Система электронной подписи

на базе ПАК «КриптоПро DSS»

Руководство администратора СЦИ (ADFS)

На 46 листах

Москва, 2020

СОДЕРЖАНИЕ

Оглавление

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 Приложении А «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 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;
- Настройка правил преобразования утверждений для доступа к КриптоПро DSS Оператора, 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):

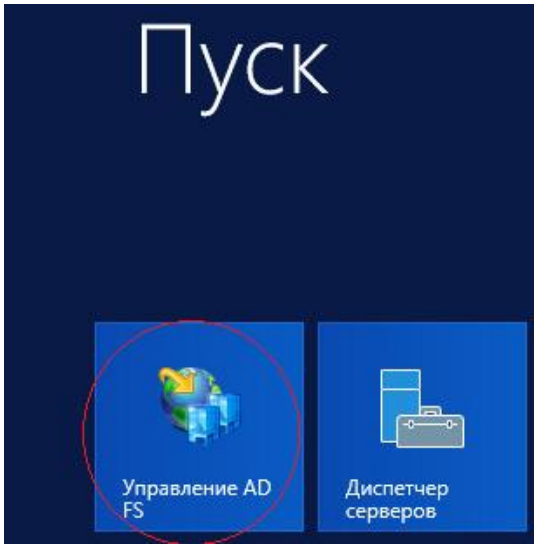

Рисунок 1. Запуск мастера управления ADFS.

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

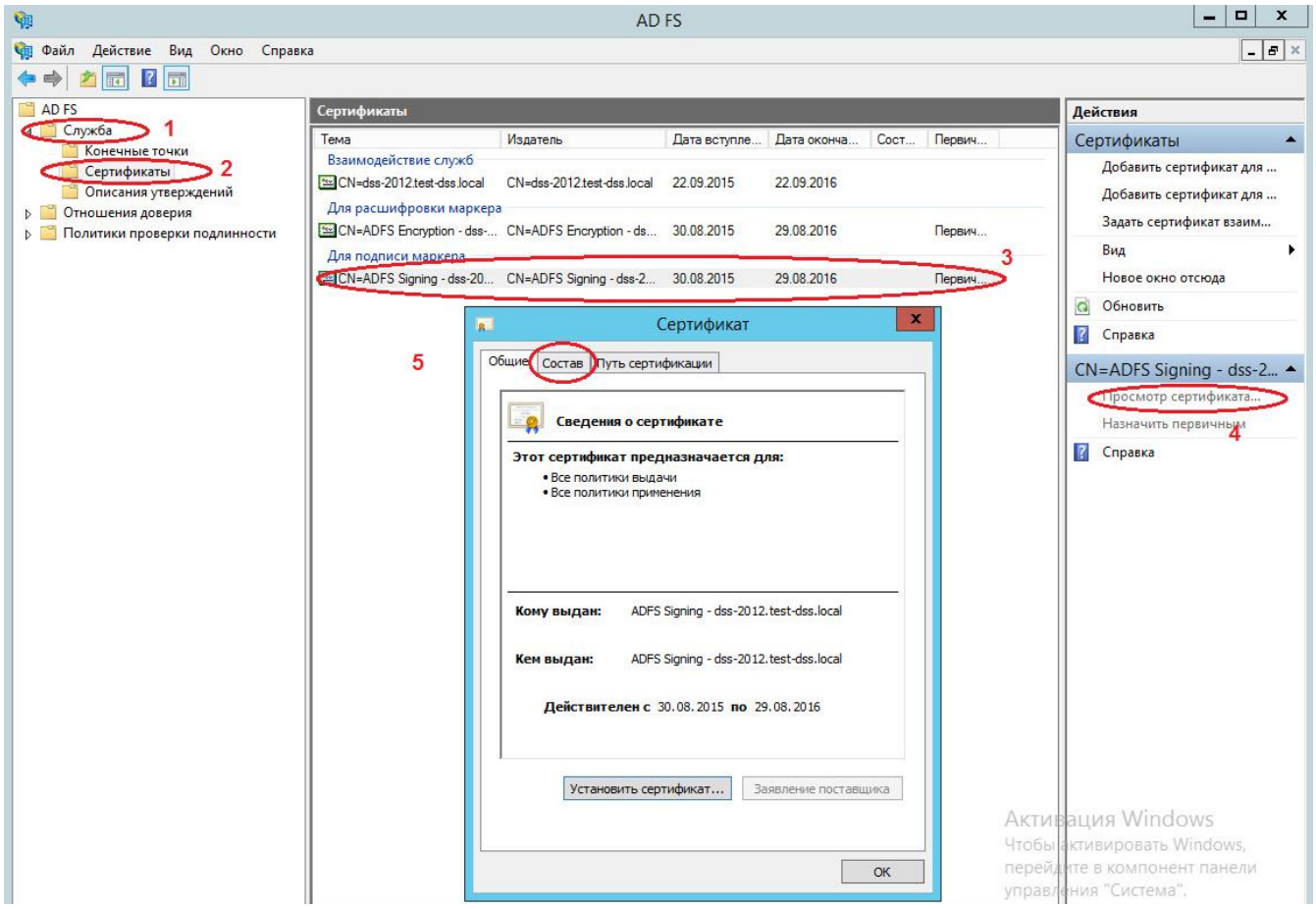

Рисунок 2. Выбор сертификата для выгрузки.

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

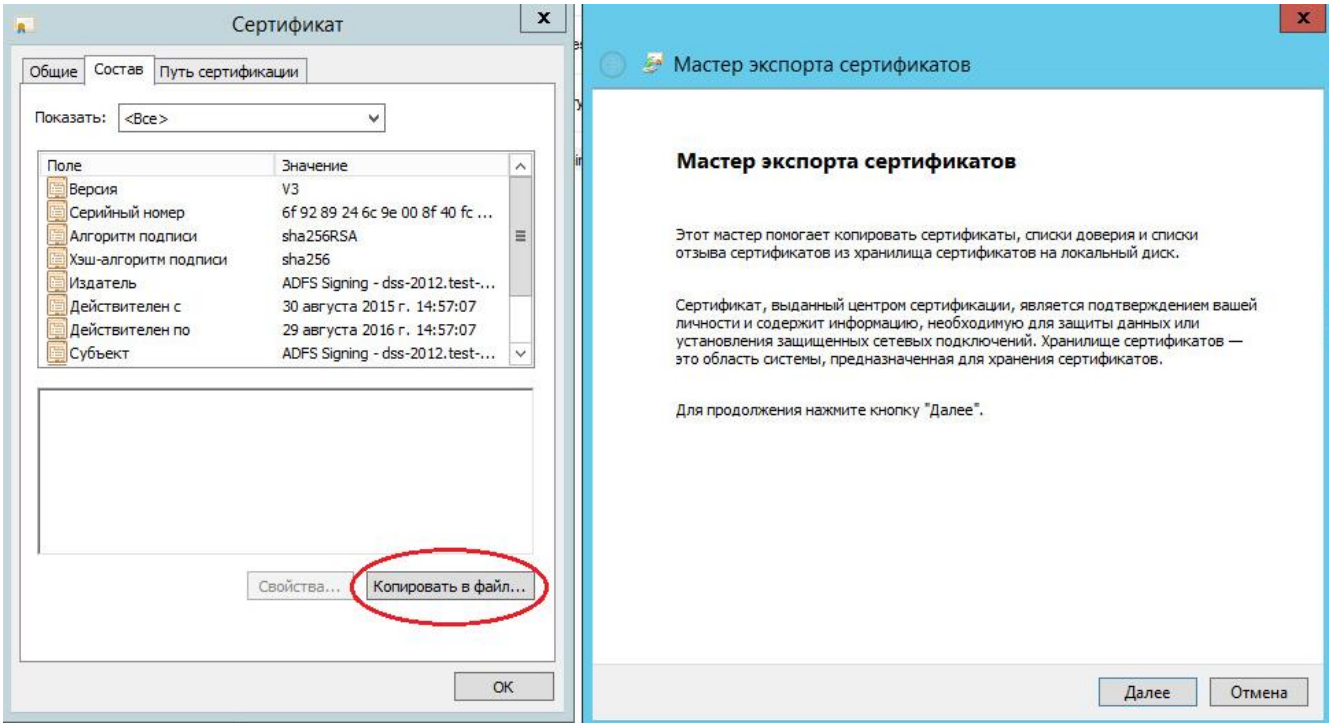

Рисунок 3. Экспорт сертификата.

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

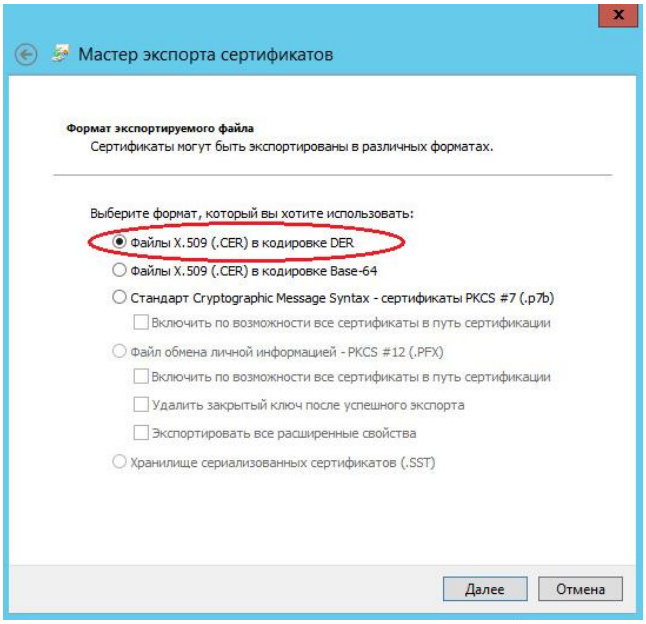

Рисунок 4. Выбор формата сохраняемого файла.

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):

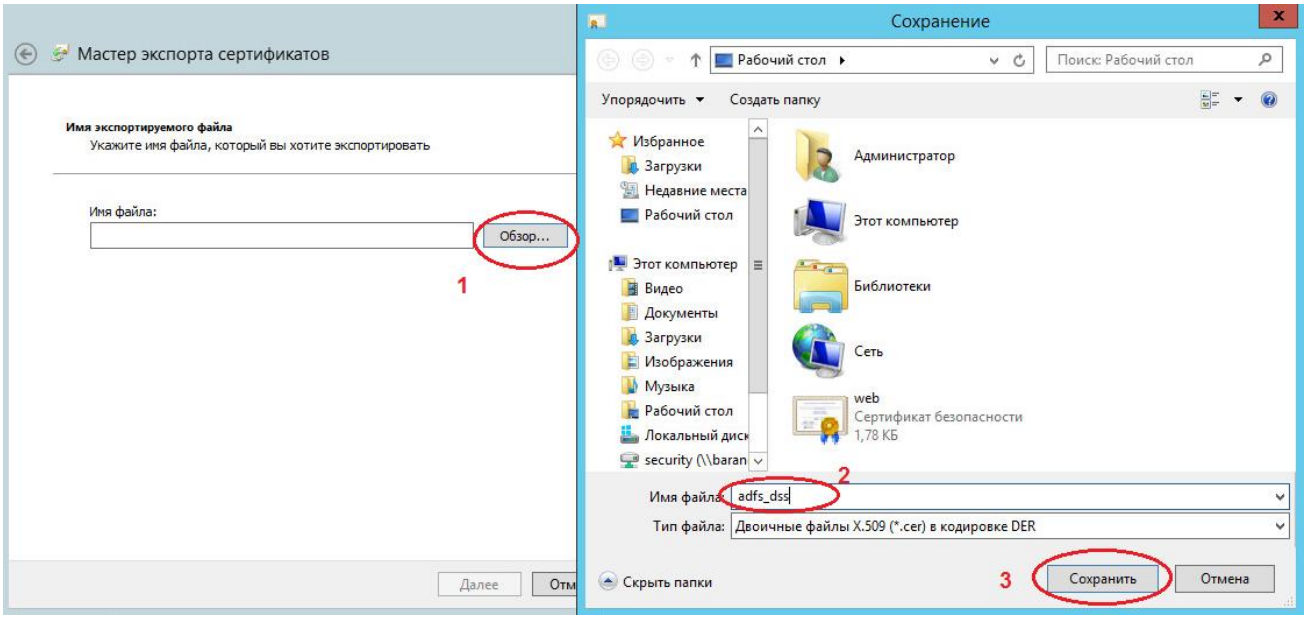

Рисунок 5. Сохранение файла с сертификатом.

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).

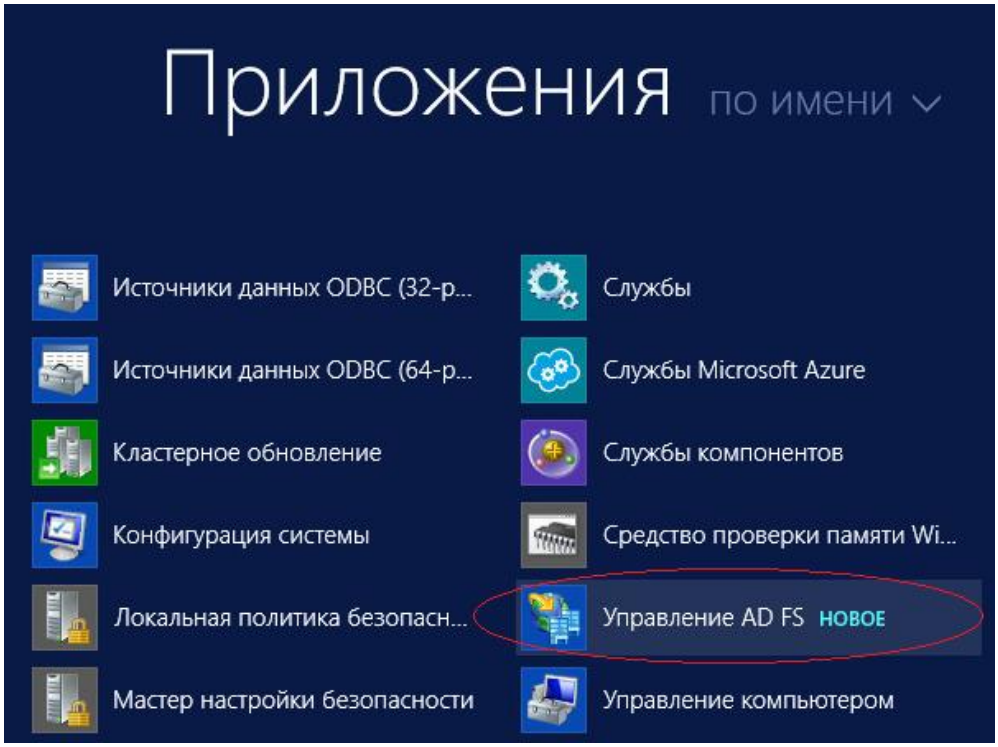

Рисунок 6. Запуск консоли управления ADFS.

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

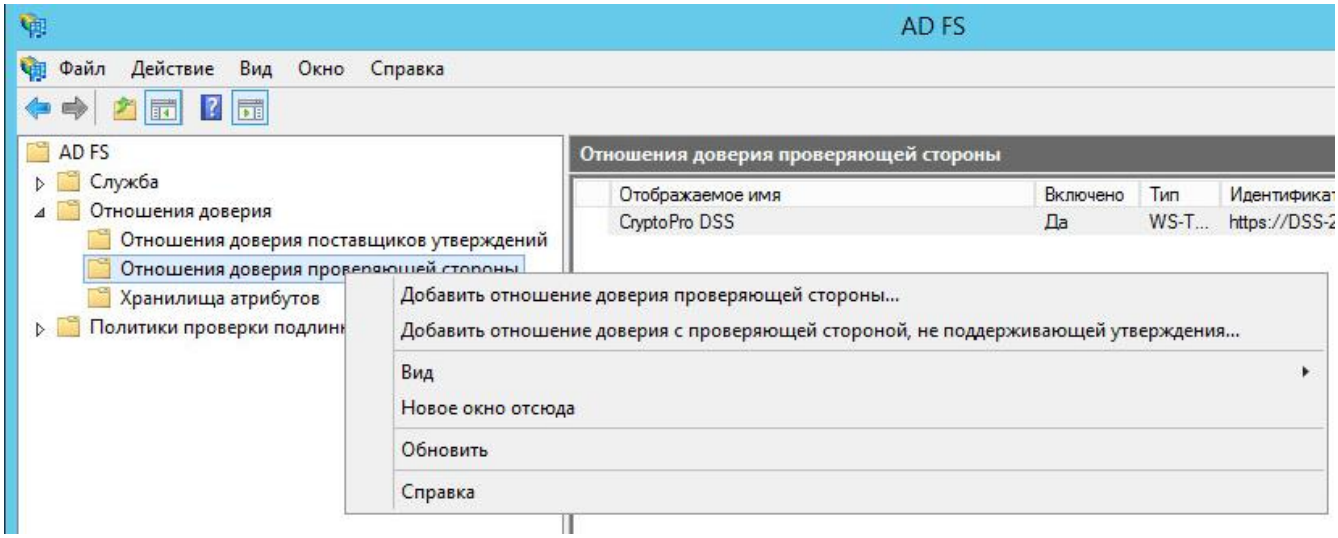

Рисунок 7. Добавление Проверяющей стороны

2.2.3. После этого откроется Мастер добавления отношений доверия проверяющей стороны. В мастере необходимо нажать кнопку *«Запустить»* (см. рисунок 8):

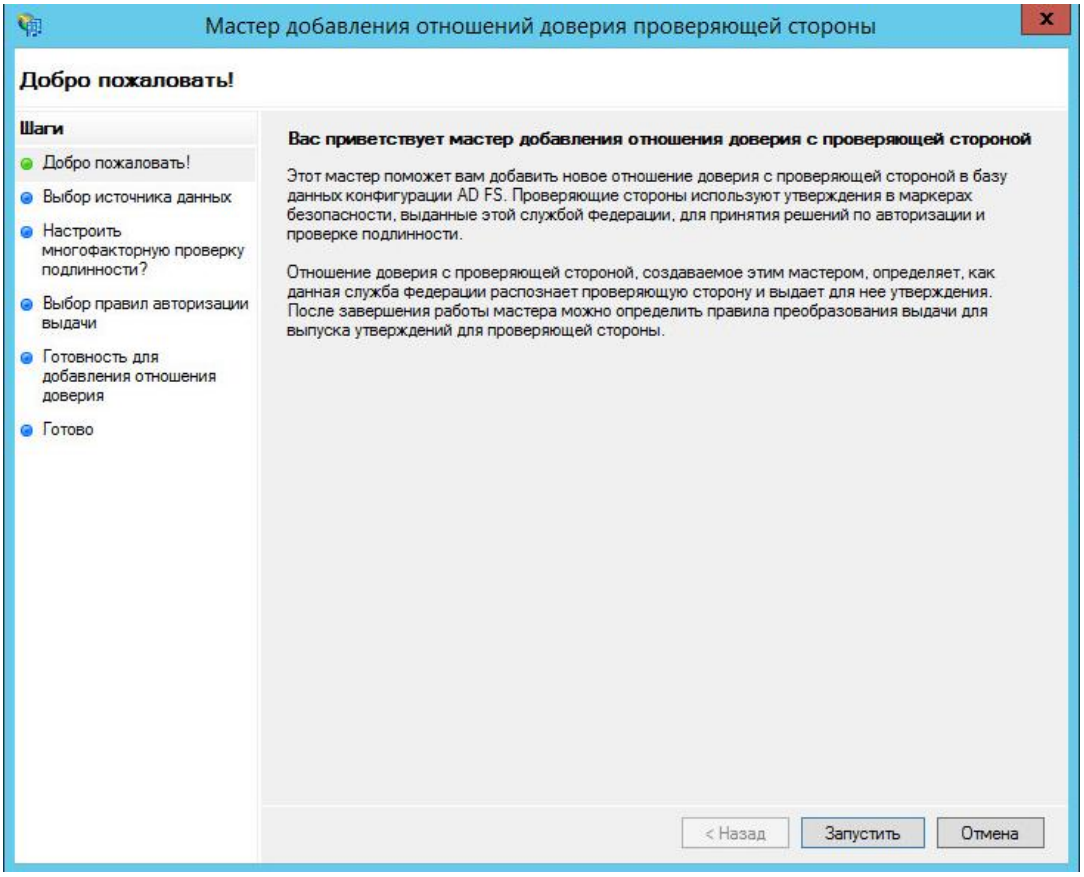

Рисунок 8. Запуск Мастера добавления отношений доверия проверяющей стороны

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):

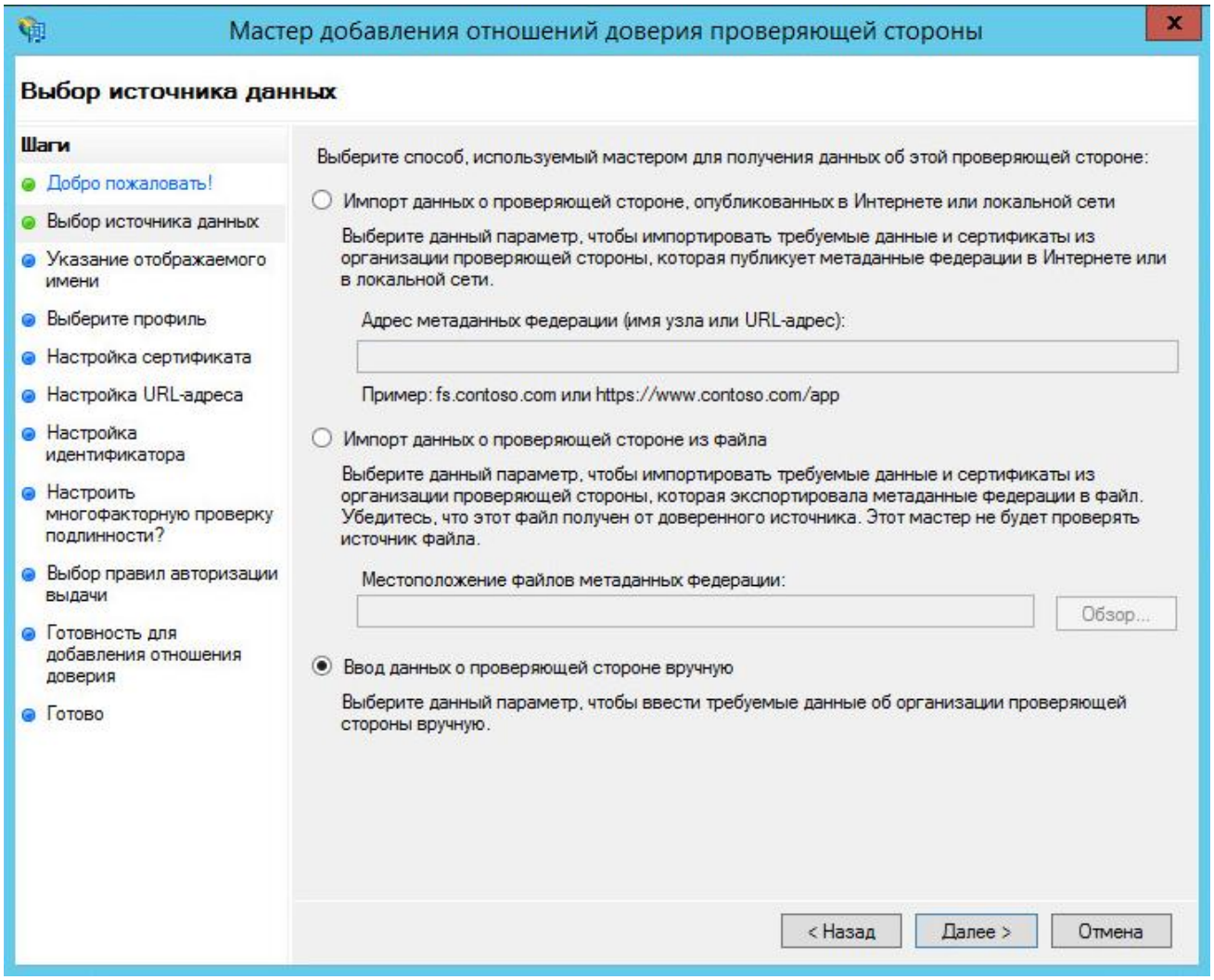

Рисунок 9. Выбор способа получения данных о проверяющей стороне

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

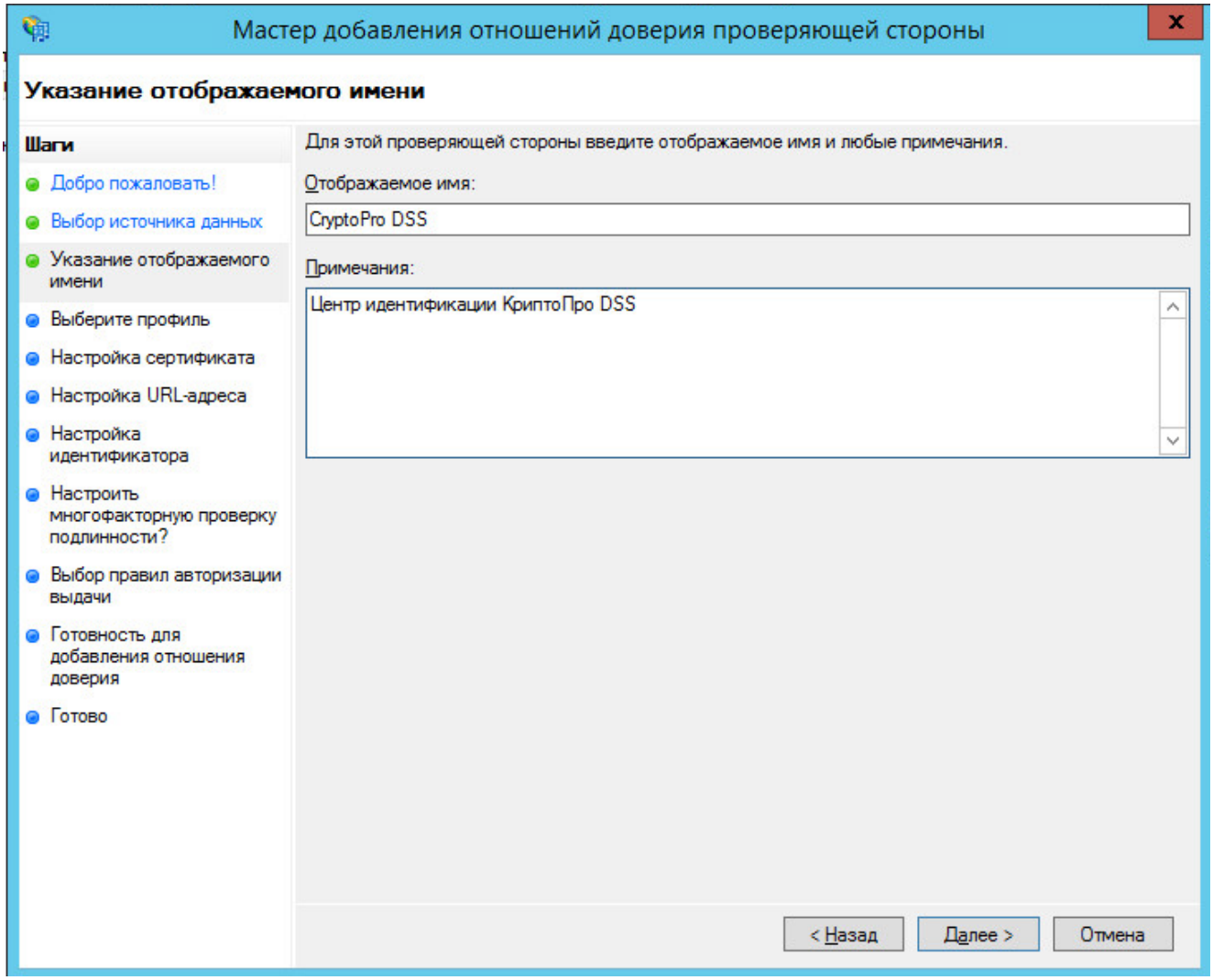

Рисунок 10. Ввод имени проверяющей стороны

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

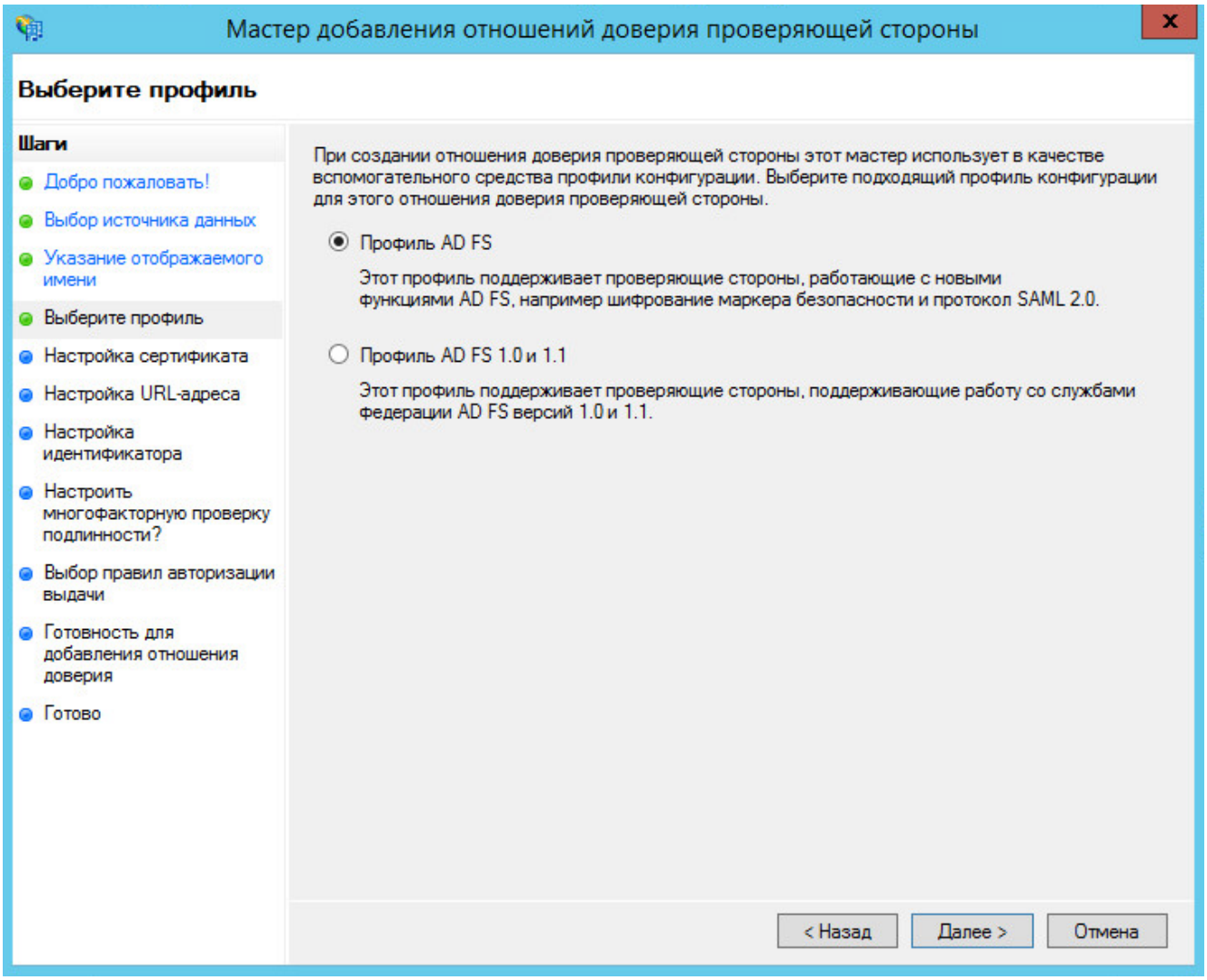

Рисунок 11. Выбор профиля ADFS

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

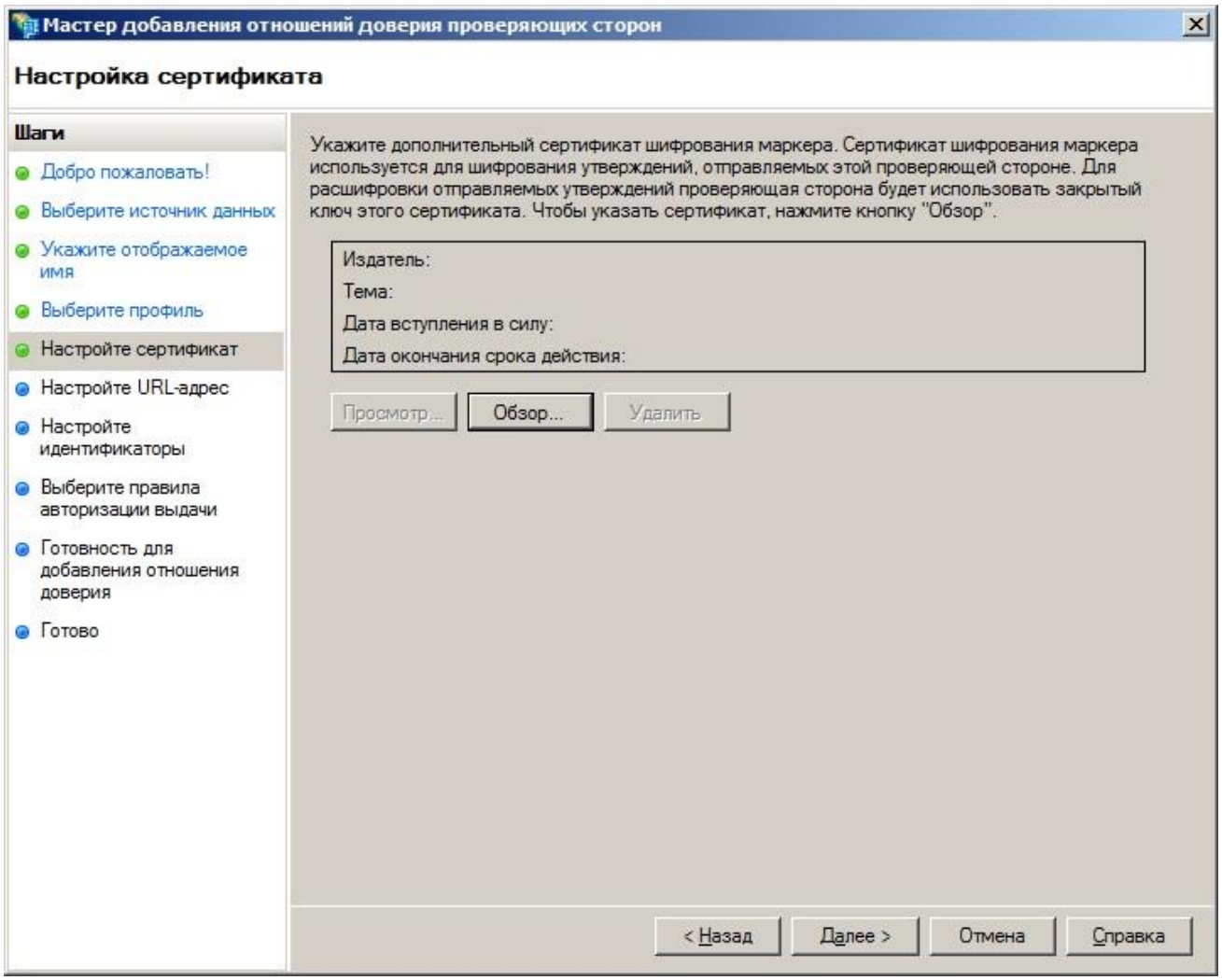

Рисунок 12. Выбор сертификата шифрования исходящего маркера

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: https://dss_hostname/STS_appname/Issue (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:

```
(Get-DssStsinstance).ApplicationName
```

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

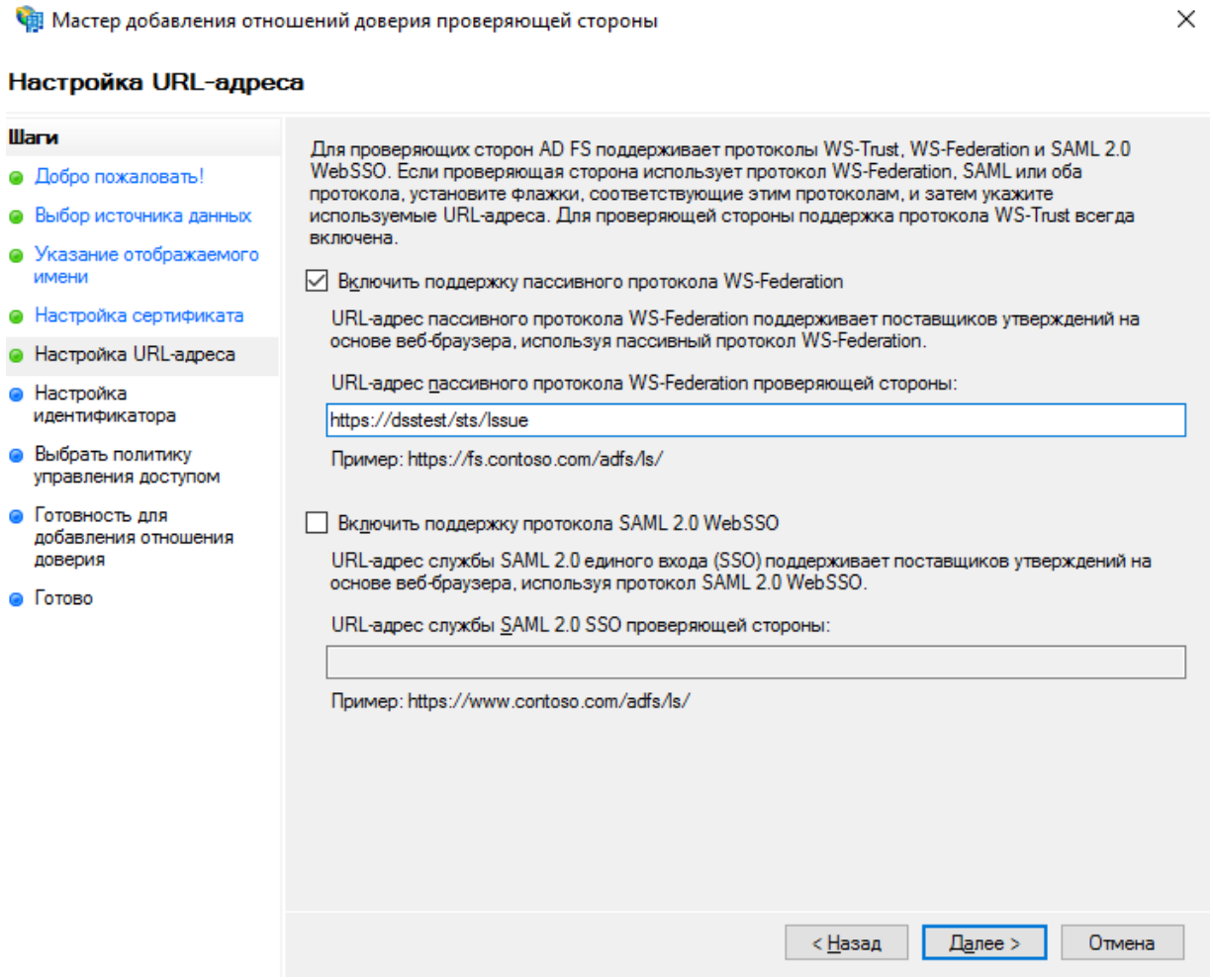

Рисунок 13. Включение поддержки WS-Federation

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

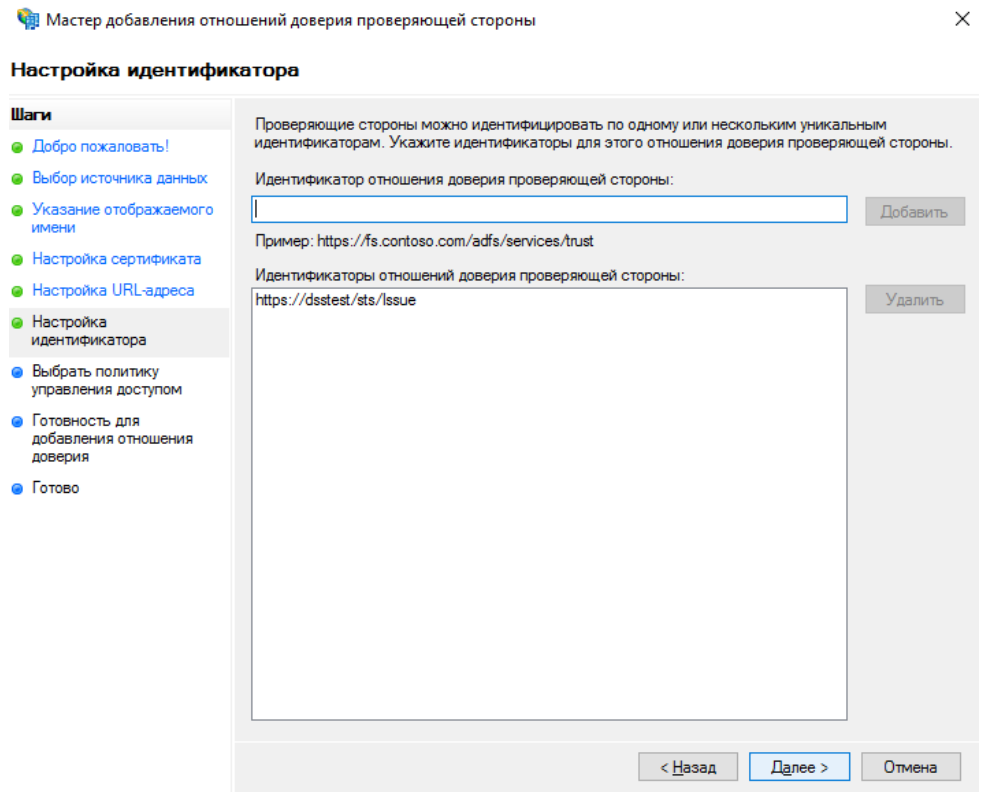

Рисунок 14. Установка дополнительных идентификаторов проверяющей стороны

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):

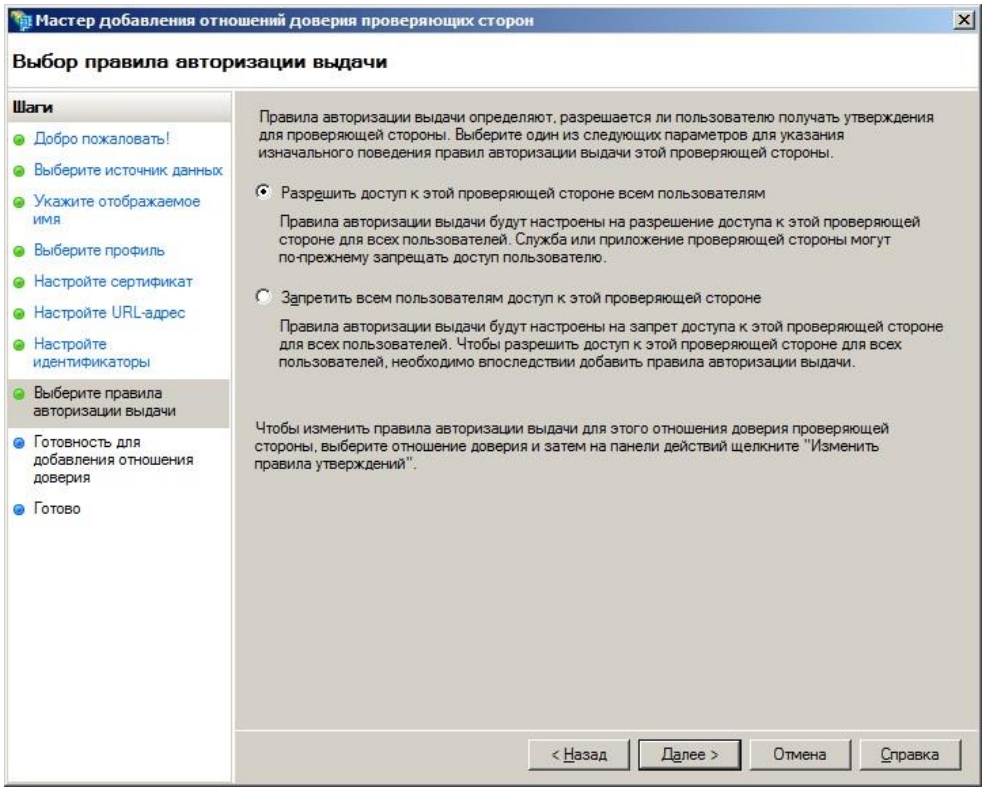

Рисунок 15. Выбор правил авторизации пользователей при доступе к проверяющей стороне

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

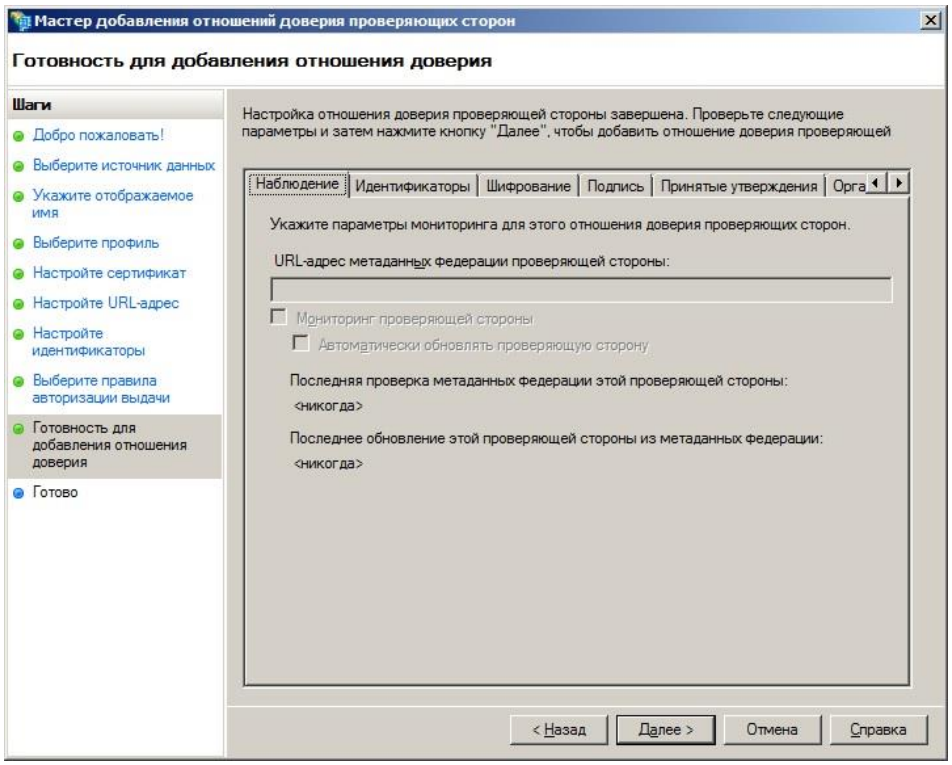

Рисунок 16. Подтверждение введённых данных для выбора правил авторизации

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

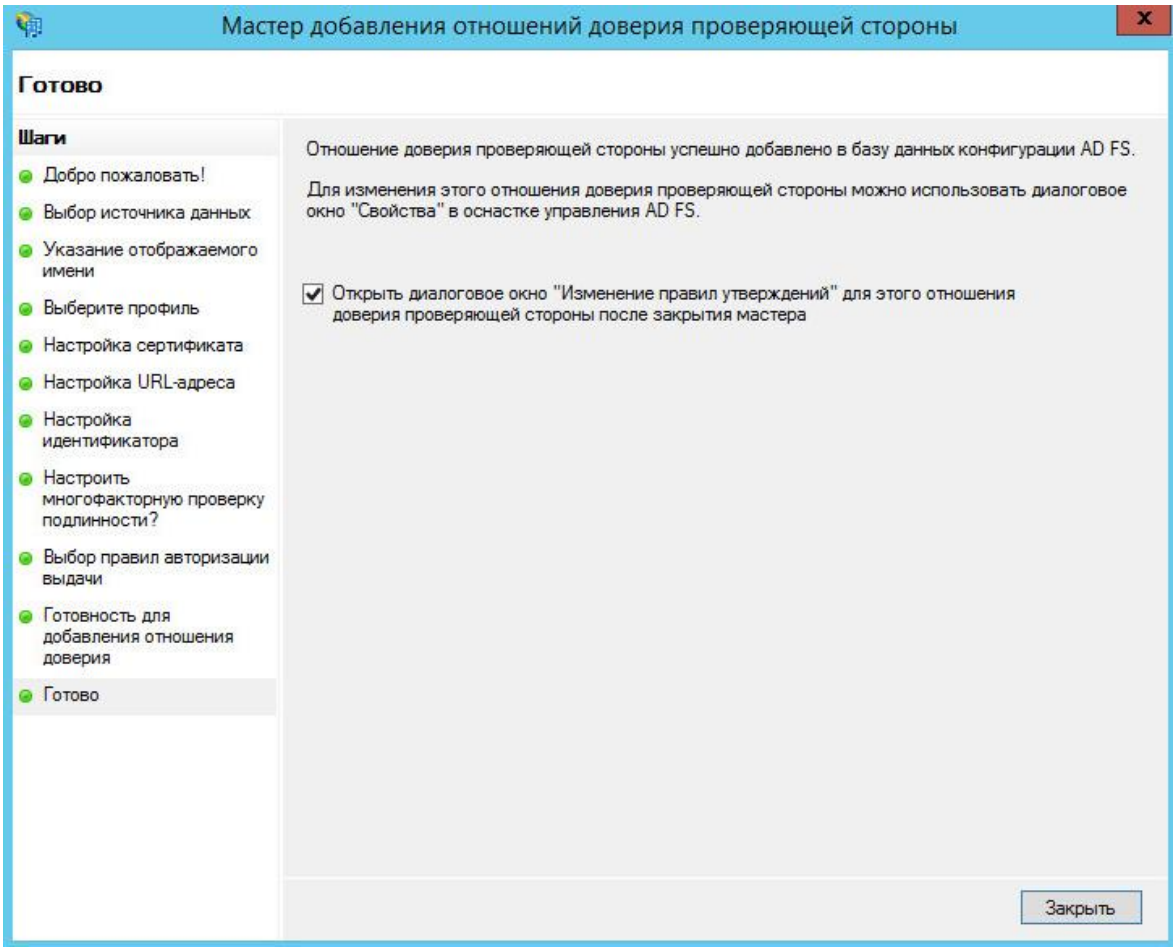

Рисунок 17. Завершение работы Мастера добавления отношений доверия проверяющей стороны

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 DSS-operator-AD@domain.ru -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 → Отношения доверия → Отношения доверия проверяющей стороны». Далее необходимо выбрать проверяющую сторону КриптоПро DSS с именем, заданным в п. 2.2.5 и нажать кнопку «Изменить правила утверждения (см. Рисунок 21):

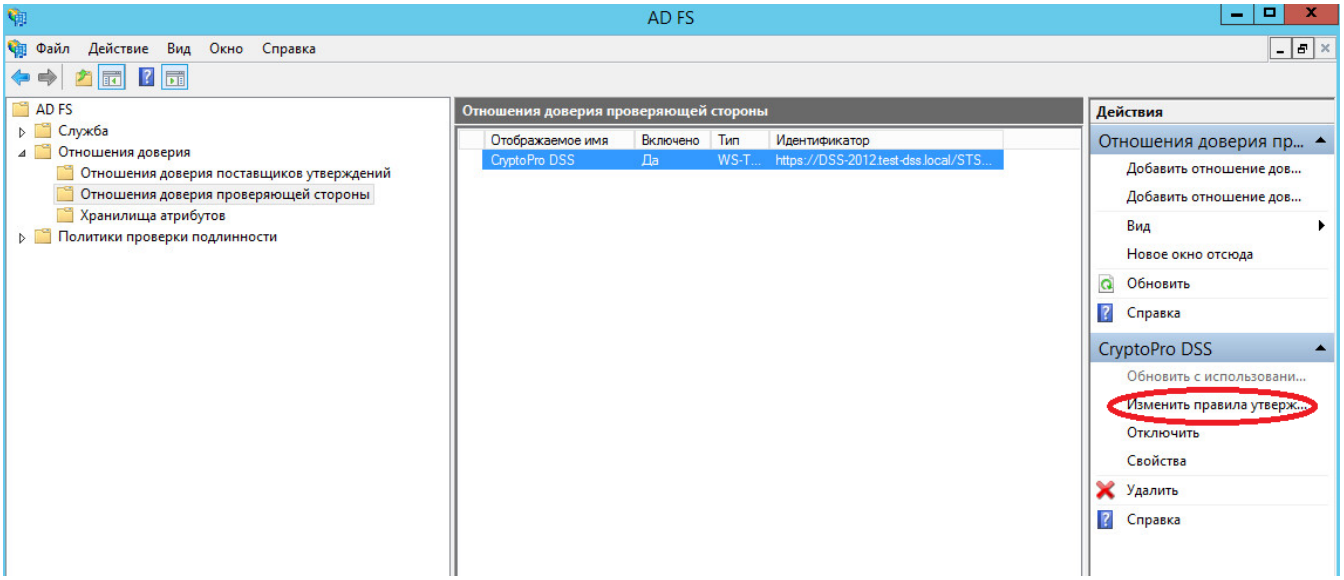

Рисунок 21. Изменение/добавление «правил утверждения»

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

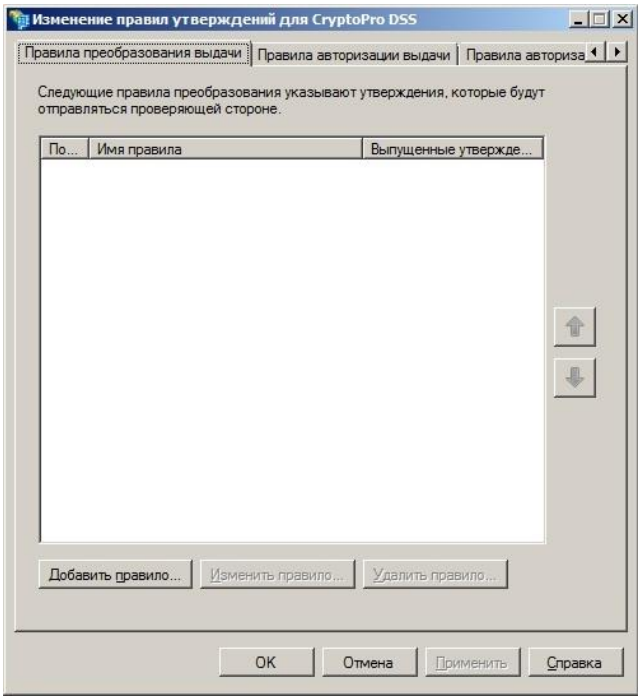

Рисунок 22. Добавление правил преобразований утверждений

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):

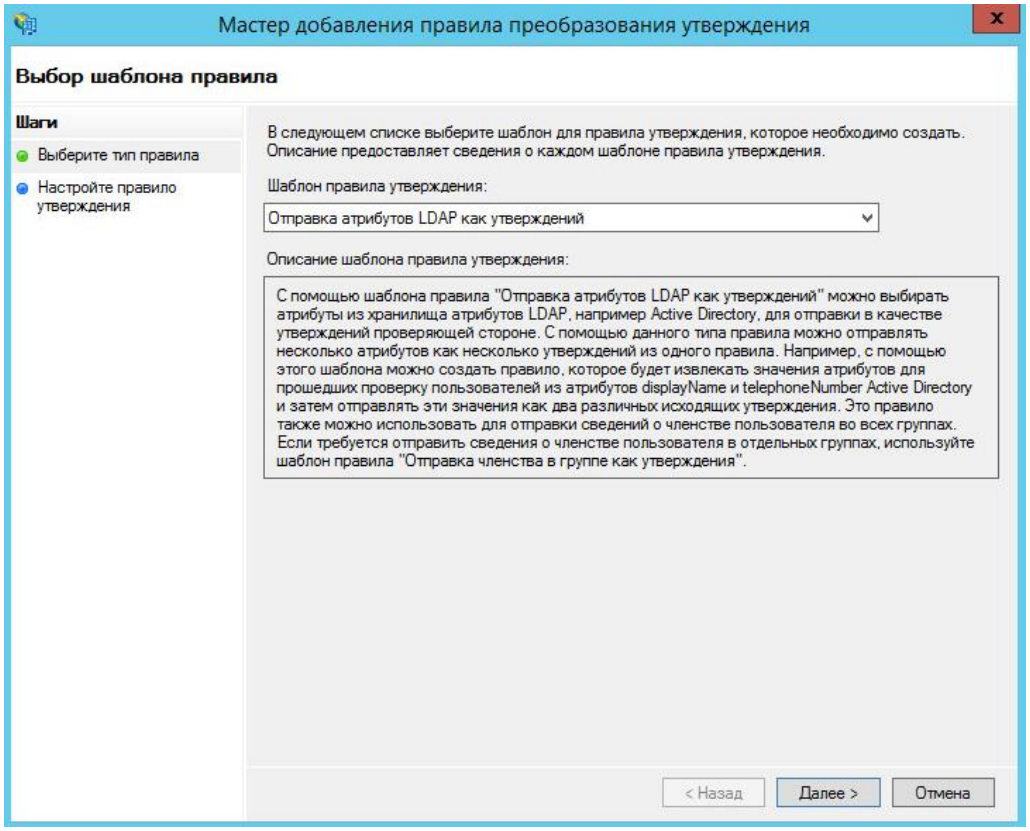

Рисунок 23. Выбор шаблона правила утверждения

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 (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name). Далее необходимо нажать кнопку *«Готово»*.

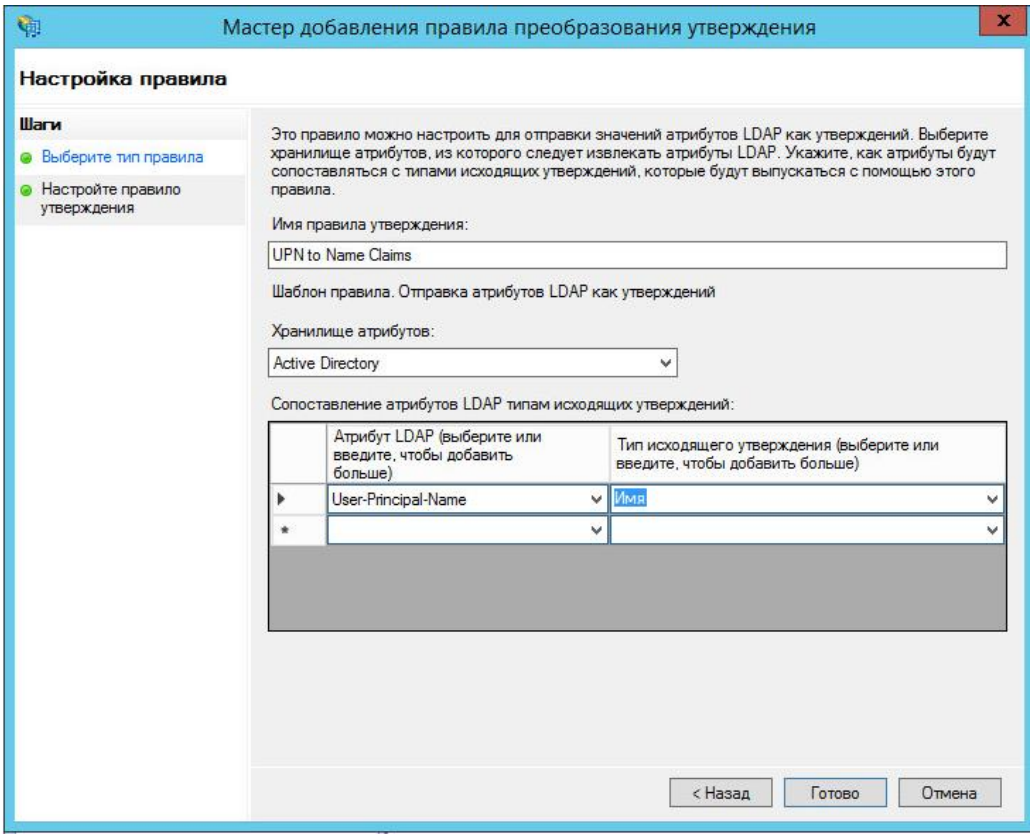

Рисунок 24. Создание правил преобразований утверждений.

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):

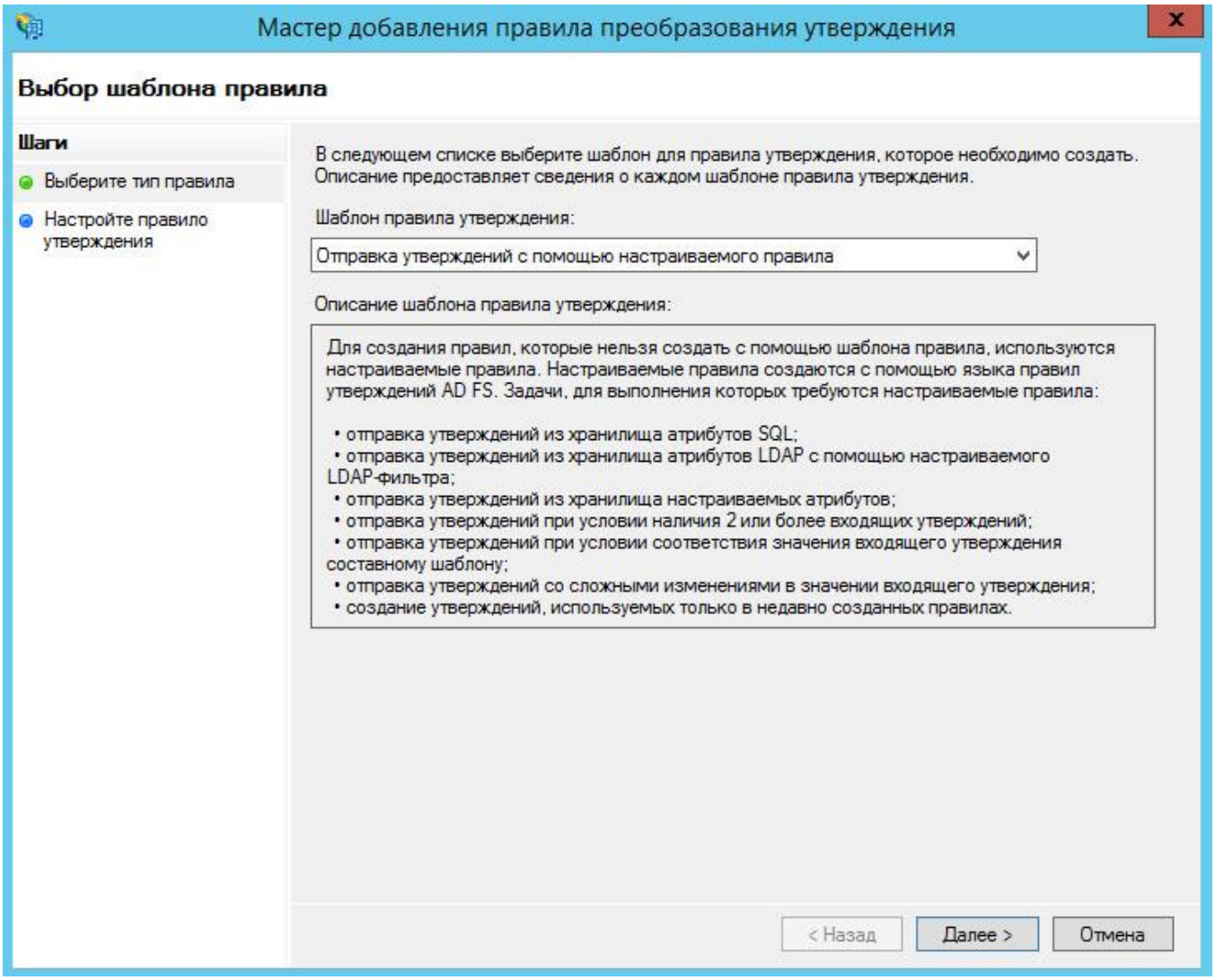

Рисунок 25. Выбор шаблона правила преобразования утверждения.

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 http://dss.cryptopro.ru/identity/claims/marker 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 TP4 ПО ПРОТОКОЛУ OPENID CONNECT 1.0

Подключение СЦИ ADFS из состава Windows Server 2016 TP4 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).

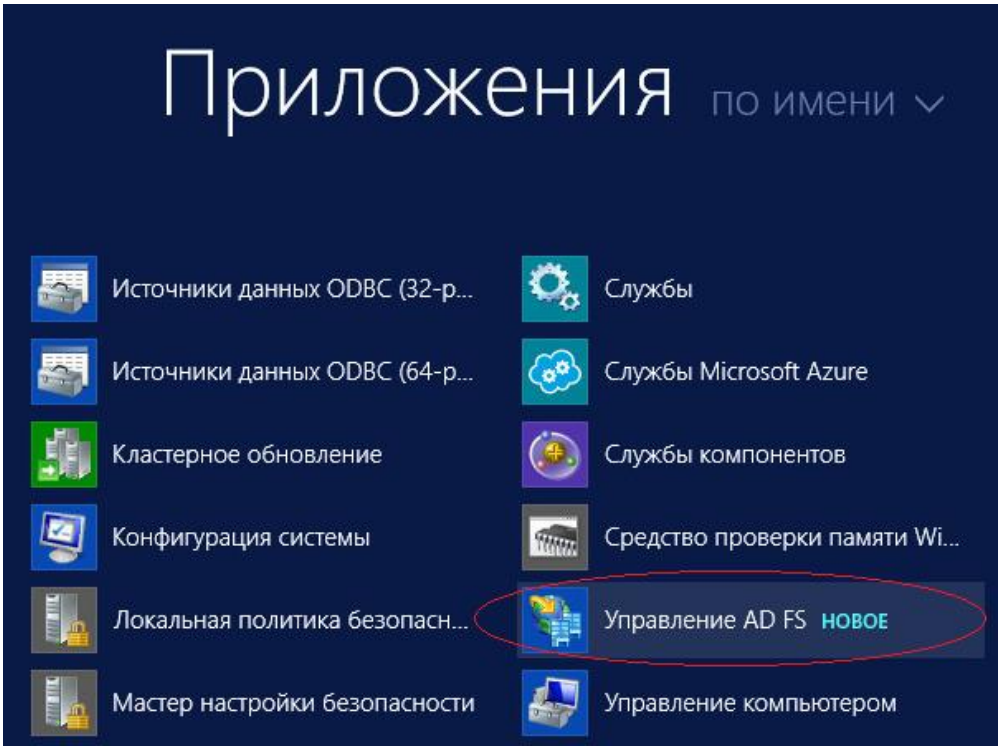

Рисунок 26. Запуск консоли управления ADFS.

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

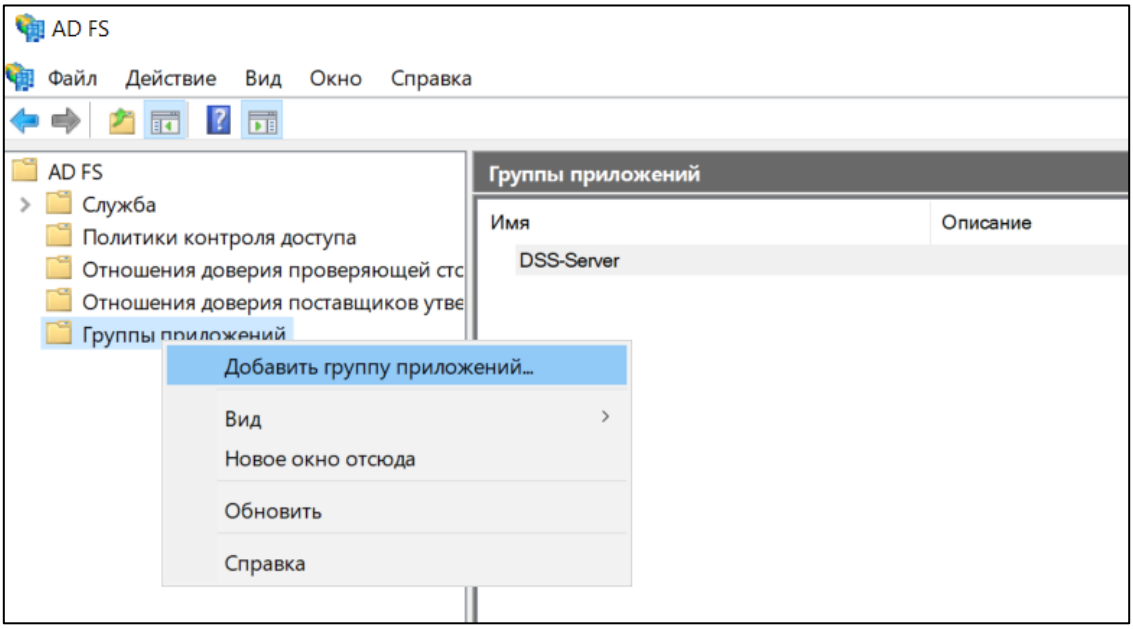

Рисунок 27. Добавление группы приложений

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):

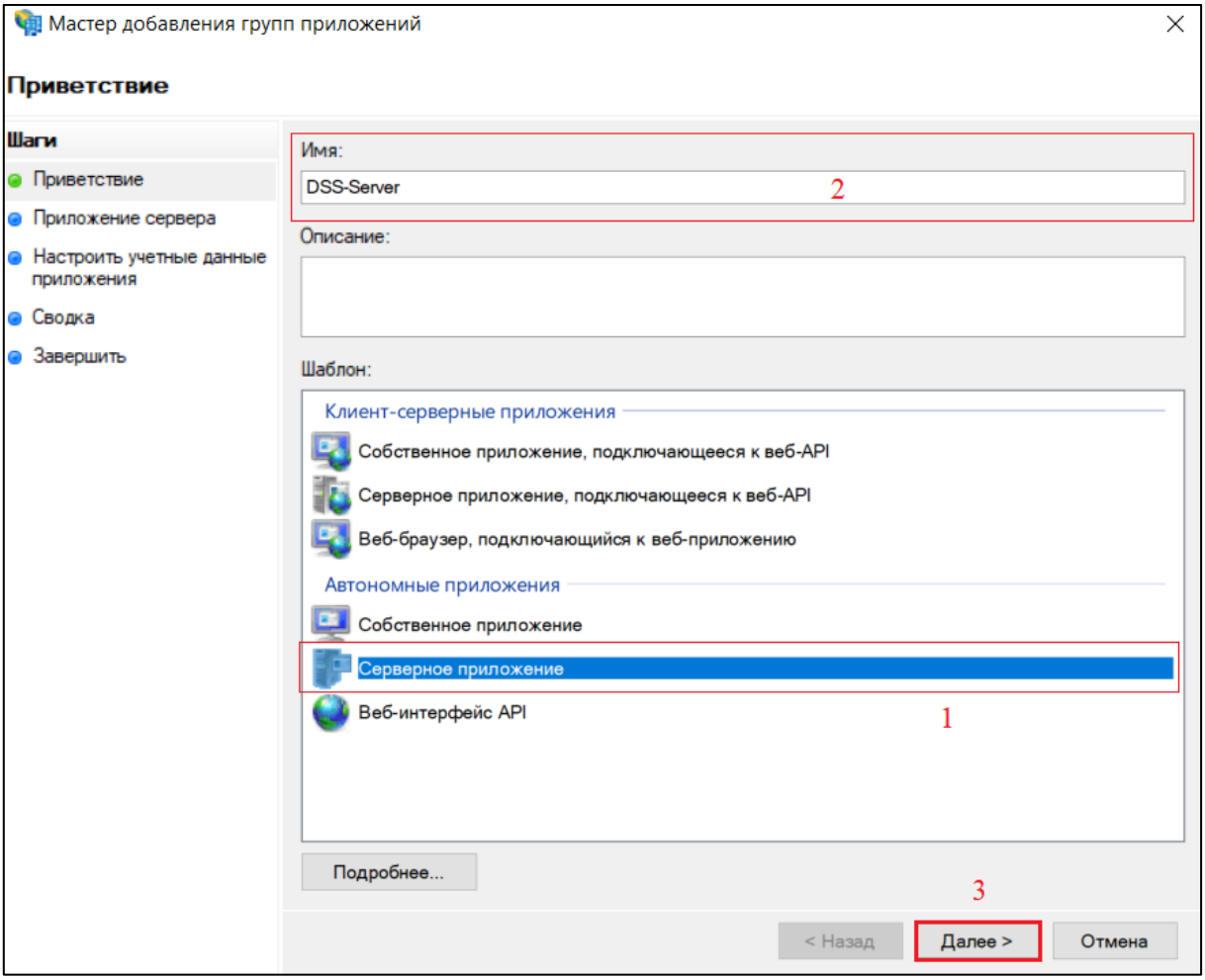

Рисунок 28. Мастер добавления групп приложений

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

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):

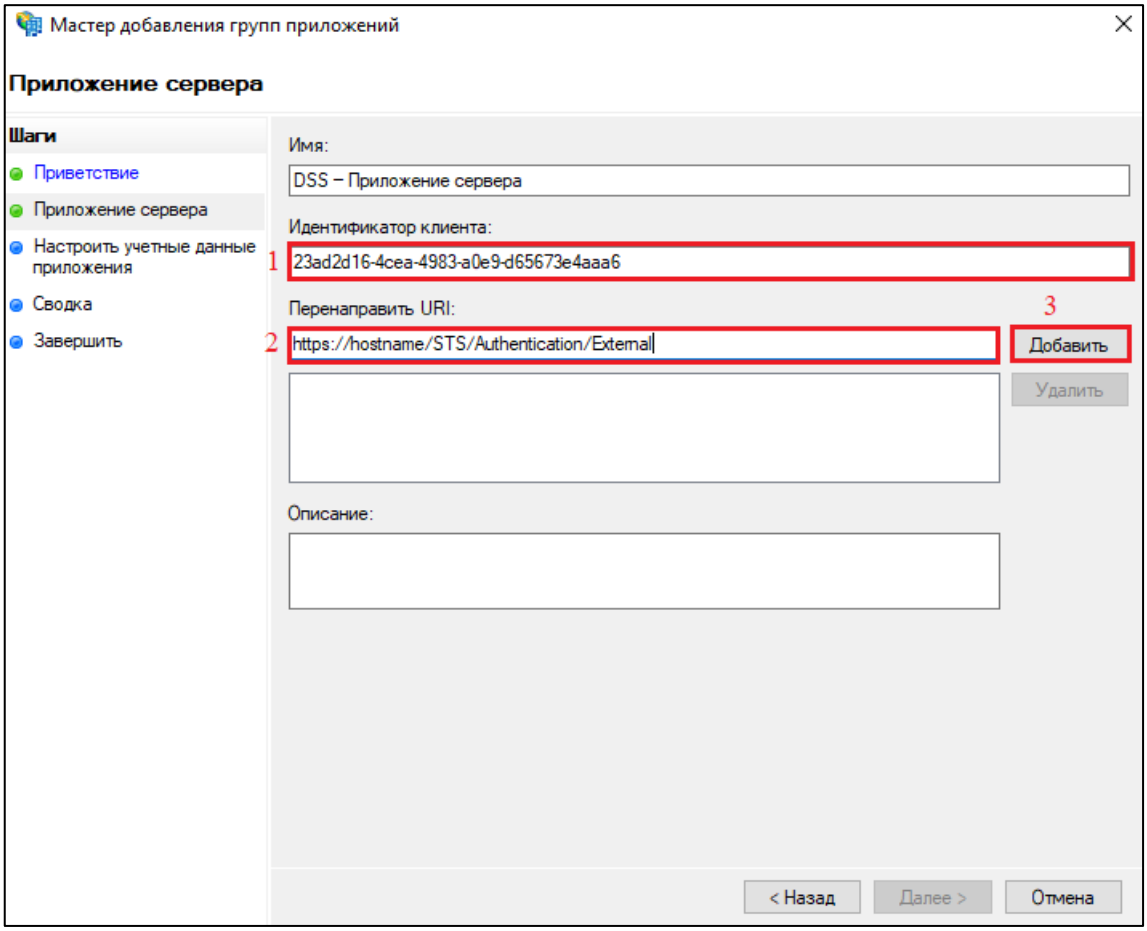

Рисунок 29. Настройка приложения сервера

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

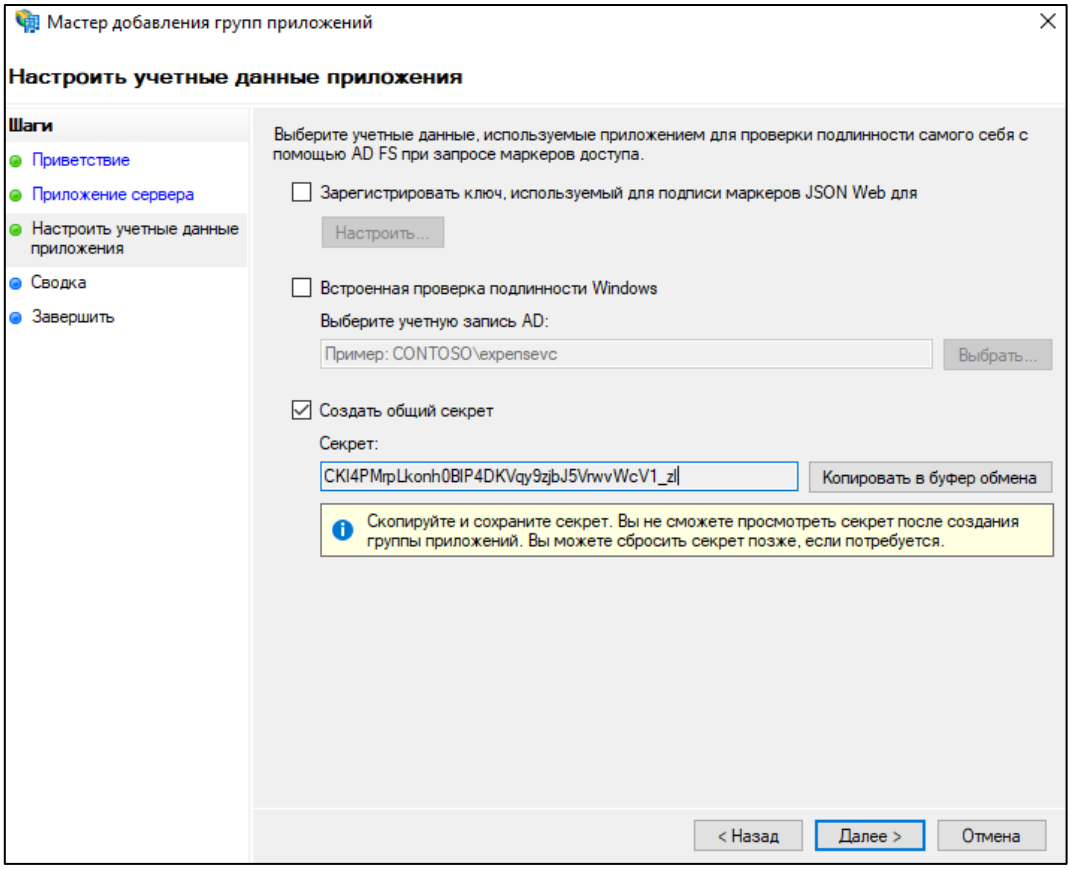

Рисунок 30. Настройка учетных данных приложения

3.1.6. В следующем окне нажать кнопку *«Далее»* (см. Рисунок 31):

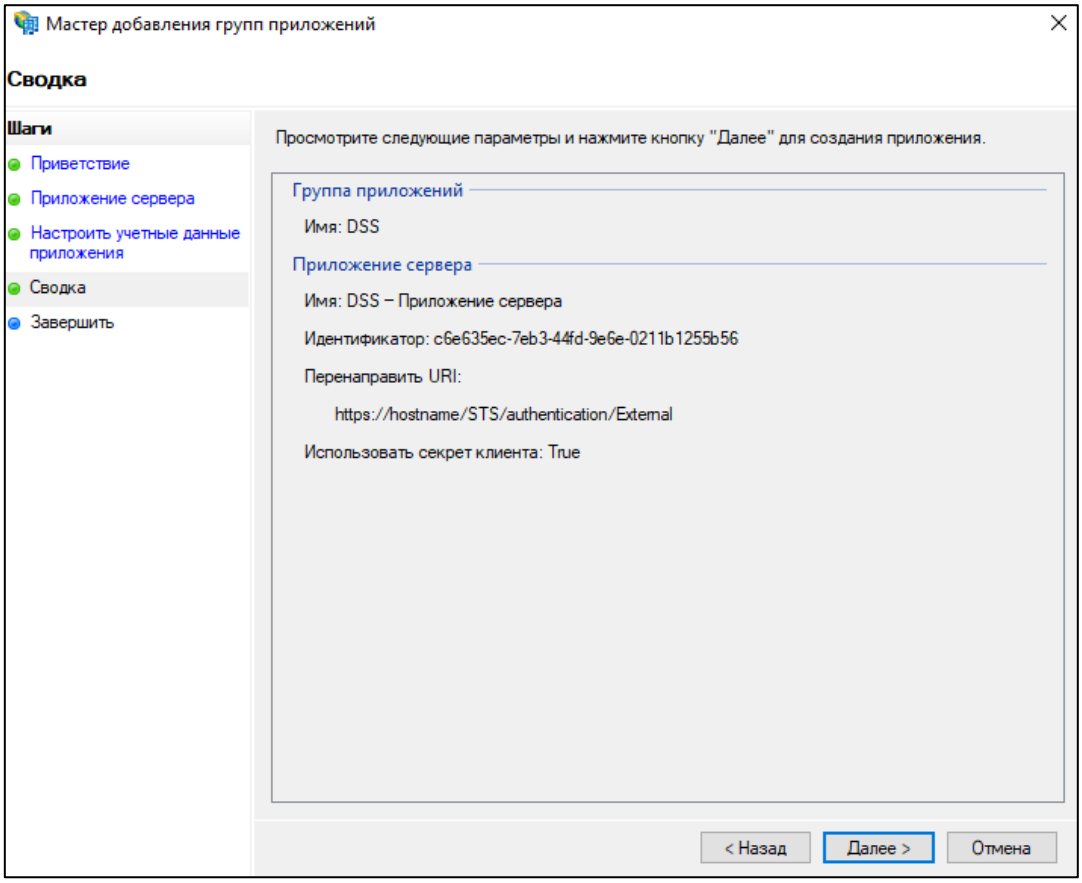

Рисунок 31. Сводка данных группы приложений и серверного приложения

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

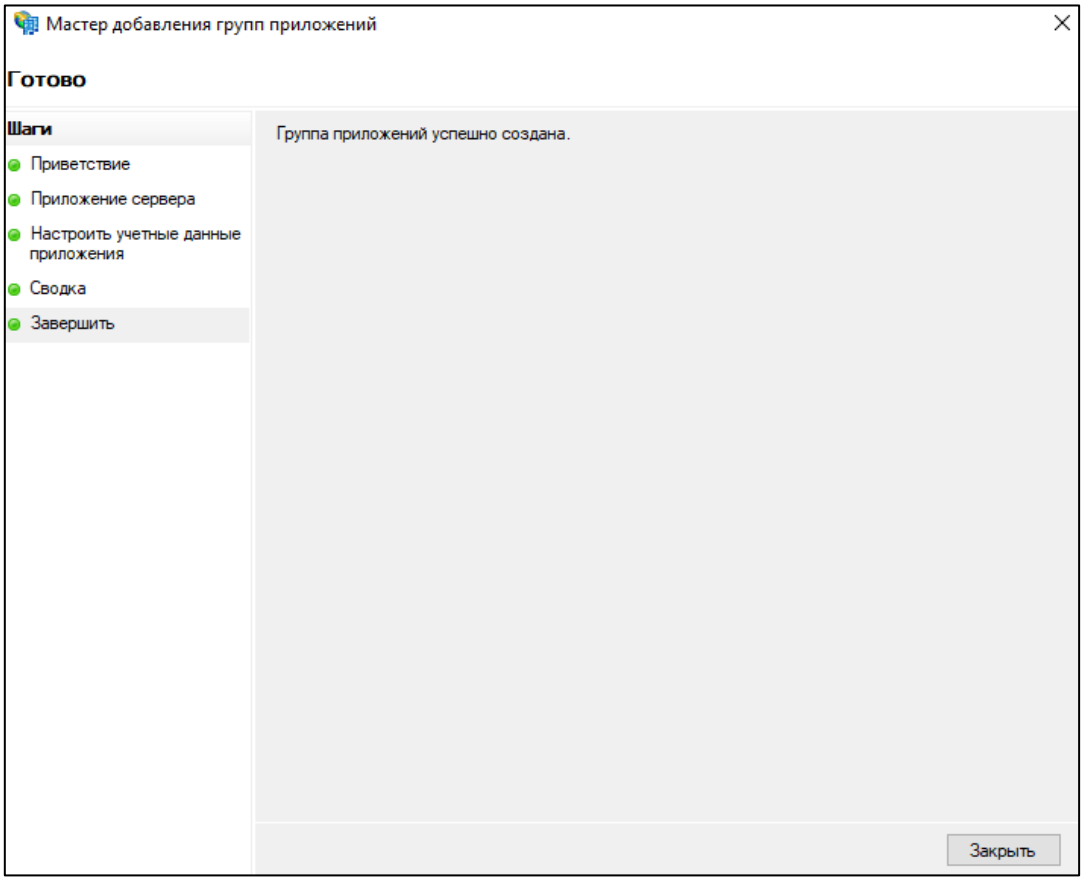

Рисунок 32. Завершение работы мастера добавления группы приложений

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

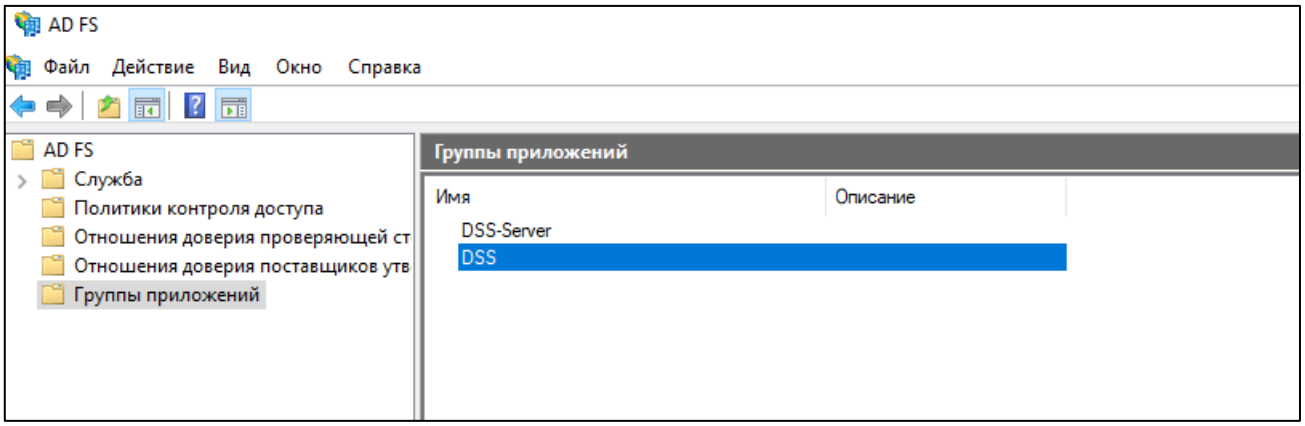

Рисунок 33. Список созданных групп приложений

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

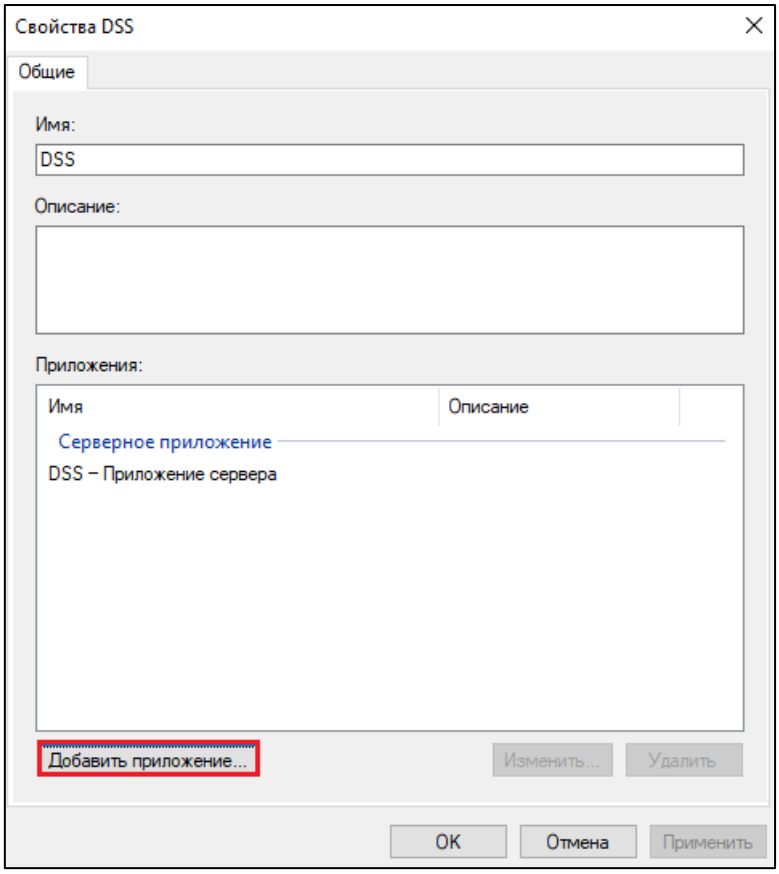

Рисунок 34. Свойства группы приложений

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

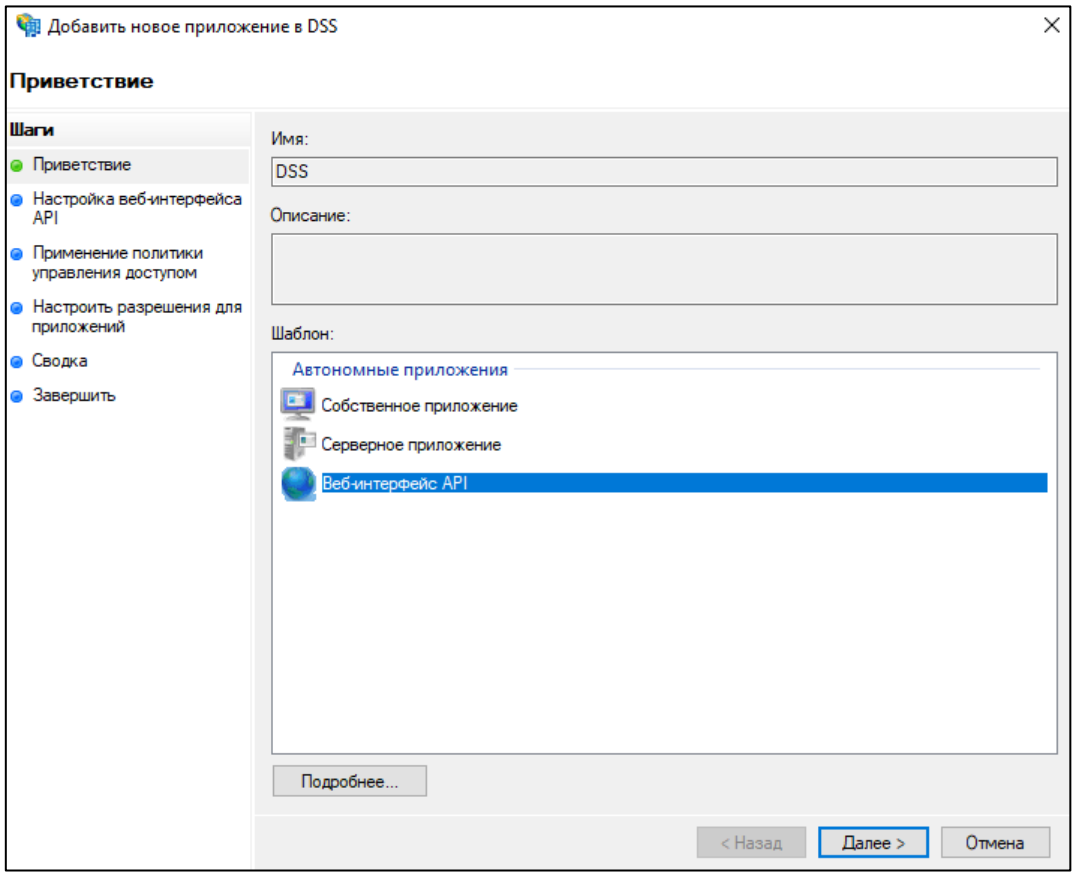

Рисунок 35. Добавление нового приложения в группу

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

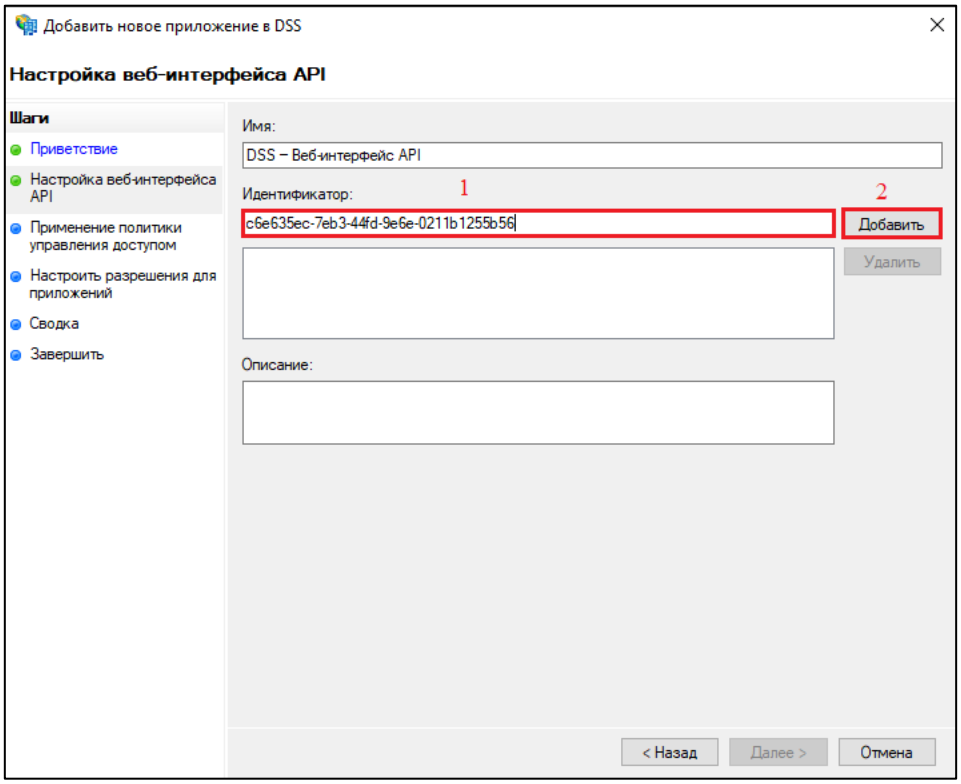

Рисунок 36. Указание идентификатора клиента

3.1.12. Выбрать политику *«Разрешение для каждого»* и нажать кнопку *«Далее»* (см. Рисунок 37):

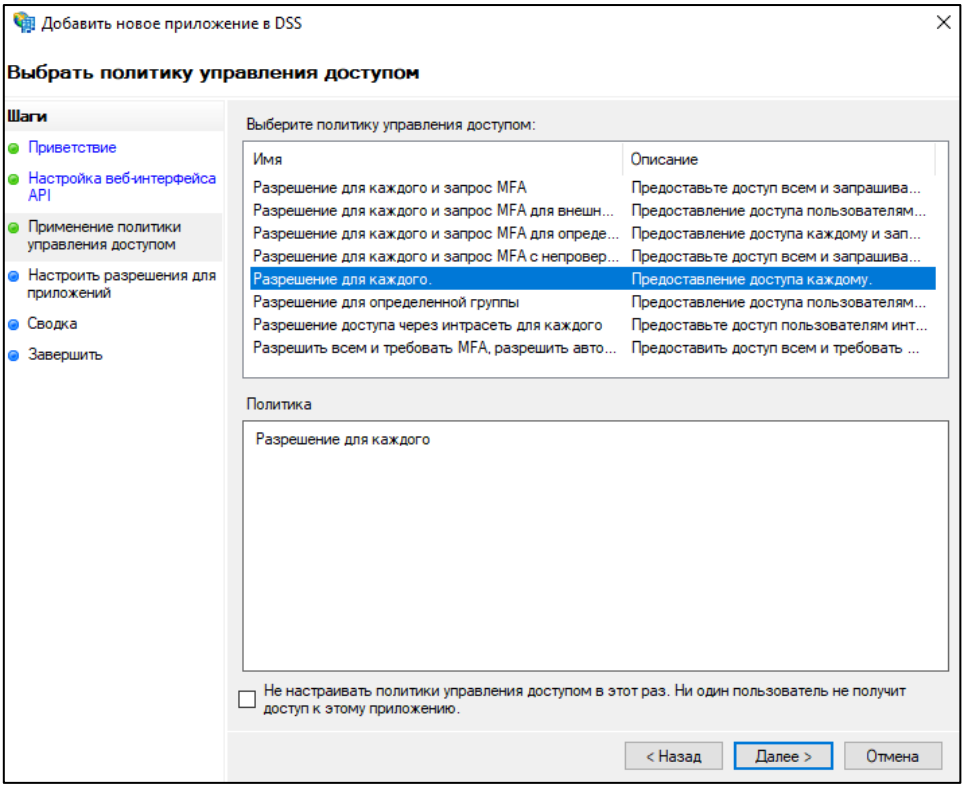

Рисунок 37. Политика управления доступом приложения

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

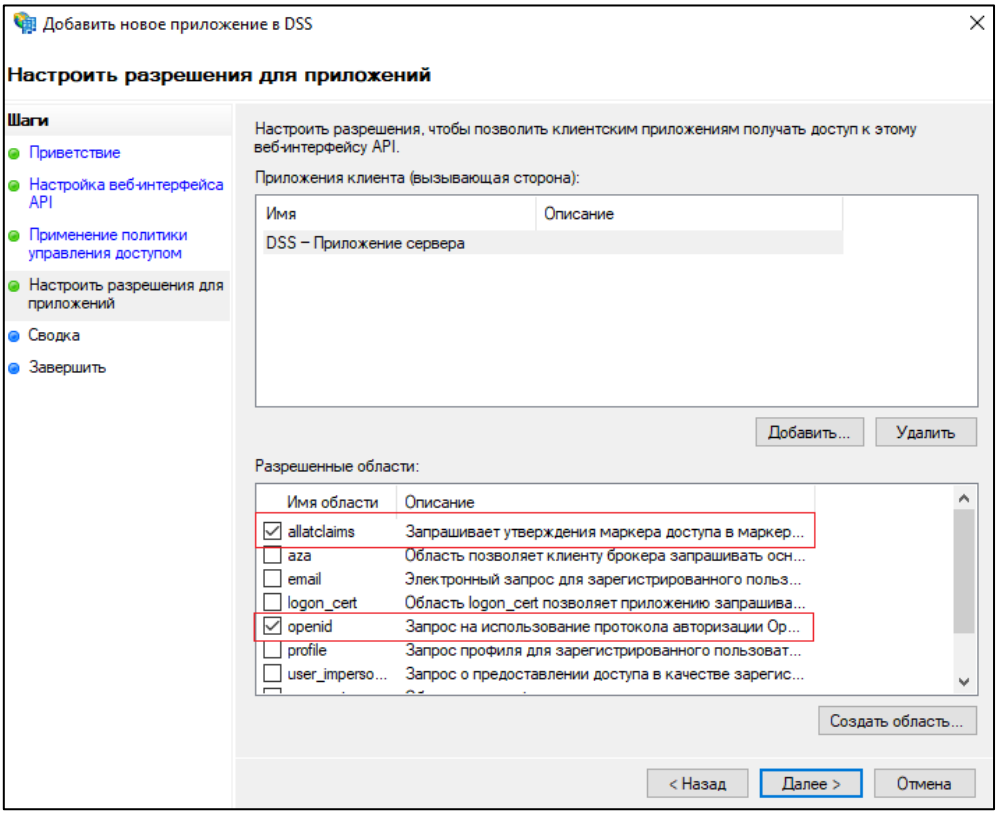

Рисунок 38. Разрешенные области приложения

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

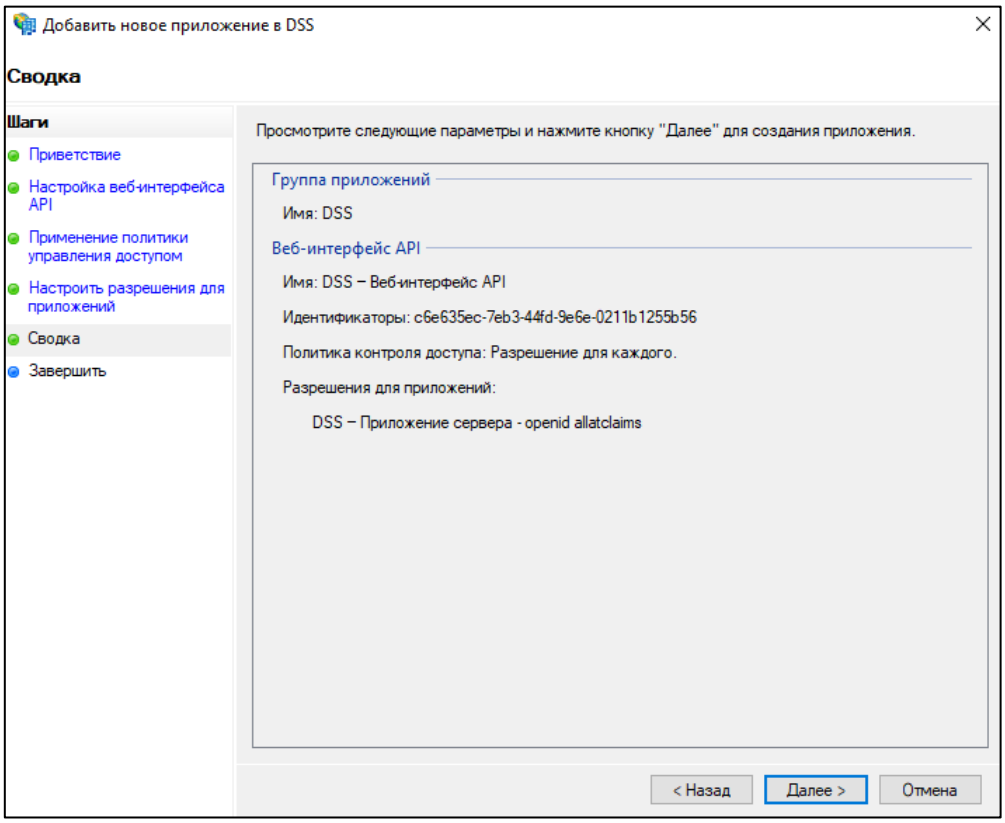

Рисунок 39. Сводка данных группы приложений и приложения веб-интерфейса

3.1.15. Нажать кнопку *«Закрыть»* (см. Рисунок 40):

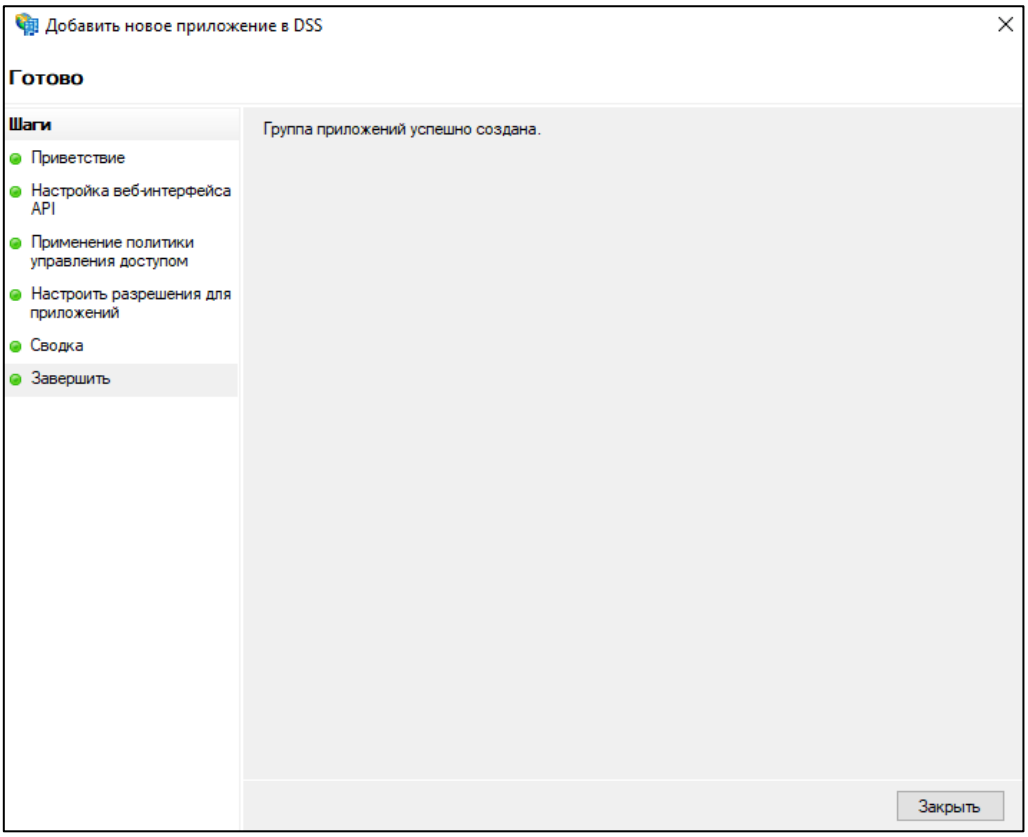

Рисунок 40. Завершение работы мастера добавления нового приложения

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 https://adfs hostname/adfs/oauth2/authorize -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 п. 3.1.5.

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):

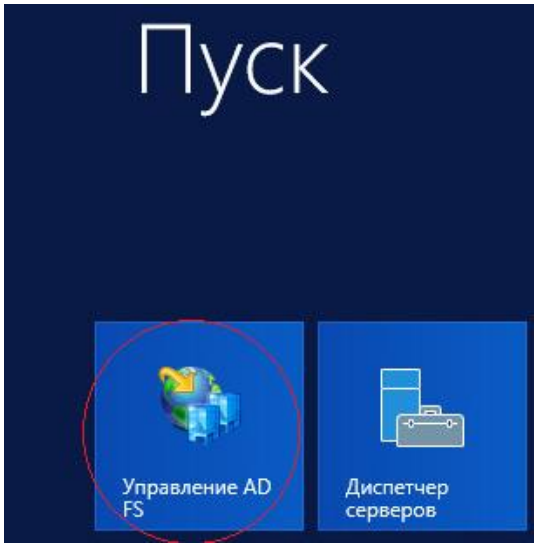

Рисунок 41. Запуск мастера управления ADFS.

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):

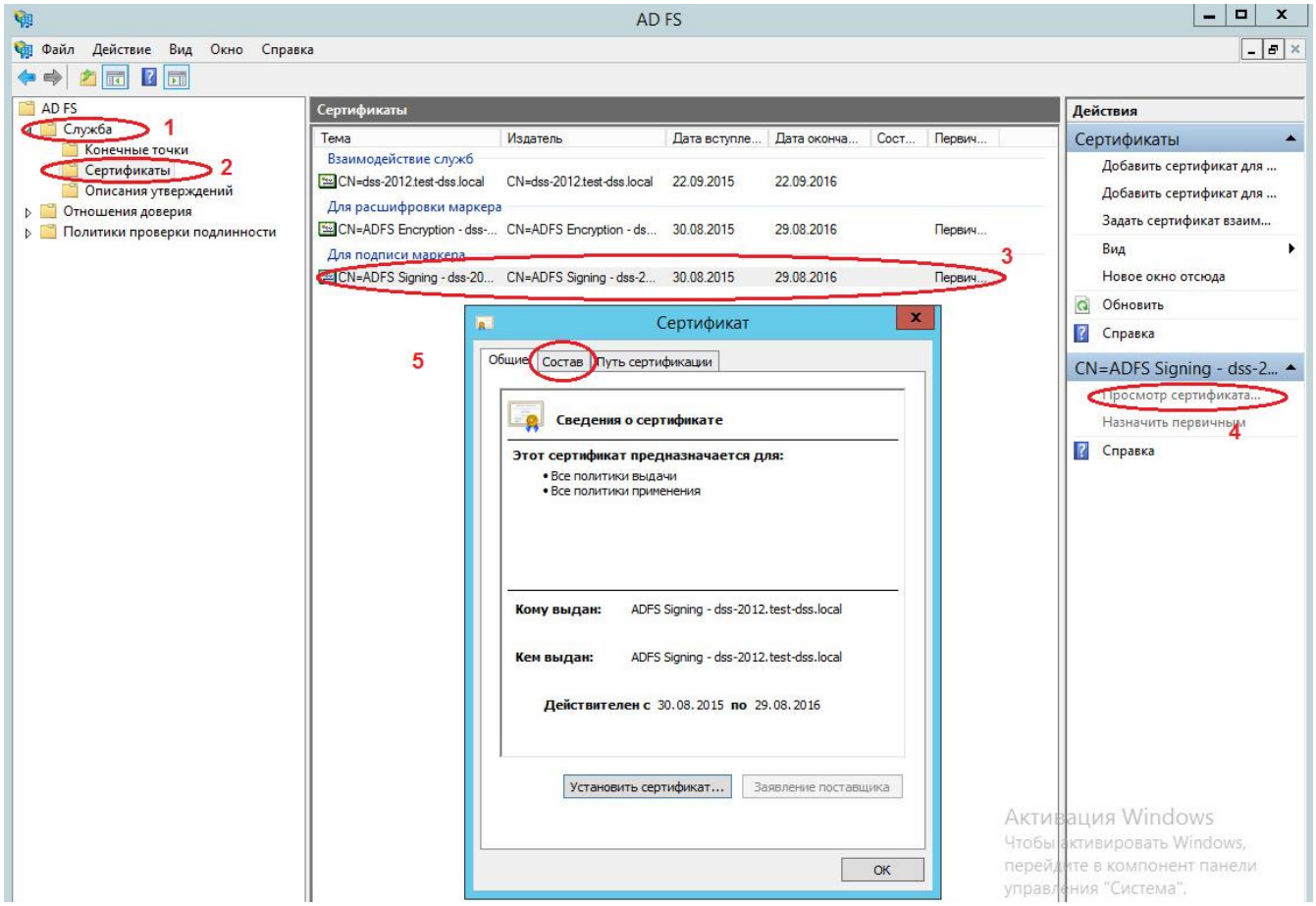

Рисунок 42. Выбор сертификата для выгрузки.

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

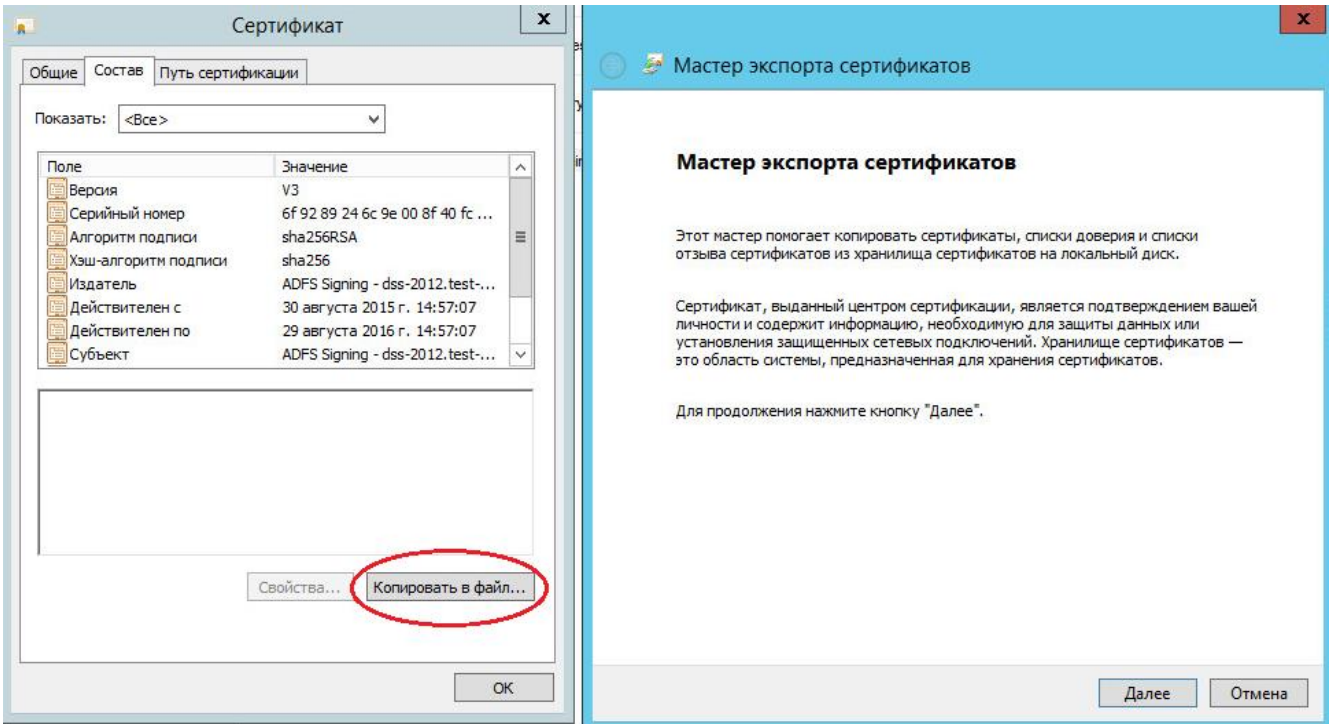

Рисунок 43. Экспорт сертификата.

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

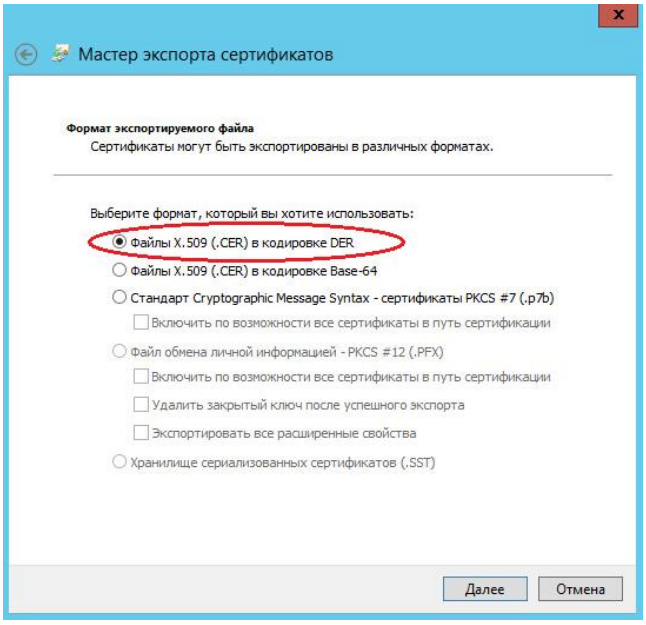

Рисунок 44. Выбор формата сохраняемого файла.

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):

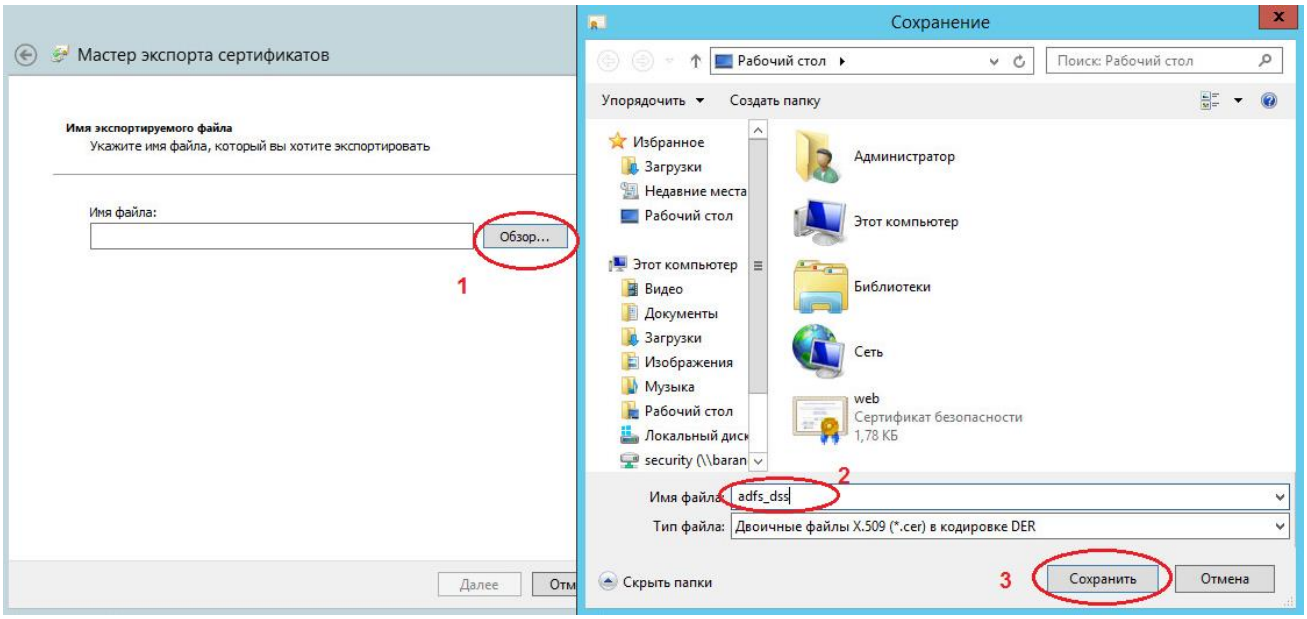

Рисунок 45. Сохранение файла с сертификатом.

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 DSS-operator-AD@domain.ru -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 п. 3.1.3 (см. Рисунок 46):

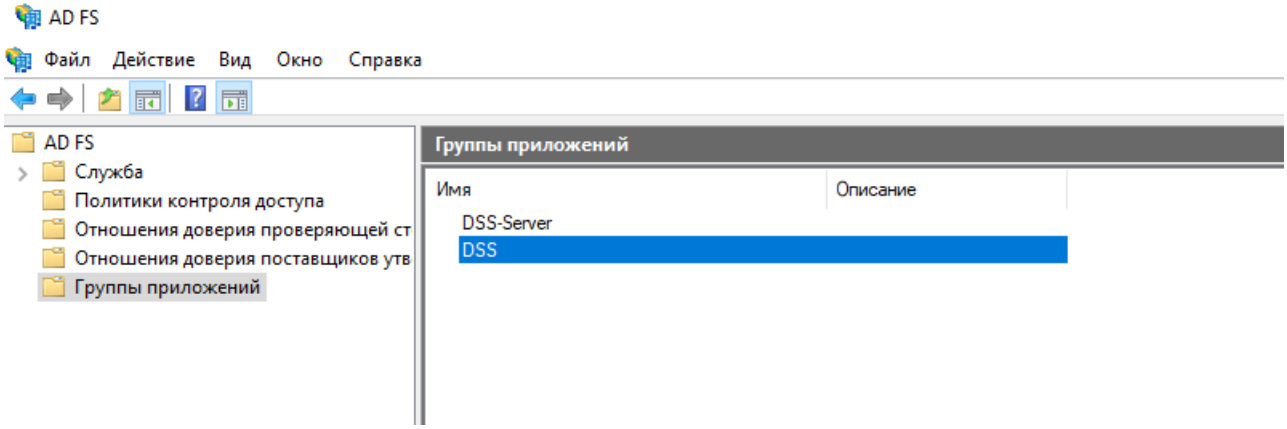

Рисунок 46. Изменение/добавление «правил утверждения»

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

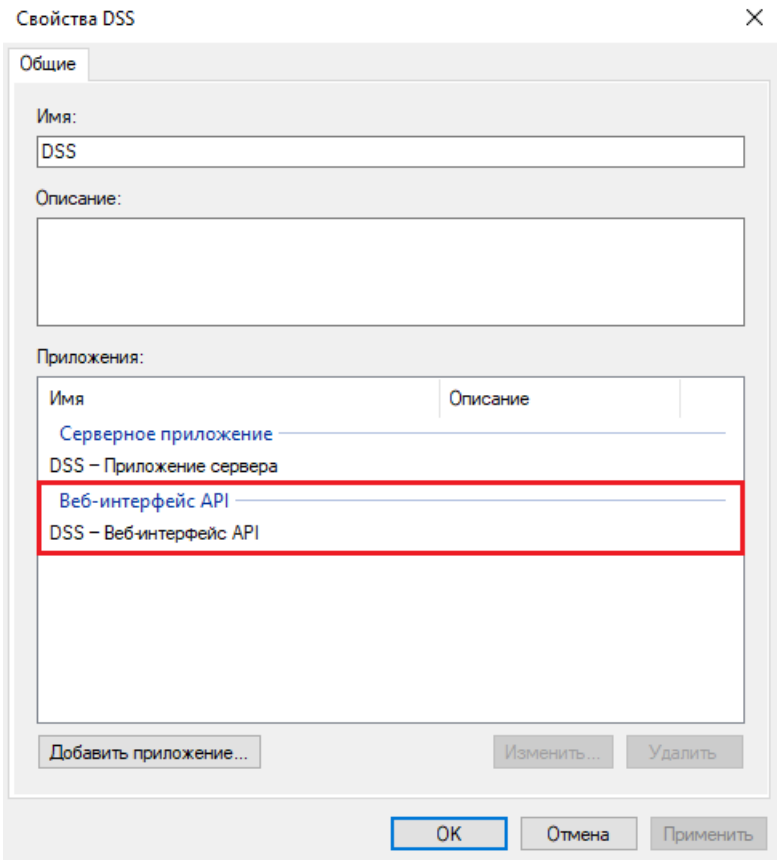

Рисунок 47. Свойства группы приложений

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

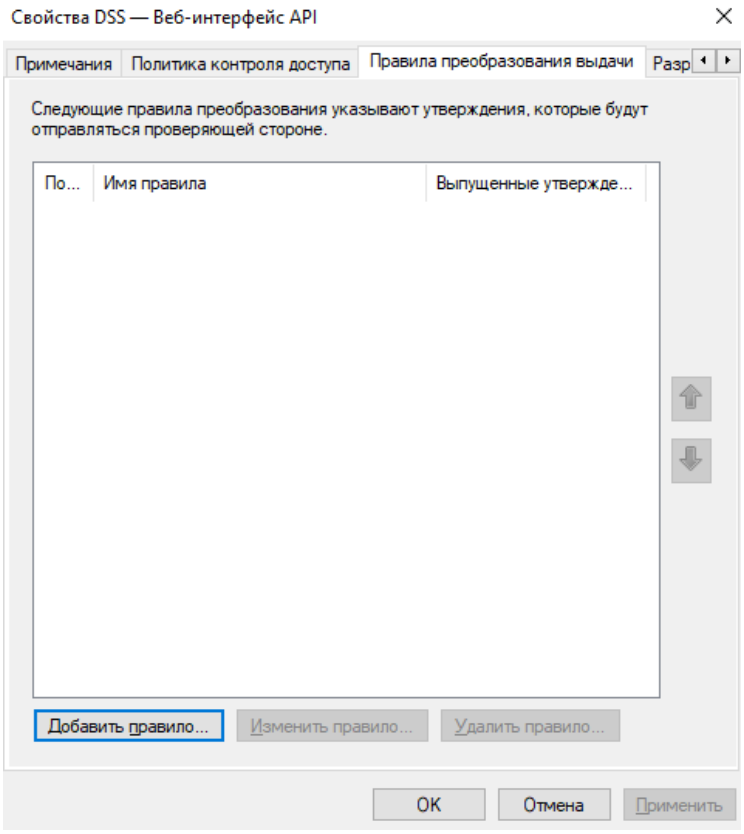

Рисунок 48. Добавление правил преобразований утверждений

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):

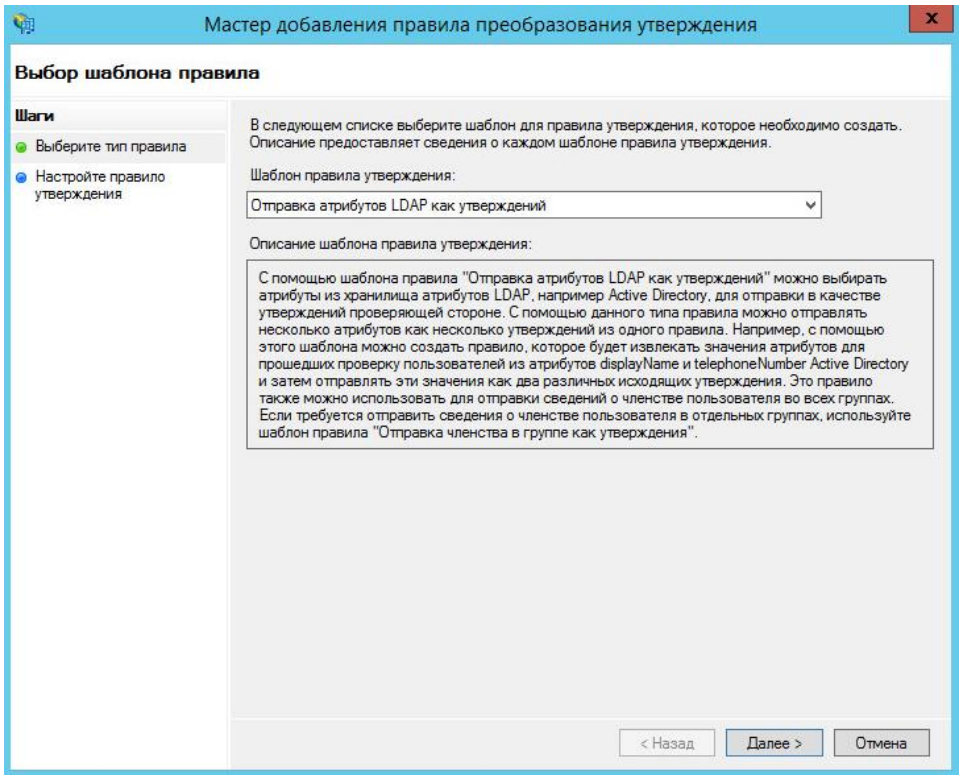

Рисунок 49. Выбор шаблона правила утверждения

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

(http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name). Далее необходимо нажать кнопку *«Готово»*.

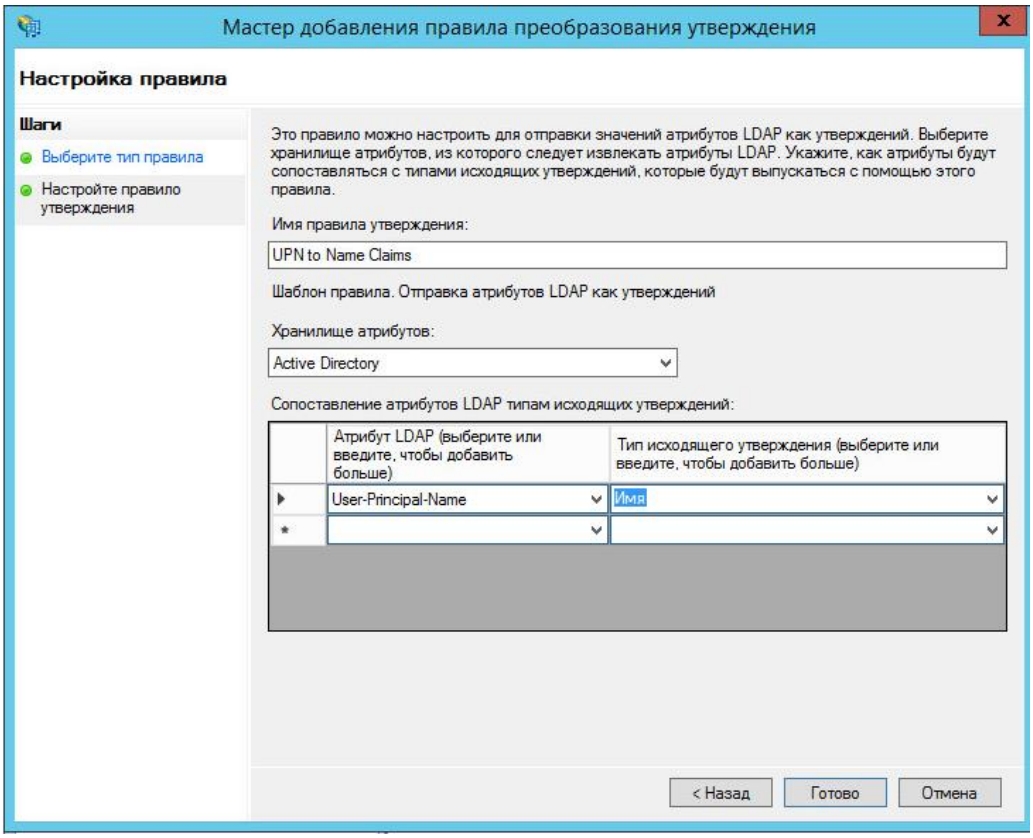

Рисунок 50. Создание правил преобразований утверждений.

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):

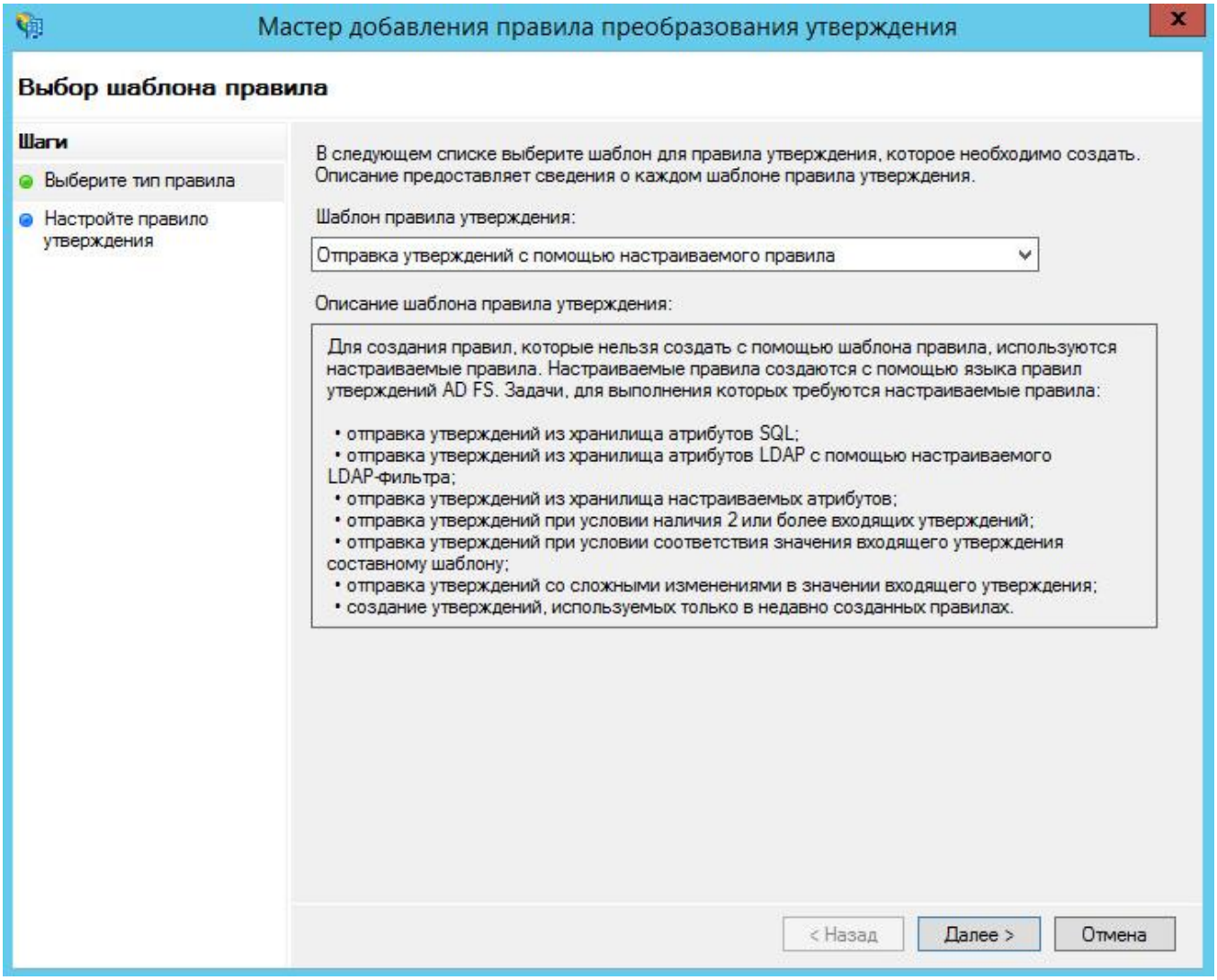

Рисунок 51. Выбор шаблона правила преобразования утверждения.

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 http://dss.cryptopro.ru/identity/claims/marker 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»*.

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/identity/claims/name	Логин	Уникальный идентификатор в пределах ЦИ
http://schemas.microsoft.com/ws/2008/06/identity/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/identity/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/identity/claims/emailaddress	Адрес электронной почты	Компонент имени субъекта, но может использоваться и самостоятельно.
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/country	Страна	Компонент имени субъекта
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince	Область	Компонент имени субъекта
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/locality	Город	Компонент имени субъекта
http://dss.cryptopro.ru/identity/claims/organization	Организация	Компонент имени субъекта
http://dss.cryptopro.ru/identity/claims/organizationunit	Отдел	Компонент имени субъекта
http://schemas.xmlsoap.org/claims/CommonName	Общее имя	Компонент имени субъекта
http://schemas.xmlsoap.org/ws/2005/05/identity/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/identity/claims/givenname	Имя, Отчество	Компонент имени субъекта

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Фамилия	Компонент имени субъекта
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/x500distinguishedname	Различительное 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 AD

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

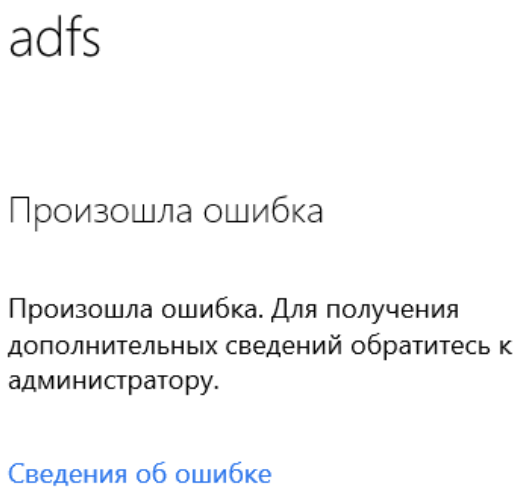

Рисунок 52. Ошибка аутентификации

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

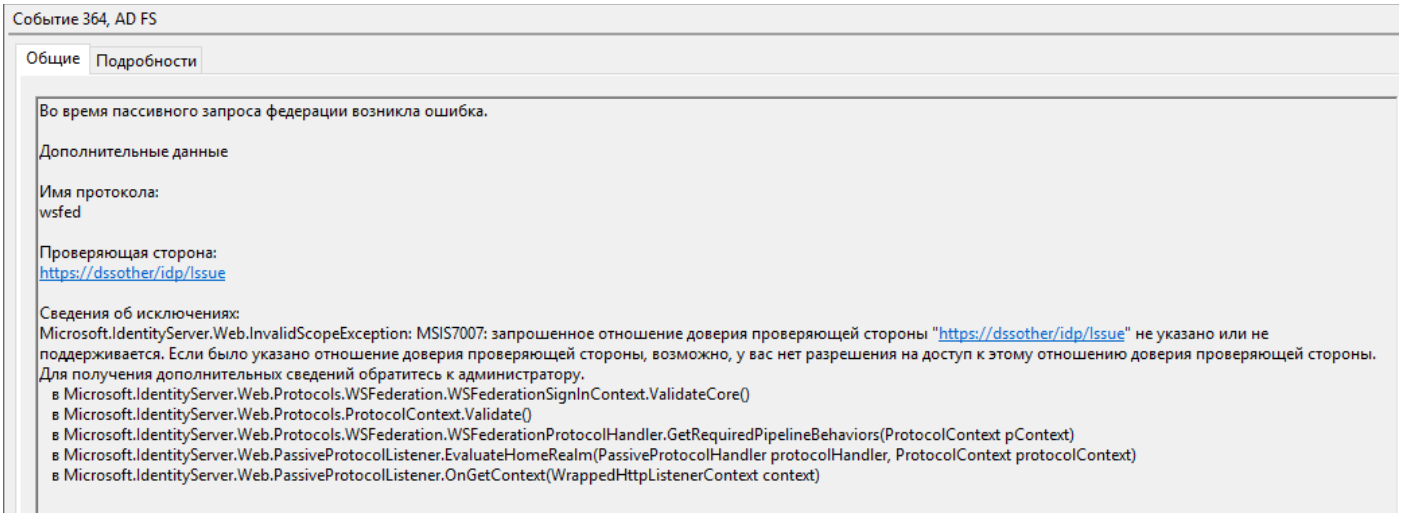

Рисунок 53. Ошибка в журнале ADFS, возникающая при попытке пройти аутентификацию

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 http://schemas.microsoft.com/ws/2008/06/identity/claims/role»* (см. рисунок 54):

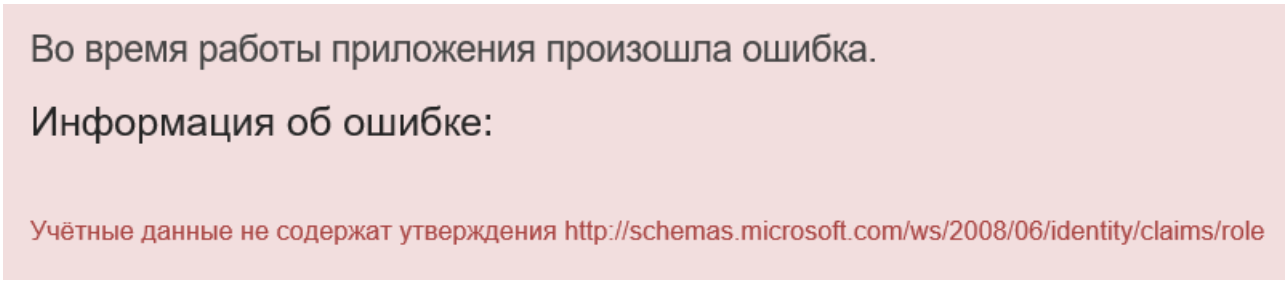

Рисунок 54. Ошибка «Учетные данные не содержат утверждения»

Возможные причины возникновения ошибки:

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

- были допущены ошибки при добавлении правил преобразования утверждений.

Б3. 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):

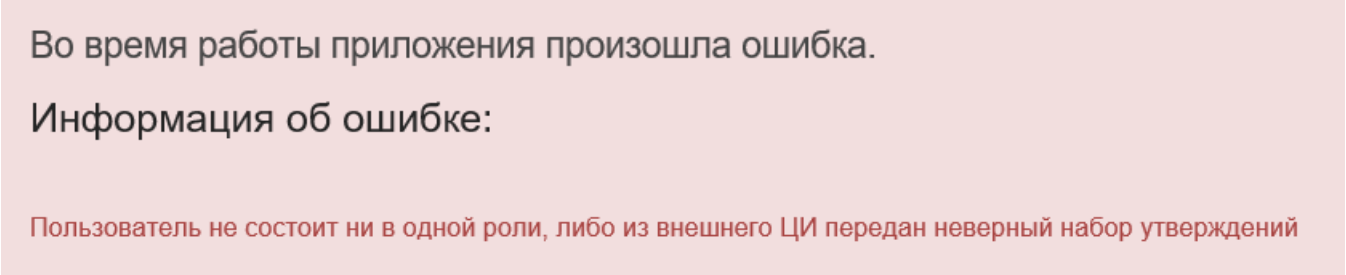

Рисунок 55. Ошибка «Пользователь не состоит ни в одной роли, либо из внешнего ЦИ передан неверный набор утверждений»

Возможные причины возникновения ошибки:

- в ADFS не добавлены правила преобразования утверждений, в соответствие с п. 2.4 – для WSFed или п. 3.4 текущего руководства – 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):

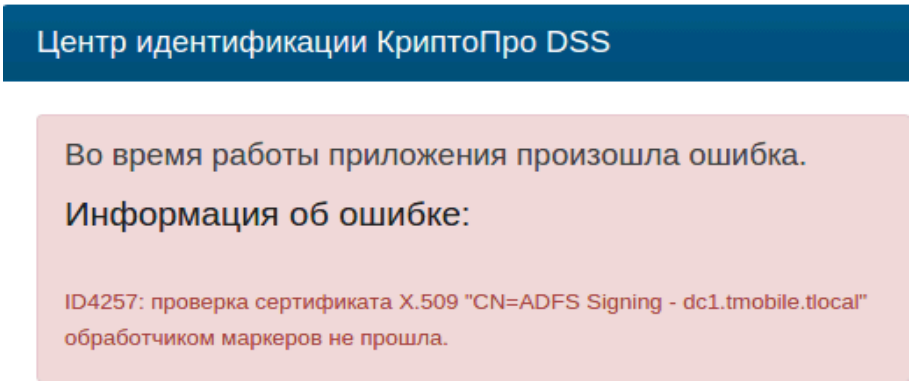

Рисунок 56. Ошибка «Проверка сертификата обработчиком маркеров не прошла»

Возможная причина возникновения ошибки:

При выполнении командлета *Add-DssIdentityProvider*, в соответствие с п. 2.1 – для WSFed или п. 3.2 текущего руководства – 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 данные должны содержать только одно утверждение: http://schemas.microsoft.com/ws/2008/06/identity/claims/role»* (см. Рисунок 57):

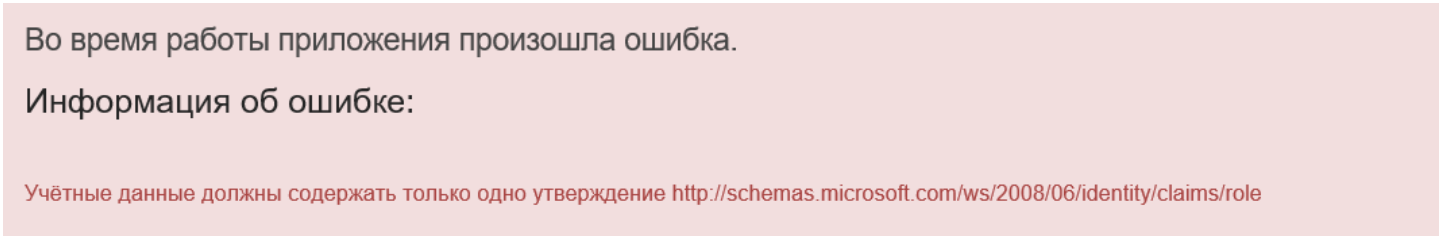

Рисунок 57. Ошибка «Учётные данные должны содержать только одно утверждение»

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 п. 2.4 – для WSFed или п. 3.4 текущего руководства – 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):

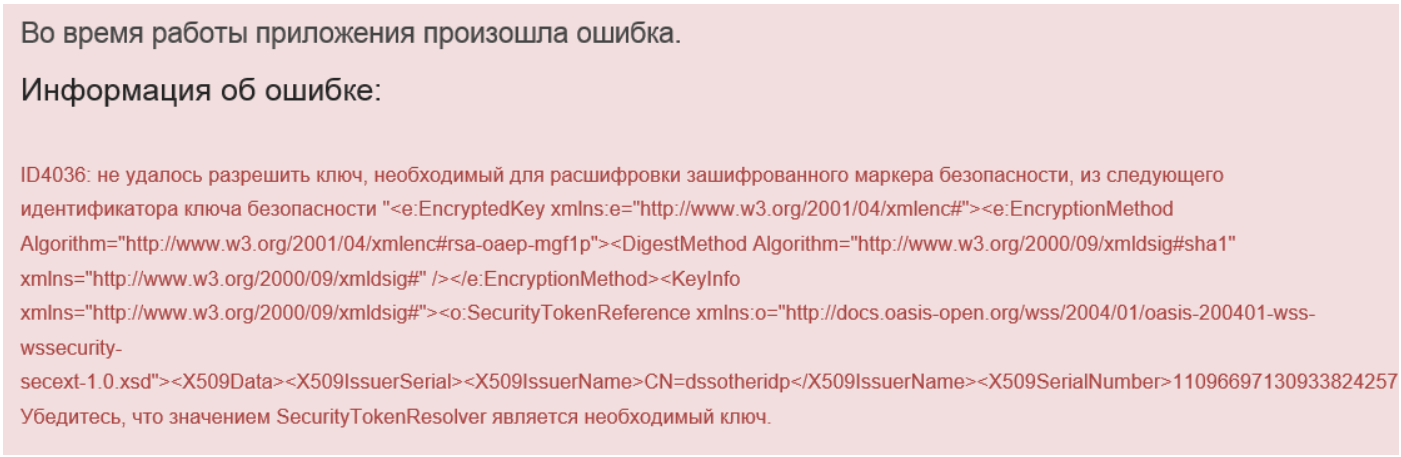

Рисунок 58. Ошибка «ID4036»

Возможные причины возникновения ошибки:

- При настройке отношений доверия проверяющей стороны по протоколу WSFed, в соответствие с п. 2.2.7 текущего руководства, 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 → Отношения доверия проверяющей стороны → Открыть свойства проверяющей стороны → Шифрование → Обзор → 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):

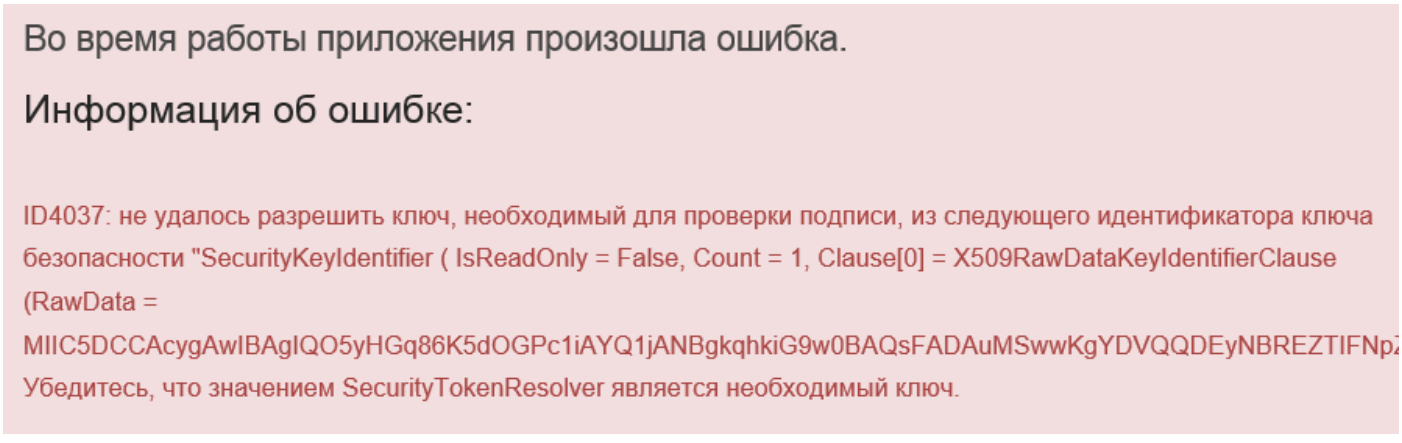

Рисунок 59. Ошибка «ID4037»

Возможные причины возникновения ошибки:

- При выполнении командлета *Add-DssIdentityProvider*, в соответствие с п. 2.1 – для WSFed или п. 3.2 текущего руководства – 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 "Отпечаток актуального сертификата подписи маркеров ADFS"* и перезапустить пул приложений ЦИ КриптоПро DSS.