I.00.000.133-004

## Электронная подпись Настройка системы Инструкция администратора

2017

## Электронная подпись. Настройка системы

Инструкция администратора Версия документа I.00.000.133-004



В зависимости от версии работа Системы может отличаться от приведенного описания. За более актуальной информацией обратитесь к справочной системе

© 2009-2017 Все права защищены.

## Содержание

1 I	Настройка Системы для работы с ЭП	4
1.1.	Переустановка сертификатов пользователя	4
1.2.	Установка ПО для использования электронной подписи для работы в	
опер	рационной системе Windows	.11
1.3.	Установка ПО для использования электронной подписи для работы в	
опер	рационной системе Linux	.12
1.4.	Загрузка сертификатов пользователей	.13

## 1 Настройка Системы для работы с ЭП

Внимание! Последние версии браузеров прекратили поддержку Java, в связи с этим необходимо переустановить компоненты для использования электронной подписи.

Для использования электронной подписи:

- 1. Установите последнюю версию FireFox (не ESR, не CryptoFox, не portable-версию).
- 2. Загрузите с сайта КриптоПро и установите последнюю версию плагина <u>https://www.cryptopro.ru/products/cades/plugin</u> (версия 2.0 для пользователей).
- 3. Установите расширение для браузера FireFox с сайта КриптоПро https://www.cryptopro.ru/sites/default/files/products/cades/extensions/firefox\_cry ptopro\_extension\_latest.xpi.
- Для каждой учетной записи пользователя Системы, который использует электронную подпись, установите сертификат: Сервис – Пользователи - в свойствах пользователя «Сертификаты» – кнопка «Добавить»;
- 5. Перезапустите Firefox, заново авторизуйтесь в Системе под учетной записью пользователя.

Важно! Если ранее были установлены сертификаты в хранилище на ПК, необходимо их сохранить, и повторно добавить для учетной записи пользователя. Подробное описание см. п. 1.1.

#### 1.1. Переустановка сертификатов пользователя

Если ранее на системе были установлены сертификаты в хранилище ОС,

необходимо их экспортировать и установить для учетной записи пользователя Системы.

Для этого:

- 1. Нажмите кнопку Пуск.
- 2. Введите в строке certmgr.msc и нажмите кнопку Enter.

Отобразится форма

работа с сертификатами.



🚡 certmgr -	[Сертификаты — текущий пользователь] – 🗖 🗙
<ul> <li>Файл Действие Вид Справка</li> <li> Файл Действие Вид Справка</li> <li> Файл Действие Вид Справка</li> <li> Сертификаты — текущий поль </li> <li> Доверенные корневые центр </li> <li> Доверенные отношения </li> <li> Промежуточные центры се </li> <li> Объект пользователя Active </li> <li> Объект пользователя </li> <li> Объект пользователя Active </li> <li> Объект пользователя </li> <li> Доверенные корневые центр </li> <li> Доверенные корневые центр </li> <li> Доверенные корневые сертя </li> </ul>	а Имя логического хранилища Доверенные корневые центры сертификации Доверительные отношения в предприятии Промежуточные центры сертификации Объект пользователя Active Directory Доверенные издатели Сертификаты, к которым нет доверия Сторонние корневые центры сертификации Доверенные лица Поставщики сертификатов проверки подлинности клиентов Другие пользователи Запросы заявок на сертификаты смарт-карты
< >>	< >

3. Раскройте папку **Личное**, **Сертификаты**. В области справа отобразится перечень сертификатов пользователей данного ПК.

🚡 certmgr - [Сертификаты —	- текущий пользователь\Лич	ное\Сертификат – 🗖	×
Файл Действие Вид Справка	3		
🗢 🔿 🖄 📆 🔂 🖨 🖌	? 📭		
🙀 Сертификаты — текущий полы	Кому выдан	Кем выдан	Cį
<ul> <li>Доверенные корневые цент</li> </ul>	🔄 *.swan.perm.ru	*.swan.perm.ru	29
Доверительные отношения			
<ul> <li>Промежуточные центры се</li> <li>Объект пользователя Active</li> </ul>			
<ul> <li>Доверенные издатели</li> <li>Сертификаты, к которым не</li> </ul>			
<ul> <li>Сторонние корневые центр</li> <li>Доверенные лица</li> </ul>			
<ul> <li>Поставщики сертификатов</li> <li>Лругие подъзователи</li> </ul>			
<ul> <li>Другис пользователи</li> <li>Запросы заявок на сертифи</li> </ul>			
Доверенные корневые серт			
< >>	<		>
Хранилище Личное содержит 1 серт	гификат.		

4. Нажмите правой кнопкой мыши на записи с сертификатом, который надо экспортировать. Отобразится контекстное меню.

🚡 certmgr - [Сертификаты —	- текущий пользователь\Лич	ное\Сертификат – 🗖 🗙
Файл Действие Вид Справка (Ф 🔿 🖄 🔝 🔏 🗎 🗙		
<ul> <li>Сертификаты — текущий поль:</li> <li>Личное</li> <li>Сертификаты</li> <li>Доверенные корневые цент</li> <li>Доверительные отношения</li> </ul>	Кому выдан Открыть Все задачи	Кем выдан С; *.swan.perm.ru 29 Открыть
<ul> <li>Промежуточные центры се</li> <li>Объект пользователя Active</li> <li>Доверенные издатели</li> <li>Сертификаты, к которым на</li> </ul>	Вырезать Копировать Удалить	Запросить сертификат с новым ключом Обновить сертификат с новым ключом Экспорт
<ul> <li>Сторонние корневае центр</li> <li>Доверенные лица</li> <li>Поставщики сертификатов</li> <li>Другие пользователи</li> <li>Запросы заявок на сертифи</li> </ul>	Свойства Справка	
Доверенные корневые серт		
< >> Перечень действий, которые могут	быть выполнены с данным элемент	

5. Выберите пункт Все задачи – Экспорт. Запустится Мастер экспорта сертификатов.

Примечание – Содержимое меню может отличаться в зависимости от типа операционной системы на ПК пользователя.

6. Следуйте указаниям Мастера, выгрузите сертификат. Для перехода между шагами Мастера используйте кнопку **Далее**. Значения параметров оставьте по умолчанию.

×	×
💿 🝜 Мастер экспорта сертификатов	📀 🗧 Мастер экспорта сертификатов
Мастер экспорта сертификатов	Формат экспортируемого файла Сертификаты могут быть экспортированы в различных форматах.
Этот мастер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов из хранилища сертификатов на локальный диск.	Выберите формат, который вы хотите использовать:
Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установрания азищиваных ставеных полконовий (такимина сертификатов —	Файлы Х. 509 (.CER) в кодировке DER Файлы Х. 509 (.CER) в кодировке Base-64
устополнити задищалном се селон подколочелини кралиницае сер и прикотоо это область систены, предназначенная для хранения сертификатов.	Стандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b) Включить по возможности все сертификаты в путь сертификации
Для продолжения нажните кнопку "Далее".	<ul> <li>Файл обмена личной информацией - PKCS #12 (.PFX)</li> <li>Включить по возможности все сертификаты в путь сертификации</li> </ul>
	Удалить закрытый ключ после успешного экспорта Экспортировать все расширенные свойства
	Хранилище сериализованных сертификатов (.SST)
Далее Отмена	Далее Отмена

7. Укажите наименование для файла-сертификата в поле **Имя файла**, нажмите кнопку **Обзор** чтобы задать место для сохранения файла на ПК, например, «Рабочий стол», нажмите кнопку **Далее**.

×
🕘 👰 Мастер экспорта сертификатов
Имя экспортируемого файла
Укажите имя фаила, который вы хотите экспортировать
1
Имя файла:
Сертификат пользователя ц Обзор
2
3
Далее Отмена

8. Завершите работу мастера с помощью кнопки Готово.

	×
🕒 🦂 Мастер экспорта серт	ификатов
	nymarob
Завершение работ	ы мастера экспорта сертификатов
Вы успешно завершили работ	у с мастером экспорта сертификатов.
Были указаны следующие па	раметры:
Файл	C:\Windows\system32\Сертификат пользова
Экспорт ключей	Нет
Включить в путь все серти	фикаты Нет
Формат файлов	Двоичные файлы X.509 (*.cer) в кодировке
<	>
	Готоро Отнена
	Тотово Отмена

Информация о результате экспорта отобразится на экране.



#### Добавьте экспортируемый сертификат для учетной записи пользователя.

Для этого:

- 1. Запустите Систему.
- 2. Выберите:
  - Сервис Пользователи в главном меню Системы;
  - Кнопку Пользователи на боковой панели АРМ администратора ЦОД;
  - В АРМ администратора МО работа с пользователями выполняется на главной форме.
- 3. Найдите пользователя, используя поля фильтра.

🔺 Нажмите чтобы свернуть/развернуть панель фильтров							
Логин:	use	Фамилия:	Фамилия				
Группа:		► Имя:	И				
Организация:	P	× Тип организации:		~			
Описание:		Заблокирован:		~			
Пользователи							
😋 Добавить 🥜 Изм	🔂 Добавить 🥜 Изменить 📄 Просмотреть 😢 Удалить 💿 Обновить 👹 Печать 🔻 🕥 Действия 🛪						
👿 Логин 🔺	Имя Фан	иилия	Группы	Организации			
🔽 useredit	имя Фан	илия	RegistryUser				

4. Нажмите кнопку Изменить. Отобразится форма Пользователь.

Пользователь: Редакт	ирование		¢ X
<b>1. Основное</b> 2. Дос	туп к АРМ		
Организация:			🔎 × 🕒 Добавить 😣 Удалить
Наименование			Тип
Название не определен	0		
Логин:	useredit 🔲 Заблокирован	Идент. МАРШа:	
Временный пароль:	•••••		
Токен:	До	: Сгенерировать	
Сотрудник	Сертификаты		
Сотрудник:		<b>v</b>	
Фамилия:	Фамилия	Полное имя: Фамилия имя	
Имя:	имя	Эл. почта:	
Отчество:		Описание:	
Группы:		🗙 🗘 Добавить 😣 Удалить	
Группа	Описание		
Сохранить			Помощь

5. Нажмите кнопку Сертификаты. Отобразится форма для загрузки сертификатов.

Пользователь: Сертификаты 🔹 🔀				
Обавить ЗУдалить 4 Печать			0/0	
Название	SHA-1	Дата начала	Дата оконч	
Сохранить			Закрыть	

6. Нажмите кнопку Добавить. Отобразится форма Загрузка сертификата.

Загрузка сертификата		¢ 🗙
Сертификат: Вы	берите файл сертификата	Открыть
Загрузить		Помощь

7. Укажите путь к файлу, который был экспортирован, с помощью кнопки **Открыть**.

•	Выгрузка файла					×
🔄 🎯 🔻 🕇 📕 Рабочий стол	¥	Ċ	Поиск: Рабочий	стол		Q,
Упорядочить 🔻 Создать папку				•	E	
🔆 Избранное 🔷 👫		1	Размер	Тиг '	^	
🚺 Загрузки 🗔 Сертификат пользова	теля ФИО.cer		1 КБ	Сер	١,	- Чет данных
🕮 Недавние места	туги моо приложение.сс		1 КБ	Тек		для
💻 Рабочий стол 🛛 🐴 Список больных по н	озологиям.xls		26 KE	Лис	4	цварительн
▲ 2017-06-02_094537.pm	I		31 KE	Φai		іросмотра.
🖳 Этот компьютер 🗸 <			707.175	>	~	
Имя файла: Сертификат пользов	ателя ФИО.cer	¥	Все файлы (*.*)			~
			Открыть		Отл	ена
					_	

8. Подтвердите загрузку с помощью кнопки Загрузить.

Загруженный сертификат отобразится в списке.

Пользователь: Сертификаты			¢ 🗙
🛟 Добавить 🔇 Удалить 🖼 Печать 🔻			1/1
Название	SHA-1	Дата начала	Дата оконч
Сертификат пользователя ФИО.cer	2bf11496e39dd7e2b495700a8891ce	30.08.2013	29.10.2032
<b>О</b> Сохранить			😧 Закрыть

- 9. Нажмите кнопку **Сохранить**. Сертификат будет добавлен для учетной записи пользователя.
- 10. Сохраните изменения для учетной записи пользователя.
- 11. Перезапустите браузер для работы в Системе, авторизуйтесь заново под учетной записью пользователя.

## 1.2. Установка ПО для использования электронной подписи для работы в операционной системе Windows

Если ранее не были установлены компоненты для применения ЭП, следует их установить:

- Для работы плагина требуется установленный КриптоПро CSP версии 4.0 и выше. Дистрибутив и инструкцию по установке можно получить по ссылке: https://www.cryptopro.ru/products/csp/downloads.
- Плагин для установки доступен для загрузки с сайта производителя: https://www.cryptopro.ru/sites/default/files/products/cades/current\_r elease\_2\_0/cadesplugin.exe

- Для браузера Chrom e(Chromium) расширение для работы плагина устанавливается автоматически при перезапуске браузера. Для Firefox необходимо установить расширение по ссылке: <u>https://www.cryptopro.ru/sites/default/files/products/cades/extensions/firefox x cryptopro\_extension\_latest.xpi</u>.
- 4. Установите сертификат удостоверяющего центра.
- 5. Установите личный сертификат пользователя.
- 6. Загрузите сертификаты пользователя в Систему (описание см. ниже).

# 1.3. Установка ПО для использования электронной подписи для работы в операционной системе Linux

Если ранее не были установлены компоненты для применения ЭП, следует их установить:

 Для работы плагина требуется установленный КриптоПро CSP версии 4.0 и выше. Дистрибутив и инструкцию по установке можно получить по ссылке: https://www.cryptopro.ru/products/csp/downloads. Для запуска установки распакуйте архив и запустите следующую команду в консоли:

sudo ./install.sh

А. Важно! Для работы плагина должен быть установлен пакет cprocsprdr-gui-gtk, при этом должен отсутствовать пакет cprocsp-rdr-gui.

 Плагин для установки доступен для загрузки с сайта производителя: https://www.cryptopro.ru/products/cades/downloads или по прямой ссылке: https://www.cryptopro.ru/sites/default/files/products/cades/current\_relea

ссылке: https://www.cryptopro.ru/sites/default/files/products/cades/current\_relea se\_2\_0/cades\_linux\_ia32.tar.gz

3. Для установки распакуйте архив и сконвертируйте все rpm-пакеты в debпакеты командой:

sudo alien -k название\_пакета.rpm

При использовании некоторых 64 битных версий КриптоПро CSP 4.0 для rpm дистрибутивов потребуется указать флаг --nodeps.

- 4. Установите каждый deb-пакет.
- Для браузера Chrome(Chromium) расширение для работы плагина устанавливается автоматически при перезапуске браузера. Для Firefox необходимо установить расширение по ссылке: https://www.cryptopro.ru/products/cades/downloads(https://www.crypto pro.ru/sites/default/files/products/cades/extensions/cryptopro\_extension\_for\_cad es\_browser\_plug\_in-1.1.1-an+fx-windows.xpi)
- 6. Установите сертификат удостоверяющего центра командой:

/opt/cprocsp/bin/ia32/certmgr -inst -store root -file <путь к файлу с сертификатом>

7. Установите личный сертификат с помощью команды:

/opt/cprocsp/bin/ia32/certmgr -inst -file <путь к файлу с сертификатом> -cont <имя контейнера>

8. Проверьте подпись на демо-

странице: https://www.cryptopro.ru/sites/default/files/products/cades/demopage/ simple.html

#### 1.4. Загрузка сертификатов пользователей

Для учетной записи пользователя должен быть загружен сертификат в систему:

- 1. Откройте форму настройки параметров учетной записи пользователя Сервис – Пользователи.
- 2. Выберите в списке учетную запись, для которой следует загрузить сертификат ключа пользователя.
- 3. Откройте форму редактирования параметров учетной записи с помощью кнопки **Изменить**.

Примечание – Если учетная запись пользователя не создана, следует добавить ее в систему.

4. Нажмите кнопку Сертификаты. Отобразится форма загрузки сертификатов пользователя.

🧞 Примечание - Сертификат должен быть в формате PKCS7.

5. Для добавления сертификата пользователя нажмите кнопку Добавить.

- 6. Укажите путь к файлу-сертификату, нажмите кнопку **Загрузить**. Сертификат будет загружен. Файл сертификата предоставляется удостоверяющим центром, при выдаче электронного ключа.
- 7. Нажмите кнопку Сохранить для сохранения внесенных изменений.
- Для применения настроек необходимо выйти из системы и авторизоваться под учетной записью пользователя, для которой были добавлены настройки.