Система электронной подписи

на базе ПАК «КриптоПро DSS»

Руководство администратора СЦИ (ADFS)

На 46 листах

СОДЕРЖАНИЕ

Оглавление
1. ОБЩИЕ ПОЛОЖЕНИЯ
2. ПОДКЛЮЧЕНИЕ СТОРОННЕГО ЦЕНТРА ИДЕНТИФИКАЦИИ ADFS 3.0 ПО ПРОТОКОЛУ WS-FEDERATION
2.1. Настройка отношения доверия между ЦИ КриптоПро DSS и ADFS 3.0
2.2. Добавление отношения доверия проверяющей стороны (Relying Party Trust, RP)7
2.3. Создание оператора, управляющего пользователями домена
2.4. Настройка правил преобразования утверждений для доступа к КриптоПро DSS Оператора, управляющего пользователями домена, и пользователей домена
3. ПОДКЛЮЧЕНИЕ СТОРОННЕГО ЦЕНТРА ИДЕНТИФИКАЦИИ ADFS WINDOWS
SERVER 2016 ТР4 ПО ПРОТОКОЛУ OPENID CONNECT 1.0
3.1. Создание группы приложений
3.2. Настройка отношения доверия между ЦИ КриптоПро DSS и ADFS Windows Server 2016TP429
3.3. Создание оператора, управляющего пользователями домена
3.4. Настройка правил преобразования утверждений для доступа к КриптоПро DSS Оператора, управляющего пользователями домена, и пользователей домена
4. «ПРОЗРАЧНАЯ» РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЕЙ AD В КРИПТОПРО DSS
ПРИЛОЖЕНИЕ А. УТВЕРЖДЕНИЯ ДОВЕРЕННОЙ СТОРОНЫ (MICROSOFT ACTIVE DIRECTORY), ПЕРЕДАВАЕМЫЕ В КРИПТОПРО DSS40
ПРИЛОЖЕНИЕ Б. ПРОБЛЕМЫ, ВОЗНИКАЮЩИЕ ПРИ АУТЕНТИФИКАЦИИ В КРИПТОПРО DSS С ИСПОЛЬЗОВАНИЕМ УЧЕТНЫХ ЗАПИСЕЙ AD42
Б1. ОШИБКА ПРИ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ AD
Б2. ОШИБКА «УЧЕТНЫЕ ДАННЫЕ НЕ СОДЕРЖАТ УТВЕРЖДЕНИЯ»
БЗ. ОШИБКА «Пользователь не состоит ни в одной роли, либо из внешнего ЦИ передан неверный набор утверждений»
Б4. ОШИБКА «ПРОВЕРКА СЕРТИФИКАТА ОБРАБОТЧИКОМ МАРКЕРОВ НЕ ПРОШЛА»
Б5. ОШИБКА «УЧЁТНЫЕ ДАННЫЕ ДОЛЖНЫ СОДЕРЖАТЬ ТОЛЬКО ОДНО УТВЕРЖДЕНИЕ»
Б6. ОШИБКА «ID4036»
Б7. ОШИБКА «ID4037»45

1. ОБЩИЕ ПОЛОЖЕНИЯ

Данный документ предназначен для специалиста, выполняющего роли Администратора Стороннего Центра Идентификации (Администратор СЦИ) и администратора системы электронной подписи (СЭП) на базе КриптоПро DSS 2.0. В документе описаны действия, необходимые для выполнения интеграции ЦИ КриптоПро DSS и СЦИ на базе Службы федерации корпоративного домена (Active Directory Federation Services, ADFS) с использованием протоколов WS-Federation (WSFed) или OpenId Connect 1.0 (Oidc).

ADFS используется для обеспечения аутентификации пользователей корпоративного домена при получении доступа к функциям СЭП.

ЦИ КриптоПро DSS напрямую с AD не взаимодействует и вся необходимая информация о пользователе, передаётся в маркере безопасности, сформированном ADFS на основе данных AD. В ADFS используется группа правил «Отправка атрибутов LDAP как утверждений», которая позволяет перекладывать поля из учётной записи пользователя AD в маркер безопасности в определённые утверждения. В этом маркере безопасности можно передать: компоненты различительного имени пользователя (Общее имя, ИНН, ОГРН и т.п.), телефон, адрес электронной почты. Полный перечень утверждений, которые могут быть переданы в ЦИ КриптоПро DSS, приведен в <u>Приложении A</u> «Утверждения доверенной стороны (Microsoft Active Directory), передаваемые в КриптоПро DSS».

Для выполнения работ по интеграции в соответствие с данным документом необходимо использование сборки КриптоПро DSS новее 2.0.3, ADFS 3.0 или выше (для подключения по протоколу WS-Federation) и ADFS в составе Windows Server 2016 TP4 или выше (для подключения по протоколу oidc). Также необходимо иметь доступ и права локального администратора к серверу с установленным компонентом ЦИ КриптоПро DSS, а также доступ и права доменного администратора к серверу с к серверу с развернутой службой ADFS.

При составлении текущего руководства использовались:

- КриптоПро DSS 2.0.2882;

- ADFS в составе Windows Server 2016 TP4 (для подключения по протоколу oidc) и ADFS 3.0 (для подключения по протоколу WS-Federation).

2. ПОДКЛЮЧЕНИЕ СТОРОННЕГО ЦЕНТРА ИДЕНТИФИКАЦИИ ADFS 3.0 ПО ПРОТОКОЛУ WS-FEDERATION

Подключение СЦИ ADFS 3.0 к ЦИ КриптоПро DSS по протоколу WS-Federation осуществляется в следующем порядке:

- Настройка отношения доверия между ЦИ КриптоПро DSS и ADFS 3.0;

- Добавления отношения доверия проверяющей стороны (Relying Party Trust, RP);

- Создание в ЦИ КриптоПро DSS оператора, управляющего пользователями домена;

- <u>Настройка правил преобразования утверждений для доступа к КриптоПро DSS Оператора,</u> управляющего пользователями домена, и пользователей домена.

2.1. Настройка отношения доверия между ЦИ КриптоПро DSS и ADFS 3.0

Для настройки отношения доверия между ЦИ КриптоПро DSS и ADFS 3.0 необходимо на сервере КриптоПро DSS сделать следующее:

Открыть PowerShell (Пуск» → Все программы → Windows Powershell) и выполнить командлеты:

Add-DssIdentityProvider -IssuerName ADFS -Title "Корпоративный Центр идентификации (ADFS)" -Description "Аутентификация корпоративных пользователей AD" -Thumbprint "Отпечаток сертификата ADFS для подписи маркера"

Set-DssIdentityProviderWSFedEndpoint -IssuerName ADFS WSFedEndpointUri https://adfs hostname/adfs/ls

Set-DssIdentityProvider -IssuerName ADFS -ShowInUi 1

где:

IssuerName – наименование СЦИ;

Title – заголовок СЦИ, отображаемый пользователю, в окне выбора Центра идентификации, при осуществлении аутентификации через-веб интерфейс КриптоПро DSS;

Description – описание СЦИ, отображаемое пользователю, в окне выбора Центра идентификации, при осуществлении аутентификации через-веб интерфейс КриптоПро DSS;

WSFedEndpointUri - адрес конечной точки ADFS для обработки пассивного сценария;

Thumbprint – отпечаток сертификата ADFS для подписи маркера. Данный сертификат должен быть помещён в хранилище «Доверенные лица» локального компьютера, на сервере КриптоПро DSS.

Сертификат выгружается с сервера ADFS после его первоначальной настройки следующим образом:

2.1.1. Открыть оснастку управления ADFS. Пуск-> Все программы-> Управление AD FS (см. рисунок 1):



Рисунок 1. Запуск мастера управления ADFS.

2.1.2. Откроется окно, выбрать последовательно «AD FS \rightarrow Служба \rightarrow Сертификаты \rightarrow Для подписи маркера». Затем открыть нужный сертификат для просмотра и нажать кнопку «Состав» (см. рисунок 2):



Рисунок 2. Выбор сертификата для выгрузки.

2.1.3. Откроется окно, нажать кнопку «Копировать в файл», откроется мастер экспорта сертификата, нажать кнопку «Далее» (см. рисунок 3).



Рисунок 3. Экспорт сертификата.

2.1.4. Откроется окно, выбрать формат сохраняемого файла, нажать кнопку «Далее» (см. рисунок 4):



Рисунок 4. Выбор формата сохраняемого файла.

2.1.5. Откроется окно, нажать кнопку «Обзор» (1), выбрать папку и указать имя для сохраняемого файла (2), нажать кнопку «Сохранить» (3) (см. Рисунок 5):



Рисунок 5. Сохранение файла с сертификатом.

2.1.6. Скопировать файл сертификата на сервер КриптоПро DSS и установить его в хранилище «Доверенные лица» локального компьютера.

2.1.7. Перезапустить пул приложений ЦИ КриптоПро DSS.

2.2. Добавление отношения доверия проверяющей стороны (Relying Party Trust, RP)

2.2.1. На сервере ADFS запустить консоль управления «Управление AD FS» (Пуск → все программы → «Управление AD FS» (см. рисунок 6).



Рисунок 6. Запуск консоли управления ADFS.

2.2.2. Откроется окно, выбрать последовательно «AD FS → Отношения доверия → Отношения доверия доверия проверяющей стороны». Нажать правой кнопкой мыши на пункте «Отношения доверия проверяющей стороны» и выбрать «Добавить отношение доверия проверяющей стороны…». (см. рисунок 7):



Рисунок 7. Добавление Проверяющей стороны

2.2.3. После этого откроется Мастер добавления отношений доверия проверяющей стороны.

В мастере необходимо нажать кнопку «Запустить» (см. рисунок 8):

Добро пожаловать!	
Шаги Добро пожаловать! Выбор источника данных Настроить многофакторную проверку подлинности? Выбор правил авторизации выдачи Готовность для доверия Готово	Вас приветствует мастер добавления отношения доверия с проверяющей стороной Этот мастер поможет вам добавить новое отношение доверия с проверяющей стороной в базу данных конфигурации AD FS. Проверяюще стороны используют утверждения в маркерах безопасности, выданные этой службой федерации, для принятия решений по авторизации и проверке подлинности. Отношение доверия с проверяющей стороной, создаваемое этим мастером, определяет, как данная служба федерации распознает проверяющую сторону и выдает для нее утверждения. После завершения работы мастера можно определить правила преобразования выдачи для выпуска утверждений для проверяющей стороны.

Рисунок 8. Запуск Мастера добавления отношений доверия проверяющей стороны

2.2.4. Произойдёт переход на следующий шаг мастера, на котором необходимо выбрать способ получения данных о проверяющей стороне *«Ввод данных о проверяющей стороне вручную»* и нажать кнопку «Далее» (см. Рисунок 9):

📬 Масте	р добавления отношений доверия проверяющей стороны	x
Выбор источника дан	ных	
 Шаги Добро пожаловать! Выбор источника данных Указание отображаемого имени Выберите профиль Настройка сертификата Настройка URL-адреса Настройка идентификатора Настройка идентификатора Настройка выбор правил авторизации выдачи Готовность для добавления отношения доверия Готово 	Выберите способ, используемый мастером для получения данных об этой проверяющей стор Импорт данных о проверяющей стороне, опубликованных в Интернете или локальной сети Выберите данный параметр, чтобы импортировать требуемые данные и сертификаты из организации проверяющей стороны, которая публикует метаданные федерации в Интерне в локальной сети. Адрес метаданных федерации (имя узла или URL-адрес): Пример: fs.contoso.com или https://www.contoso.com/app Импорт данных о проверяющей стороны из файла Выберите данный параметр, чтобы импортировать требуемые данные и сертификаты из организации проверяющей стороны, которая экспортировала метаданные федерации в ф Убедитесь, что этот файл получен от доверенного источника. Этот мастер не будет провер источник файла. Местоположение файлов метаданных федерации: Местоположение файлов метаданных федерации: Выберите данный параметр, чтобы ввести требуемые данные об организации проверяющей стороны вручную.	зоне: 4 эте или айл. эять зор
	< Назад Далее > Отм	лена

Рисунок 9. Выбор способа получения данных о проверяющей стороне

2.2.5. Указать отображаемое имя проверяющей стороны, а также примечания (см. рисунок 10):

🧌 Масто	ер добавления отношений доверия проверяющей стороны	x
Указание отображаем	иого имени	
Шаги	Для этой проверяющей стороны введите отображаемое имя и любые примечания.	
🥃 Добро пожаловать!	Отображаемое имя:	
😠 Выбор источника данных	CryptoPro DSS	
 Указание отображаемого имени 	Примечания:	
Выберите профиль	Центр идентификации КриптоПро DSS	^
 Настройка сертификата 		
😑 Настройка URL-адреса		
 Настройка идентификатора 		~
 Настроить многофакторную проверку подлинности? 		
 Выбор правил авторизации выдачи 		
 Готовность для добавления отношения доверия 		
🖌 Готово	< <u>Н</u> азад Д <u>а</u> лее > Отмена	

Рисунок 10. Ввод имени проверяющей стороны

2.2.6. После указания отображаемого имени на следующем шаге необходимо выбрать «Профиль ADFS» и нажать кнопку «Далее» (см. Рисунок 11):

🧌 Масте	ер добавления отношений доверия проверяющей стороны
Выберите профиль	
 Шаги Добро пожаловать! Выбор источника данных Указание отображаемого имени Выберите профиль Настройка сертификата Настройка URL-адреса Настройка URL-адреса Настройка идентификатора Настройка идентификатора Настроить многофакторную проверку подлинности? Выбор правил авторизации выдачи Готовность для добавления отношения доверия Готово 	При создании отношения доверия проверяющей стороны этот мастер использует в качестве вспомогательного средства профили конфигурации. Выберите подходящий профиль конфигурации для этого отношения доверия проверяющей стороны. • Профиль AD FS Этот профиль AD FS, например шифрование маркера безопасности и протокол SAML 2.0. • Профиль AD FS 1.0 и 1.1 Этот профиль noддерживает проверяющие стороны, поддерживающие работу со службами федерации AD FS версий 1.0 и 1.1.
	< Назад Далее > Отмена

Рисунок 11. Выбор профиля ADFS

2.2.7. Далее будет предложен выбор сертификата шифрования исходящего маркера – эту операцию можно пропустить, нажав кнопку *«Далее»* (см. Рисунок 12):

📬 Мастер добавления отно	ошений доверия проверяющих сторон	×
Настройка сертифика	та	
 Шаги Добро пожаловать! Выберите источник данных Укажите отображаемое имя Выберите профиль Настройте сертификат Настройте URL-адрес Настройте правила авторизации выдачи Готовность для добавления отношения доверия Готово 	Укажите дополнительный сертификат шифрования маркера. Сертификат шифрования маркера используется для шифрования утверждений, отправляемых этой проверяющай стороне. Для использовать закрытый иле отого сертификата. Чтобы указать сертификат, нажинте кнопку "Обзор". Издатель: Тема: Дата вступления в силу: Дата окончания срока действия: Просмотр Обзор Удалить Удалить	
	< <u>Н</u> азад Далее > Отмена <u>С</u> правк	

Рисунок 12. Выбор сертификата шифрования исходящего маркера

Примечание: в случае, если предполагается использование протокола WS-Trust – на данном шаге руководства необходимо выбрать сервисный сертификат ЦИ КриптоПро DSS, который выгружается из хранилища *«Личные»* локального компьютера сервера КриптоПро DSS и переносится на сервер ADFS.

Узнать отпечаток сервисного сертификата ЦИ КриптоПро DSS можно, выполнив на сервере КриптоПро DSS командлет в Powershell:

```
(Get-DssStsProperties).ServiceCertificate
```

2.2.8. Выбрать пункт «Включить поддержку пассивного протокола WS-Federation» и в качестве адреса пассивного протокола WS-Federation проверяющей стороны указать: <u>https://dss_hostname/STS_appname/Issue</u> (с соблюдением регистра). После этого необходимо нажать кнопку «Далее».

Где:

Dss_hostname – адрес сервера КриптоПро DSS;

STS_appname – имя приложения ЦИ КриптоПро DSS, которое можно узнать, выполнив на

сервере DSS в Powershell командлет:

Настройка URL-адреса

(Get-DssStsinstance).ApplicationName

Пример задания URL-адреса пассивного протокола WS-Federation проверяющей стороны на Рисунке 13:

훾 Мастер добавления отношений доверия проверяющей стороны

Х

Шаги Э Добро пожаловать! Выбор источника данных Указание отображаемого имени Настройка сертификата Настройка URL-адреса	Для проверяющих сторон AD FS поддерживает протоколы WS-Trust, WS-Federation и SAML 2.0 WebSSO. Если проверяющая сторона использует протокол WS-Federation, SAML или оба протокола, установите флажки, соответствующие этим протоколам, и затем укажите используемые URL-адреса. Для проверяющей стороны поддержка протокола WS-Trust всегда включена. ✓ Включить поддержку пассивного протокола WS-Federation URL-адрес пассивного протокола WS-Federation поддерживает поставщиков утверждений на основе веб-браузера, используя пассивный протокол WS-Federation.
 Настройка идентификатора 	URL-адрес <u>п</u> ассивного протокола WS-Federation проверяющей стороны: https://dsstest/sts/lssue
 Выбрать политику управления доступом 	Пример: https://fs.contoso.com/adfs/ls/
 Готовность для добавления отношения доверия Готово 	Вк <u>л</u> ючить поддержку протокола SAML 2.0 WebSSO URL-адрес службы SAML 2.0 единого входа (SSO) поддерживает поставщиков утверждений на основе веб-браузера, используя протокол SAML 2.0 WebSSO. URL-адрес службы <u>S</u> AML 2.0 SSO проверяющей стороны:
	Пример: https://www.contoso.com/adfs/ls/ < Назад Далее > Отмена

Рисунок 13. Включение поддержки WS-Federation

2.2.9. Откроется окно настройки идентификаторов. Необходимо нажать кнопку «Далее» (см. рисунок 14):

Паги	Проверяющие стороны можно идентифицировать по одному или нескольким	уникальным
Добро пожаловать!	идентификаторам. Укажите идентификаторы для этого отношения доверия пр	оверяющей стороны
Выбор источника данных	Идентификатор отношения доверия проверяющей стороны:	
Указание отображаемого		Добавит
имени	Пример: https://fs.contoso.com/adfs/services/trust	
Настройка сертификата	Идентификаторы отношений доверия проверяющей стороны:	
) Настройка URL-адреса	https://dsstest/sts/lssue	Удалить
 Настройка идентификатора 		
 Выбрать политику управления доступом 		
Готовность для добавления отношения доверия		
Готово		

Рисунок 14. Установка дополнительных идентификаторов проверяющей стороны

2.2.10. В окне выбора правил авторизации выдачи выберите пункт «*Разрешить доступ к этой* проверяющей стороне всем пользователям» и нажмите кнопку «Далее» (см. Рисунок 15):



Рисунок 15. Выбор правил авторизации пользователей при доступе к проверяющей стороне

2.2.11. Откроется окно подтверждения введённых данных, в котором необходимо нажать кнопку «Далее» (см. Рисунок 16):



Рисунок 16. Подтверждение введённых данных для выбора правил авторизации

2.2.12. В открывшемся окне необходимо нажать кнопку «Закрыть» (см. Рисунок 17).

01080	
 Шаги Добро пожаловать! Выбор источника данных Указание отображаемого	Отношение доверия проверяющей стороны успешно добавлено в базу данных конфигурации AD FS
имени Выберите профиль Настройка сертификата Настройка URL-адреса Настройка идентификатора Настройка идентификатора Настройка идентификатора Настройка идентификатора Выбор правил авторизации	Для изменения этого отношения доверия проверяющей стороны можно использовать диалоговое
выдачи Готовность для	окно "Свойства" в оснастке управления AD FS.
добавления отношения	✓ Открыть диалоговое окно "Изменение правил утверждений" для этого отношения
доверия Готово	доверия проверяющей стороны после закрытия мастера

Рисунок 17. Завершение работы Мастера добавления отношений доверия проверяющей стороны

2.3. Создание оператора, управляющего пользователями домена

Управление Пользователями домена и их сертификатами в КриптоПро DSS осуществляет Оператор, также зарегистрированный в одном AD с Пользователями (т.е. являющийся пользователем того же AD).

В качестве учетной записи Оператора должна использоваться отдельная учетная запись Пользователя AD (далее в руководстве - «*DSS-operator-AD*»). Это обусловлено тем, что Оператор DSS не имеет права подписывать документы в КриптоПро DSS.

Порядок создания Оператора следующий:

2.3.1. Создать в AD группу пользователей «DSS-Operators».

2.3.2. Перенести в группу «DSS-Operators» имеющуюся учетную запись пользователя, назначенного Оператором, или создать в этой группе новую четную запись пользователя AD для выполнения функций по управлению Пользователями КриптоПро DSS и их сертификатами.

2.3.3. На сервере КриптоПро DSS зарегистрировать Оператора, выполнив следующий командлет в Powershell:

Add-DssIdentityOperator -Login <u>DSS-operator-AD@domain.ru</u> -IssuerName ADFS -Name "Имя оператора DSS"

где:

IssuerName – наименование СЦИ;

Login – полное доменное имя Оператора;

Name – имя Оператора.

2.3.4. Перезапустить пул приложений ЦИ КриптоПро DSS.

Примечание: начиная со сборки КриптоПро DSS 2.0.3143, управление пользователями домена и их сертификатами в КриптоПро DSS могут осуществлять также Операторы ЦИ КриптоПро DSS (по умолчанию – состоящие в группе *«Default»*).

При необходимости можно указать особую группу ЦИ КриптоПро DSS, выполнив командлет в Powershell на сервере КриптоПро DSS:

Set-DssIdentityProvider -IssuerName ADFS -DefaultGroupName «Имя группы»

После выполнения вышеуказанного командлета, Операторы, состоящие в указанной группе, смогут управлять пользователями домена и их сертификатами.

2.4. Настройка правил преобразования утверждений для доступа к КриптоПро DSS

Оператора, управляющего пользователями домена, и пользователей домена.

Для аутентификации в КриптоПро DSS Оператора и пользователей AD необходимо добавить четыре основных правила. Правила должны быть добавлены в той же последовательности, что описана ниже.

2.4.1. На сервере ADFS запустить консоль управления «Управление AD FS» и выбрать последовательно «AD FS \rightarrow Отношения доверия \rightarrow Отношения доверия проверяющей стороны». Далее необходимо выбрать проверяющую сторону КриптоПро DSS с именем, заданным в <u>п. 2.2.5</u> и нажать кнопку «Изменить правила утверждения (см. Рисунок 21):



Рисунок 21. Изменение/добавление «правил утверждения»

2.4.2. Откроется окно добавления правил преобразований утверждений, в котором необходимо нажать кнопку *«Добавить правило….»* (см. рисунок 22):

По	Имя правила	Выпущенн	ые утвержде	
				1 +

Рисунок 22. Добавление правил преобразований утверждений

2.4.3. Откроется окно мастера добавления правил преобразования утверждений. Необходимо выбрать из выпадающего списка шаблон *«Отправка атрибута LDAP как утверждений»* и нажать кнопку *«Далее»* (см. Рисунок 23):

астер добавления правила преобразования утверждения					
вила					
В следующем списке выберите шаблон для правила утверждения, которое необходимо создать. Описание предоставляет сведения о каждом шаблоне правила утверждения.					
Шаблон правила утверждения:					
Отправка атрибутов LDAP как утверждений 🗸 🗸					
Описание шаблона правила утверждения:					
С помощью шаблона правила "Оттравка атрибутов LDAP как утверждений" можно выбирать атрибуты из хранилища атрибутов LDAP, например Active Directory, для оттравки в качестве утверждений проверяющей стороне. С помощью данного типа правила. Например, с помощью этого шаблона можно создать правило, которое будет извлекать значения атрибутов для прошедших проверку пользователей из атрибутов displayName и telephoneNumber Active Directory и затем оттравлять эти значения как дав различных исходящих утверждения. Это правило, также можно использовать для оттравки сведений о членстве пользователя во всех группах. Если требуется оттравить сведения о членстве пользователя в отдельных группах, используйте шаблон правила "Оттравка членства в группе как утверждения".					
< Назад Далее > Отмена					

Рисунок 23. Выбор шаблона правила утверждения

2.4.4. В следующем окне необходимо заполнить поля так, как представлено на рисунке 24. Данное преобразование переложит имя учётной записи Windows в утверждение name (<u>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</u>). Далее необходимо нажать кнопку *«Готово»*.

		to a contention in proceede	зования утверждения		
Настройка правила					
Шаги	Это правило можно настроить для отправки значений атрибутов LDAP как утверждений. Выберите хранилище атрибутов, из которого следует извлекать атрибуты LDAP. Укажите, как атрибуты будут сопоставляться с типами исходящих утверждений, которые будут выпускаться с помощью этого правила. Имя правила утверждения:				
😔 Выберите тип правила					
 Настройте правило утверждения 					
	UPN	to Name Claims			
	Шабл Храни	он правила. Отправка атрибутов LDAP и илище атрибутов:	ак утверждений		
	Active Directory				
	Сопоставление атрибутов LDAP типам исходящих утверждений:				
		Атрибут LDAP (выберите или введите, чтобы добавить больше)	Тип исходящего утверждения (выбер введите, чтобы добавить больше)	ите или	
	•	User-Principal-Name	Имя	~	
				~	

Рисунок 24. Создание правил преобразований утверждений.

2.4.5. Нажать кнопку «Добавить правило». Откроется окно мастера добавления правил преобразования утверждений. Необходимо выбрать из выпадающего списка шаблон «Отправка утверждений с помощью настраиваемого правила» и нажать кнопку «Далее» (см. Рисунок 25):

Выбор шаблона пра	вила
	DATIC
апи	В следующем списке выберите шаблон для правила утверждения, которое необходимо создать.
Выберите тип правила	Описание предоставляет сведения о каждом шаблоне правила утверждения.
Настройте правило	Шаблон правила утверждения:
утверждения	Отправка утверждений с помощью настраиваемого правила 🗸
	Описание шаблона правила утверждения:
	Для создания правил, которые нельзя создать с помощью шаблона правила, используются настраиваемые правила. Настраиваемые правила создаются с помощью языка правила: • отправка утверждений из хранилища атрибутов SQL; • отправка утверждений из хранилища атрибутов LDAP с помощью настраиваемого LDAP-фильтра; • отправка утверждений из хранилища настраиваемых атрибутов; • отправка утверждений по условии наличия 2 или более входящих утверждений; • отправка утверждений при условии соответствия значения входящего утверждения; составному шаблону; • отправка утверждений со сложными изменениями в значении входящего утверждения; • создание утверждений, используемых только в недавно созданных правилах.

Рисунок 25. Выбор шаблона правила преобразования утверждения.

2.4.6. Задать имя правила «Operator-Marker» и сценарий правила:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
Value == "S-1-5-21-867187777-3747453982-3702868088-75768", Issuer == "AD AUTHORITY"]
=> add(Type = "http://dss.cryptopro.ru/identity/claims/marker", Value = "true",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, ValueType = c.ValueType);
```

Это правило добавляет во входной набор утверждений утверждение с типом <u>http://dss.cryptopro.ru/identity/claims/marker</u> и со значением «true». Данное утверждение будет использовано при обработке последующих правил, в качестве индикатора, обозначающего, что маркер выпускается для оператора.

Значение *«S-1-5-21-867187777-3747453982-3702868088-75768»* в сценарии – это SID группы *«DSS-Operators»*, который можно узнать, выполнив на AD в Powershell командлет:

Get-ADGroup -Filter {Name -eq "DSS-Operators"}

После задания имени правила и сценария правила необходимо нажать кнопку «Готово».

2.4.7. Нажать кнопку «Добавить правило». Откроется окно мастера добавления правил преобразования утверждений. Необходимо выбрать из выпадающего списка шаблон «Отправка утверждений с помощью настраиваемого правила» и нажать кнопку «Далее».

2.4.8. Задать имя правила «Operator-Admins» и сценарий правила:

```
c:[Type == "http://dss.cryptopro.ru/identity/claims/marker", Value == "true",
Issuer == "AD AUTHORITY"]
```

=> issue(Type = "http://schemas.microsoft.com/ws/2008/06/identity/claims/role",
Value = "Admins", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, ValueType =
c.ValueType);

Это правило добавляет в выпускаемый маркер утверждение http://shemas.microsoft.com/ws/2008/06/identity/claims/role со значением «Admins», для входного набора утверждений из предыдущего правила.

После задания имени правила и сценария правила необходимо нажать кнопку «Готово».

2.4.9. Нажать кнопку «Добавить правило». Откроется окно мастера добавления правил преобразования утверждений. Необходимо выбрать из выпадающего списка шаблон «Отправка утверждений с помощью настраиваемого правила» и нажать кнопку «Далее».

2.4.10. Задать имя правила «Users» и сценарий правила:

```
NOT EXISTS([Type == "http://dss.cryptopro.ru/identity/claims/marker"])
```

=> issue(Type = "http://schemas.microsoft.com/ws/2008/06/identity/claims/role",
Value = "Users");

Это правило добавляет в выпускаемый маркер утверждение http:// schemas.microsoft.com/ws/2008/06/identity/claims/role со значением «Users», для входного набора утверждений из предыдущего правила.

После задания имени правила и сценария правила необходимо нажать кнопку «Готово».

3. ПОДКЛЮЧЕНИЕ СТОРОННЕГО ЦЕНТРА ИДЕНТИФИКАЦИИ ADFS WINDOWS SERVER 2016 ТР4 ПО ПРОТОКОЛУ OPENID CONNECT 1.0

Подключение СЦИ ADFS из состава Windows Server 2016 ТР4 к ЦИ КриптоПро DSS по протоколу OpenId Connect 1.0 осуществляется в следующем порядке:

- Создание группы приложений;

- Настройка отношения доверия между ЦИ КриптоПро DSS и ADFS Windows Server 2016 TP4;
- Создание оператора, управляющего пользователями домена;
- Настройка правил преобразования утверждений для доступа к КриптоПро DSS Оператора,

управляющего пользователями домена, и пользователей домена.

3.1. Создание группы приложений

3.1.1. На сервере ADFS запустить консоль управления «Управление AD FS» (Пуск → все программы → «Управление AD FS» (см. рисунок 26).



Рисунок 26. Запуск консоли управления ADFS.

3.1.2 Откроется окно, нажать правой кнопкой мыши на пункте «Группы приложений» и выбрать пункт «Добавить группу приложений» (см. Рисунок 27):

N AD FS		
🏟 Файл Действие Вид Окно Справка	a	
🔶 🏟 🙇 📰 🛛 🖬		
AD FS	Группы приложений	
Служба	Имя	Описание
Отношения доверия проверяющей стс	DSS-Server	
📔 Отношения доверия поставщиков утве		
📔 Группы приложений		
Добавить группу прилож	кений	
Вид	>	
Новое окно отсюда		
Обновить		
Справка		

Рисунок 27. Добавление группы приложений

3.1.3. После этого откроется мастер добавления групп приложений. Выбрать из списка шаблонов «Серверное приложение» (1), указать имя приложения (2), а затем нажать кнопку «Далее»
(3) (см. Рисунок 28):

翰 Мастер добавления груп	п приложений				×
Приветствие					
Шаги	Имя:				
Приветствие	DSS-Server		2		
 Приложение сервера 	0				
 Настроить учетные данные приложения 	Описание:				
😑 Сводка					
 Завершить 	Шаблон:				
	Клиент-серверны Собственное пр Серверное пр Веб-браузер, Автономные при Собственное п Собственное п Серверное пр	ые приложения приложение, подключаю иложение, подключаю подключающийся к вей ложения приложение иложение ис API	ющееся к веб-АРІ щееся к веб-АРІ б-приложению	1	
	Подробнее			3	
			< Назад	Далее >	Отмена

Рисунок 28. Мастер добавления групп приложений

3.1.4. Откроется окно. Необходимо скопировать и сохранить значение из поля «Идентификатор клиента» (1). Затем в поле «Перенаправить URI» (2) указать адрес: <u>https://hostname/STS/Authentication/External</u>

Где:

hostname – адрес сервера КриптоПро DSS;

STS - имя приложения ЦИ КриптоПро DSS, которое можно узнать, выполнив на сервере DSS, в Powershell, командлет:

(Get-DssStsinstance).ApplicationName

После указания адреса – нажать кнопку «Добавить» (3) (см. Рисунок 29):

훾 Мастер добавления груг	nn	приложений	×
Приложение сервера			
Шаги		Имя:	
Приветствие		DSS – Приложение сервера	
Приложение сервера		Идентификатор клиента:	
 Настроить учетные данные приложения 	1	23ad2d16-4cea-4983-a0e9-d65673e4aaa6	
😑 Сводка		Перенаправить URI:	3
🧧 Завершить	2	https://hostname/STS/Authentication/External	Добавить
			Удалить
		Описание:	
		< Назад Далее >	Отмена

Рисунок 29. Настройка приложения сервера

3.1.5. В окне настройки учетных данных приложения требуется установить чекбокс «*Co3damb* общий секрет». Далее необходимо скопировать и сохранить значение из поля «*Cekpem*». После этого – нажать кнопку далее (см. Рисунок 30):



Рисунок 30. Настройка учетных данных приложения



훾 Мастер добавления груп	п приложений	×
Сводка		
Шаги	Просмотрите следующие параметры и нажмите кнопку "Далее" для создания приложения.	
 Приветствие Приложение сервера Настроить учетные данные приложения Сводка Завершить 	Группа приложений Имя: DSS Приложение сервера Имя: DSS – Приложение сервера Идентификатор: c6e635ec-7eb344fd-9e6e-0211b1255b56 Перенаправить URI: https://hostname/STS/authentication/External Использовать секрет клиента: True	

Рисунок 31. Сводка данных группы приложений и серверного приложения

3.1.7. В окне завершения мастера добавления группы приложений нажать кнопку *«Закрыть»* (см. Рисунок 32):

🏟 Мастер добавления груп	п приложений Х
Готово	
Шаги	Группа приложений успешно создана.
Приветствие	
Приложение сервера	
 Настроить учетные данные приложения 	
🥥 Сводка	
🥥 Завершить	
	Закрыть

Рисунок 32. Завершение работы мастера добавления группы приложений

3.1.8. Откроется окно со списком созданных групп приложений. Открыть созданную группу приложений двойным кликом мышью (см. Рисунок 33):

🐐 AD FS							
翰 Файл Действие Вид Окно Справка							
AD FS	🔫 🐨 🖆 🛄 🛄 🛄 🚰 Группы приложений						
 Служба Политики контроля доступа Отношения доверия проверяющей ст Отношения доверия поставщиков утв Группы приложений 	Имя DSS-Server DSS	Описание					

Рисунок 33. Список созданных групп приложений

3.1.9. В окне свойств группы приложений необходимо нажать кнопку *«Добавить приложение»* (см. Рисунок 34):

Свойства DSS				×
Общие				
Имя:				
DSS				
Описание:				
Приложения:				
Имя		Описан	1e	
Серверное приложение				
DSS – Приложение сервера				
		_		
Добавить приложение		V	Ізменить	Удалить
	(Ж	Отмена	Применить

Рисунок 34. Свойства группы приложений

3.1.10. Выбрать из списка шаблонов *«Веб-интерфейс API»*. Нажать кнопку *«Далее»* (см. Рисунок 35):

🇌 Добавить новое приложе	ение в DSS
Приветствие	
Шаги	Имя:
 Приветствие 	DSS
 Настройка веб-интерфейса API 	Описание:
 Применение политики управления доступом 	
 Настроить разрешения для приложений 	Шаблон:
🥥 Сводка	Автономные приложения
 Завершить 	Собственное приложение Серверное приложение Вебчинтерфейс АРІ
	Подробнее
	< Назад Далее > Отмена

Рисунок 35. Добавление нового приложения в группу

3.1.11. В поле идентификатор требуется указать значение идентификатора клиента, полученное в <u>п. 3.1.4</u>, а затем – нажать кнопку *«Добавить»* (1). После этого необходимо нажать кнопку *«Далее»* (2) (см. Рисунок 36):

훾 Добавить новое приложе	ение в DSS	×
Настройка веб-интере	фейса АРІ	
Шаги	Имя:	
Приветствие	DSS – Веб-интерфейс API	
 Настройка веб-интерфейса API 	Идентификатор: 1	2
 Применение политики управления доступом 	c6e635ec-7eb3-44fd-9e6e-0211b1255b56	Добавить
 Настроить разрешения для приложений 		Удалить
😑 Сводка		
🧧 Завершить	Описание:	
	< Назад Далее >	Отмена

Рисунок 36. Указание идентификатора клиента

3.1.12. Выбрать политику «Разрешение для каждого» и нажать кнопку «Далее» (см. Рисунок

37):

-				
🖬 Добавить новое приложение в DSS				
Выбрать политику упр	равления доступом			
Шаги	Выберите политику управления доступом:			
 Приветствие Настройка веб-интерфейса API Применение политики управления доступом Настроить разрешения для приложений 	Имя Разрешение для каждого и запрос MFA Разрешение для каждого и запрос MFA для внешн Разрешение для каждого и запрос MFA для опреде Разрешение для каждого и запрос MFA с непровер Разрешение для каждого.	Описание Предоставьте доступ всем и запрашива Предоставление доступа пользователям Предоставление доступа каждому и зап Предоставьте доступ всем и запрашива Предоставление доступа каждому.		
приложении © Сводка © Завершить	Разрешение для определенной группы Разрешение доступа через интрасеть для каждого Разрешить всем и требовать MFA, разрешить авто	Предоставление доступа пользователям Предоставьте доступ пользователям инт Предоставить доступ всем и требовать		
	Политика Разрешение для каждого	гот раз. Ни один пользователь не получит		
		< Назад Далее > Отмена		

Рисунок 37. Политика управления доступом приложения

3.1.13. В списке разрешенных областей необходимо отметить области *«allatclaims»* и *«openid»*. Затем – нажать кнопку *«Далее»* (см. Рисунок 38):

🏟 Добавить новое приложе	ние в DSS		×
Настроить разрешени	я для приложе	ний	
Шаги Приветствие	Настроить разреше веб-интерфейсу АР	ения, чтобы позволить клиентским приложениям получать д I.	оступ к этому
 Настройка веб-интерфейса 	Приложения клиен	та (вызывающая сторона):	
АРТ Применение политики управления поступом	Имя DSS – Приложени	Описание не сервера	
 Настроить разрешения для приложений 			
⊚ Сводка ⊛ Завершитъ	Разрешенные обла	Добави	ть Удалить
	Имя области allatclaims aza mail logon_cert openid profile user_imperso	Описание Запрашивает утверждения маркера доступа в маркер Область позволяет клиенту брокера запрашивать осн Электронный запрос для зарегистрированного польз Область logon_cert позволяет приложению запрашива Запрос на использование протокола авторизации Ор Запрос профиля для зарегистрированного пользоват Запрос о предоставлении доступа в качестве зарегис	Создать область
		< Назад Дале	е > Отмена

Рисунок 38. Разрешенные области приложения

3.1.14. В следующем окне нажать кнопку «Далее» (см. Рисунок 39):

Сводка Шали Приветствие Настройка вебчитерфейса АРI Лрименения политики управления доступом Настройкъ разрешения для приложений Соводка Завершитъ Saвершитъ Saвершитъ	훾 Добавить новое приложе	ние в DSS	×
Шаги Просмотрите следующие параметры и нажмите кнопку "Далее" для создания приложения. • Приветствие Просмотрите следующие параметры и нажмите кнопку "Далее" для создания приложения. • Настройка вебинтерфейса дР! Имя: DSS • Сводка Имя: DSS - Вебинтерфейс дР! • Завершить Имя: DSS - Вебинтерфейс дР! • Обрука Оплитика контроля доступа: Разрешение для каждого. • Разрешения для приложений: DSS - Приложение сервера - openid allatclaims	Сводка		
< Назад Далее > Отмена	Шаги © Приветствие Настройка вебчинтерФейса АРI © Применение политики управления доступом Настроить разрешения для приложений © Сводка © Завершить	Просмотрите следнощие параметры и нажмите кнопку "Далее" для создания приложения. Группа приложений Имя: DSS Веб-интерфейс API Идентификаторы: c6e635ec-7eb3-44fd-9e6e-0211b1255b56 Политика контроля доступа: Разрешение для каждого. Разрешения для приложений: DSS – Приложение сервера - openid allatclaims (Назад Далее > Отмеже	

Рисунок 39. Сводка данных группы приложений и приложения веб-интерфейса

🏟 Добавить новое приложе	ение в DSS X
Готово	
Шаги	Группа приложений успешно создана.
Приветствие	
 Настройка веб-интерфейса API 	
 Применение политики управления доступом 	
 Настроить разрешения для приложений 	
😑 Сводка	
• Завершить	
	Закрыть

Рисунок 40. Завершение работы мастера добавления нового приложения

3.2. Настройка отношения доверия между ЦИ КриптоПро DSS и ADFS Windows Server 2016 TP4

Для настройки отношения доверия между ЦИ КриптоПро DSS и ADFS Windows Server 2016 TP4 необходимо на сервере КриптоПро DSS сделать следующее:

Открыть PowerShell (Пуск» → Все программы → Windows Powershell) и выполнить командлеты:

Add-DssIdentityProvider -IssuerName adfs_oidc -Title "Корпоративный Центр идентификации (ADFS)" -Description "Аутентификация корпоративных пользователей AD" -Thumbprint "Отпечаток сертификата ADFS для подписи маркера"

Set-DssIdentityProviderOidcEndpoint -IssuerName adfs_oidc -AuthorizationEndpoint <u>https://adfs hostname/adfs/oauth2/authorize</u> -ClientId «Идентификатор клиента» -ClientSecret «Секрет клиента» -Scopes "openid allatclaims"

Set-DssIdentityProvider -IssuerName adfs oidc -ShowInUi 1

Где:

IssuerName – наименование СЦИ;

Title – заголовок СЦИ, отображаемый пользователю, в окне выбора Центра идентификации, при осуществлении аутентификации через-веб интерфейс КриптоПро DSS;

Description – описание СЦИ, отображаемое пользователю, в окне выбора Центра идентификации, при осуществлении аутентификации через-веб интерфейс КриптоПро DSS;

AuthorizationEndpoint - адрес конечной точки ADFS;

ClientId – значение идентификатора клиента, полученное в п. 3.1.4;

ClientSecret – секрет клиента, полученный в <u>п. 3.1.5</u>.

Thumbprint – отпечаток сертификата ADFS для подписи маркера. Данный сертификат должен быть помещён в хранилище «Доверенные лица» локального компьютера, на сервере КриптоПро DSS.

Сертификат выгружается с сервера ADFS после его первоначальной настройки следующим образом:

3.2.1. Открыть оснастку управления ADFS. Пуск-> Все программы-> Управление AD FS (см. рисунок 41):



Рисунок 41. Запуск мастера управления ADFS.

3.2.2. Откроется окно, выбрать последовательно «AD FS → Служба → Сертификаты → Для подписи маркера». Затем открыть нужный сертификат для просмотра и нажать кнопку «Состав» (см. рисунок 42):

a	AD FS	_ D X
🏘 Файл Действие Вид Окно Справ	ка	_ 8 ×
🗢 🔿 📶 🚺 🖬		
AD FS	Сертификаты	Действия
Служоа Конечные точки	Тема Издатель Дата вступле Дата оконча Сост Перви	ч Сертификаты 🔺
Сертификаты 💙 2	Взаимодействие служб	Добавить сертификат для
Описания утверждений		Добавить сертификат для
 Отношения доверия Политики проверки подлинности 		Задать сертификат взаим
	Для подписи маркера	3 Вид 🕨
	CN=ADFS Signing - dss-20 CN=ADFS Signing - dss-2 30.08.2015 29.08.2016 Переи	Новое окно отсюда
		Обновить
	. Сертификат	🛛 Справка
	5 Общие Состав Путь сертификации	CN=ADFS Signing - dss-2
		Просмотр сертификата
	Сведения о сертификате	Назначить первичным
		4 Справка
	• Все политики выдачи	
	• Все политики применения	
	Кому выдан: ADFS Signing - dss-2012.test-dss.local	
	Кем выдан: ADFS Signing - dss-2012.test-dss.local	
	Деиствителен с 30.08.2015 по 29.08.2016	
	Установить сертификат Заявление поставщика	
		Активация Windows
		Чтобы активировать Windows,
	OK	переидите в компонент панели

Рисунок 42. Выбор сертификата для выгрузки.

3.2.3. Откроется окно, нажать кнопку «Копировать в файл», откроется мастер экспорта сертификата, нажать кнопку «Далее» (см. рисунок 43).



Рисунок 43. Экспорт сертификата.

3.2.4. Откроется окно, выбрать формат сохраняемого файла, нажать кнопку «Далее» (см. рисунок 44):



Рисунок 44. Выбор формата сохраняемого файла.

3.2.5. Откроется окно, нажать кнопку «Обзор» (1), выбрать папку и указать имя для сохраняемого файла (2), нажать кнопку «Сохранить» (3) (см. Рисунок 45):

	сохранение
📀 🄗 Мастер экспорта сертификатов	💿 💿 – 🛧 🔳 Рабочий стол 🕨 🗸 🗸 Поиск: Рабочий стол 🔎
	Упорядочить 🔻 Создать папку
Имя экспортируемого файла Укажите имя файла, который вы хотите экспортировать	✓ Избранное
Иня файла: Обзор	Редовние места Рабочий стол Этот компьютер
1	Р Этот компьютер II Библиотеки
	В Загрузки В Изображения Сеть
	и музыка Рабочий стол Докальный диск web Сертификат безопасности 1,78 КБ
	Z security (\\baran ∨ Имя файла adfs_dss √
	Тип файла: Двоичные файлы X.509 (*.cer) в кодировке DER 🗸 🗸
Далее Отк	Скрыть папки Скрыть папки Отмена

Рисунок 45. Сохранение файла с сертификатом.

3.2.6. Скопировать файл сертификата на сервер КриптоПро DSS и установить его в хранилище «Доверенные лица» локального компьютера.

3.2.7. Перезапустить пул приложений ЦИ КриптоПро DSS.

3.3. Создание оператора, управляющего пользователями домена

Управление Пользователями домена и их сертификатами в КриптоПро DSS осуществляет Оператор, также зарегистрированный в одном AD с Пользователями (т.е. являющийся пользователем того же AD).

В качестве учетной записи Оператора должна использоваться отдельная учетная запись Пользователя AD (далее в руководстве - «*DSS-operator-AD*»). Это обусловлено тем, что Оператор DSS не имеет права подписывать документы в КриптоПро DSS.

Порядок создания Оператора следующий:

3.3.1. Создать в AD группу пользователей «DSS-Operators».

3.3.2. Перенести в группу «DSS-Operators» имеющуюся учетную запись пользователя, назначенного Оператором, или создать в этой группе новую четную запись пользователя AD для выполнения функций по управлению Пользователями КриптоПро DSS и их сертификатами.

3.3.3. На сервере КриптоПро DSS зарегистрировать Оператора, выполнив следующий командлет в Powershell:

Add-DssIdentityOperator -Login <u>DSS-operator-AD@domain.ru</u> -IssuerName ADFS -Name "Имя оператора DSS"

где:

IssuerName – наименование СЦИ;

Login – полное доменное имя Оператора;

Name – имя Оператора.

3.3.4. Перезапустить пул приложений ЦИ КриптоПро DSS.

Примечание: начиная со сборки КриптоПро DSS 2.0.3143, управление пользователями домена и их сертификатами в КриптоПро DSS могут осуществлять также Операторы ЦИ КриптоПро DSS (по умолчанию – состоящие в группе *«Default»*).

При необходимости можно указать особую группу ЦИ КриптоПро DSS, выполнив командлет в Powershell на сервере КриптоПро DSS:

Set-DssIdentityProvider -IssuerName adfs_oidc -DefaultGroupName «Имя группы»

После выполнения вышеуказанного командлета, Операторы, состоящие в указанной группе, смогут управлять пользователями домена и их сертификатами.

3.4. Настройка правил преобразования утверждений для доступа к КриптоПро DSS

Оператора, управляющего пользователями домена, и пользователей домена.

Для аутентификации в КриптоПро DSS Оператора и пользователей AD необходимо добавить четыре основных правила. Правила должны быть добавлены в той же последовательности, что описана ниже.

3.4.1. На сервере ADFS запустить консоль управления «Управление AD FS», перейти на вкладку *«Группы приложений»* и выбрать группу приложений с именем, указанным в <u>п. 3.1.3</u> (см. Рисунок 46):

N AD FS						
翰 Файл Действие Вид Окно Справка 👉 🐟 🔀 📆 🖬						
AD FS	Группы приложений					
 Служба Политики контроля доступа Отношения доверия проверяющей ст Отношения доверия поставщиков утв Отношения доверия поставщиков утв Группы приложений 	Имя DSS-Server DSS	Описание				

Рисунок 46. Изменение/добавление «правил утверждения»

3.4.2. Открыть двойным кликом в свойствах группы приложений приложение типа *«Веб-интерфейс API»*, созданное в <u>п. 3.1.10</u> (см. Рисунок 47):

Свойства DSS	×
Общие	
Имя:	
DSS	
Описание:	
Приложения:	
Имя	Описание
Серверное приложение	
DSS – Приложение сервера	
Веб-интерфейс АРІ	
DSS – Веб-интерфейс API	
Добавить приложение	Изменить Удалить
	ОК Отмена Применить

Рисунок 47. Свойства группы приложений

3.4.3. Перейти на вкладку «Правила преобразования выдачи» и нажать кнопку «Добавить правило...» (см. Рисунок 48):

Свойства DSS — Веб-интерфейс API	×
Примечания Политика контроля доступа	Правила преобразования выдачи Разр 4 🕨
Следующие правила преобразования указ отправляться проверяющей стороне.	вывают утверждения, которые будут
По Имя правила	Выпущенные утвержде
Добавить правило <u>И</u> зменить пра	зило ⊻далить правило ОК Отмена <u>П</u> рименить

Рисунок 48. Добавление правил преобразований утверждений

3.4.4. Откроется окно мастера добавления правил преобразования утверждений. Необходимо выбрать из выпадающего списка шаблон *«Отправка атрибута LDAP как утверждений»* и нажать кнопку *«Далее»* (см. Рисунок 49):

Ýa N	Иастер добавления правила преобразования утверждения х
Выбор шаблона пра	вила
Шаги 🥥 Выберите тип правила	В следующем списке выберите шаблон для правила утверждения, которое необходимо создать. Описание предоставляет сведения о каждом шаблоне правила утверждения.
😔 Настройте правило	Шаблон правила утверждения:
утверждения	Отправка атрибутов LDAP как утверждений 🗸 🗸
	Описание шаблона правила утверждения:
	С помощью шаблона правила "Отправка атрибутов LDAP как утверждений" можно выбирать атрибуты из хранилища атрибутов LDAP, например Active Directory, для отправии в качестве утверждений проверяющей стороне. С помощью данного типа правила можно отправлять несколько атрибутов как несколько утверждений из одного правила. Например, с помощью этого шаблона можно создать правило, которое будет извлекать значения атрибутов для прошедиих проверку пользователей из атрибутов displeyName и telephoneNumber Active Directory и затем отправлять эти значения как два различных исходящих утверждения. Это правило также можно использовать для отправки сведений о членстве пользователя во всех группах. Если требуется отправить сведения о членстве пользователя во всех группах, используйте шаблон правила. "Отправка членства в группе как утверждения".

Рисунок 49. Выбор шаблона правила утверждения

3.4.5. В следующем окне необходимо заполнить поля так, как представлено на рисунке 50. Данное преобразование переложит имя учётной записи Windows в утверждение name (<u>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</u>). Далее необходимо нажать кнопку

«Готово».

Настройка правила				
Выберите тип правилаНастройте правило утверждения	Это правило можно настроить для отправки значений атрибутов LDAP как утверждений. Выберите хранилище атрибутов, из которого следует извлекать атрибуты LDAP. Укажите, как атрибуты будут сопоставляться с типами исходящих утверждений, которые будут выпускаться с помощью этого правила.			
	UPN	to Name Claims		
	Шабл Храни	он правила. Отправка атрибутов LDAP ка илище атрибутов:	ак утвержд	ений
	Active Directory V			
	Сопо	ставление атрибутов LDAP типам исходя	щих утверж	сдений:
	Атрибут LDAP (выберите или введите, чтобы добавить больше) Тип исходящего утверждения (выберите или введите, чтобы добавить больше)			
	•	User-Principal-Name	Имя	Ŷ
	*	×		~

Рисунок 50. Создание правил преобразований утверждений.

3.4.6. Нажать кнопку «Добавить правило». Откроется окно мастера добавления правил преобразования утверждений. Необходимо выбрать из выпадающего списка шаблон «Отправка утверждений с помощью настраиваемого правила» и нажать кнопку «Далее» (см. Рисунок 51):

Выбор шаблона правила

апи	В следующем списке выберите шаблон для правила утверждения, которое необходимо создать.				
Выберите тип правила	Описание предоставляет сведения о каждом шаблоне правила утверждения.				
Настройте правило	Шаблон правила утверждения:				
утверждения	Отправка утверждений с помощью настраиваемого правила 🗸 🗸				
	Описание шаблона правила утверждения:				
	Для создания правил, которые нельзя создать с помощью шаблона правила, используются настраиваемые правила. Настраиваемые правила создаются с помощью языка правил утверждений AD FS. Задачи, для выполнения которых требуются настраиваемые правила: отправка утверждений из хранилища атрибутов SQL; отправка утверждений из хранилища атрибутов LDAP с помощью настраиваемого LDAP-фильтра; отправка утверждений из хранилища настраиваемых атрибутов; отправка утверждений при условии наличия 2 или более входящих утверждений; отправка утверждений при условии соответствия значения входящего утверждения; отправка утверждений со сложными изменениями в значении входящего утверждения; создание утверждений, используемых только в недавно созданных правилах. 				

Рисунок 51. Выбор шаблона правила преобразования утверждения.

3.4.7. Задать имя правила «Operator-Marker» и сценарий правила:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
Value == "S-1-5-21-867187777-3747453982-3702868088-75768", Issuer == "AD AUTHORITY"]
=> add(Type = "http://dss.cryptopro.ru/identity/claims/marker", Value = "true",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, ValueType = c.ValueType);
```

Это правило добавляет во входной набор утверждений утверждение с типом <u>http://dss.cryptopro.ru/identity/claims/marker</u> и со значением «true». Данное утверждение будет использовано при обработке последующих правил, в качестве индикатора, обозначающего, что маркер выпускается для оператора.

Значение «*S*-1-5-21-867187777-3747453982-3702868088-75768» в сценарии – это SID группы «*DSS-Operators*», который можно узнать, выполнив на AD в Powershell командлет:

Get-ADGroup -Filter {Name -eq "DSS-Operators"}

После задания имени правила и сценария правила необходимо нажать кнопку «Готово».

3.4.8. Нажать кнопку «Добавить правило». Откроется окно мастера добавления правил преобразования утверждений. Необходимо выбрать из выпадающего списка шаблон «Отправка утверждений с помощью настраиваемого правила» и нажать кнопку «Далее».

4

3.4.9. Задать имя правила «Operator-Admins» и сценарий правила:

c:[Type == "http://dss.cryptopro.ru/identity/claims/marker", Value == "true", Issuer == "AD AUTHORITY"]

=> issue(Type = "http://schemas.microsoft.com/ws/2008/06/identity/claims/role",
Value = "Admins", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, ValueType =
c.ValueType);

Это правило добавляет в выпускаемый маркер утверждение http://shemas.microsoft.com/ws/2008/06/identity/claims/role со значением «Admins», для входного набора утверждений из предыдущего правила.

После задания имени правила и сценария правила необходимо нажать кнопку «Готово».

3.4.10. Нажать кнопку «Добавить правило». Откроется окно мастера добавления правил преобразования утверждений. Необходимо выбрать из выпадающего списка шаблон «Отправка утверждений с помощью настраиваемого правила» и нажать кнопку «Далее».

3.4.11. Задать имя правила «Users» и сценарий правила:

```
NOT EXISTS([Type == "http://dss.cryptopro.ru/identity/claims/marker"])
=> issue(Type = "http://schemas.microsoft.com/ws/2008/06/identity/claims/role",
Value = "Users");
```

Это правило добавляет в выпускаемый маркер утверждение http:// schemas.microsoft.com/ws/2008/06/identity/claims/role со значением «Users», для входного набора утверждений из предыдущего правила.

После задания имени правила и сценария правила необходимо нажать кнопку «Готово».

4. «ПРОЗРАЧНАЯ» РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЕЙ AD В КРИПТОПРО DSS

В КриптоПро DSS реализована поддержка «прозрачной» регистрации пользователей СЦИ, что позволяет пользователям AD пройти аутентификацию в КриптоПро DSS без необходимости выполнения предварительной регистрации данного пользователя Оператором.

Для включения «прозрачной» регистрации пользователей требуется выполнить командлет в Powershell на сервере КриптоПро DSS:

(Set-DssAccountPolicy -AccountCreationMode Transparent

После выполнения указанного выше командлета требуется перезапустить пул приложений ЦИ КриптоПро DSS.

Примечание: при осуществлении «прозрачной» регистрации пользователей методы вторичной аутентификации КриптоПро DSS не назначаются для пользователей автоматически. Методы вторичной аутентификации могут быть назначены пользователем в его личном кабинете, а также Оператором в его личном кабинете или с использованием API КриптоПро DSS.

Также при «прозрачной» регистрации пользователей для них не создается никаких сертификатов в автоматическом режиме.

ПРИЛОЖЕНИЕ А. УТВЕРЖДЕНИЯ ДОВЕРЕННОЙ СТОРОНЫ (MICROSOFT ACTIVE DIRECTORY), ПЕРЕДАВАЕМЫЕ В КРИПТОПРО DSS

В ПАК «КриптоПро DSS» могут быть переданы следующие утверждения:

Таблица 1. Утверждения доверенной стороны (Microsoft Active Directory), передаваемые в ПАК «КриптоПРО DSS»

Идентификатор утверждения	Описание	Комментарии
Обязательные		
http://schemas.xmlsoap.org/ws/2005/05/identit y/claims/name	Логин	Уникальный идентификатор в пределах ЦИ
http://schemas.microsoft.com/ws/2008/06/iden tity/claims/role	Роль пользователя в DSS	Users (пользователь) или Admins (оператор)
Опциональные		
http://dss.cryptopro.ru/identity/claims/group	Группа пользователей	Группа пользователей в DSS
http://schemas.xmlsoap.org/ws/2005/05/identit y/claims/mobilephone	Номер мобильного телефона	
http://dss.cryptopro.ru/identity/claims/ogrn	ОГРН	Компонент имени субъекта
http://dss.cryptopro.ru/identity/claims/ogrnip	ОГРНИП	Компонент имени субъекта
http://dss.cryptopro.ru/identity/claims/snils	СНИЛС	Компонент имени субъекта
http://dss.cryptopro.ru/identity/claims/inn	ИНН	
http://schemas.xmlsoap.org/ws/2005/05/identit y/claims/emailaddress	Адрес электронной почты	Компонент имени субъекта, но может использоваться и самостоятельно.
http://schemas.xmlsoap.org/ws/2005/05/identit y/claims/country	Страна	Компонент имени субъекта
http://schemas.xmlsoap.org/ws/2005/05/identit y/claims/stateorprovince	Область	Компонент имени субъекта
http://schemas.xmlsoap.org/ws/2005/05/identit y/claims/locality	Город	Компонент имени субъекта
http://dss.cryptopro.ru/identity/claims/organiza tion	Организация	Компонент имени субъекта
http://dss.cryptopro.ru/identity/claims/organiza tionunit	Отдел	Компонент имени субъекта
http://schemas.xmlsoap.org/claims/CommonN ame	Общее имя	Компонент имени субъекта
http://schemas.xmlsoap.org/ws/2005/05/identit y/claims/streetaddress	Адрес	Компонент имени субъекта
http://dss.cryptopro.ru/identity/claims/title	Должность	Компонент имени субъекта
http://dss.cryptopro.ru/identity/claims/initials	Инициалы	Компонент имени субъекта
http://schemas.xmlsoap.org/ws/2005/05/identit y/claims/givenname	Имя, Отчество	Компонент имени субъекта

http://schemas.xmlsoap.org/ws/2005/05/identit y/claims/surname	Фамилия	Компонент имени субъекта
http://schemas.xmlsoap.org/ws/2005/05/identit y/claims/x500distinguishedname	Различительно е имя субъекта сертификата	В значение этого клейма можно положить полностью различительное имя субъекта сертификата, в таком случае передавать отдельно каждый компонент не требуется. Значение данного утверждения должно быть предварительно закодировано в соответствии с правилами X500.

ПРИЛОЖЕНИЕ Б. ПРОБЛЕМЫ, ВОЗНИКАЮЩИЕ ПРИ АУТЕНТИФИКАЦИИ В КРИПТОПРО DSS С ИСПОЛЬЗОВАНИЕМ УЧЕТНЫХ ЗАПИСЕЙ AD

Б1. Ошибка при аутентификации пользователя АD

При аутентификации пользователя AD в КриптоПро DSS появляется ошибка (см. рисунок 52):



Произошла ошибка

Произошла ошибка. Для получения дополнительных сведений обратитесь к администратору.

Сведения об ошибке

Рисунок 52. Ошибка аутентификации

При анализе журнала ADFS можно обнаружить следующую ошибку (см. рисунок 53):



Рисунок 53. Ошибка в журнале ADFS, возникающая при попытке пройти аутентификацию

Возможная причина возникновения ошибки: указан некорректный адрес проверяющей стороны КриптоПро DSS в ADFS/адрес указан без соблюдения регистра.

Б2. Ошибка «Учетные данные не содержат утверждения»

При аутентификации пользователя AD в КриптоПро DSS, после ввода учетных данных, появляется ошибка «Учетные данные не содержат утверждения <u>http://schemas.microsoft.com/ws/2008/06/identity/claims/role»</u> (см. рисунок 54):

Во время работы приложения произошла ошибка.

Информация об ошибке:

Учётные данные не содержат утверждения http://schemas.microsoft.com/ws/2008/06/identity/claims/role

Рисунок 54. Ошибка «Учетные данные не содержат утверждения»

Возможные причины возникновения ошибки:

в ADFS не добавлены правила преобразования утверждений, в соответствие с <u>п. 2.4</u> – для
 WSFed или <u>п. 3.4 текущего руководства</u> – для Oidc.

- были допущены ошибки при добавлении правил преобразования утверждений.

БЗ. Ошибка «Пользователь не состоит ни в одной роли, либо из внешнего ЦИ передан неверный набор утверждений»

При аутентификации пользователя AD в КриптоПро DSS, после ввода учетных данных, появляется ошибка «Пользователь не состоит ни в одной роли, либо из внешнего ЦИ передан неверный набор утверждений» (см. рисунок 55):

Во время работы приложения произошла ошибка.

Информация об ошибке:

Пользователь не состоит ни в одной роли, либо из внешнего ЦИ передан неверный набор утверждений

Рисунок 55. Ошибка «Пользователь не состоит ни в одной роли, либо из внешнего ЦИ передан неверный набор утверждений»

Возможные причины возникновения ошибки:

- в ADFS не добавлены правила преобразования утверждений, в соответствие с <u>п. 2.4</u> – для WSFed или <u>п. 3.4 текущего руководства</u> – для Oidc;

- были допущены ошибки при добавлении правил преобразования утверждений;

- осуществляется аутентификация в личном кабинете пользователя КриптоПро DSS, с использованием учетной записи пользователя AD, состоящего в группе Операторов.

Б4. Ошибка «Проверка сертификата обработчиком маркеров не прошла»

При аутентификации пользователя AD в КриптоПро DSS появляется ошибка «Проверка сертификата обработчиком маркеров не прошла» (см. Рисунок 56):

Центр идентификации КриптоПро DSS Во время работы приложения произошла ошибка. Информация об ошибке: ID4257: проверка сертификата X.509 "CN=ADFS Signing - dc1.tmobile.tlocal" обработчиком маркеров не прошла.

Рисунок 56. Ошибка «Проверка сертификата обработчиком маркеров не прошла» Возможная причина возникновения ошибки:

При выполнении командлета *Add-DssIdentityProvider*, в соответствие с <u>п. 2.1</u> – для WSFed или <u>п. 3.2 текущего руководства</u> – для Oidc, был указан отпечаток неправильного сертификата.

Б5. Ошибка «Учётные данные должны содержать только одно утверждение»

При аутентификации оператора AD в КриптоПро DSS появляется ошибка «Учётные данныедолжнысодержатьтолькоодноутверждение:http://schemas.microsoft.com/ws/2008/06/identity/claims/role»(см. Рисунок 57):

Во время работы приложения произошла ошибка.

Информация об ошибке:

Учётные данные должны содержать только одно утверждение http://schemas.microsoft.com/ws/2008/06/identity/claims/role

Рисунок 57. Ошибка «Учётные данные должны содержать только одно утверждение» Возможная причина возникновения ошибки:

С ADFS приходит маркер, который содержит в себе два утверждения *Role*, что вызвано ошибками при добавлении правил преобразования утверждений в соответствие с <u>п. 2.4</u> – для WSFed или <u>п. 3.4 текущего руководства</u> – для Oidc.

Б6. Ошибка «ID4036»

При аутентификации пользователя/оператора AD в КриптоПро DSS появляется ошибка «ID4036: не удалось разрешить ключ, необходимый для расшифровки зашифрованного маркера безопасности, из следующего идентификатора ключа безопасности» (см. рисунок 58):

Во время работы приложения произошла ошибка.

Информация об ошибке:

ID4036: не удалось разрешить ключ, необходимый для расшифровки зашифрованного маркера безопасности, из следующего идентификатора ключа безопасности "<e:EncryptedKey xmlns:e="http://www.w3.org/2001/04/xmlenc#"><e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"><DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" xmlns="http://www.w3.org/2000/09/xmldsig#" /></e:EncryptionMethod>

xmlns="http://www.w3.org/2000/09/xmldsig#"><o:SecurityTokenReference xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-

secext-1.0.xsd"><X509Data><X509IssuerSerial><X509IssuerName>CN=dssotheridp</X509IssuerName><X509SerialNumber>11096697130933824257 Убедитесь, что значением SecurityTokenResolver является необходимый ключ.

Рисунок 58. Ошибка «ID4036»

Возможные причины возникновения ошибки:

- При настройке отношений доверия проверяющей стороны по протоколу WSFed, в соответствие с <u>п. 2.2.7 текущего руководства</u>, был выбран сертификат, не соответствующий актуальному сервисному сертификату ЦИ КриптоПро DSS.

- На стороне КриптоПро DSS была выполнена замена сервисного сертификата ЦИ DSS, однако данный сертификат не был заменен в настройках проверяющей стороны ADFS (консоль управления ADFS \rightarrow Отношения доверия проверяющей стороны \rightarrow Открыть свойства проверяющей стороны \rightarrow Шифрование \rightarrow Обзор \rightarrow Выбрать актуальный сервисный сертификат ЦИ КриптоПро DSS).

Б7. Ошибка «ID4037»

При аутентификации пользователя/оператора AD в КриптоПро DSS появляется ошибка «Не удалось разрешить ключ, необходимый для проверки подписи, из следующего идентификатора ключа безопасности» (см. рисунок 59):

Во время работы приложения произошла ошибка.

Информация об ошибке:

ID4037: не удалось разрешить ключ, необходимый для проверки подписи, из следующего идентификатора ключа безопасности "SecurityKeyIdentifier (IsReadOnly = False, Count = 1, Clause[0] = X509RawDataKeyIdentifierClause (RawData =

MIIC5DCCAcygAwIBAgIQO5yHGq86K5dOGPc1iAYQ1jANBgkqhkiG9w0BAQsFADAuMSwwKgYDVQQDEyNBREZTIFNp2 Убедитесь, что значением SecurityTokenResolver является необходимый ключ.

Рисунок 59. Ошибка «ID4037»

Возможные причины возникновения ошибки:

- При выполнении командлета *Add-DssIdentityProvider*, в соответствие с <u>п. 2.1</u> – для WSFed или <u>п. 3.2 текущего руководства</u> – для Oidc, был указан отпечаток неправильного сертификата.

- Был опубликован новый сертификат подписи маркеров ADFS, однако отпечаток данного сертификата не был указан на стороне КриптоПро DSS. Необходимо установить актуальный сертификат подписи маркеров в хранилище «Доверенные лица» локального компьютера сервера DSS, выполнить командлет: *Set-DssIdentityProvider -IssuerName ADFS -Thumbprint "Omneчаток актуального сертификата подписи маркеров ADFS"* и перезапустить пул приложений ЦИ КриптоПро DSS.