

**Средство защиты информации  
«SecurePackRus»**

Версия 3.0

**Руководство администратора безопасности  
Аутентификация**

ЖТЯИ.00106-01 90 03

Листов 13



Компания «КРИПТО-ПРО»

2019

Компания «КРИПТО-ПРО», 2019. Все права защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании «КРИПТО-ПРО» этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию и передаче третьим лицам с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны компании «КРИПТО-ПРО».

ООО «КРИПТО-ПРО»

Адрес 127018, г. Москва, ул. Сущевский Вал, дом 18

Телефон +7 (495) 995-4820

e-mail [info@cryptopro.ru](mailto:info@cryptopro.ru)

Web [www.cryptopro.ru](http://www.cryptopro.ru)

## Оглавление

Список сокращений .....	4
1. Введение .....	5
2. Поддерживаемые ключевые носители .....	5
3. Порядок настройки системы .....	6
3.1. Настройка домена предприятия .....	6
3.1.1. Доверие к УЦ .....	6
3.1.2. Разрешение аутентификации по сертификатам УЦ .....	6
3.1.3. Обеспечение доступности сертификата УЦ .....	7
3.2. Настройка контроллеров домена .....	8
3.2.1. Выпуск сертификата КД, используя КриптоПро УЦ .....	8
3.3. Настройка пользовательских рабочих мест .....	11
3.3.1. Выпуск пользовательского сертификата, используя КриптоПро УЦ .....	11
3.3.2. Создание сертификата пользователя с помощью HTML-формы. ....	11
3.3.3. Создание сертификата пользователя на АРМ Администратора КриптоПро УЦ. ....	12
Список литературы .....	13

## Список сокращений

<b>АИС</b>	Автоматизированная информационная система
<b>АРМ</b>	Автоматизированное рабочее место
<b>АС</b>	Автоматизированная система
<b>ЗПС</b>	Замкнутая программная среда
<b>ИС</b>	Информационная система
<b>НСД</b>	Несанкционированный доступ
<b>ОС</b>	Операционная система
<b>ПАК</b>	Программно-аппаратный комплекс
<b>ПКЗИ</b>	Подсистема криптографической защиты информации
<b>ПО</b>	Программное обеспечение
<b>ППО</b>	Прикладное программное обеспечение
<b>СЗИ</b>	Средство или система защиты информации
<b>СКЗИ</b>	Средство криптографической защиты информации
<b>СХКИ</b>	Средство хранения конфиденциальной информации

# 1. Введение

Данное руководство предназначено для администраторов средства защиты информации «Secure Pack Rus» версия 3.0 (сокращенные названия изделия – Secure Pack Rus 3.0 или SPR 3.0). В руководстве содержатся сведения, необходимые администраторам для настройки и управления механизмами аутентификации пользователей.

Настоящий документ содержит описание процесса настройки средства сетевой аутентификации в доменной инфраструктуре под управлением Microsoft Window Server 2003 R2/Server 2008 R2/ Server 2012/ Server 2012 R2/ Server 2016 и рабочими станциями под управлением ОС Microsoft Windows XP/Windows 7/8/8.1/10.

Для функционирования КриптоПро Winlogon требуется, чтобы были правильно настроены рабочая станция для входа, домен и контроллеры домена. Домен должен доверять Удостоверяющему Центру (УЦ) аутентифицировать пользователей с помощью сертификатов данного УЦ. Рабочая станция для входа и контроллеры домена должны обладать правильно настроенными сертификатами.

Как и в любой реализации ИОК, все участники должны доверять корневому УЦ, который подписал сертификат выпускающего УЦ. Контроллеры домена и рабочие станции для входа должны доверять корневому УЦ.

Установка ПО и необходимые настройки для выполнения указанных требований описаны в последующих разделах.

## 2. Поддерживаемые ключевые носители

КриптоПро Winlogon Клиент поддерживает следующие типы смарт-карт:

- российские интеллектуальные карты (РИК1, Оскар) с использованием считывателей смарт-карт, поддерживающий протокол PS/SC (GemPlus GCR-410, Towitoko, Oberthur OCR126 и др.);
- электронный ключ с интерфейсом USB.

КриптоПро Winlogon KDC для хранения секретного ключа KDC может использовать любой ключевой носитель, поддерживаемый КриптоПро CSP.

## 3. Порядок настройки системы

### 3.1. Настройка домена предприятия

#### 3.1.1. Доверие к УЦ

Контроллеры домена и рабочие станции должны доверять УЦ для обеспечения возможности входа пользователей по смарт-картам.

Если рассматриваемый УЦ, выпускающий сертификаты для входа со смарт-картой, является корневым, то его сертификат должен быть установлен в хранилища *Доверенные корневые центры сертификации* указанных компьютеров. Если же данный УЦ является подчинённым, то в это хранилище необходимо установить сертификат корневого УЦ, на котором заканчивается цепочка сертификатов выпускающего УЦ.

Описанную процедуру рекомендуется выполнить с использованием возможностей групповых политик домена Windows. Для этого в оснастке Групповые политики на контроллере домена в узле *Конфигурация компьютера → Конфигурация Windows → Параметры безопасности → Политики открытого ключа → Доверенные корневые центры сертификации* выполните импорт требуемого сертификата.



Следует отметить, что файл импортируемого сертификата не должен содержать в себе цепочек сертификатов и СОС.

После применения настроенной таким образом групповой политики на всех компьютерах домена данный сертификат появится в хранилище *Доверенные корневые центры сертификации*.

#### 3.1.2. Разрешение аутентификации по сертификатам УЦ

Чтобы сертификаты УЦ могли использоваться для аутентификации в домене и входа со смарт-картой, домен должен явно доверять этому УЦ. Для этого в Active Directory в хранилище *NTAuth* должен быть прописан сертификат этого УЦ.

Чтобы поместить сертификат УЦ в это хранилище, сохраните его в файл и выполните следующую команду:

```
certutil -dspublish -f<filename>NTAuthCA
```

Здесь <filename> – имя файла с сертификатом.

Программа *certutil* устанавливается вместе со службами сертификации Microsoft на ОС Windows 2000, а также присутствует в любой поставке ОС Windows Server 2003 и более поздних. Для успешной публикации необходимо, чтобы учётная запись, под которой выполняется команда, входила в группу администраторов домена.

Более подробно процедура помещения корневого сертификата УЦ в хранилище *NTAuth* см. (1).

### **3.1.3. Обеспечение доступности сертификата УЦ**

Если рассматриваемый УЦ, выпускающий сертификаты для входа со смарт-картой, является корневым, то его сертификат должен быть установлен в хранилища *Доверенные корневые центры сертификации* контроллеров домена и рабочих станций для входа. Если же данный УЦ является подчинённым, то возникает необходимость поиска его сертификата для подтверждения цепочки.

Для этого рекомендуется включение особого расширения *AIA* (*Доступ к информации о центре сертификации*) в сертификаты пользователей, выпущенные этим центром. Расширение *AIA* включает в себя путь к файлу сертификата данного центра сертификации, который должен быть доступен для всех пользователей системы (быть опубликованным по доступному для пользователей адресу в сети предприятия по протоколам LDAP, HTTP).

## 3.2. Настройка контроллеров домена

### 3.2.1. Выпуск сертификата КД, используя КриптоПро УЦ

Для всех контроллеров домена необходимо выпустить сертификаты открытых ключей, которые будут использоваться контроллерами для аутентификации и защиты соединения.

Для выпуска сертификата и установки сертификата контроллера домена необходимо выполнить следующую последовательность действий:

1. Узнайте DNS-имя и идентификатор GUID контроллера домена. Для этого на контроллере домена в панели управления компьютера запустите панель *КриптоПро CSP* и на вкладке *Winlogon* нажмите кнопку *Экспортировать*. Нужная информация будет помещена в буфер обмена. Сохраните эти данные, например, в текстовый файл и перейдите на компьютер АРМ Администратора.
2. В *АРМ Администратора КриптоПро УЦ* создайте пользователя, который будет соответствовать контроллеру домена. Задайте дополнительные параметры DNS-имя и GUID для этого пользователя (узел *Свойства* в контекстном меню).
3. В *АРМ Администратора КриптоПро УЦ* создайте HTML-форму для автономной работы пользователя, соответствующего контроллеру домена (узел *Все задачи* → *Создать* → *HTML-форму для автономной работы* в контекстном меню). В качестве типа запроса на сертификат укажите *Сертификат контроллера домена(winlogon)*. Обратите внимание, что в форме должен использоваться КриптоПро CSP.
4. Перенесите созданную HTML-форму на компьютер контроллера домена и запустите её. Для корректной работы формы необходимо разрешить отображение активного содержимого в настройках Internet Explorer. Создайте в форме запрос на сертификат (см. Рисунок ). Галочку *Подписать запрос* ставить не нужно.



Обратите внимание, что при создании запроса на сертификат с помощью HTML-формы она обязательно должна быть запущена из локального каталога компьютера, на котором планируется её заполнение. Данное требование обусловлено ограничениями безопасности Internet Explorer.



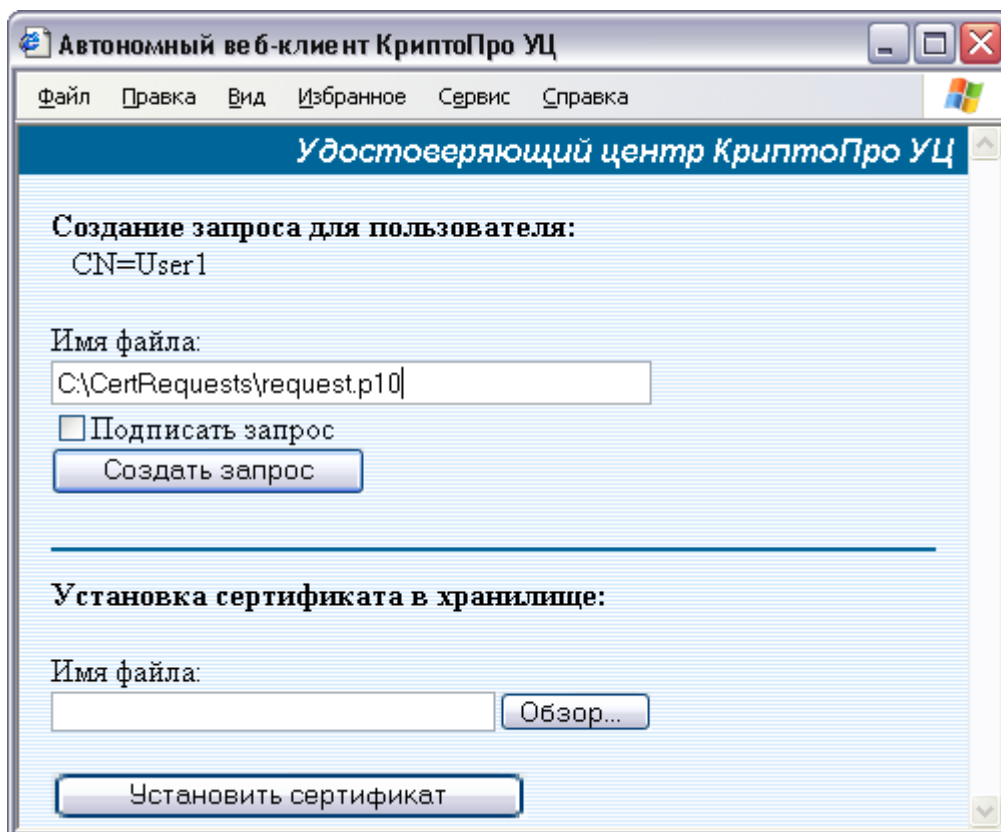


Рисунок 1. HTML-форма для автономной работы пользователя.

5. В приложении панели управления *КриптоПро CSP* на вкладке *Winlogon* необходимо отметить галочку *Использовать алгоритмы КриптоПро CSP на KDC*.
6. Перенесите запрос на сертификат на АРМ Администратора и выпустите для соответствующего пользователя сертификат по запросу.
7. Перенесите сертификат на компьютер контроллера домена и установите его с помощью той же HTML-формы.
8. Удалите другие сертификаты контроллера домена, если они есть, из хранилища *Личные* локального компьютера и перезагрузите его.

Описанные действия повторите для всех контроллеров вашего домена.



Если в вашем домене есть или планируется развернуть центр сертификации Microsoft в режиме ЦС предприятия (Enterprise CA), то необходимо предотвратить автоматический выпуск сертификатов контроллеров доменов, которые могут помешать работе КриптоПро Winlogon. Для этого в оснастке *Центр сертификации* удалите шаблоны сертификатов *Контроллер домена* и *Проверка подлинности контроллера домена* из списка шаблонов (см. Рисунок ) с целью запрета автоматической выдачи сертификатов по данным шаблонам.

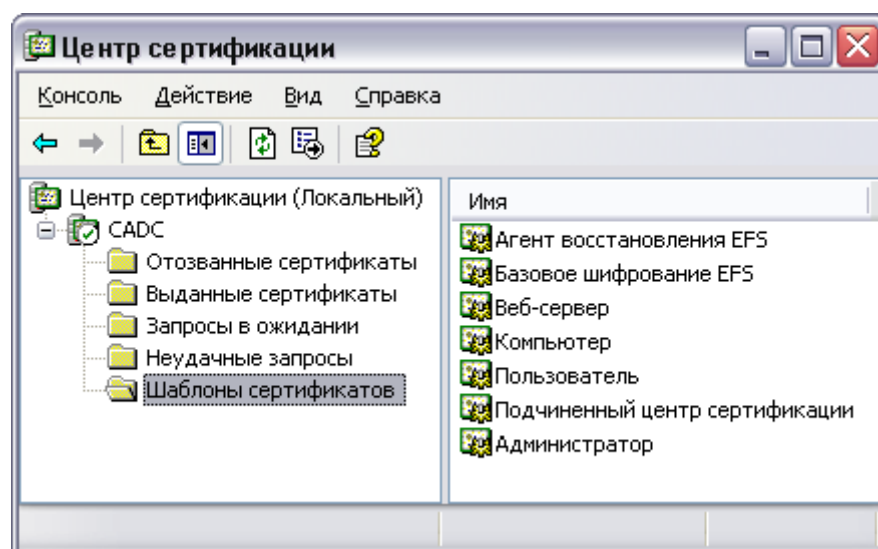


Рисунок 2. Список допустимых шаблонов сертификатов Центра сертификации.

### 3.3. Настройка пользовательских рабочих мест

#### 3.3.1. Выпуск пользовательского сертификата, используя КриптоПро УЦ

Каждый пользователь должен обладать смарт-картой (или USB токеном), содержащей закрытый ключ и сертификат для аутентификации в домене.

Требования к сертификату входа со смарт-картой и рабочей станции:

- Сертификат пользователя должен содержать правильное имя учётной записи (User Principal Name) в поле Subject Alternative Name сертификата.
- На рабочей станции для входа со смарт-картой должны быть установлены драйверы для устройства чтения смарт-карт, это устройство и используемый носитель должны быть установлены в панели управления КриптоПро CSP как считыватель и носитель, в свойствах носителя должна быть установлена галочка «Использовать для входа в операционную систему», если таковая имеется.

Выпуск таких сертификатов осуществляется на *АРМ Администратора КриптоПро УЦ*. Существует два различных варианта выпуска сертификата пользователя для входа со смарт-картой:

- Создание сертификата с помощью HTML-формы, аналогично созданию сертификата контроллера домена.
- Создание сертификата непосредственно на АРМ Администратора КриптоПро УЦ.



Обратите внимание, что при создании запроса на сертификат с помощью HTML-формы она обязательно должна быть запущена из локального каталога компьютера, на котором планируется её заполнение. Данное требование обусловлено ограничениями безопасности Internet Explorer.

#### 3.3.2. Создание сертификата пользователя с помощью HTML-формы.

1. В *АРМ Администратора КриптоПро УЦ* создайте нового пользователя. При создании пользователя укажите дополнительный параметр UPN (UserPrincipalName). Этот параметр также можно задать или изменить у существующего пользователя (узел *Свойства* в контекстном меню). UPN пользователя может отличаться от имени учётной записи, используемой для входа в компьютер, но чаще всего они совпадают. UPN имеет формат user1@domain.com.
2. В АРМ Администратора КриптоПро УЦ создайте HTML-форму для автономной работы пользователя (узел *Все задачи* → *Создать* → *HTML-форму для автономной работы* в контекстном меню). В качестве типа запроса на сертификат укажите *Сертификат входа со смарт-картой*. Обратите внимание, что в форме должен использоваться КриптоПро CSP.
3. Перенесите созданную HTML-форму на рабочую станцию для входа со смарт-картой и запустите её. Для корректной работы формы необходимо разрешить отображение активного содержимого в настройках Internet Explorer. Создайте в форме запрос на сертификат.

4. Перенесите запрос на сертификат на АРМ Администратора и выпустите для соответствующего пользователя сертификат по запросу.
5. Перенесите сертификат на рабочую станцию для входа со смарт-картой и установите его с помощью HTML-формы.

### **3.3.3.Создание сертификата пользователя на АРМ Администратора КriptoПро УЦ.**

На рабочем месте привилегированного пользователя, выпускающего сертификаты для пользователей с использованием АРМ Администратора, должны быть установлены драйверы для устройства чтения смарт-карт. Это устройство и используемый носитель должны быть установлены в панели управления КriptoПро CSP как считыватель и носитель, в свойствах носителя должна быть установлена галочка *Использовать для входа в операционную систему*, если таковая имеется.

Для выпуска сертификата пользователя с использованием АРМ Администратора необходимо выполнить следующую последовательность действий:

1. В *АРМ Администратора КriptoПро УЦ* создайте нового пользователя. При создании пользователя укажите дополнительный параметр UPN (UserPrincipalName). Этот параметр также можно задать или изменить у существующего пользователя (узел *Свойства* в контекстном меню).UPNпользователя может отличаться от имени учётной записи, используемой для входа в компьютер, но чаще всего они совпадают. UPNимеет формат user1@domain.com.
2. Выпустите сертификат для данного пользователя, где в качестве типа запроса на сертификат укажите *Сертификат входа со смарт-картой*. Ключевую пару сгенерируйте на смарт-карте и установите сертификат в контейнер.

После этого смарт-карта может использоваться для аутентификации в домене Windows.

## Список литературы

1. Компания "**Microsoft**". How to import third-party certification authority (CA) certificates into the Enterprise NTAAuth store. *Microsoft Support*. [В Интернете] <https://support.microsoft.com/en-us/help/295663/how-to-import-third-party-certification-authority-ca-certificates-into>.

2. Компания "**КРИПТО-ПРО**". Формуляр. *Средство защиты информации «Secure Pack Rus» версия 3.0*. ЖТЯИ.00106-01 30 01.