Система электронной подписи

на базе КриптоПро Ключ

Руководство администратора СЦИ (ADFS)

На 23 листах

Москва, 2025

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 Ключ. В документе описаны действия, необходимые для выполнения интеграции ЦИ КриптоПро Ключ и СЦИ на базе Службы федерации корпоративного домена (Active Directory Federation Services, ADFS) с использованием протокола OpenId Connect 1.0 (Oidc).

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

ЦИ КриптоПро Ключ напрямую с ADFS не взаимодействует (**исключение** – сценарий использования JSON Web Key Set ADFS для проверки целостности и неизменности маркеров доступа СЦИ), 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 Ключ, приведен в Приложении А «Утверждения доверенной стороны (Microsoft Active Directory), передаваемые в КриптоПро Ключ».

Для выполнения работ по интеграции в соответствие с данным документом необходимо использование ADFS в составе Windows Server 2016 TP4 или выше (с поддержкой подключения по протоколу Oidc). Кроме этого необходимо иметь доступ и права администратора Сервисов КриптоПро Ключ, а также доступ и права доменного администратора на сервере ADFS.

При составлении текущего руководства использовались:

- КриптоПро Ключ 1.0.857;
- ADFS в составе Windows Server 2016 TP4.

2. ИНТЕГРАЦИЯ СТОРОННЕГО ЦЕНТРА ИДЕНТИФИКАЦИИ ADFS WINDOWS SERVER 2016 TP4 ПО ПРОТОКОЛУ OPENID CONNECT 1.0

Интеграция СЦИ ADFS из состава Windows Server 2016 TP4 и ЦИ КриптоПро Ключ по протоколу OpenId Connect 1.0 осуществляется в следующем порядке:

- Создание группы приложений;
- Настройка отношения доверия между ЦИ КриптоПро Ключ и ADFS;
- Создание оператора, управляющего пользователями домена;
- Настройка правил преобразования утверждений для доступа к КриптоПро Ключ Оператора, управляющего пользователями домена, и пользователей домена.

2.1. Создание группы приложений

2.1.1. На сервере ADFS запустить консоль управления «Управление AD FS» (Пуск → все программы → «Управление AD FS» (см. рисунок 1).

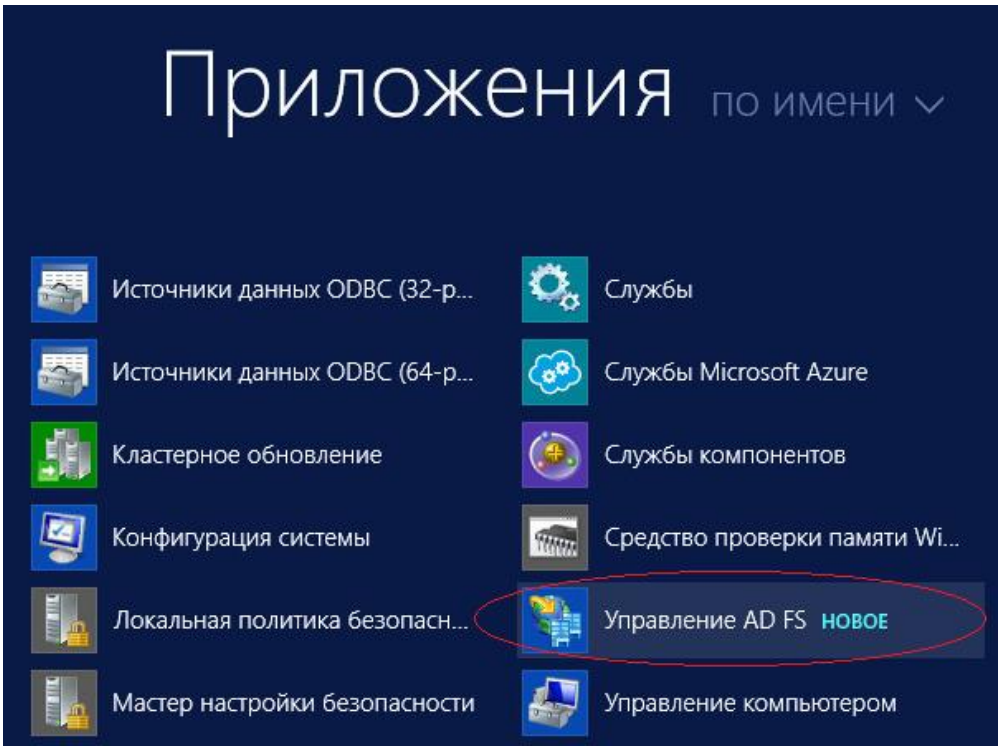

Рисунок 1. Запуск консоли управления ADFS.

2.1.2 Откроется окно, нажать правой кнопкой мыши на пункте *«Группы приложений»* и выбрать пункт *«Добавить группу приложений»* (см. Рисунок 2):

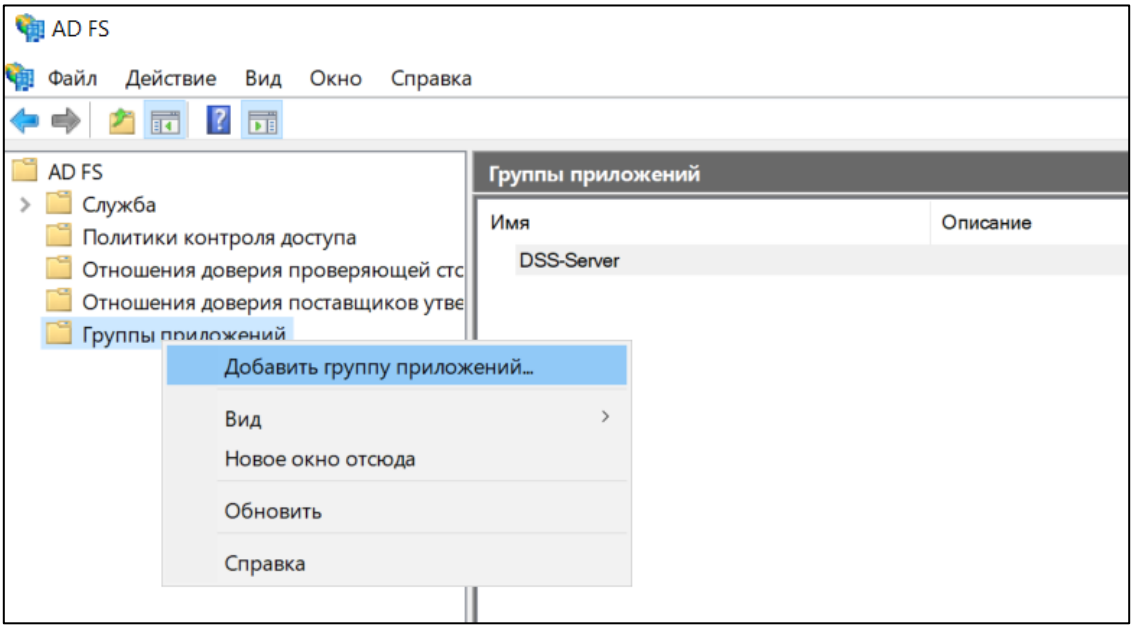

Рисунок 2. Добавление группы приложений

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

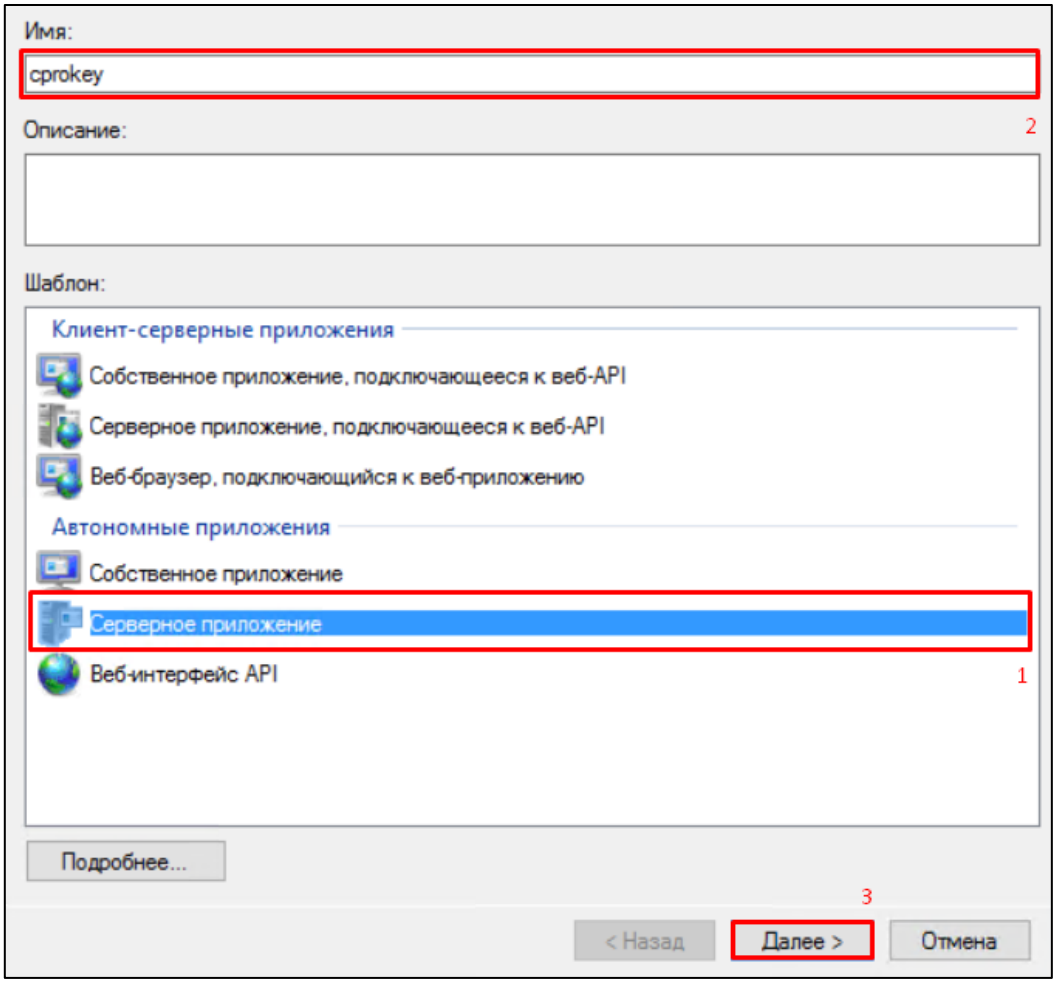

Рисунок 3. Мастер добавления групп приложений

2.1.4. Откроется окно. Необходимо скопировать и сохранить значение из поля *«Идентификатор клиента»* (1). Затем в поле *«Перенаправить URI»* (2) указать адрес формата: https://hostname/sts/signin-oidc

Где:

- hostname – адрес сервера КриптоПро Ключ;
- sts - имя приложения ЦИ КриптоПро Ключ, которое можно узнать, выполнив на сервере КриптоПро Ключ командлет:

```
(Get-IdsInstance).ApplicationName
```

После указания адреса – нажать кнопку *«Добавить»* (3), а затем нажать кнопку *«Далее»* (4) (см. Рисунок 4):

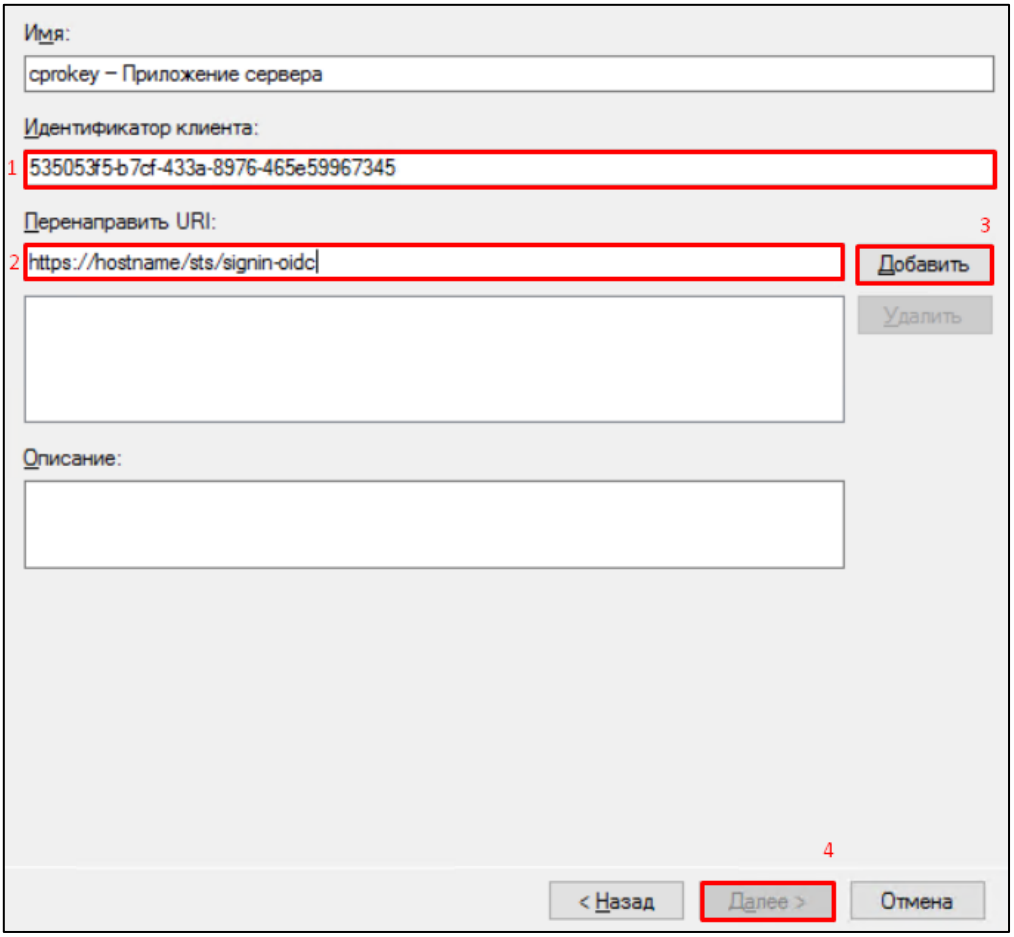

Рисунок 4. Настройка приложения сервера

2.1.5. 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 5):

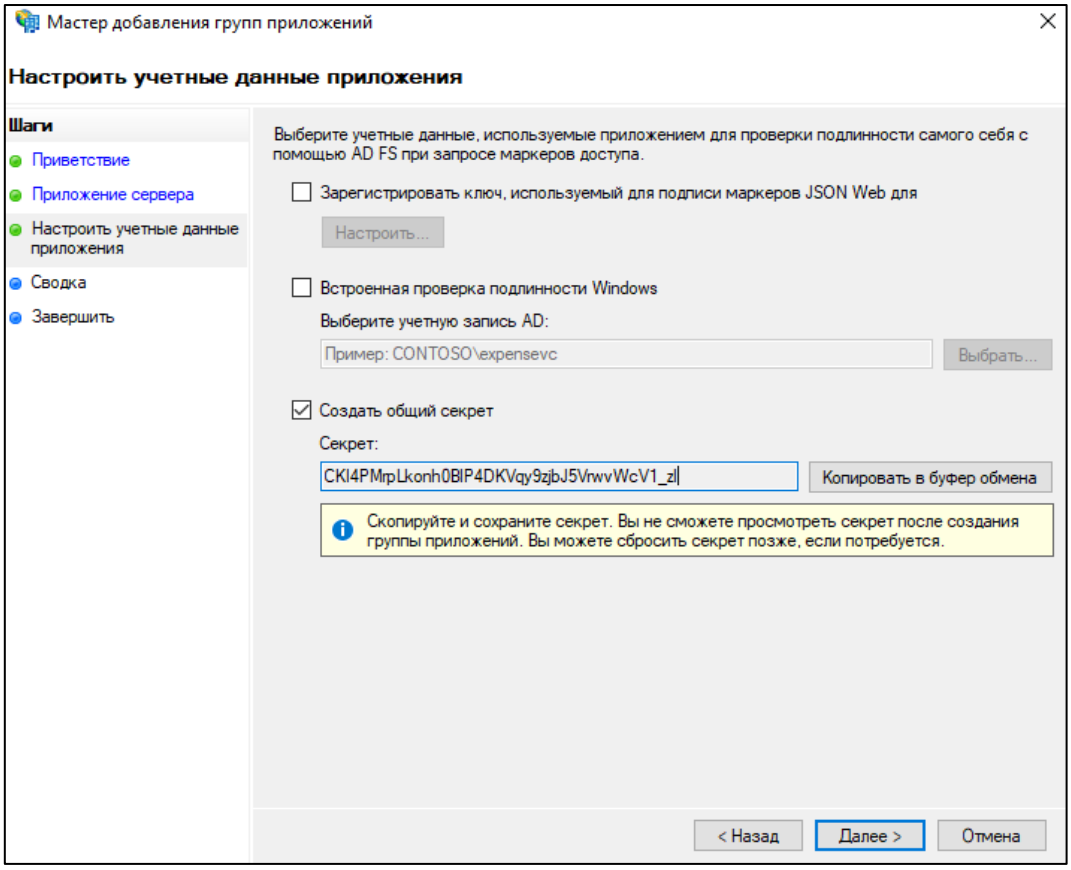

Рисунок 5. Настройка учетных данных приложения

2.1.6. В следующем окне нажать кнопку *«Далее»* (см. Рисунок 6):

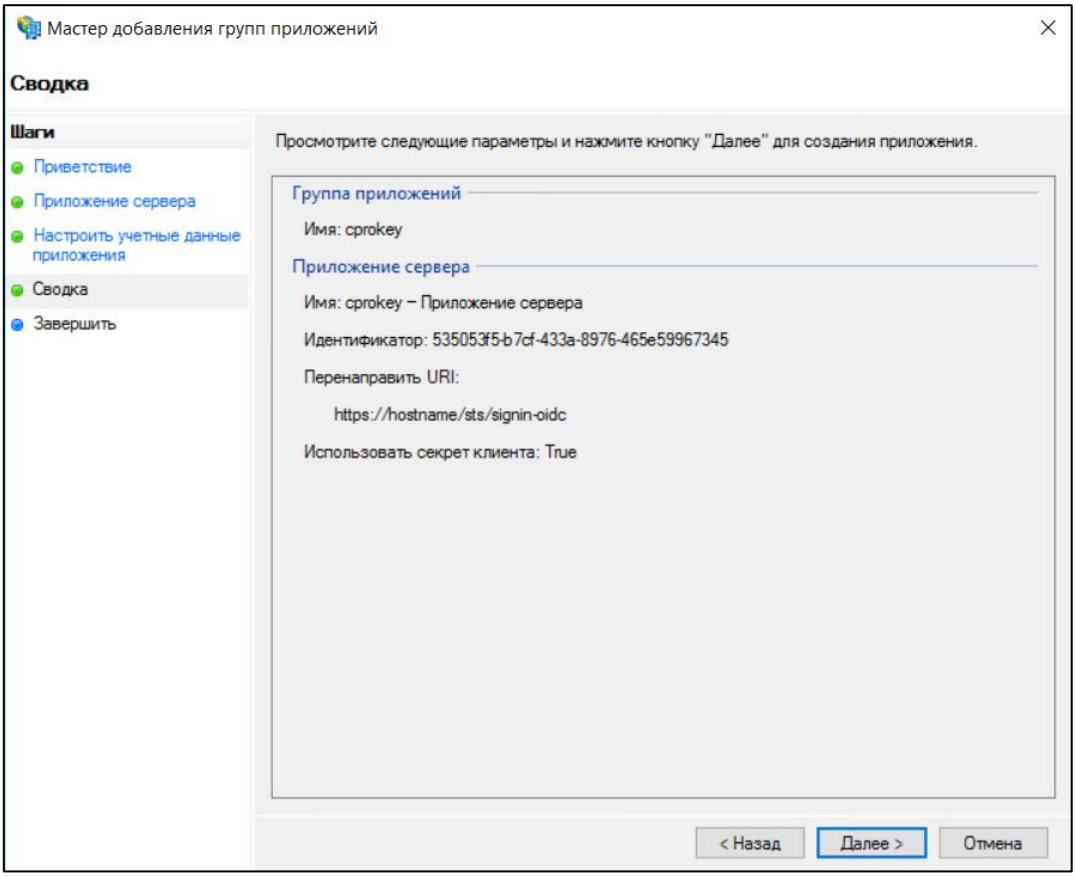

Рисунок 6. Сводка данных группы приложений и серверного приложения

2.1.7. В окне завершения мастера добавления группы приложений нажать кнопку *«Закрыть»* (см. Рисунок 7):

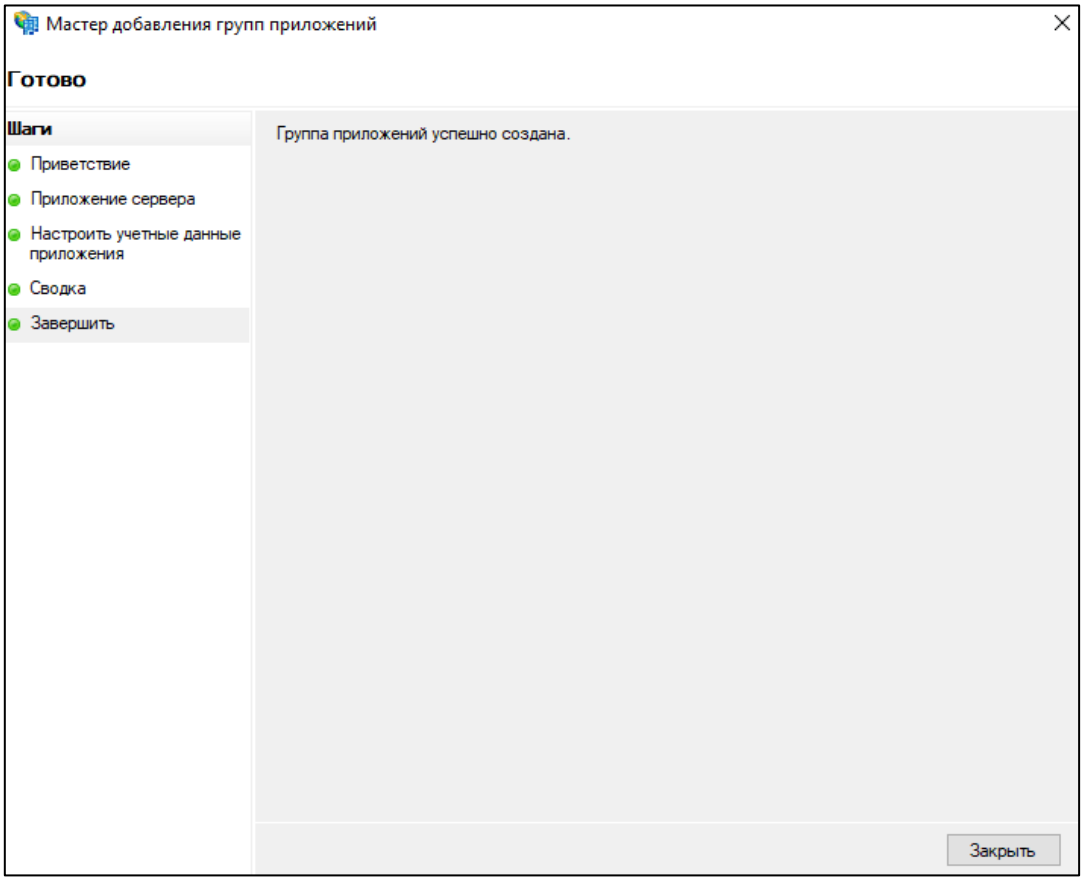

Рисунок 7. Завершение работы мастера добавления группы приложений

2.1.8. Откроется окно со списком созданных групп приложений. Открыть созданную группу приложений двойным кликом мышью (см. Рисунок 8):

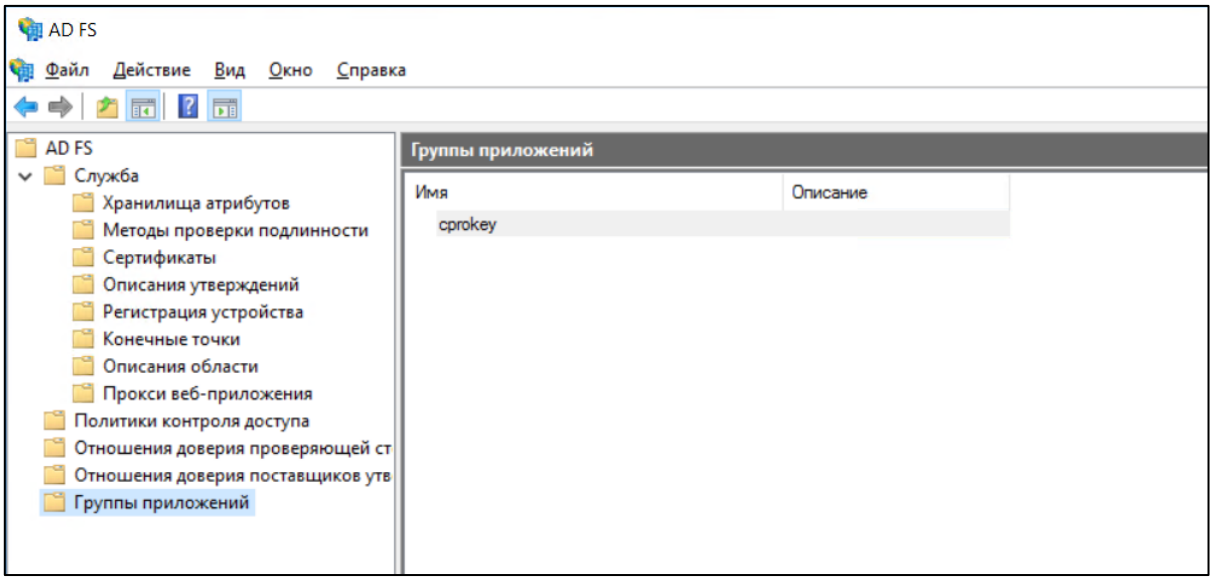

Рисунок 8. Список созданных групп приложений

2.1.9. В окне свойств группы приложений необходимо нажать кнопку *«Добавить приложение»* (см. Рисунок 9):

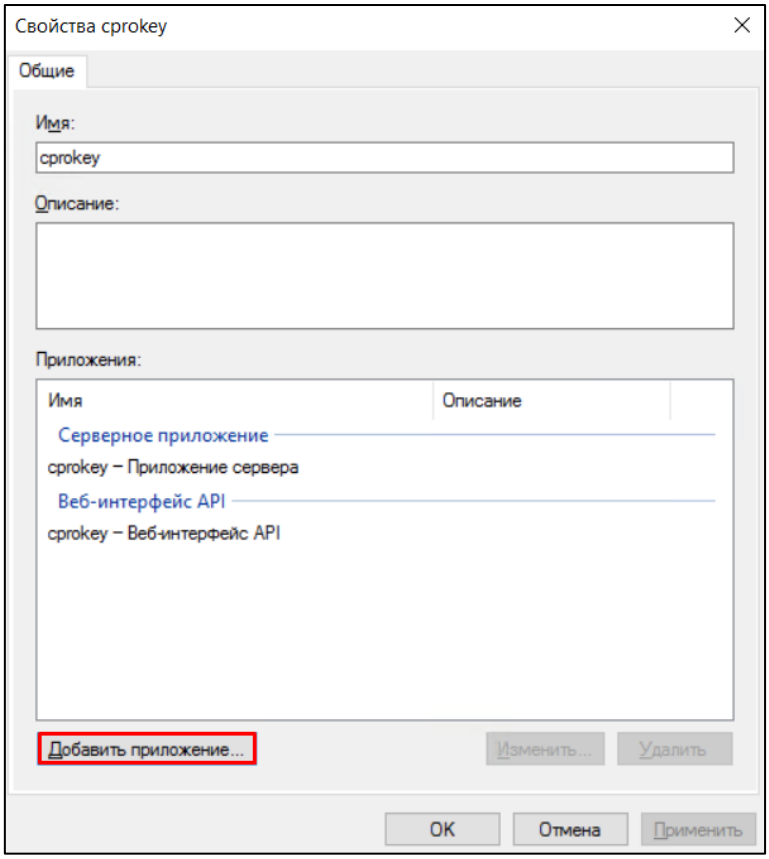

Рисунок 9. Свойства группы приложений

2.1.10. Выбрать из списка шаблонов *«Веб-интерфейс API»*. Нажать кнопку *«Далее»* (см. Рисунок 10):

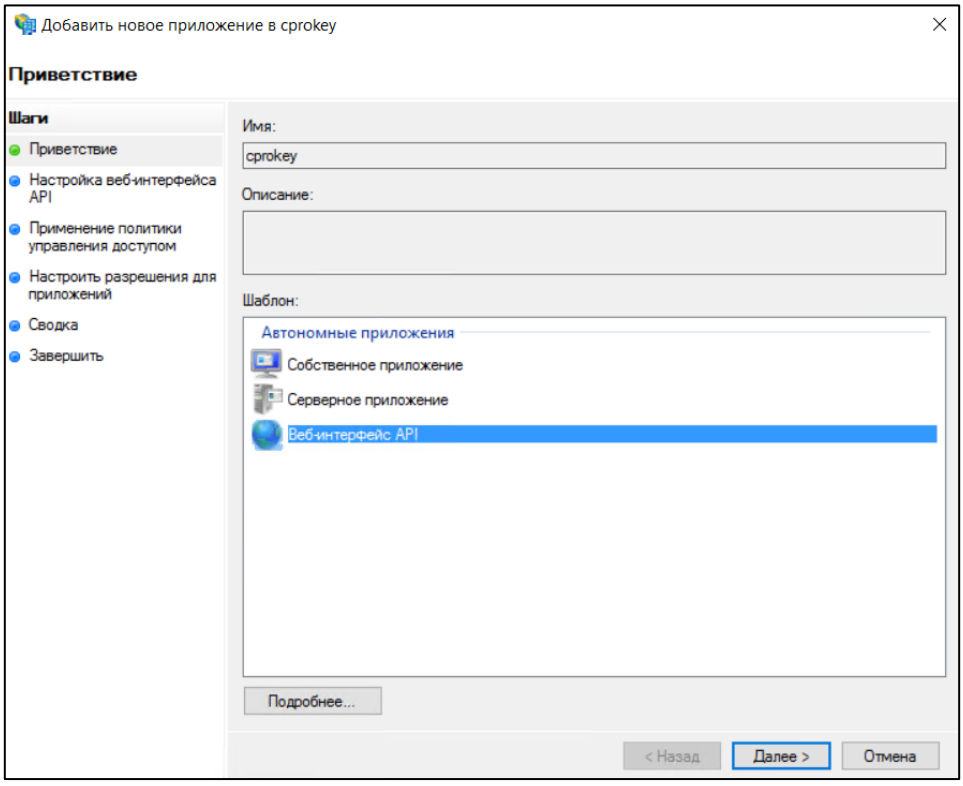

Рисунок 10. Добавление нового приложения в группу

2.1.11. В поле идентификатор (1) требуется указать значение идентификатора клиента, полученное в п. 2.1.4, а затем – нажать кнопку *«Добавить»* (2). После этого необходимо нажать кнопку *«Далее»* (3) (см. Рисунок 11):

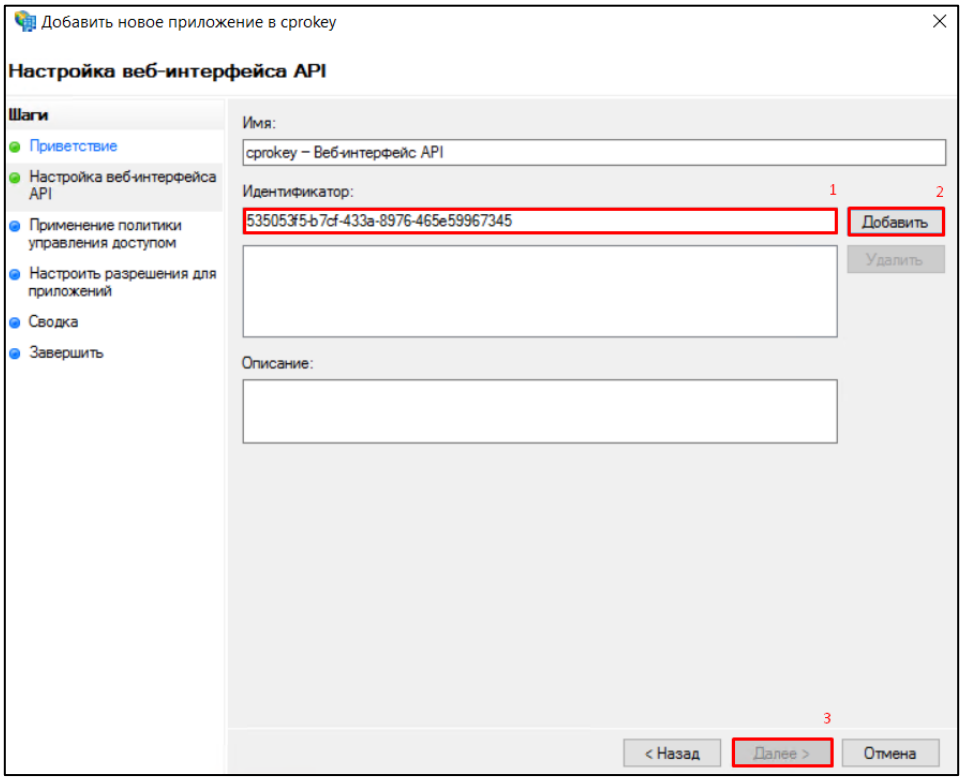

Рисунок 11. Указание идентификатора клиента

2.1.12. Выбрать политику *«Разрешение для каждого»* и нажать кнопку *«Далее»* (см. Рисунок 12):

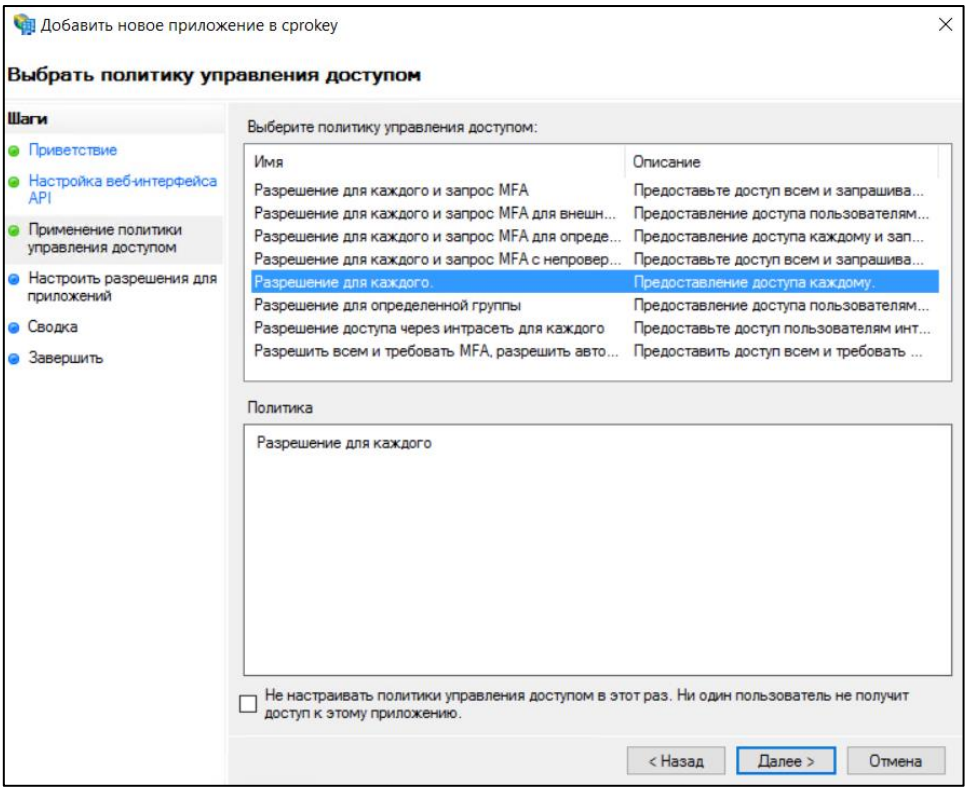

Рисунок 12. Политика управления доступом приложения

2.1.13. В списке разрешенных областей необходимо отметить области *«allatclaims»* и *«openid»*. Затем – нажать кнопку *«Далее»* (см. Рисунок 13):

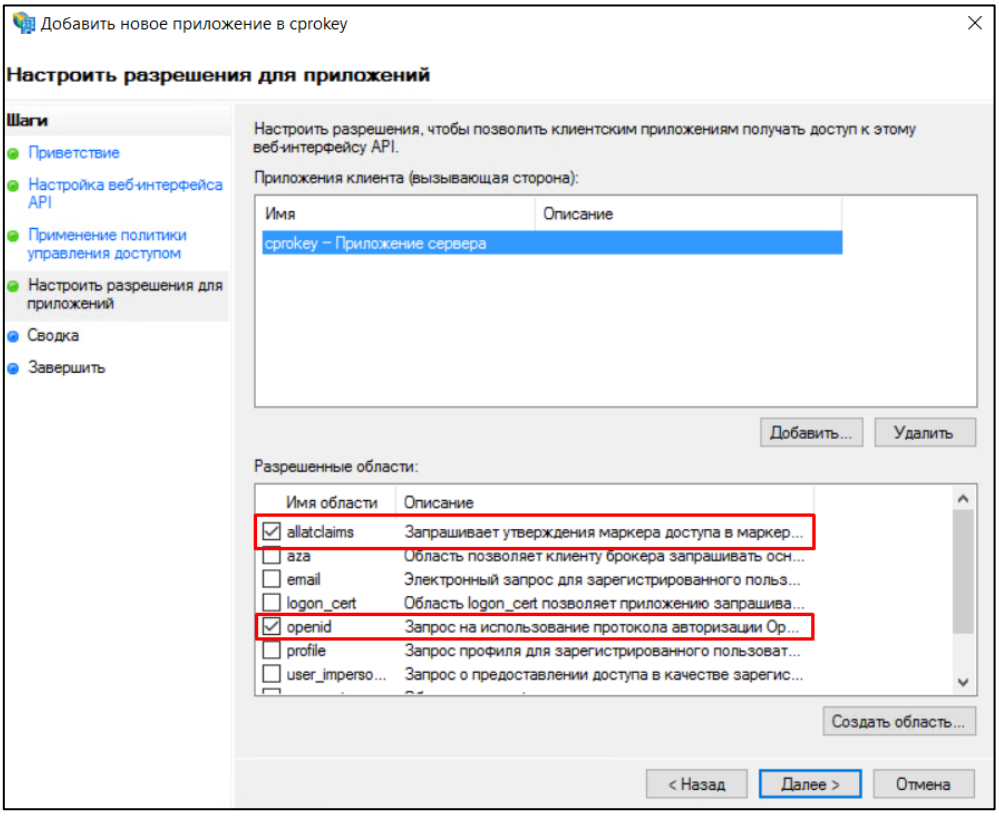

Рисунок 13. Разрешенные области приложения

2.1.14. В следующем окне нажать кнопку *«Далее»* (см. Рисунок 14):

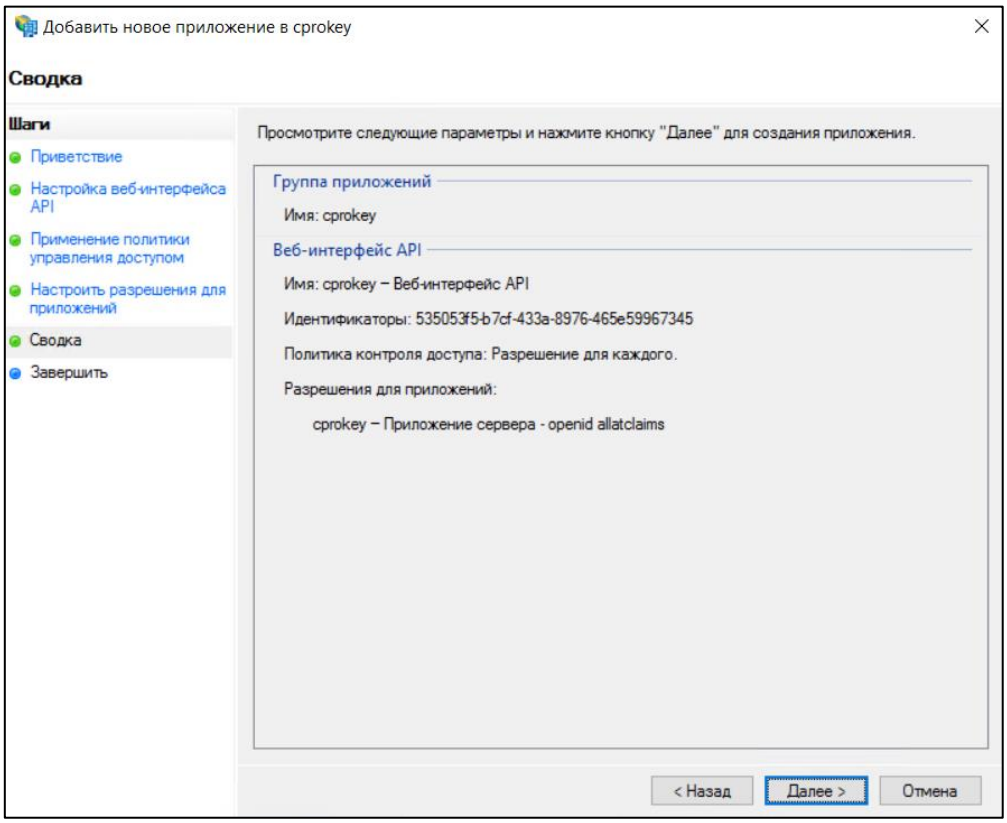

Рисунок 14. Сводка данных группы приложений и приложения веб-интерфейса

2.1.15. Нажать кнопку *«Закрыть»* (см. Рисунок 15):

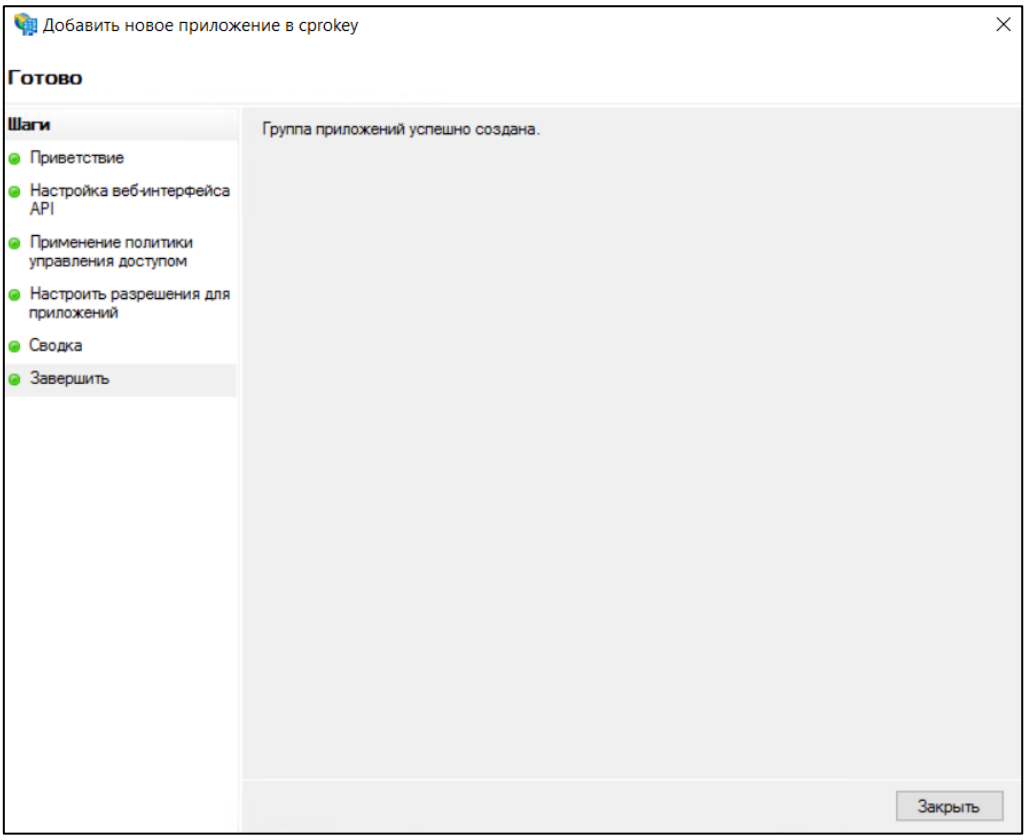

Рисунок 15. Завершение работы мастера добавления нового приложения

2.2. Настройка отношения доверия между ЦИ КриптоПро Ключ и ADFS

2.2.1. Открыть оснастку управления ADFS. Пуск-> Все программы-> Управление AD FS (см. рисунок 16):

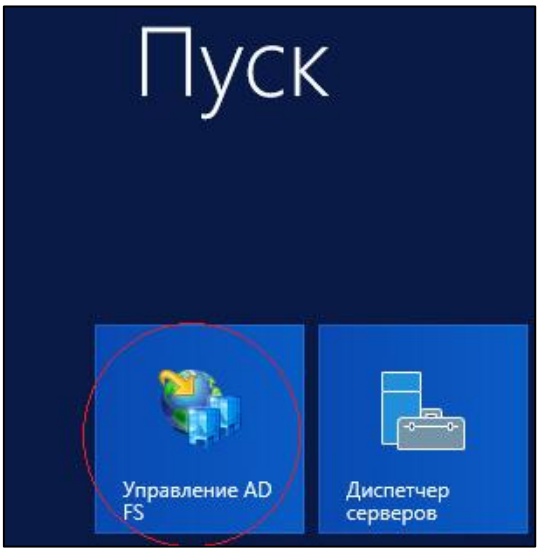

Рисунок 16. Запуск мастера управления ADFS.

2.2.2. Откроется окно, выбрать последовательно «AD FS → Служба → Сертификаты → Для подписи маркера». Затем открыть нужный сертификат для просмотра и нажать кнопку «Состав» (см. рисунок 17):

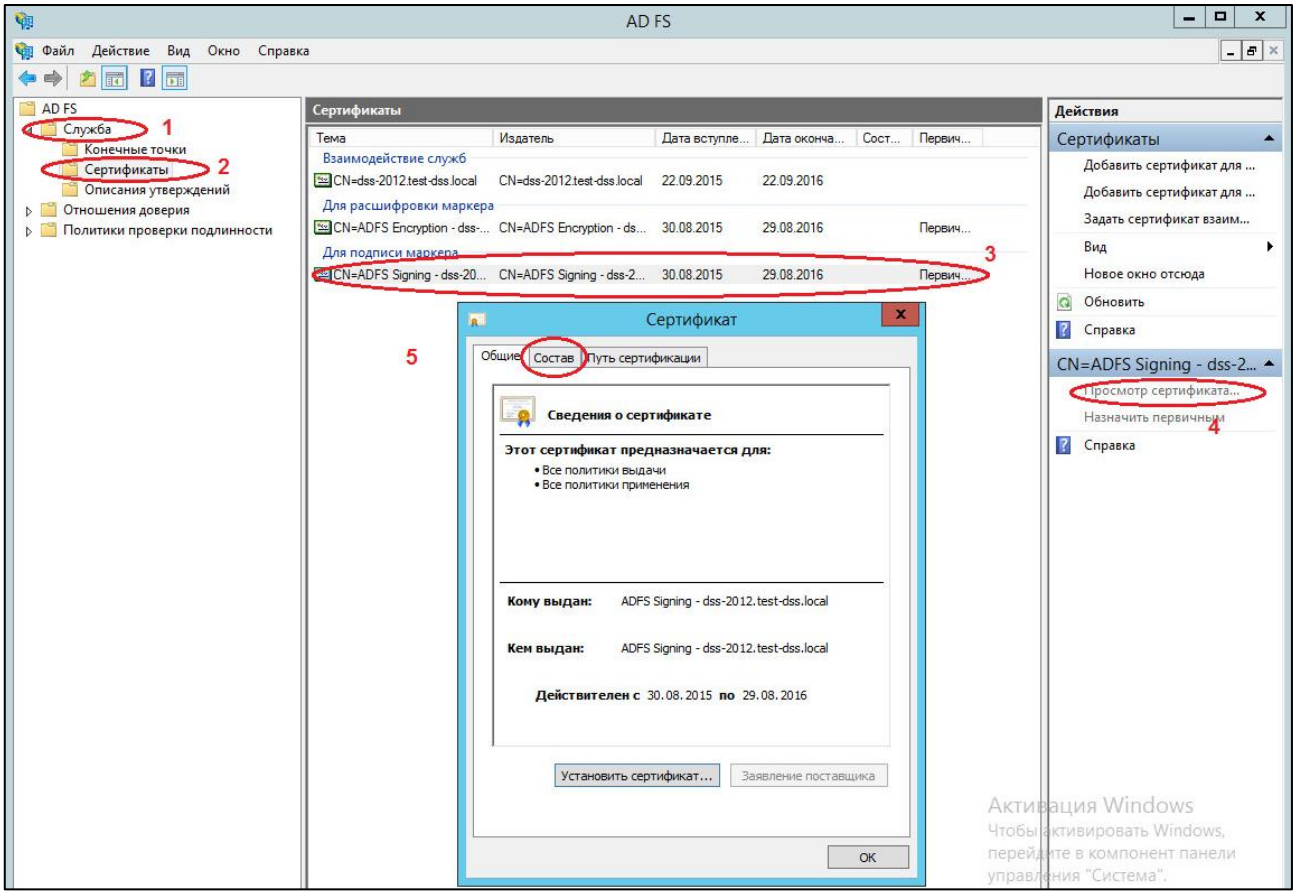

Рисунок 17. Выбор сертификата для выгрузки.

2.2.3. Откроется окно, нажать кнопку «Копировать в файл», откроется мастер экспорта сертификата, нажать кнопку «Далее» (см. рисунок 18).

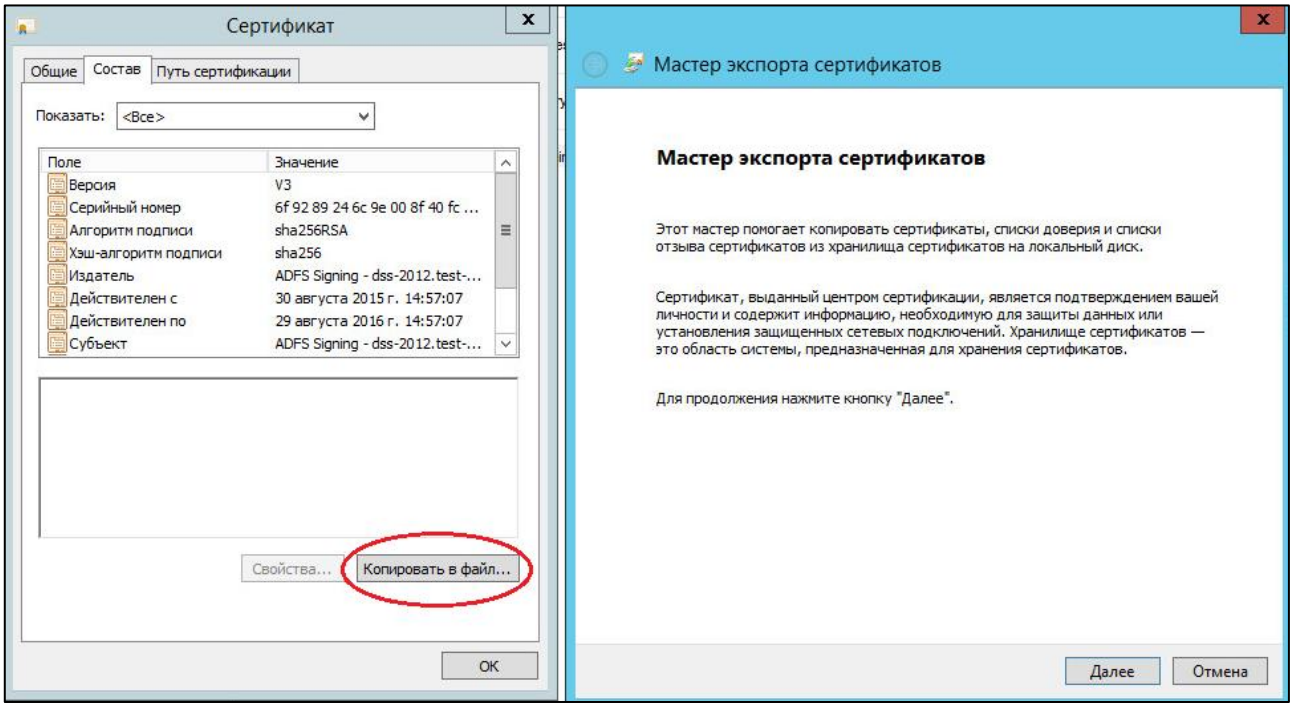

Рисунок 18. Экспорт сертификата.

2.2.4. Откроется окно, выбрать формат сохраняемого файла, нажать кнопку «Далее» (см. рисунок 19):

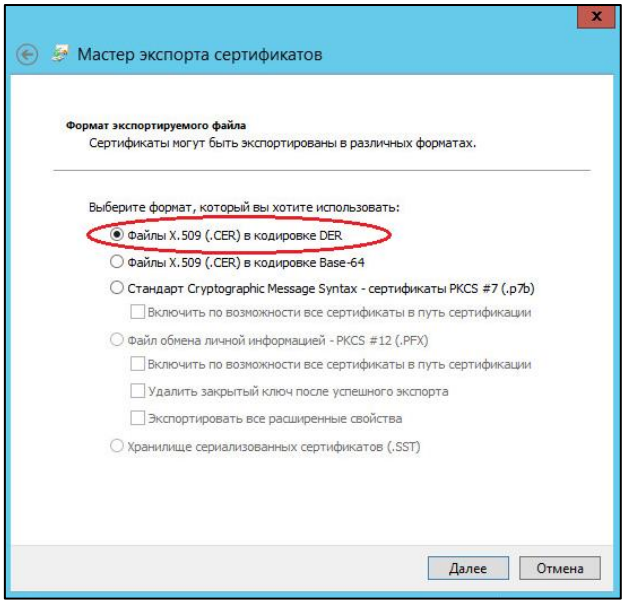

Рисунок 19. Выбор формата сохраняемого файла.

2.2.5. Откроется окно, нажать кнопку *«Обзор»* (1), выбрать директорию и указать имя для сохраняемого файла (2), нажать кнопку «Сохранить» (3) (см. Рисунок 20):

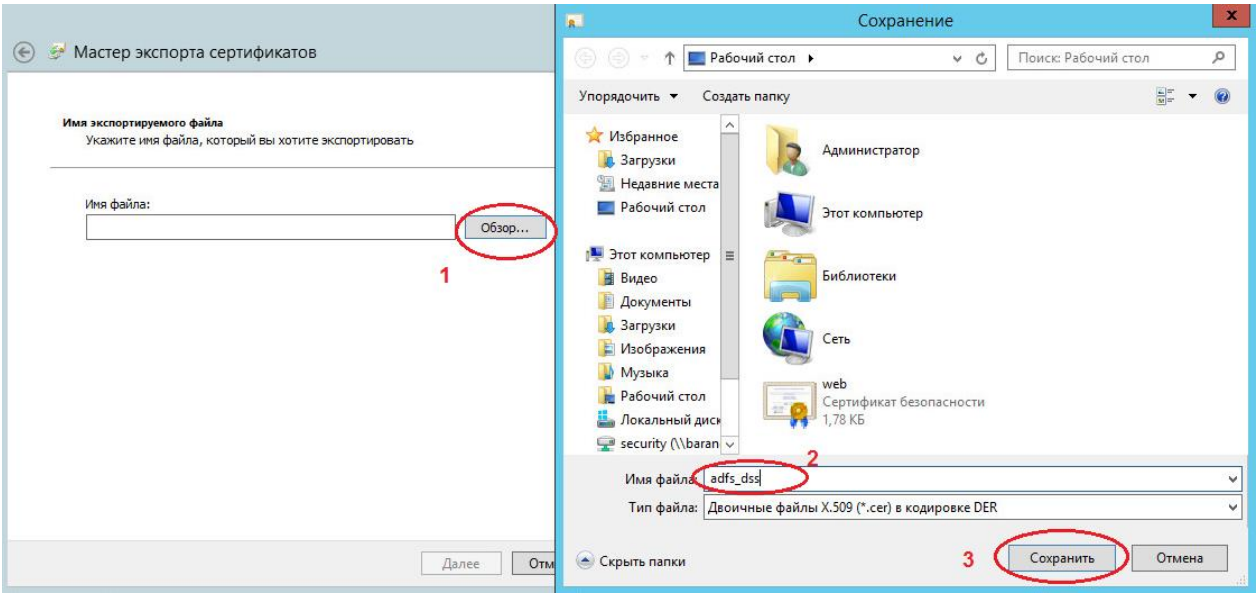

Рисунок 20. Сохранение файла с сертификатом.

2.2.6. Скопировать файл сертификата для подписи маркера на сервер КриптоПро Ключ

2.2.7. Для настройки отношения доверия между ЦИ КриптоПро Ключ и ADFS, на сервере КриптоПро Ключ необходимо выполнить следующие командлеты:

```
#Добавление СЦИ
Add-IdsIdentityProvider -IssuerName "https://adfs_hostname/adfs" -Name ADFS

#Добавление сертификата ADFS для подписи маркера
Add-IdsIdentityProviderSigningCertificate -IssuerName "https://adfs_hostname/adfs" -
Certificate /opt/to/sign_marker_certificate.cer

#Настройка конечных точек ADFS
Set-IdsIdentityProviderOidcEndpoint -IssuerName "https://adfs_hostname/adfs" -
AuthorizationEndpoint "https://adfs_hostname/adfs/oauth2/authorize" -ClientId
"идентификатор клиента" -ClientSecret "секрет клиента" -Scopes "openid allatclaims"
```

```
#Включение отображения СЦИ на веб-интерфейсе КриптоПро Ключ
Set-IdsIdentityProvider -IssuerName "https://adfs_hostname/adfs" -ShowInUi 1

#Активация СЦИ в КриптоПро Ключ
Enable-IdsIdentityProvider -IssuerName https://adfs_hostname/adfs

#Перезапуск ЦИ КриптоПро Ключ для применения изменений
Restart-IdsInstance
```

Где:

- IssuerName – IdTokenIssuer ADFS. Может быть получен выводом командлета на сервере ADFS:

```
(Get-AdfsProperties).IdTokenIssuer.AbsoluteUri
```

- Name – произвольное имя СЦИ, отображаемое в веб-интерфейсе КриптоПро Ключ;
- Certificate – путь к файлу сертификата для подписи маркера ADFS;
- AuthorizationEndpoint - адрес конечной точки ADFS;
- ClientId – значение идентификатора клиента, полученное в п. 2.1.4;
- ClientSecret – секрет клиента, полученный в п. 2.1.5.

2.2.8 (**опционально**). Настроить проверку целостности и неизменности маркеров доступа СЦИ в JSON Web Key Set ADFS (Jwks). Данная проверка исключает необходимость добавления сертификата ADFS для подписи маркера в настройках СЦИ КриптоПро Ключ.

Для включения проверки в Jwks, на сервере КриптоПро Ключ необходимо выполнить следующие командлеты:

```
#Включение проверки в Jwks
Set-IdsIdentityProviderOidcEndpoint -IssuerName "https://adfs_hostname/adfs" -JwksUri
"https://adfs_hostname/adfs/discovery/keys"

#Перезапуск ЦИ КриптоПро Ключ для применения изменений
Restart-IdsInstance
```

2.3. Создание оператора, управляющего пользователями домена

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

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

Порядок создания Оператора следующий:

2.3.1. Создать в AD группу пользователей с произвольным именем (далее в руководстве «*cprokey-operators*»).

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

2.3.3. На сервере КриптоПро Ключ зарегистрировать Оператора, выполнив следующие командлеты:

```
#Регистрация Оператора
Add-IdsIdentityOperator -Login ad-operator@domain.ru -Name "Имя оператора" -IssuerName
"https://adfs_hostname/adfs"

#Перезапуск ЦИ КриптоПро Ключ для применения изменений
Restart-IdsInstance
```

Где:

- Login - UPN Оператора;
- Name – имя Оператора в произвольном формате.

2.4. Настройка правил преобразования утверждений для доступа к КриптоПро Ключ Оператора, управляющего пользователями домена, и пользователей домена.

Для аутентификации в КриптоПро Ключ 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», перейти на вкладку *«Группы приложений»* и выбрать группу приложений с именем, указанным в п. 2.1.3 (см. Рисунок 21):

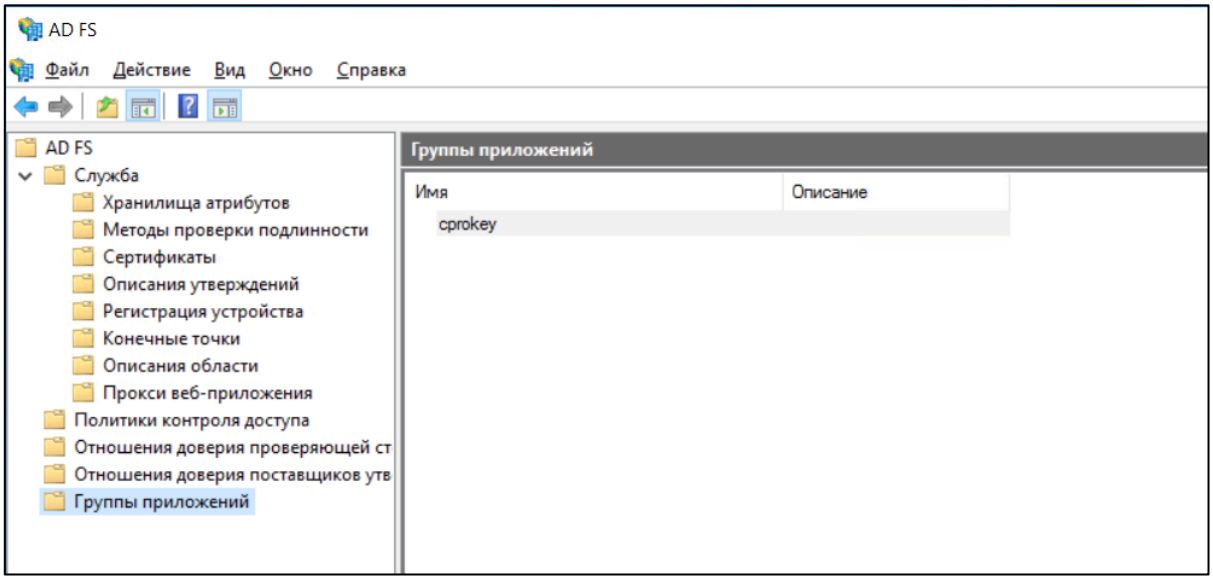

Рисунок 21. Изменение/добавление «правил утверждения»

2.4.2. Открыть двойным кликом в свойствах группы приложений приложение типа *«Веб-интерфейс API»*, созданное в п. 2.1.10 (см. Рисунок 22):

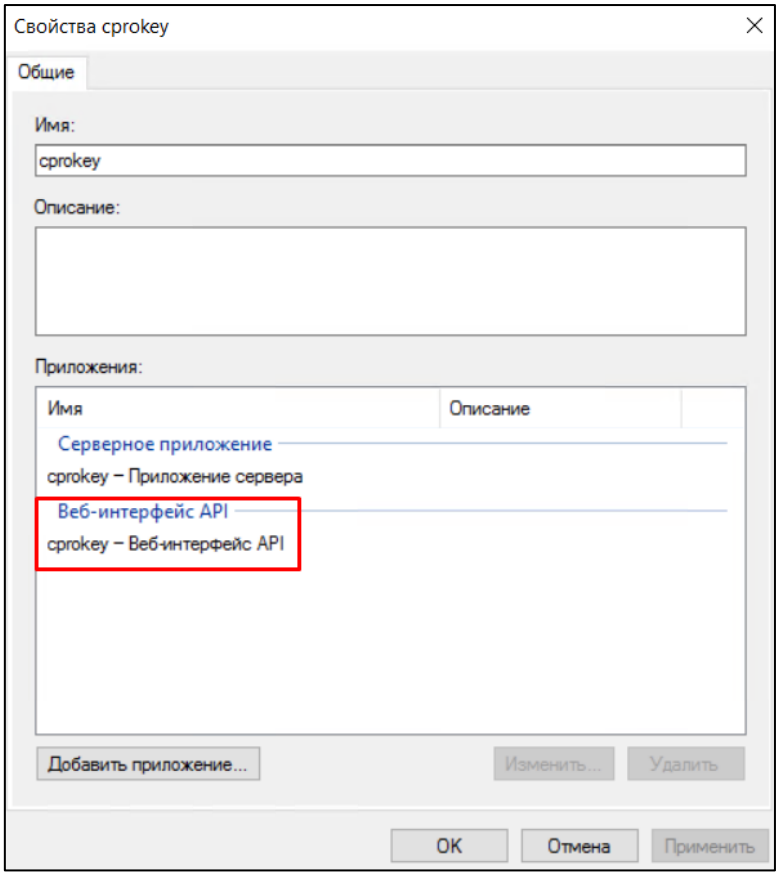

Рисунок 22. Свойства группы приложений

2.4.3. Перейти на вкладку *«Правила преобразования выдачи»* и нажать кнопку *«Добавить правило…»* (см. Рисунок 23):

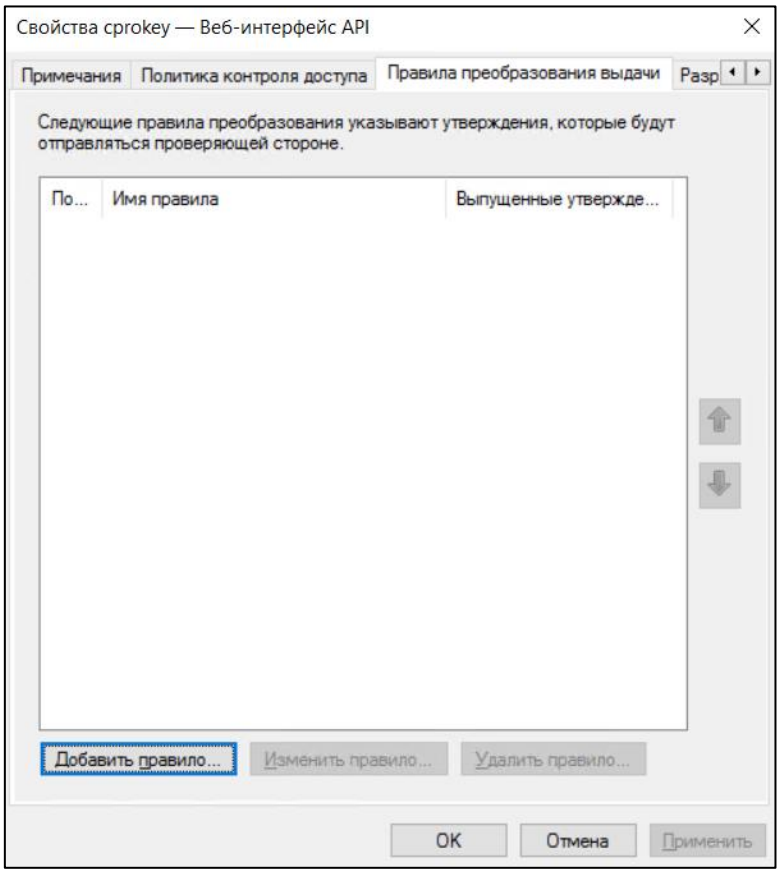

Рисунок 23. Добавление правил преобразований утверждений

2.4.4. Откроется окно мастера добавления правил преобразования утверждений. Необходимо выбрать из выпадающего списка шаблон *«Отправка атрибута LDAP как утверждений»* и нажать кнопку *«Далее»* (см. Рисунок 24):

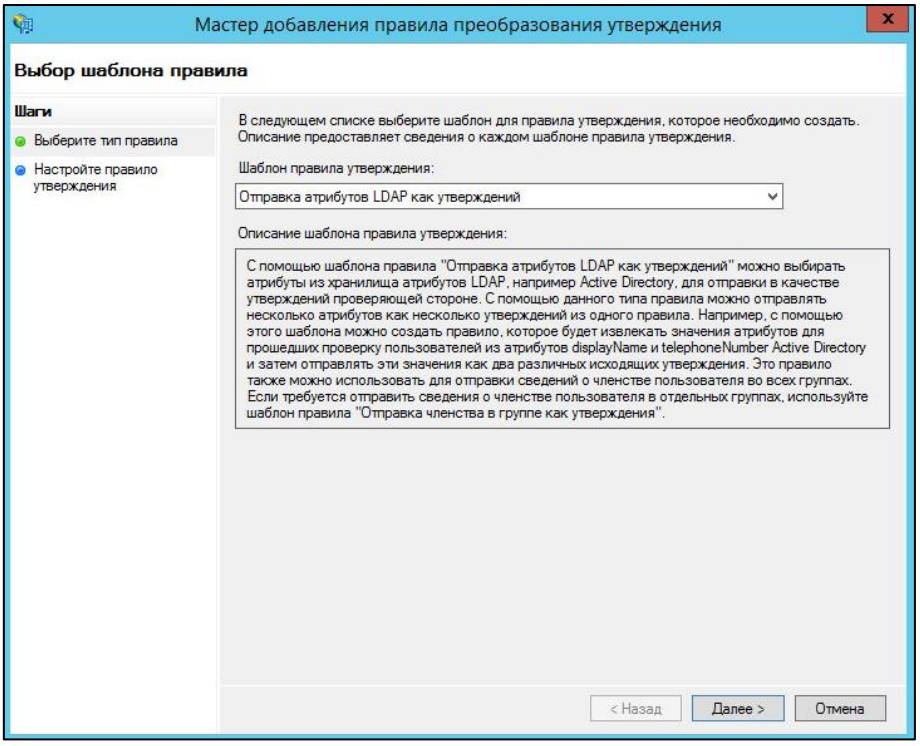

Рисунок 24. Выбор шаблона правила утверждения

2.4.5. В следующем окне необходимо заполнить поля так, как представлено на рисунке 25. Данное преобразование переложит имя учётной записи пользователя из атрибута UPN в утверждение name (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name). Далее необходимо нажать кнопку *«Готово»*.

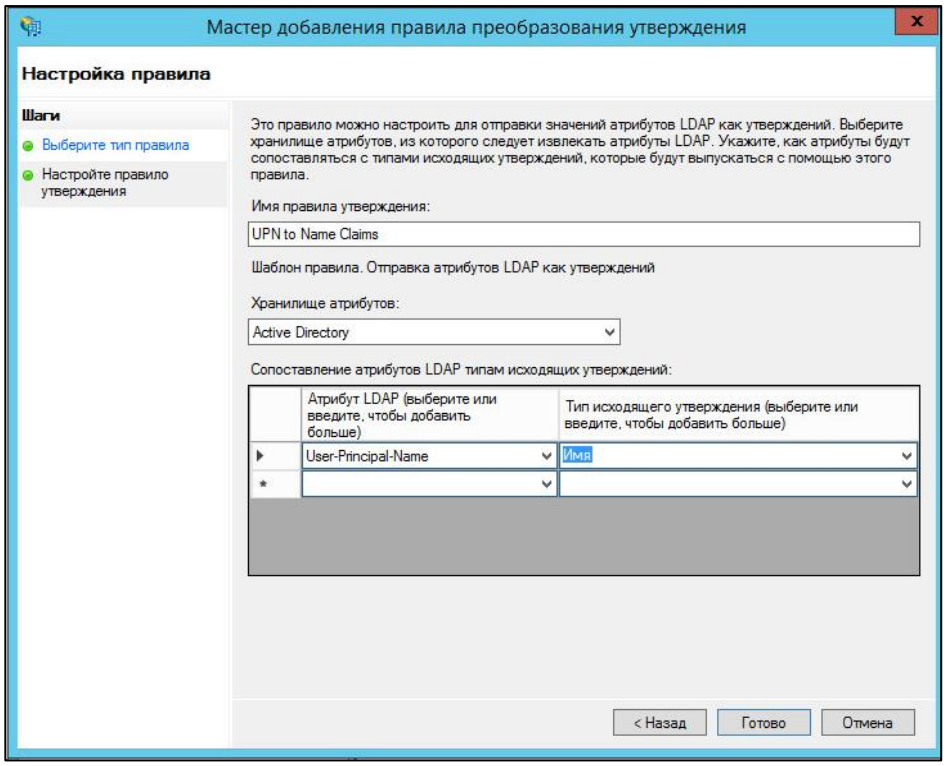

Рисунок 25. Создание правил преобразований утверждений.

2.4.6. 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 26):

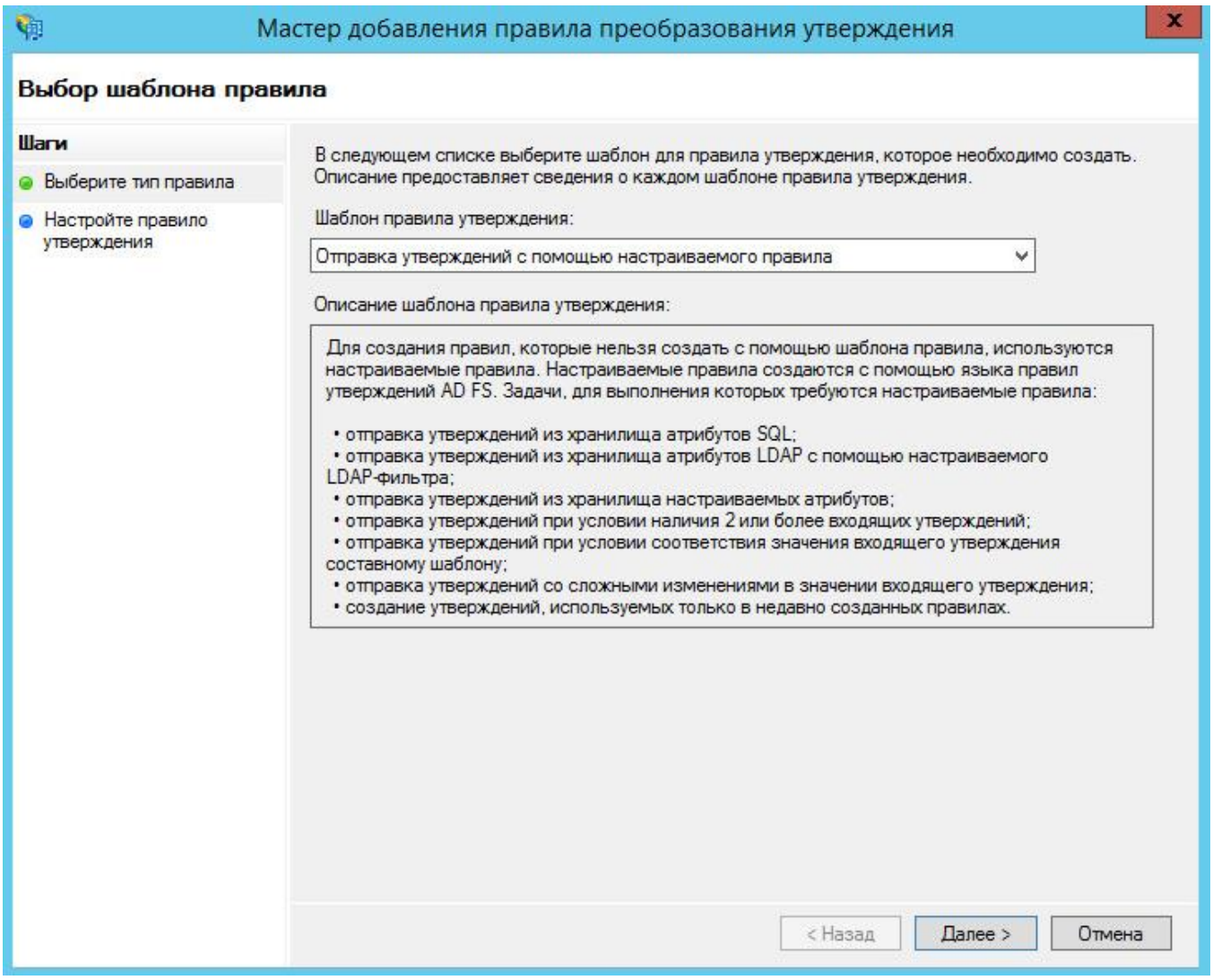

Рисунок 26. Выбор шаблона правила преобразования утверждения.

2.4.7. 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 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 правиле – это SID группы «*cprokey-operators*», который можно узнать, выполнив на AD командлет:

```
Get-ADGroup -Filter {Name -eq "cprokey-operators"}
```

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

2.4.8. 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»*.

2.4.9. Задать имя правила *«Operator-role»* 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»*.

2.4.10. 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»*.

2.4.11. Задать имя правила *«Users-role»* 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. «ПРОЗРАЧНАЯ» РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЕЙ AD В КРИПТОПРО КЛЮЧ

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

Для включения «прозрачной» регистрации пользователей требуется выполнить следующий командлет на сервере КриптоПро Ключ:

```
#Включение прозрачной регистрации
Set-IdsAccountPolicy -AccountCreationMode Transparent

#Перезапуск ЦИ КриптоПро Ключ для применения изменений
Restart-IdsInstance
```

Примечание: при осуществлении «прозрачной» регистрации пользователей методы вторичной аутентификации КриптоПро Ключ 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 применением API КриптоПро Ключ.

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

В КриптоПро Ключ могут быть переданы следующие утверждения:

Идентификатор утверждения	**Описание**	**Комментарии**
Обязательные		
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Логин	Уникальный идентификатор в пределах СЦИ
http://schemas.microsoft.com/ws/2008/06/identity/claims/role	Роль пользователя в КриптоПро Ключ	Users (пользователь) или Admins (оператор)
Опциональные		
http://dss.cryptopro.ru/identity/claims/group	Группа пользователей	Группа пользователей КриптоПро Ключ
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone	Номер мобильного телефона	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	Компонент имени субъекта
http://dss.cryptopro.ru/identity/claims/innle	ИНН ЮЛ	Компонент имени субъекта
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.