### Система электронной подписи

## на базе КриптоПро Ключ

Руководство администратора СЦИ (ADFS)

На 23 листах

## СОДЕРЖАНИЕ

Оглавление
1. ОБЩИЕ ПОЛОЖЕНИЯ
2. ИНТЕГРАЦИЯ СТОРОННЕГО ЦЕНТРА ИДЕНТИФИКАЦИИ ADFS WINDOWS SERVER 2016 ТР4 ПО ПРОТОКОЛУ OPENID CONNECT 1.0
2.1. Создание группы приложений
2.2. Настройка отношения доверия между ЦИ КриптоПро Ключ и ADFS12
2.3. Создание оператора, управляющего пользователями домена
2.4. Настройка правил преобразования утверждений для доступа к КриптоПро Ключ Оператора, управляющего пользователями домена, и пользователей домена16
3. «ПРОЗРАЧНАЯ» РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЕЙ АД В КРИПТОПРО КЛЮЧ21
ПРИЛОЖЕНИЕ А. УТВЕРЖДЕНИЯ ДОВЕРЕННОЙ СТОРОНЫ (MICROSOFT ACTIVE DIRECTORY), ПЕРЕДАВАЕМЫЕ В КРИПТОПРО КЛЮЧ22

#### 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 <u>Приложении A «Утверждения доверенной стороны (Microsoft Active Directory), передаваемые в КриптоПро Ключ»</u>.

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 ТР4 ПО ПРОТОКОЛУ OPENID CONNECT 1.0

Интеграция СЦИ ADFS из состава Windows Server 2016 ТР4 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;

- <u>Настройка правил преобразования утверждений для доступа к КриптоПро Ключ Оператора,</u>

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):

N AD FS		
훾 Файл Действие Вид Окно Справка	a	
🔶 🏟 💋 📰 📓 🖬		
AD FS	Группы приложений	
	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 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):

Имя:			
cprokey			
Описание:			2
Шаблон:			
Клиент-серверные приложения			
🛐 Собственное приложение, подключающееся к ве	e6-API		
🜇 Серверное приложение, подключающееся к веб	API		
🛐 Веб-браузер, подключающийся к веб-приложени	ю		
Автономные приложения			
📃 Собственное приложение			
Серверное приложение			
Веб-интерфейс АРІ			1
-			
Подробнее			
		3	
	< Назад	Далее >	Отмена

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: <u>https://hostname/sts/signin-oidc</u>

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):

И <u>м</u> я:	
сргокеу – Приложение сервера	
Идентификатор клиента:	
1 535053f5-b7cf-433a-8976-465e59967345	
Перенаправить URI:	3
2 https://hostname/sts/signin-oidc	Добавить
	<u>У</u> далить
Описание:	
4	0
< <u>Н</u> азад Д <u>а</u> лее >	Отмена

#### Рисунок 4. Настройка приложения сервера

2.1.5. В окне настройки учетных данных приложения требуется установить чекбокс «*Co3damb* 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):

частер добавления труп	приложении	~
Сводка		
Шаги	Просмотрите следующие параметры и нажмите кнопку "Далее" для создания приложения.	
<ul> <li>Приветствие</li> <li>Приложение сервера</li> <li>Настроить учетные данные приложения</li> <li>Сводка</li> </ul>	Группа приложений Имя: сргокеу Приложение сервера	
• Завершить	Идентификатор: 535053f5-b7cf-433a-8976-465e59967345 Перенаправить URI: https://hostname/sts/signin-oidc Использовать секрет клиента: True	
	< Назад Далее > Отмен	на

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):

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

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):

翰 <u>Ф</u> айл <u>Д</u> ействие <u>В</u> ид <u>О</u> кно <u>С</u> правка	
С С С С С С С С С С С С С С С С С С С	
<ul> <li>Служба</li> <li>Хранилища атрибутов</li> <li>Методы проверки подлинности</li> <li>Сертификаты</li> <li>Описания утверждений</li> <li>Регистрация устройства</li> <li>Конечные точки</li> <li>Описания области</li> <li>Прокси веб-приложения</li> <li>Политики контроля доступа</li> <li>Отношения доверия проверяющей ст</li> <li>Отношения доверия поставщиков утв</li> <li>Группы приложений</li> </ul>	

Рисунок 8. Список созданных групп приложений

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

Свойства сргокеу			×
Общие			
И <u>м</u> я:			
cprokey			
Описание:			
Приложения:			
Имя	Описа	ние	
серверное приложение сервера			
Веб-интерфейс АРІ			
cprokey – Веб-интерфейс API			
Добавить приложение		<u>И</u> зменить	<u>У</u> далить
	OK	Отмена	Применить

Рисунок 9. Свойства группы приложений

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

🧌 Добавить новое прилож	ение в сргокеу	×
Приветствие		
Шапи	Имя:	
Приветствие	cprokey	
<ul> <li>Настройка веб-интерфейса API</li> </ul>	Описание:	
<ul> <li>Применение политики управления доступом</li> </ul>		
<ul> <li>Настроить разрешения для приложений</li> </ul>	Шаблон:	
😑 Сводка	Автономные приложения	
Завершить	Собственное приложение Серверное приложение Вебинтерфейс АР! Подробнее	
	< Назад Далее > Отмена	

Рисунок 10. Добавление нового приложения в группу

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

輸 Добавить новое прилож	ение в сргокеу	×
Настройка веб-интере	рейса API	
Шаги	Имя:	
Приветствие	сргокеу – Веб-интерфейс API	
<ul> <li>Настройка веб-интерфейса API</li> </ul>	Идентификатор:	1 2
<ul> <li>Применение политики управления доступом</li> </ul>	535053f5-b7cf-433a-8976-465e59967345	Добавить
<ul> <li>Настроить разрешения для приложений</li> </ul>		Удалить
😑 Сводка		
😑 Завершить	Описание:	
	3	3
	< Назад Далее >	Отмена

Рисунок 11. Указание идентификатора клиента

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

12):

Шаги	Выберите политику управления доступом:	
<ul> <li>Приветствие</li> <li>Настройка вебчитерфейса АРІ</li> <li>Применение политики управления доступом</li> <li>Настроить разрешения для приложений</li> <li>Сводка</li> <li>Завершить</li> </ul>	Имя Разрешение для каждого и запрос МFA 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. Разрешение для определенной группы Разрешение доступа через интрасеть для каждого Разрешить всем и требовать MFA, разрешить авто	Описание Предоставьте доступ всем и запрашива Предоставление доступа пользователям Предоставление доступа каждому и зап Предоставление доступа каждому. Предоставление доступа каждому. Предоставьте доступ пользователям инт Предоставьте доступ пользователям инт
	Политика Paspeшeние для каждого Paspeшeние для каждого	тот раз. Ни один пользователь не получит

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):

훾 Добавить новое прилож	ение в cprokey	×
Настроить разрешени	ия для приложений	
Шаги Приветствие  Настройка вебчинтерфейса	Настроить разрешения, чтобы позволить клиентским приложениям п веб интерфейсу API. Приложения клиента (вызывающая сторона):	олучать доступ к этому
<ul> <li>АРІ</li> <li>Применение политики управления доступом</li> <li>Настроить разрешения для</li> </ul>	Имя Описание сргокеу – Приложение сервера	
<ul> <li>Сводка</li> <li>Завершить</li> </ul>	Разрешенные области:	Добавить Удалить
	Имя области Описание allatclaims Запрашивает утверждения маркера доступа в м. аza Область позволяет клиенту брокера запрашиват email Электронный запрос для зарегистрированного п logon_cett Область logon_cett позволяет приложению запра openid Запрос на использование протокола авторизаци profile Запрос профиля для зарегистрированного польз user_imperso Запрос о предоставлении доступа в качестве за	аркер Ъ осн Юльз щива иор зоват регис
	< Назад	Далее > Отмена

Рисунок 13. Разрешенные области приложения

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

🏟 Добавить новое приложе	ение в сргокеу	×
Сводка		
Шаги Приветствие Настройка веб-интерфейса АРІ Применение политики управления доступом Настроить разрешения для приложений Сводка Завершить	Просмотрите следующие параметры и нажмите кнопку "Далее" для создания приложения. Группа приложений Имя: cprokey Веб-интерфейс АРI Имя: cprokey – Веб-интерфейс АРI Идентификаторы: 53505375-b7cf-433a-8976-465e59967345 Политика контроля доступа: Разрешение для каждого. Разрешения для приложения: сprokey – Приложение сервера - openid allatclaims	
	< Назад Далее > Отме	на

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

輸 Добавить новое прилож	ение в сргокеу Х
Готово	
Шаги	Группа приложений успешно создана.
Приветствие	
<ul> <li>Настройка веб-интерфейса API</li> </ul>	
<ul> <li>Применение политики управления доступом</li> </ul>	
<ul> <li>Настроить разрешения для приложений</li> </ul>	
😑 Сводка	
🤪 Завершить	
	Закрыть

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):

<b>\$</b>		AD FS		_ 🗆 X
🏟 Файл Действие Вид Окно Справ	Ka			_ # ×
AD FS	Сертификаты			Действия
Конечные точки	Тема Издатель Взаимодействие спокб	Дата вступле Дата оконча	Сост Первич	Сертификаты 🔺
Сертификаты 2	CN=dss-2012.test-dss.local CN=dss-2012.t	est-dss.local 22.09.2015 22.09.2016		Добавить сертификат для
<ul> <li>Описания утверждении</li> <li>Отношения доверия</li> </ul>	Для расшифровки маркера			Добавить сертификат для
Политики проверки подлинности	Second Se	ryption - ds 30.08.2015 29.08.2016	Первич	Вил
	Для подписи маркера CN=ADFS Signing - dss-20 CN=ADFS Sign	ning - dss-2 30.08.2015 29.08.2016	Первич.	Новое окно отсюда
			Y	о Обновить
	8	Сертификат		🛿 Справка
	5 Общие Состав	Путь сертификации		CN=ADFS Signing - dss-2 🔺
				Просмотр сертификата
	Свед	цения о сертификате		Назначить первичным
	Этот серти • Все по	фикат предназначается для: литики выдачи		👔 Справка
	Bce no	литики применения		
	Кому выла	ADES Signing - dss-2012 test-dss local		
	Kony Balde	M. ADI 5 Signing - 033-2012. (Cat-033.1008)		
	Кем выдан	ADFS Signing - dss-2012.test-dss.local		
	Beier	PUT 0 20 00 2015 pp 20 00 2016		
	Денст	BUTENER C 30.08.2013 NO 25.08.2010		
	Ус	ановить сертификат Заявление поста	вщика	
			Акт	ивация Windows
			Чтоб	ы активировать Windows,
			ок упра	вления "Система".

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).

Сертификат	
Общие Состав Путь сертификации	🝍 🔘 🥏 Мастер экспорта сертификатов
Показать: <bce> ✓      Поле    Эначение      Версия    V3      Серийный номер    6f 92 89 24 6c 9e 00 8f 40 fc      Алгорити подписи    sha256RSA      Хзш-алгорити подписи    sha256      Издатель    ADFS Signing - dss-2012.test      Действителен с    30 августа 2015 г. 14:57:07      Субъект    ADFS Signing - dss-2012.test      Субъект    ADFS Signing - dss-2012.test</bce>	Мастер экспорта сертификатов Этот мастер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов из хранилища сертификатов на локальный диск. Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установления защищенных сетевых подключений. Хранилище сертификатов — это область системы, предназначенная для хранения сертификатов. Для продолжения нажните кнопку "Далее".
OK	Далее Отмена

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
#Hacтройка 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 <u>п. 2.1.5</u>.

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 <u>п. 2.1.3</u> (см. Рисунок 21):

翰 AD FS							
🇌 <u>Ф</u> айл <u>Д</u> ействие <u>В</u> ид <u>О</u> кно <u>С</u> правк	a						
📔 AD FS	Группы приложений						
🗸 🚞 Служба	14.00	0	1				
🧾 Хранилища атрибутов	RWIN	Описание					
📔 Методы проверки подлинности	cprokey						
🧮 Сертификаты							
🧮 Описания утверждений							
Регистрация устройства							
🧮 Конечные точки							
🧮 Описания области							
📔 Прокси веб-приложения							
📔 Политики контроля доступа							
📔 Отношения доверия проверяющей ст							
🧮 Отношения доверия поставщиков утв							
📔 Группы приложений							

Рисунок 21. Изменение/добавление «правил утверждения»

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

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

Рисунок 22. Свойства группы приложений

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

Тримечан	ия Политика	а контроля доступа	Правила прео	бразования выдачи	Pasp 4
Следую отправл	щие правила г іяться провер:	преобразования ука яющей стороне.	зывают утверж	дения, которые буду	т
По	Имя правила	1	Выпу	ценные утвержде	
Доба	вить правило	. Изменить пра	вило ⊻д	алить правило	

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):

Выбор шаблона правила:      Шаги     выберите тип правила     Настройте правила     Настройте правила     Настройте правила     Тописание предоставляет сведения о каждом шаблоне правила утверждения.      Шаблон правила утверждения:     Шаблон правила утверждения:     Отлисание шаблона правила утверждения     Описание шаблона правила утверждения     Описание шаблона правила утверждения     Потравка атрибутов LDAP как утверждения     Описание шаблона правила утверждения     Описание шаблона правила утверждения     описание предоставляет сведения о каждом шаблоне правила утверждения     шаблон правила утверждения:     Отлисание шаблона правила "Отправка атрибутов LDAP как утверждений" можно выбирать     аутибуты из хранилица атрибутов LDAP наку утверждений можно отправила.     Тописание шаблона правила "Отправка атрибутов LDAP как утверждений" можно выбирать     аутибуты из хранилица атрибутов создать правило, которое будет извлекать значения в как изверждения     со помощью использовать правило, которое будет извлекать значения в создащих троерку пользователя в отдельных группах, используйте     шаблон правила "Отправка членства в группе как утверждения".	<b>\$</b>	Мастер добавления правила преобразования утверждения	×
<ul> <li>Шапи</li> <li>В следующем списке выберите шаблон для правила утверждения, которое необходимо создать. Описание предоставляет сведения о каждом шаблоне правила утверждения.</li> <li>Настройте правило утверждения</li> <li>Настройте правило утверждения</li> <li>Спомощью цаблон правила утверждения:</li> <li>Описание шаблона правила утверждения:</li> <li>Спомощью шаблона правила "Оправка а трибутов LDAP как утверждений" можно выбирать атрибуты из хранилища атрибутов LDAP, например Active Directory, для отправки в качестве утверждений но оконо создать правило, которое будет извлекать значения атрибутов для прошедших проверку пользовать рая потравих а драбутов для чое будет извлекать значения атрибутов в для прошедиих пооверку пользовать для отправих и сходящих утверждения. Это правило также можно использовать для отправих сведений о иленстве пользователя в осек группах. Если требуется отправить сведения о членстве пользователя в осек группах. Если требуется отправить сведения о членстве пользователя в осек группах. Спо правила "Отправка членства в группе как утверждения".</li> </ul>	Выбор шаблона г	равила	
Таска подкло исполно у полно и правила седения о членстве пользователи во деектруппах. Если требуется отправить сведения о членстве пользователя в отдельных группах, используйте шаблон правила "Отправка членства в группе как утверждения".	Выбор шаблона пра Шаги	равила 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 утверждения. С помощью шаблона правила утверждения. С помощью шаблона правила "Отправка атрибутов LDAP как утверждений" можно выбирать атрибутов из утверждений, по создать. С помощью шаблона правила утверждения. С помощью шаблона правила "Отправка атрибутов LDAP как утверждений" можно выбирать атрибутов из утверждения. С помощью шаблона правила "Отправка атрибутов LDAP как утверждений" можно выбирать атрибутов из утверждений, по создать правила из одного плавила. Например, с помощью зого и шаблона можно создать правило, которое будет извлекать значения ятибутов для проделяль эти уначения как два различных исходяцих утверждения.	
		также можно использовать для отправки сведений о членстве пользователя во всех группах. Если требуется отправить сведения о членстве пользователя в отдельных группах, используйте шаблон правила "Отправка членства в группе как утверждения".	

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

пастроика правила					
<ul> <li>Выберите тип правила</li> <li>Настройте правило утверждения</li> </ul>	Это п храни сопос прави Имя п	равило можно настроить для отправки илище атрибутов, из которого следует и ставляться с типами исходящих утверж ила. правила утверждения:	зна 13вл сден	ачений атрибутов LDAP лекать атрибуты LDAP. ний, которые будут выпу	как утверждений. Выберите Укажите, как атрибуты будут скаться с помощью этого
	UPN	to Name Claims			
	Шабл Храні	юн правила. Отправка атрибутов LDAP илище атрибутов:	как	с утверждений	
	Active Directory V				
	Сопоставление атрибутов LDAP типам исходящих утверждений:				
		Атрибут LDAP (выберите или введите, чтобы добавить больше)		Тип исходящего утверя введите, чтобы добавит	сдения (выберите или ъ больше)
	•	User-Principal-Name	-	Имя	~
			~		Ŷ

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):

翰 N	астер добавления правила преобразования утверждения
Выбор шаблона пра	вила
<ul> <li>Выберите тип правила</li> <li>Настройте правило утверждения</li> </ul>	В следующем списке выберите шаблон для правила утверждения, которое необходимо создать. Описание предоставляет сведения о каждом шаблоне правила утверждения. Шаблон правила утверждения: Отравка утверждений с помощью настраиваемого правила Списание 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 настраиваемого LDAP-филь тра: • отправка утверждений из хранилища атрибутов SQL: • отправка утверждений из хранилища атрибутов SQL: • отправка утверждений из хранилища атрибутов SQL: • отправка утверждений из хранилища настраиваемых атрибутов; • отправка утверждений из исловии наличия 2 или более входящису утверждений; • отправка утверждений при условии наличия 2 или более входящисо утверждения; • отправка утверждений при условии изменениями в значения входящего утверждения; • отправка утверждений, используемых только в недавно созданных правилах.
	< Назад Далее > Отмена

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 <u>http://dss.cryptopro.ru/identity/claims/marker</u> 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:

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 АРІ 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/identit y/claims/name	Логин	Уникальный идентификатор в пределах СЦИ
http://schemas.microsoft.com/ws/2008/06/iden tity/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/identit y/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/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.