MyDssServer.Common.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.MyDssServer.Crypto.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.MyDssServer.Data.Migration.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.MyDssServer.Diagnostics.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.MyDssServer.Service.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.MyDssServer.Utility.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.PowerShell.Common.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.PowerShell.MyDssServerInternal.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\EntityFramework.SqlServer.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\QRCoder.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\zxing.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\zxing.presentation.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\Web.config
```

DSS Lite

```
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\bin\CryptoPro.DSS.Common.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\bin\CryptoPro.DSS.PowerShell.Common.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\bin\CryptoPro.DSS.PowerShell.LSS.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\bin\DSS.SignatureServer.Diagnostics.CryptoPro-DSS-
SignServer.etwManifest.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\bin\DSS.SignatureServer.Diagnostics.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\bin\DSS.SignatureServer.Lite.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\bin\itextsharp.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\CryptoPro.DSS.Common.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\DSS.SignatureServer.Diagnostics.CryptoPro-DSS-
SignServer.etwManifest.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\DSS.SignatureServer.Diagnostics.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\DSS.SignatureServer.Lite.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\DSS.SignatureServer.LiteWebApi.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\itextsharp.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\LightInject.WebApi.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\Microsoft.Owin.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\Microsoft.Owin.Host.SystemWeb.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\Owin.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\System.Net.Http.Formatting.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\System.Web.Cors.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\System.Web.Http.Cors.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\System.Web.Http.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\System.Web.Http.Owin.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\System.Web.Http.Tracing.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\Web.config
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\Web.config
```

Разделяемые сервисами компоненты

```
C:\Program Files\Crypto Pro\DSS\Plugins\Audit\DSS.Audit.AuditPlugin.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\Aspose.Words.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\CryptoPro.DSS.AnalyticsService.ReportPlugins.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\DSS.DocumentConverter.AuditRecords.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\DSS.DocumentConverter.Dtbs.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\DSS.DocumentConverter.eTokenPass.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\DSS.DocumentConverter.ExtractDocument.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\DSS.DocumentConverter.Feitian.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\DSS.DocumentConverter.Gemalto.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\DSS.DocumentConverter.Image.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\DSS.DocumentConverter.PdfStub.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\DSS.DocumentConverter.Preview.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\DSS.DocumentConverter.Word.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\itextsharp.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Custom\CryptoPro.DSS.Identity.Authentication.Notification.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Custom\CryptoPro.DSS.PushService.Mfms.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Custom\CryptoPro.DSS.PushService.Notification.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Custom\DSS.PushService.NotificationEx.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Custom\DSS.SimAuth.Notification.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Custom\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Custom\PushSharp.Apple.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Custom\PushSharp.Core.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Custom\PushSharp.Google.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Email\DSS.EmailService.SmtpPlugin.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Formatter\DSS.MessageFormatter.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Sms\AxSms64.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Sms\DevinoSmsPlugin.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Sms\DSS.SmsService.Mfms.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Sms\DSS.SmsService.MtsSms.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Sms\DSS.SmsService.SmppPlugin.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Sms\DSS.SmsService.SmsGate.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Sms\DSS.SmsService.Smsinfo.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Sms\DSS.SmsService.StubPlugin.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Transforms\CryptoPro.DSS.Xml.Transforms.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Transport\DSS.Notification.Transport.dll
C:\Program Files\Crypto Pro\DSS\Shared\DSS.SignatureServer.Data.AuditMigration.dll
```

Файлы под контролем целостности

В КриптоПро DSS должны быть охвачены контролем целостности следующие файлы:

Сервис Подписи

```
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DbMigrator.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.Common.Clients.Rest.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.Common.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.Common.Enrollment.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.Common.Notification.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.Common.Web.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.DocumentStore.Client.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.Operations.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.Operations.EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.Operations.EntityFramework.Migration.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.PowerShell.Common.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.PowerShell.SignServer.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\CryptoPro.DSS.SignatureServer.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\DSS.SignatureServer.Data.CommonMigration.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\DSS.SignatureServer.Data.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\DSS.SignatureServer.Data.Migration.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\DSS.SignatureServer.Diagnostics.CryptoPro-DSS-
SignServer.etwManifest.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\DSS.SignatureServer.Diagnostics.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\DSS.SignatureServer.Host.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\DSS.SignatureServer.Managers.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\DSS.SignatureServer.Services.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\EntityFramework.SqlServer.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\itextsharp.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\SignServer\bin\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.Common.Clients.Rest.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.Common.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.Common.Enrollment.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.Common.Notification.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.Common.Web.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.DocumentStore.Client.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.Operations.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.Operations.EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.Operations.EntityFramework.Migration.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.PowerShell.Common.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.SignatureServer.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\CryptoPro.DSS.SignatureServer.Web.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\DSS.SignatureServer.Data.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\DSS.SignatureServer.Diagnostics.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\DSS.SignatureServer.Managers.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\EntityFramework.SqlServer.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\itextsharp.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\LightInject.WebApi.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\Microsoft.Owin.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\Microsoft.Owin.Host.SystemWeb.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\Microsoft.Owin.Security.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\Microsoft.Owin.Security.Jwt.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\Microsoft.Owin.Security.OAuth.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\Owin.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\System.IdentityModel.Tokens.Jwt.dll
```

```
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\System.Net.Http.Formatting.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\System.Web.Cors.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\System.Web.Http.Cors.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\System.Web.Http.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\System.Web.Http.Owin.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\bin\System.Web.Http.Tracing.dll
C:\Program Files\Crypto Pro\DSS\SignServer\rest\web.config
C:\Program Files\Crypto Pro\DSS\SignServer\Web.config
```

Центр Идентификации

```
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\csc.exe.config
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\Microsoft.Build.Tasks.CodeAnalysis.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\Microsoft.CodeAnalysis.CSharp.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\Microsoft.CodeAnalysis.CSharp.Scripting.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\Microsoft.CodeAnalysis.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\Microsoft.CodeAnalysis.Scripting.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\Microsoft.DiaSymReader.Native.amd64.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\Microsoft.DiaSymReader.Native.x86.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.AppContext.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Collections.Immutable.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Console.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Diagnostics.FileVersionInfo.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Diagnostics.StackTrace.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.IO.Compression.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.IO.FileSystem.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.IO.FileSystem.Primitives.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.IO.Pipes.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Reflection.Metadata.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Security.AccessControl.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Security.Claims.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Security.Cryptography.Algorithms.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Security.Cryptography.Encoding.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Security.Cryptography.Primitives.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Security.Cryptography.X509Certificates.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Security.Principal.Windows.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Text.Encoding.CodePages.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.ValueTuple.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Xml.ReaderWriter.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Xml.XmlDocument.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Xml.XPath.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\System.Xml.XPath.XDocument.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\roslyn\VBCSCompiler.exe.config
C:\Program Files\Crypto Pro\DSS\STS\bin\ru\Microsoft.AspNet.Identity.Core.resources.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\x64\libsass.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\AjaxMin.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Antlr3.Runtime.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Antlr4.Runtime.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Base3264-UrlEncoder.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\BouncyCastle.Crypto.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\BundleTransformer.Core.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\BundleTransformer.MicrosoftAjax.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\BundleTransformer.SassAndScss.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DbMigrator.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Analytics.Web.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Common.Clients.Rest.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Common.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Common.Notification.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Common.OpenIdConnect.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Common.Web.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.DocumentStore.Client.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Identity.Diagnostics.CryptoPro-DSS-
IdentityService.etwManifest.dll
```

```
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Identity.Diagnostics.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Identity.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Identity.EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Identity.EntityFramework.Migration.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Identity.Host.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Identity.Services.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Identity.Web.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Operations.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Operations.EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.Operations.EntityFramework.Migration.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.PowerShell.Common.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\CryptoPro.DSS.PowerShell.STS.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\EntityFramework.SqlServer.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\LibSassHost.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\LightInject.Web.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\LinqKit.EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.AspNet.Identity.Core.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.AspNet.Identity.EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.AspNet.Identity.Owin.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.AspNet.SignalR.Core.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.AspNet.SignalR.SqlServer.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.AspNet.SignalR.SystemWeb.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.CodeDom.Providers.DotNetCompilerPlatform.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.IdentityModel.Protocol.Extensions.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.Owin.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.Owin.Host.SystemWeb.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.Owin.Security.Cookies.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.Owin.Security.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.Owin.Security.Jwt.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.Owin.Security.OAuth.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.Owin.Security.WsFederation.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Microsoft.Web.Infrastructure.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\Owin.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.IdentityModel.Tokens.Jwt.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Net.Http.Formatting.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.Cors.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.Helpers.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.Http.Cors.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.Http.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.Http.Owin.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.Http.WebHost.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.Mvc.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.Optimization.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.Razor.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.WebPages.Deployment.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.WebPages.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\System.Web.WebPages.Razor.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\WebGrease.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\zxing.dll
C:\Program Files\Crypto Pro\DSS\STS\bin\zxing.presentation.dll
C:\Program Files\Crypto Pro\DSS\STS\Web.config
```

Веб-интерфейс Пользователя

```
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\x64\libsass.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\AjaxMin.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\Antlr3.Runtime.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\BundleTransformer.Core.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\BundleTransformer.MicrosoftAjax.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\BundleTransformer.SassAndScss.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\CryptoPro.DSS.Common.dll
```

```
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\CryptoPro.DSS.Common.Notification.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\CryptoPro.DSS.Common.OpenIdConnect.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\CryptoPro.DSS.Common.Web.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\DSS.Web.Frontend.Admins.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\LibSassHost.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\LightInject.Web.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\Microsoft.IdentityModel.Protocol.Extensions.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\Microsoft.Owin.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\Microsoft.Owin.Host.SystemWeb.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\Microsoft.Owin.Security.Cookies.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\Microsoft.Owin.Security.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\Microsoft.Owin.Security.Jwt.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\Microsoft.Owin.Security.OAuth.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\Microsoft.Web.Infrastructure.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\Owin.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\System.IdentityModel.Tokens.Jwt.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\System.Net.Http.Formatting.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\System.Web.Helpers.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\System.Web.Http.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\System.Web.Http.Owin.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\System.Web.Mvc.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\System.Web.Optimization.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\System.Web.Razor.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\System.Web.WebPages.Deployment.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\System.Web.WebPages.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\System.Web.WebPages.Razor.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\bin\WebGrease.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\Views\Web.config
C:\Program Files\Crypto Pro\DSS\Frontend\Admins\Web.config
C:\Program Files\Crypto Pro\DSS\Frontend\bin\x64\libsass.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\AjaxMin.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\Antlr3.Runtime.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\BundleTransformer.Core.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\BundleTransformer.MicrosoftAjax.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\BundleTransformer.SassAndScss.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.Analytics.Client.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.Analytics.Web.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.Cmis.Client.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.Cmis.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.Common.Clients.Rest.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.Common.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.Common.Notification.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.Common.OpenIdConnect.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.Common.Web.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.DocumentStore.Client.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.PowerShell.Common.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.PowerShell.Frontend.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.SignatureServer.Clients.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.SignatureServer.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.VerificationService.Web.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\CryptoPro.DSS.VerificationService.WebApi.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\DSS.Web.Frontend.Diagnostics.CryptoPro-DSS-
Frontend.etwManifest.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\DSS.Web.Frontend.Diagnostics.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\DSS.Web.Frontend.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\LibSassHost.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\LightInject.Web.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\Microsoft.IdentityModel.Protocol.Extensions.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\Microsoft.Owin.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\Microsoft.Owin.Host.SystemWeb.dll
```

```
C:\Program Files\Crypto Pro\DSS\Frontend\bin\Microsoft.Owin.Security.Cookies.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\Microsoft.Owin.Security.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\Microsoft.Owin.Security.Jwt.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\Microsoft.Owin.Security.OAuth.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\Microsoft.Web.Infrastructure.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\Owin.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\System.IdentityModel.Tokens.Jwt.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\System.Net.Http.Formatting.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\System.Web.Helpers.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\System.Web.Http.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\System.Web.Http.Owin.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\System.Web.Mvc.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\System.Web.Optimization.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\System.Web.Razor.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\System.Web.WebPages.Deployment.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\System.Web.WebPages.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\System.Web.WebPages.Razor.dll
C:\Program Files\Crypto Pro\DSS\Frontend\bin\WebGrease.dll
C:\Program Files\Crypto Pro\DSS\Frontend\Views\Web.config
C:\Program Files\Crypto Pro\DSS\Frontend\Web.config
```

Сервис Аудита

```
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\x64\libsass.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\AjaxMin.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\Antlr3.Runtime.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\BundleTransformer.Core.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\BundleTransformer.MicrosoftAjax.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\BundleTransformer.SassAndScss.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DbMigrator.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Analytics.Data.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Analytics.Data.Migration.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Analytics.Diagnostics.CryptoPro-DSS-
Analytics.etwManifest.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Analytics.Diagnostics.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Analytics.Host.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Analytics.Services.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Analytics.Web.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Analytics.WebApi.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Common.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Common.Notification.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Common.Web.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Identity.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.Identity.EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.PowerShell.Analytics.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\CryptoPro.DSS.PowerShell.Common.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\EntityFramework.SqlServer.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\LibSassHost.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\LightInject.Web.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\LightInject.WebApi.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\Microsoft.AspNet.Identity.Core.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\Microsoft.AspNet.Identity.EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\Microsoft.Owin.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\Microsoft.Owin.Host.SystemWeb.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\Microsoft.Owin.Security.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\Microsoft.Owin.Security.Jwt.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\Microsoft.Owin.Security.OAuth.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\Microsoft.Web.Infrastructure.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\Owin.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\System.IdentityModel.Tokens.Jwt.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\System.Net.Http.Formatting.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\System.Web.Helpers.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\System.Web.Http.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\System.Web.Http.Owin.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\System.Web.Mvc.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\System.Web.Optimization.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\System.Web.Razor.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\System.Web.WebPages.Deployment.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\System.Web.WebPages.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\System.Web.WebPages.Razor.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\bin\WebGrease.dll
C:\Program Files\Crypto Pro\DSS\AnalyticsService\Web.config
```

Сервис Обработки Документов

```
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\csc.exe.config
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\Microsoft.Build.Tasks.CodeAnalysis.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\Microsoft.CodeAnalysis.CSharp.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\Microsoft.CodeAnalysis.CSharp.Scripting.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\Microsoft.CodeAnalysis.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\Microsoft.CodeAnalysis.Scripting.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\Microsoft.DiaSymReader.Native.amd64.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\Microsoft.DiaSymReader.Native.x86.dll
```

```
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.AppContext.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Collections.Immutable.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Console.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Diagnostics.FileVersionInfo.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Diagnostics.StackTrace.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.IO.Compression.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.IO.FileSystem.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.IO.FileSystem.Primitives.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.IO.Pipes.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Reflection.Metadata.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Security.AccessControl.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Security.Claims.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Security.Cryptography.Algorithms.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Security.Cryptography.Encoding.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Security.Cryptography.Primitives.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Security.Cryptography.X509Certificates.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Security.Principal.Windows.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Text.Encoding.CodePages.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.ValueTuple.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Xml.ReaderWriter.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Xml.XmlDocument.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Xml.XPath.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\System.Xml.XPath.XDocument.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Roslyn\VBCSCompiler.exe.config
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DbMigrator.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.Common.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.Common.Notification.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.DocumentStore.Data.Migration.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.DocumentStore.Data.Migration.NoFileStream.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.DocumentStore.Diagnostics.CryptoPro-DSS-
DocumentStore.etwManifest.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.DocumentStore.Diagnostics.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.DocumentStore.EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.DocumentStore.WebApi.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.PowerShell.Common.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\CryptoPro.DSS.PowerShell.DocumentStore.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\EntityFramework.SqlServer.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\itextsharp.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\LightInject.WebApi.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Microsoft.CodeDom.Providers.DotNetCompilerPlatform.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Microsoft.Owin.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Microsoft.Owin.Host.SystemWeb.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Microsoft.Owin.Security.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Microsoft.Owin.Security.Jwt.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Microsoft.Owin.Security.OAuth.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\Owin.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\System.IdentityModel.Tokens.Jwt.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\System.Net.Http.Formatting.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\System.Web.Http.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\System.Web.Http.Owin.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\System.Web.Http.Tracing.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\bin\System.Web.Http.WebHost.dll
C:\Program Files\Crypto Pro\DSS\DocumentStore\Web.config
```

Сервис Взаимодействия с мобильным приложением (DSS SDK)

```
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\ru\Microsoft.AspNet.Identity.Core.resources.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Analytics.Client.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Common.Clients.Rest.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Common.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Common.Enrollment.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Common.Notification.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.DocumentStore.Client.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.DocumentStore.Client.dll.config
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Identity.Clients.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Identity.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.MyDss.ApiGateway.Diagnostics.CryptoPro-DSS-
MyDssApiGateway.etwManifest.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.MyDss.ApiGateway.Diagnostics.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.MyDss.ApiGateway.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.MyDss.ApiGateway.dll.config
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Operations.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Powershell.Common.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.Powershell.MyDssApiGateway.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.SignatureServer.Clients.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\CryptoPro.DSS.SignatureServer.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\LightInject.WebApi.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Microsoft.AspNet.Identity.Core.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Microsoft.AspNet.WebApi.Versioning.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Microsoft.Owin.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Microsoft.Owin.Host.SystemWeb.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Microsoft.Owin.Security.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Microsoft.SqlServer.ConnectionInfo.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Microsoft.SqlServer.Dmf.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Microsoft.SqlServer.Management.Sdk.Sfc.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Microsoft.SqlServer.ServiceBrokerEnum.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Microsoft.SqlServer.Smo.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Microsoft.SqlServer.SqlEnum.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\Owin.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\System.Net.Http.Formatting.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\System.Web.Cors.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\System.Web.Http.Cors.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\System.Web.Http.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\bin\System.Web.Http.Owin.dll
C:\Program Files\Crypto Pro\DSS\MyDssApiGateway\Web.config
```

myDSS Server (myDSS 1.0)

```
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DbMigrator.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.Common.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.Common.Notification.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.Common.Web.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.MyDssServer.Cache.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.MyDssServer.Common.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.MyDssServer.Diagnostics.CryptoPro-DSS-
MyDssServer.etwManifest.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.MyDssServer.Diagnostics.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.MyDssServer.ExternalData.Migration.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.MyDssServer.ExternalServiceManagers.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.MyDssServer.InteractionPushService.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.MyDssServer.InteractionService.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.MyDssServer.Utility.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.PowerShell.Common.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\CryptoPro.DSS.PowerShell.MyDssServerExternal.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\EntityFramework.SqlServer.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\bin\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerExternal\Web.config
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DbMigrator.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.Common.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.Common.Notification.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.Common.Web.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.MyDssServer.Cache.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.MyDssServer.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.MyDssServer.Common.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.MyDssServer.Crypto.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.MyDssServer.Data.Migration.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.MyDssServer.Diagnostics.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.MyDssServer.Service.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.MyDssServer.Utility.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.PowerShell.Common.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\CryptoPro.DSS.PowerShell.MyDssServerInternal.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\EntityFramework.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\EntityFramework.SqlServer.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\QRCoder.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\zxing.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\bin\zxing.presentation.dll
C:\Program Files\Crypto Pro\DSS\MyDssServerInternal\Web.config
```

DSS Lite

```
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\bin\CryptoPro.DSS.Common.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\bin\CryptoPro.DSS.PowerShell.Common.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\bin\CryptoPro.DSS.PowerShell.LSS.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\bin\DSS.SignatureServer.Diagnostics.CryptoPro-DSS-
SignServer.etwManifest.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\bin\DSS.SignatureServer.Diagnostics.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\bin\DSS.SignatureServer.Lite.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\bin\itextsharp.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\CryptoPro.DSS.Common.Cryptography.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\CryptoPro.DSS.Common.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\CryptoPro.DSS.Common.Utils.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\DSS.SignatureServer.Diagnostics.CryptoPro-DSS-
SignServer.etwManifest.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\DSS.SignatureServer.Diagnostics.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\DSS.SignatureServer.Lite.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\DSS.SignatureServer.LiteWebApi.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\itextsharp.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\LightInject.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\LightInject.WebApi.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\Microsoft.Owin.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\Microsoft.Owin.Host.SystemWeb.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\Owin.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\System.Net.Http.Formatting.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\System.Web.Cors.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\System.Web.Http.Cors.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\System.Web.Http.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\System.Web.Http.Owin.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\bin\System.Web.Http.Tracing.dll
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\rest\Web.config
C:\Program Files\Crypto Pro\DSS\LiteSignatureService\Web.config
```

Разделяемые сервисами компоненты

```
C:\Program Files\Crypto Pro\DSS\Plugins\Audit\DSS.Audit.AuditPlugin.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\Aspose.Words.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\CryptoPro.DSS.AnalyticsService.ReportPlugins.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\DSS.DocumentConverter.AuditRecords.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\DSS.DocumentConverter.Dtbs.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\DSS.DocumentConverter.eTokenPass.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\DSS.DocumentConverter.ExtractDocument.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\DSS.DocumentConverter.Feitian.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\DSS.DocumentConverter.Gemalto.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\DSS.DocumentConverter.Image.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\DSS.DocumentConverter.PdfStub.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\DSS.DocumentConverter.Preview.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\DSS.DocumentConverter.Word.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\itextsharp.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Converters\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Custom\CryptoPro.DSS.Identity.Authentication.Notification.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Custom\CryptoPro.DSS.PushService.Mfms.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Custom\CryptoPro.DSS.PushService.Notification.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Custom\DSS.PushService.NotificationEx.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Custom\DSS.SimAuth.Notification.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Custom\Newtonsoft.Json.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Custom\PushSharp.Apple.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Custom\PushSharp.Core.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Custom\PushSharp.Google.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Email\DSS.EmailService.SmtpPlugin.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Formatter\DSS.MessageFormatter.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Sms\AxSms64.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Sms\DevinoSmsPlugin.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Sms\DSS.SmsService.Mfms.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Sms\DSS.SmsService.MtsSms.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Sms\DSS.SmsService.SmppPlugin.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Sms\DSS.SmsService.SmsGate.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Sms\DSS.SmsService.Smsinfo.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Sms\DSS.SmsService.StubPlugin.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Transforms\CryptoPro.DSS.Xml.Transforms.dll
C:\Program Files\Crypto Pro\DSS\Plugins\Transport\DSS.Notification.Transport.dll
C:\Program Files\Crypto Pro\DSS\Shared\DSS.SignatureServer.Data.AuditMigration.dll
```