Инструкция по работе с плагином CryptoPro и УКЭП

Содержание:

- 1. Установка ПО для работы с УКЭП
- 2. Установка программы КриптоПро
- 3. Загрузка и установка КриптоПро ЭЦП Browser plug-in:
- 4. Активация использования «КриптоПро ЭЦП Browser plug-in»
- 5. Проверка работы плагина «КриптоПро ЭЦП Browser plug-in»
- 6. Добавление корневых сертификатов в список доверенных
- 7. <u>Требования к составу и содержанию обязательных параметров сертификата</u> <u>УКЭП</u>
- 8. <u>Часто задаваемые вопросы</u>

1. Установка ПО для работы с УКЭП

Для работы С УКЭП необходимо загрузить и установить драйвер Рутокен, для этого:

1.1. Необходимо перейти по прямой <u>ссылке</u>или перейти в раздел «<u>Центр загрузки</u>» сайта Рутокен (<u>https://www.rutoken.ru/</u>– Поддержка – Центр загрузки) (Рис.1.1)

Продукты 👻 Решения 💙	∙ Технологии 🛩	Поддержка 🜱 Заказ 🜱	Центр загруз	ки 👻 🌞 Разработчику
Главная	а > <u>Поддержка</u> > Цен	вопрос-ответ		
	ЛРАЙВ	 Центр загрузки 	ows	
		 Документация 	Joins	
	Пользовате	 Сервис диагностики 		ИНСТРУКЦИИ
ЦЕНТР ЗАГРУЗКИ	Для того чтобы у установочный фа	 База знаний 	dows, загрузите	Настройка и
Doolingoou and Windows	завершения проц	Форун	К КОМПЬЮТЕРУ.	эксплуатация Руто

Рис. 1.1 — Рутокен – Поддержка – Центр загрузки

- 1.2. Выбрать версию драйвера Рутокен, соответствующую установленной ОС. Ниже в примере рассмотрим загрузку драйвера для ОС Windows:
 - 1.2.1 Для загрузки Драйвера Рутокен для Windows необходимо кликнуть по ссылке «Драйверы Рутокен для Windows, EXE» (Рис. 1.2):

Продукты У Решения	У Технологии у Поллержка у Заказ у Центр заги	рузкі
продукты тешения		
Главна	а > Поллерукка > Центр загрузки > Лрайверы для Windows	
<u>Trabila</u>	т х <u>педдерлиц</u> х <u>центр запуули</u> х дральеры для ніпосиз	
	драйверы для широws	
	Пользователям Рутокен ~	
ВОПРОС-ОТВЕТ ЦЕНТР ЗАГРУЗКИ	ДГАЛІДСТВІ ДЛА VVIINDOVVS	
 ВОПРОС-ОТВЕТ ЦЕНТР ЗАГРУЗКИ Драйверы для Windows 	ДРАИЛДЕР ВІ ДЛА WINDOWS Пользователям Рутокен ~ Для того чтобы установить драйверы Рутокен для Windows, загрузите установочный файл, запустите его и следуйте указаниям установщика. После завершения процесса установки подключите Рутокен к компьютеру.	(ME10)
ВОПРОС-ОТВЕТ ЦЕНТР ЗАГРУЗКИ = Драйверы для Windows = Драйверы для macOS	ДРАИЛДЕР ВІ ДЛА ИЛИДОИИЗ Пользователям Рутокен • Для того чтобы установить драйверы Рутокен для Windows, загрузите установочный файл, запустите его и следуйте указаниям установщика. После завершения процесса установки подключите Рутокен к компьютеру.	6

Рис. 1.2 — Загрузка драйвера Рутокен для ОС Windows

1.3. Откроется новая страница «Лицензионное соглашение» (Рис.1.3):

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ



Рис. 1.3 — Страница «Лицензионное соглашение»

1.3.1 Необходимо принять условия Лицензионного соглашения (поставить галку и кликнуть по кнопке «условия приняты») (Рис. 1.4):



Рис. 1.4 — Согласие с условиями Лицензионного соглашения

1.4. Перейти к загрузке драйвера Рутокен (Рис. 1.5):



- Рис. 1.5 Перейти в загрузки и сохранить установочный файл драйвера Рутокен
- 1.4.1 Открыть сохраненный файл и установить драйвер Рутокен, выполнив загруженный установщик (Рис. 1.6).

] Драйверы Рутокен	- 🗆 X
рутокен	
ДРАЙВЕРЫ РУТОКЕН Начало установки	
✓ Создать на Рабочем столе ярлык Панели управления Рутокен	Установить Версия: 4.3.4.0

Рис. 1.6 — Установить Драйвер Рутокен

1.4.2 Дождаться завершение установки и «закрыть» (Рис.1.7)



Рис. 1.7 — Драйвер Рутокен установлен

2. Установка программы КриптоПро

Для установки программы КриптоПро необходимо:

2.1 Зарегистрироваться на сайте СтуртоРго:

2.1.1 Открыть форму регистрации, заполнив обязательные поля (Рис. 2.1)

криптопро	Ключевое сл	тоПро	рмации				Поиса
О компании Продукты	Услуги	Партнёры	Поддержка	Приобретение	Загрузка	Блог	Форум
Главная > Профиль пользовател Профиль пользовател	มาต 1 Я				Купи	ть	
Регистрация Вход Информация об учетной запис	Забыли п	аропь?					2

Рис. 2.1 — Открытие формы регистрации на сайте <u>CryptoPro</u>

2.1.2 После заполнения формы регистрации принять «Согласие на обработку персональных данных», ввести проверочный код из предложенной картинки, нажать кнопку «Регистрация» (Рис. 2.2)

Введите код	
Этот вопрос задается для того, чтобы выяснить, являете автоматическую спам-рассылку. 2341	есь ли Вы человеком или представляете из себя
Какой код на картинке?: *	

Рис. 2.2 — Подтверждение регистрации на сайте СтуртоРго

2.2 Перейти в раздел «Центр загрузки» сайта <u>КриптоПро</u> (Загрузка – КриптоПро CSP) или по <u>ссылке</u> (Рис. 2.3):

КриптоПро Ключевое слово в защите информации	Поиск
О компании Продукты Услуги Партнёры <mark>Поддержка</mark> Приобретение	Загрузка Блог ПФорум
Главная Центр загрузки Перейти к загрузке файлов для указанного продукта: • КриптоПро СSP • КриптоПро УЦ • КриптоПро УЦ 1.5 • КриптоПро УЦ 2.0	Купить
КриптоПро Шлюз УЦ-СМЭВ	N112 (

Рис. 2.3 — Раздел «Центр загрузки» сайта КриптоПро

2.3 Принять условия Лицензионного соглашения и перейти к загрузке (Рис. 2.4):



Рис. 2.4 — Согласие с условиями Лицензионного соглашения

2.4 Выбрать последнюю сертифицированную версию КриптоПро CSP (Рис. 2.5)

Криптопро Ключевое слово в защите информации	Поиск
О компании Продукты Услуги I Партнёры I Поддержка I Приоб	ретение Загрузка Блог Форум
Главная > Продукты > СКЗИ КриптоПро СSP КриптоПро CSP - Загрузка файлов	СКЗИ КриптоПро CSP Использование
Предварительные несертифицированные версии	КриптоПро TLS Совместимость реализаций TLS
<u>КриптоПро CSP 4.0 R4</u> для <u>Windows, macOS</u> и <u>UNIX</u> (несертифицированный)	КриптоПро EAP-TLS
<u>КриптоПро CSP 3.9 R3 для Windows, UNIX и macOS</u> (несертифицированный)	i Apache
КриптоПро CSP 5.0 для Windows, macOS и UNIX (несертифицированный)	КриптоПро Java CSP
КриптоПро CSP для Google Android (несертифицированный)	КриптоПро Winlogon
0	Библиотека считывателей
Сертифицированные версии	Загрузка файлов
КриптоПро CSP 4.0 R3 для Windows, macOS и UNIX	История версий
КриптоПро CSP 3.9 R2 для Windows, UNIX и macOS	Сравнение версий

Рис. 2.5 — Выбор последней сертифицированной версии КриптоПро CSP

2.5 Загрузить программу КриптоПро CSP, соответствующую ОС (Рис. 2.6). Для Windows:

-KOHTPOJSHAR CYNN FOCT: 86A2828881 MD5: 8b828b6ef14	18 8135102723/ d0dd5be7106	A88E97891CF919981CBAB035A12207C98A1ED36AD357 68bb6d98b1f
1977 (Andrewski 1977) (207	00000000000	
универсальный у сохраняются)	становщи	к (настройки, ключи и сертификаты при обновлении

Сертифицированные версии

<u>КриптоПро CSP 4.0 R</u>	<u>3 для Windows, macOS</u> и <u>UNIX</u>		
<u>КриптоПро CSP 3.9 F</u>	Открытие «CSPSetup.exe»		×
Сертифицирова	Вы собираетесь открыть:		
<u>КриптоПро CSP 3.6 F</u>	являющийся: Binary File из https://www.cryptopro.ru		
КриптоПро CSP 3.6 д	Вы хотите сохранить этот файл?		
СКЗИ с долговре		Сохранить файл	Отмена

- Рис. 2.6 Загрузка программы КриптоПро СЅР
- 2.6 Установить программу КриптоПро, для этого нужно выполнить ранее загруженный установщик (Рис. 2.7).
 - КриптоПро СSP 4.0.9842
 Благодарим за выбор КриптоПро CSP. http://www.cryptopro.ru
 Установить (рекомендуется) Продукт будет установлен в конфигурации КС1 и языком операционной системы с настройками по-умолчанию.

Рис. 2.7 — Установка программы КриптоПро СЅР

3. Загрузка и установка КриптоПро ЭЦП Browser plug-in:

3.1 Перейти по прямой <u>ссылке</u> или выбрать продукт «КриптоПро ЭЦП Browser plug- in» в разделе «Продукты» сайта <u>КриптоПро</u> (https://www.cryptopro.ru/ – Продукты – КриптоПро ЭЦП Browser plug-in) (Рис. 3.1):



Рис. 3.1 — Выбор продукта «КриптоПро ЭЦП Browser plug-in»

3.2 Загрузить актуальную версию КриптоПро ЭЦП Browser plug-in (для пользователей) (Рис. 3.2):

Скачать актуальную версию КриптоПро ЭЦП Browser plug-in:

версия 2.0 для пользователе кака загрузка версии плагина, соответствующей Вашей ОС) » версия 2.0 для пользователей (автоматическая загрузка версии плагина, соответствующей

Вашей ОС)

 Актуальна 	Открытие «cadesplugin.exe» X
 Поддержи КриптоПр 	Вы собираетесь открыть:
 Для Місто 	📧 cadesplugin.exe
других О(являющийся: Binary File из. https://www.covptopro.ru
Компонен	Вы хотите сохранить этот файл?
данную в	Сохранить файл Отмена
 Минималь 	

Рис. 3.2 — Загрузка КриптоПро ЭЦП Browser plug-in

3.3 Установить «КриптоПро ЭЦП Browser plug-in», для этого нужно выполнить panee загруженный установщик (Рис. 3.3):

КриптоПро ЭЦП Browser plug-in			\times
Установить Кр	иптоПро ЭЦП Bro	wser plug-in?	
	Да	Нет]

Рис. 3.3 — Установка КриптоПро ЭЦП Browser plug-in

3.4 Перезагрузить браузер

КриптоПро ЭЦП Browser plug-in	\times
КриптоПро ЭЦП Browser plug-in успешно установлен. Для корректной работы КриптоПро ЭЦП Browser plug-in может потребоваться перезапустить браузер.	
ОК	

4. Активация плагина «КриптоПро ЭЦП Browser plug-in»:

Чтобы активировать плагин «КриптоПро ЭЦП» в Вашем браузере, кликните по одной из ссылок ниже, в зависимости от используемого Вами браузера.

Google Chrome Yandex Browser Opera

4.1 Google Chrome

Необходимо перейти по ссылке для установки расширения в интернет-магазине Chrome: https://chrome.google.com/webstore/detail/cryptopro-extension-for-c/iifchhfnnmpdbibifmljnfjhpififfog?hl=ru

Рис. 3.4 — Завершение установки КриптоПро ЭЦП Browser plug-in

И нажать "Установить" (Рис.4.1)

0530P	ОТЗЫВЫ	ПОДДЕРЖКА	ПОХОЖИЕ		
🗲 🕶 Принир истольсови	an X			- • ×	Совместимо с вашим устройство
	Deepoid Dee	COQUERAIN SILEN (JUURIUM 1944 SILEN (JUURIUM 1944) COSTO (Salaryan Silen Fish)	Opendia ND/Instatuta Beguna tanàna sitema Beguna tanàna sitema Dimini Ama		г эсцирение позволяет использовать КриттоПро ЭЦП Вгожее ріцеїна 6 орзузере. Для работы требует установленного ЭЦП Browser plug-in. Данное расширение позволяет использовать учисни КритоПро ЭЦП Browser plug-in в орзузерах на основе Сплотии (бодое Ситопе, Орга, Яндекс. Браузер и др.). Для работы требует установленного КриттоПро ЭЦП Browser plug-in.
				<u>,</u>	 Сайт Сообщить о нарушении Дополнительная информация Версик: 1.2.4 Обновлено: 27 ноября 2017 г. Размер: 63.11КІВ

Рис. 4.1 — Установка CryptoPro Extension

В дальнейшем включить или отключить плагин вы можете в настройках браузера «Дополнительные инструменты» — «Расширения» (Рис.4.2)

				07	k 8	
	Mar	Новая вкладка	1		Ct	I+T
	FIX	Новое окно			Ctr	I+N
NA	14	Новое окно в	режиме инкогнито	a	rl+Shi	14 N
P NA	10	История				
10	19	Загрузки			Ct	r(+1)
AV	A	Закладки				
1/1		Масштаб		- 100 %	÷	::
1///	A	Печать			c	(+P
11/2		Трансляция				
	2	Найти			Ct	(+F
ить страницу как	Ctrl+S	Дополнительн	ые инструменты			
на рабочий стол		Unuasian	Вырезать	Колиповать	Dem	BUTh.
All and a second		Vonchille		noninpopulo	DUIG	-
ие данных о просмотренных страницах.	Ctrl+Shift+Del	Настройки		in a ground	DUIG	
име данных о просмотренных страницах. рения	Ctrl+Shift+Del	Настройки Справка			DUIG	
е данных о проснотренных страницах. ния ер задач	Ctrl+Shift+Del Shift+Esc	Настройки Справка		no spoor o	DUTE	

 $\leftarrow \rightarrow \mathbf{C}$ \bigcirc Chrome | chrome://extensions



Примечание: Если расширения «CryptoPro Extension for CAdES Browser Plug-in» нет в списке доступных, нужно перезапустить браузер.

4.2 Yandex Browser

Скачайте расширение по ссылке и нажмите установить (Рис.4.3)



Рис. 4.3 — Установка CryptoPro Extension Yandex Browser

Возможно потребуется дополнительно включить расширение, для этого необходимо зайти в раздел «Дополнения» и включить КриптоПро ЭЦП, затем перезапустить браузер (Рис.4.4)



Рис. 4.4 — Активация CryptoPro Extension Yandex Browser

4.3 Opera

Для корректной работы плагина необходимо добавить расширение КриптоПро: Орега – расширение доступно по <u>ссылке</u>. (Рис.4.5)



Рис. 4.5 — Установка CryptoPro Extension Opera

Нажать «Добавить в Opera»

Зайти в меню в Opera – расширения и отметить все чекбоксы на вкладке Extensions: (Рис.4.6)



Рис. 4.6 — Активация CryptoPro Extension Opera

5. Проверка работы плагина

Перейдите на специальную страницу

Если отображается «плагин недоступен» (Рис.5.1):



Рис. 5.1 — Плагин СтурtоРго недоступен

Необходимо выполнить действия указаны в п.4

Если приложения установлены, при входе на страницу появится предупреждение о том, что плагин запрашивает доступ к ключам и сертификатам (Рис.5.2).



Рис. 5.2 — Подтвердить доступ

Необходимо согласится.

Если у вас появляется сообщения, то Плагин успешно установлен на компьютер:



6. Добавление корневых сертификатов в список доверенных

Для выполнения добавления сертификатов предварительно необходимо:

- 6.1 Скачать файл открытого ключа УКЭП или иметь на руках носитель с установленным сертификатом, например, <u>USB ключ "Рутокен КП"</u>.
- 6.2 Открыть свойства персонального сертификата (Рис. 6.1) (пример <u>USB ключ "Рутокен КП"</u>) Открыть Панель управления Рутокен – Сертификаты – Выбрать сертификат – Свойства



тие. 0.1 Открытие своисть переопального сертификата в программет утокен

6.3 Открыть корневой сертификат (Рис. 6.2) (верхний в цепочке сертификатов) Путь сертификации – Корневой сертификат – Просмотр сертификата

🐖 Сертификат	×
Общие Состав Путь сертификации	
Путь сертификации Тестовый УЦ ООО "КРИПТО-ПРО" (УЦ 2.0) Ванов Сергей Иванович	
Просмотр сертификата	
Состояние сертификата:	
Этот сертификат действителен.	
ОК	

Рис. 6.2 — Открытие корневого сертификата в программе Рутокен

Экспорт корневого сертификата (Рис. 6.3) Состав-Копировать в файл - Далее-далее. 6.4

дмі	инистрирование Сертифик	аты Настройки О программе
	Сертификат	
C	Общие Состав Путь сертиф	икации
	🐖 Сертификат	
	Общие Состав Путь сер	тификации
		• •
	Показать: <Все>	~
	Поле	Значение
	Версия	V3
	Серийный номер	34 68 1e 40 cb 41 ef 33 a9 a0
	🛄 Алгоритм подписи	GOST R 34.11/34.10-2001
	🛄 Хэш-алгоритм подпис	и GOST R 34.11-94
	Издатель	Головной удостоверяющий
	Действителен с	20 июля 2012 г. 15:31:14
	Деиствителен по	1/июля 2027г. 15:31:14
	,	
		Свойства Копировать в файл

Рис. 6.3 — Экспорт корневого сертификата в программе Рутокен

6.5 Выбрать директорию и имя экспортированного сертификата Выбрать директорию и имя файла – Далее – Готово (Рис. 6.4)

💼 Сохранение	×
← → <hr/> <h<< td=""><td>Ą</td></h<<>	Ą
Упорядочить 🔻 Создать папку	
> ≱ Быстрый доступ OneDrive	
 Этот компьютер Видео 	
> 🔮 Документы	
> 🖶 Загрузки > 📰 Изображения	
> 🤚 Музыка	
> Рабочий стол	>
Имя файла: CoreCertificate CryptoPro	~
Тип файла: Двоичные файлы X.509 (*.cer) в кодировке DER	~
Скрыть папки Сохранить	Отмена
Рис. 6.4 — Сохранение корневого сертификата в программе Рутокен	

 6.6 Добавление корневого сертификата в список доверенных (Рис. 6.5)
 Выбрать файл сертификата – Установить сертификата - Локальный компьютер – Автоматически выбрать хранилище на основе типа сертификата – Далее

💂 Сертификат	\times
Общие Состав Путь сертификации	
Сведения о сертификате	-
Этот сертификат предназначается для: • Подтверждает удаленному компьютеру идентификацию вашего компьютера • Защищает сообщения электронной почты • Electronic signature tool КС1 • Electronic signature tool КС2 • 1.2.643.6.3.1.4.1	
Установить сертификат Заявление поставщика	
ок	

Рис. 6.5 — Добавление корневого сертификата в список доверенных

6.7 Выбор хранилища для установки корневого сертификата необходимо установить в Доверенные корневые центры сертификации и Доверенные издатели (Рис. 6.6) Поместить все сертификаты в следующее хранилище – Обзор... – Доверенные корневые центры сертификации + Доверенные издатели – ОК – Далее – Готово

Xp	анилище сертификатов
	Хранилища сертификатов - это системные области, в которых хранятся сертификаты.
	Windows автоматически выберет хранилище, или вы можете указать расположение сертификата вручную.
1	Поместить все сертификаты в следующее хранилище
	Выбор хранилища сертификата X Выберите хранилище сертификатов, которое вы
3	 Личное Доверенные корневые центры сертис Доверительные отношения в предпри Промежуточные центры сертификаци

Рис. 6.6 — Выбор хранилища для установки корневого сертификата

После выполнения завершения установки всех программ, плагинов и сертификатов нужно перезагрузить ПК.

7. Требования к составу и содержанию обязательных параметров сертификата УКЭП

🐖 Сертификат	×
Общие Состав Путь сертификации	
Показать: <Все>	~
Поле	Значение
Версия	V3
📴 Серийный номер	34 68 Ja 40 do 41 ef 33 eft e
Алгоритм подписи	10007 R 34.11/34.10-2001
Ш Хэш-алгоритм подписи Излатель	Головной удостоверяющий
Действителен с	толовной удостоверяющи
Плействителен по	17.mmm 10177+ 14-71-14
*	2
24 40 27 all all 75 10 23 c8 d8 31 ad 84 77 2a 78 all % 48 c3 ad ad 07 5a 75 c4 2 % all 8a 5a 73 42 24 ac 2a ad 90 7a at	11 57 50 tee 86 c5 6a 83 4a 37 26 2 54 91 57 c8 37 21 6a 6a 70 3a 83 73 37 a1 6a
Свойст	ва Копировать в файл
	ОК

7.1 Состав обязательных полей/параметров (см.Рис.7.1.):

Рис. 7.1 Обязательные поля сертификата УКЭП

7.1.1 Поле «Версия».

Поле «Версия» (version) должна быть не ниже 3.

7.1.2 Поле «Серийный номер».

Поле «Серийный номер» (serialNumber) должно содержать серийный номер сертификата подписи, уникальный в пределах серийных номеров всех сертификатов, выданных

Удостоверяющим центром (УЦ), издавшего сертификат УКЭП.

7.1.3 Поле «Издатель сертификата».

Поле «Издатель сертификата» (issuer) должно содержать ФИО (при наличии) уполномоченного лица УЦ либо псевдоним издателя сертификата.

7.1.4 Поля, обозначающие срок действия сертификата «Действителен с» и «Действителен по».

Поле «Срок действия сертификата» должно содержать дату начала и дату истечения срока действия СКП в формате UTC.

7.1.5 Поле «Открытый ключ» должно содержать:

- название и алгоритм формирования открытого ключа. (Для формирования открытого ключа в соответствии с государственными стандартами Российской Федерации – ГОСТ Р 34.11/34.10-2001;

- параметры и значение открытого ключа уполномоченного лица УЦ.

7.1.6 Поле, обозначающее владельца сертификата «Субъект».

7.2 Свойства параметра «Владелец сертификата» / «Субъект», см. Рис.7.2:

щие Соста	в Путь сертифик	ации	
оказать: <	Bce>	~	
Поле Алгоритм Хэш-алго Издатель Действит Действит	подписи ритм подписи телен с телен по	Значение	^
Субъект		tereneral maples, reneral	
Субъект Открыты Параметт	й ключ ы открытого кл	6007 R 34 10-2011 (512 8m) N: 11 M 47 % 85 81 81 81 81 91	~

Рис.7.2 Свойства поля «Владелец сертификата» / «Субъект» сертификата УКЭП

7.2.1 Поле «Владелец сертификата» / «Субъект» содержит следующие компоненты имени и формируется следующим образом:

- Параметр «Общее имя» (**CN**, Common Name), содержащий фамилию, имя, отчество (при наличии) владельца сертификата УКЭП – физического лица;

- параметр «Идентификационный номер налогоплательщика владельца сертификата УКЭП – юридического лица, **INN**» (для владельца УКЭП юридического лица);

- параметр «Основной государственный регистрационный номер владельца УКЭП –

юридического лица, OGRN» (для владельца УКЭП юридического лица);

- параметр «Страховой номер индивидуального лицевого счета владельца УКЭП сертификата физического лица, SNILS» (для физического лица);

- параметр «Должность (T, Title)», содержащий должность владельца сертификата УКЭП для юридических лиц;

- параметр «Организация (O, Organization)», содержащий название юридического лица;

- параметр «Город (L, Locality)», содержащий название населенного пункта, в котором расположена организация владельца сертификата;

- параметр «Страна (С)», содержащая название страны, в которой расположена организация владельца сертификата;

- параметр «Адрес, STREET»;

- параметр «Адрес электронный почты (E, EMail)», содержащий адрес электронной почты владельца сертификата ключа подписи.

8. Часто задаваемые вопросы

8.1 Можно ли подписать документ без наличия ключевого носителя (USB ключа Рутокен)?

Обеспечение аппаратной генерации ключей и формирования ЭП происходит в микропроцессоре ключевого носителя (например, <u>USB кл юч "Рут окен К П"</u>.), поэтому наличие ключевого носителя является обязательным условием для подписания.

8.2 Как просмотреть список сертификатов, доступных для выбора в браузере?

Для просмотра списка установленных сертификатов нужно открыть список персональных сертификатов, выполнить следующие действия (Рис. 8.1):

Панель управления – Сеть и интернет – Свойства браузера – Содержание – Сертификаты – Личные



Рис. 8.1 — Просмотр списка установленных персональных сертификатов

Для просмотра списка сертификатов в программе Рутокен необходимо выполнить действия (Рис. 8.2):

Подключить ключевой носитель – Открыть Панель управления Рутокен – Сертификаты



Рис. 8.2 — Просмотр списка сертификатов ключевого носителя, проверить валидность сертификата

Для просмотра статуса сертификата, необходимо открыть список сертификатов ключевого носителя (Рис. 8.2) и выбрать необходимый сертификат. Статус сертификата отобразится в области основной информации.

Также можно просмотреть валидность всей цепочки для выбранного сертификата. Для этого нужно открыть свойства сертификата и просмотреть цепочку сертификатов (перейти на вкладку Путь сертификата) (Рис. 8.3)

Статус сертификата, выбранного из цепочки, отобразится в области Состояние сертификата. Подключить ключевой носитель – Открыть Панель управления Рутокен – Сертификаты – Свойства – Путь сертификации – Выбрать сертификат из цепочки

Панель управл Панель управля	ления Рутокен Х
Администрирова	ние Сертификаты Настроики Опрограмме
Подключенн	сертификат
Rutoken S	Общие Состав Путь сертификации
Илана	Путь сертификации
	Г Тестовый УЦ ООО "КРИПТО-ПРО" (УЦ 2.0)
Имя	
(Иванов С te-4b35a6	
Иванов А te-78e899;	
Гадельши te-da8303	
AO "MCII RaUser-fc0	
	Просмотр сертификата
	Состояние сертификата:
	Этот сертификат действителен.
₩	
Импортирова	OK
	Закрыть

Рис. 8.3 — Просмотр статуса сертификата из цепочки сертификатов

8.3 Как добавить новый сертификат, в список доступных для выбора вбраузере? Доступные для выбора сертификаты можно посмотреть в хранилище персональных сертификатов (пример ОС Windows) (Рис. 8.1).

При использовании программы Рутокен, добавление персональных сертификатов происходит автоматически, для этого должен быть проставлен признак «Зарегистрирован» для соответствующего (проставлен по умолчанию) сертификата в Рутокен (Рис. 8.4).



Рис. 8.4 — Просмотр признака Registered сертификатов ключевого носителя

Ручное добавления персонального сертификата аналогично добавлению корневых сертификатов, при этом на этапе выбора хранилища нужно установить значение «Личное» (Рис. 8.1):

Поместить все сертификаты в следующее хранилище – Обзор... – Личное – ОК – Далее – Готово

8.4 Как экспортировать файл сертификата из хранилища ПК, ключевого носителя Для экспорта файла сертификата из хранилища ПК нужно выполнить действия (Рис. 8.5):

Панель управления – Сеть и интернет – Свойства браузера – Содержание – Сертификаты – Личные (Открыть соответствующее хранилище сертификатов) – Выбрать сертификат – Экспорт... – Далее – Нет, не экспортировать закрытый ключ – Далее – Далее – Обзор.. – заполнить имя и путь файла – Далее – Готово

Серти	фикаты								>
азначени	ie:	<bce3< th=""><th>></th><th></th><th></th><th></th><th></th><th></th><th>~</th></bce3<>	>						~
Личные	Другие по	льзова	тели	Промежуточ	чные це	нтры серти	фикации	Довереннь	•
Кому в	зыдан		Кем в	зыдан		Срок де	Понятн	ое имя	
E Visa	нов Андрей І	1ванович	уц с	ю "крипто-г	IPO"	01.12.2017	APNS ce	ertificate	
Импорт	Эк	спорт		Удалить				Дополнительн	0
Импорт. Назначен Проверк	Эки ния сертиф а подлинно	спорт	Вера,	Удалить	длинно	сти клиента	1	Дополнительн	0
Импорт. Назначен Проверк	Эки ния сертиф а подлинно	спорт иката ости сер	вера,	Удалить Проверка по	одлинно	сти клиента	1	Дополнительн	0

Рис. 8.5 — Экспорт файла сертификата из хранилища ПК

Для экспорта файла сертификата из ключевого носителя нужно выполнить действия (Рис. 8.6): Подключить ключевой носитель – Открыть Панель управления Рутокен – Сертификаты – Свойства – Выбрать сертификат – Экспорт — Обзор – заполнить имя и путь файла – Экспорт



Рис. 8.6 — Экспорт файла сертификата из ключевого носителя средствами программы Рутокен

8.5 Как удалить из списка сертификатов, доступных для выбора в браузере, неактуальные записи (отозванные, просроченные...)

Доступные для выбора сертификаты можно посмотреть в хранилищеперсональных сертификатов (Рис. 8.7). Для удаления персональных сертификатов в ПК, рекомендуется:

Извлечь из ПК <u>USB ключ</u> (например, <u>"Рутокен КП"</u>)- Открыть хранилище персональных сертификатов – Выбрать неактуальную запись – Remove

начени	ie:	<bce></bce>					
иные	Другие по	ользоват	ели І	Промежуточные цен	нтры сертифика	ации Дов	вереннь
Кому в	зыдан		Кем вы	ыдан	Срок дейст	гвия	
БИВ	анов Андр	ей Ив	уц о	ОО "КРИПТО-ПРО".	01.12.2017	7	
Б	анов Серге	ей Ив	уц о	юо "Крипто-Про".	28.06.2017	7	
<							
К	Эк	спорт		Удалить		Допо	лнительн
< Імпорт азначен	Эко ния сертиф	спорт		Удалить		Допо	лнительн
< Імпорт азначен	Эко ния сертиф	спорт		Удалить		Допо	лнительн

Рис. 8.7 — Удаление сертификата из хранилища ПК

8.6 Ошибка при подписании документов на портале smbfin.ru АИС НГС

Описание ошибки «Ошибка создания подписи A certificate chain could not be built to a trusted root authority» (см.скриншот Рис.8.8):

<					N	СП Банк
асп – навная раникца ортала	Заявка				ВИЗАД ДАЛЕЕ ЗАПОЛНИТЬ ПОЗЖЕ	отмена
19001	S			•		
ивности	COLUMN SERVICE					
он агенты	докоменты заявки РЕДАСТИРОВАТь	Costadorat 10	00 AK5 "Eapwep"" •			
	·		w wy y min - why game	THE REAL PROPERTY OF		
	Халим паспорта главноге бузгалтера (асе стра	450	Ошибка создания подписи A certificate chain could			
	∅ nacnopranveesa.zip ×	подлисать	not be built to a trusted root authority. (0x8008010A)			
200						
		Stoffsell, Drie				
	E house					
	Колин паспорта руководителя организации (а	е страници)				
	0 nacrogr Pułstwoa KNO pdł 兴	подписать				
	DOSABUTE GARD PEDAKTHPOBATE					
	Si Januar					
	Справка НФНС о состоянии раснетов по налог.	ня, сборан, пенля, штрафая	а, процентам организаций - с даты выдачи которой по диту п	одачи замени прошло не болие 30 ка	ендарных дней	
	🖉 справка из налоговой pdf 🗙	подписать				

Рис. 8.8 — Ошибка создания подписи

Для решения проблемы нужно:

8.6.1. Проверить валидность цепочки сертификатов на ключевом носителе

Для просмотра списка цепочки сертификатов в программе Рутокен необходимо выполнить действия (Рис. 8.9):

Подключить ключевой носитель – Открыть Панель Управления Рутокен – Сертификаты

дминистрирование Сертификаты Настр Подключенные Рутокен Rutoken S 0	оойки Опрог	рамме Ввести PIN	-код
Иванов Андрей Иванович Спурtо-Pro GOST R 34.10-2001 Спурtо Спурtо-Pro GOST R 34.10-2001 Спурtо Сертификат действителен З	ographic Service	Provider	
Имя	Истекае	т Зарегистрі	ирован
Иванов Сергей Иванович te-4b35a676-a2f7-47ed-b9cb-8c8ef1ae	28.06.201	7 🗹	
Иванов Андрей Иванович te-78e899a5-5500-46b0-9175-750ce2d6		7 🗹	
Гадельшин Рамиль Саловатович te-da8303d5-d868-48c7-b23b-0f59bd0	211.201	7	
АО "МСП Банк" RaUser-fc0c7c8a-8971-45c0-96d1-68e5	11.03.201	7	
	Экспортироват	Ж ъ Удалить	1 Свойств

Рис. 8.9 — Просмотр списка сертификатов ключевого носителя, проверка валидности сертификата

Далее нужно просмотреть валидность всей цепочки для выбранного сертификата.

Для этого необходимо открыть свойства сертификата и просмотреть цепочку сертификатов (перейти на вкладку Путь сертификации) (Рис. 8.10)

Статус сертификата, выбранного из цепочки, отобразится в области Статус сертификата. Необходимо просмотреть статусы всех сертификатов цепочки.

Если в цепочке есть невалидные сертификаты – подписание документов невозможно.

Подключить ключевой носитель – Открыть Панель управления Рутокен – Сертификаты – Свойства – Путь сертификации – Выбрать сертификат из цепочки

	1
🐒 Панель управления	Рутокен Х
Администрирование	Сертификаты Настройки О программе
Подключенні 🐖 С	Сертификат
🥜 Rutoken S Общ	ие Состав Путь сертификации
Ивано Слуро-	Iуть сертификации ☐ Тестовый УЦ ООО "КРИПТО-ПРО" (УЦ 2.0) ☐ Иванов Андрей Иванович
Имя	
Иванов С te-4b35a6	
Гадельши te-da8303	
RaUser-fc0	
	Просмотр сертификата
Coo	стояние сертификата:
Эт	гот сертификат действителен.
Импортирова	OK
	Закрыть

Рис. 8.10 — Просмотр статуса сертификата из цепочки сертификатов

8.6.2 Просмотреть список сертификатов ПК

Для просмотра списка установленных сертификатов нужно открыть список персональных сертификатов, выполнить следующие действия (Рис. 8.11):

Панель управления – Сеть и интернет – Свойства браузера – Содержание – Сертификаты – Личные + Доверенные корневые центры сертификации + Доверенные издатели

В хранилище Личные – должен быть только один сертификат пользователя, соответствующий сертификату на ключевом носителе

В хранилищах Доверенные корневые центры сертификации + Доверенные издатели – должны быть корневые сертификаты, соответствующие корневым сертификатам (наивысший в цепочке сертификатов) на ключевом носителе

В хранилище Издатели, не имеющие доверия – не должно быть сертификатов, входящих в состав цепочки ключевого носителя. В случае отсутствия в хранилище корневых сертификатов, их нужно дополнительно установить из ключевого носителя.



Рис. 8.11 — Просмотр списка установленных персональных сертификатов

8.6.3 Проверить подписание документов на сайте CryptoPro по ссылке

Проверка создания электронной подписи CAdES-BES

Для проверки нужно выполнить действия (Рис. 8.12):

Подключить ключевой носитель <u>USB ключ</u> – Открыть страницу <u>Проверка создания электронной</u> <u>подписи CAdES-BES</u> [1] – Выбрать проверяемый сертификат в области «Сертификат» [2] – Загрузить файл [3] (который не удалось подписать в АИС НГС) – Нажать кнопку «Подписать файл» [4] – Проверить результат формирования подписи [4]

Secure https://www.cryptopro.ru/sites/default/files/products/cades/demopage/cades_bes_file.htm	x 🕱 🖬
Проверка создания электронной к	∾о подписи CAdES-BES
Плагин загружен. • Версия плагина: 2.0.13027 Версия криптопровайдера: 4.0.9842 Криптопровайдер: Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider	 О КриптоПро ЭЦП Browser plug- in Инструкция по работе с плагино Скачать плагин
Сертификат:	
Сч-иванов Андреи иванович, обдан. 01.05.2017 14.14.41	Угроз не обнаружено
¥	
Информация о сертификате	
Впалепен: СN=Иванов Андрей Иванович	
Издатель: СN="Тестовый УЦ ООО ""КРИПТО-ПРО"" (УЦ 2.0)"	
Выдан: 01.09.2017 14:14:41	
Действителен до: 01.12.2017 14:24:41	
Криптопровайдер: Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider	
Алгоритм ключа: GOST R 34.10-2001	
Загрузить файл:	
Choose File Документ1.txt 3	
Подписать файл 4	
Тодпись сформирована успешно: 5	
MTTPV0Y1KoZThycNA0cCoTTPU5CCD84CA0ExDD4KBeYch0MCAekE4D4XRekohk369w8RBw5eCe0T	
MIIPYQYJKoZINvCNAQcCoIIPUJCCD04CAQEXDDAKBgYqhQYCAgkFADAXBgkqhki69w68BwGgCgQI A X07q8-z17fkgggyMMIIE3cCB16gAu1Bag1QEk1FXRJAuoDkEU3REs-037A1BgYqhQYCAgWhgesx GoAblgblqqhQrktAIIMTAthlcroubAATQQDIG20BgGCCGFAu6Base BgrwMDC3MTcVMcSCDTEXIDAe	
MIIPYQYJkoZINvCNAQcCoIIPUJCC084CAQExDDAKBgYqnQYCAgkFADAXBgkqhki69w8BbwGgCQI AD7g8-217KgggvMIIIE3cC816gAu1Bag1QEk1FXRJAudoKEU38Es-0317A1BgYqnQYCAghwgesx DohlegluqnQtkatIMITAticcucMaAITQ9DID8186gCC6FAu6Bast BgwMID23HTCWC5OTEXIDAE Bgkqnki63w9BCQEUELIJJJmSY1335cHkvCH3vLnJ1HRJub#vDVQQDA2qDLC-03HQLCyBLAXCLA3 BglvQaTA1JVSUJUFVDVQQDEChtC83JgtClcc84SBUFC0133gnCgC8J41JVvLAAVDVQQD	
NIIPVQVJKoZINvcNAQcCoIIPUjCCD04CAQEXDDAKBgYqhQVCAgKFADAXBgkqhki69w8BbwGgCgQI xO7g8-11FKgggvHVIIE3cC816gAw1BAg1QEK1FXRUAwDKEU38Es-0317A18gYqhQVCAgHwgesx SDAWBgUqhQVkARINMTAzIIzcw/DAAHTQ0NDE4NBgGCCqFAw0BAwEBgwwMDc3VTcMVDc5OTEXIDAe BgkqhkiGswBGCgEHENL3LmsN×335cHkvcHV.u.h.31HRWsWVQQCD02cqNLC=VHQutCy0LAxCaJ1 BglVBAYTAJ1VVSUNIKVVQQXDB2chtCe3Ag1tCeAKQDWCF0KLQn33Qn2cg8741MVVARAVVQQD D3QotC12VHgKt=04LR365CH(SCHVCHV.u.h.31HRWsWVQQDD2cg8741MVVARAVVQQD 03QotC12VHgKt=04LR365CH(SCHVCHVCLCLCLQntCg80)G9C1304787_00ACe11AoAKPQ 03QotC12VHgKt=04LR365CH(SCHVCHVCLCLCLQntCg80)G9C1304787_00ACe11AoAKPQ 03QotC12VHgBHDB4CGCEABAg1tCaQMCB9AUCHVCLCLQDaebawbBL00ACe11VHA	

Рис. 8.12 — Проверка подписание документов на сайте CryptoPro

8.7 Сообщение: «Сертификат недоступен или не найден закрытый ключ/Ошибка при подписи сертификатов»

- проверить вставлен ли токен;
- выполнить скрипт;
- истекла лицензия:

Для продления лицензии необходимо зайти в Пуск - Крипто-ПРО - КриптоПро CSP (Рис.8.13)



Проверяем версию продукта (должно быть 4.0....) и срок действия сертификата "Постоянная" (Рис.8.14)

Если срок действия истек (Рис.8.15), необходимо ввести серийный номер (Рис.8.16). Его можно найти в письме из банка с темой: "Важно! Прекращение работы подписи документов токеном" и датой отправки в период с 13.04 - 18.04.

🙋 КриптоПро С	SP			×		
Алгоритмы Общие	Безопасность Оборудование	Winlogon Сервис	Настройки TLS Дополнительно	ł		
	С <u>гурtoPro CSP</u> Версия продукта: 4.0.9708 Версия ядра СКЗИ: 4.0.9006 КС1					
Запустить Лицензия Серийный на	с правами администр	<u>атора</u>		1		
Владелец: Организаци:	Use R:	r L				
Срок действ Тип лицензи Первая уста	ия Постоянная и: Клиентская новка: 31.03.2016	Вво	Покупка			

Рис. 8.14 — Стурто Pro CSP. Срок действия - Постоянная

лгоритмы Бе	зопасность Winlogon Настройки TLS
Общие Обор	удование Сервис Дополнительно
СтурьоРго С © Компания Запустить с прав	Версия продукта: 4.0.9708 Версия ядра СКЗИ: 4.0.9006 КС1 КРИПТО-ПРО. Все права защищены. ами администратора
Пицензия	
Серийный номер:	CONTRACTOR CONT
Владелец:	User
Организация:	Influence in the Influe
Срок действия	Истекла Покупка
Тип лицензии:	Серверная
Первая установка:	31.03.2016 Ввод лицензии
риптоПро CSP	l un hour à un comme
риптоцро ССР Алгоритмы Бе Общие Обор С <u>ryptoPro CS</u> © Компания	зопасность Winlogon Настройки TLS кудование Сервис Дополнительно Версия продукта: 4.0.9708 Версия ядра СКЗИ: 4.0.9006 КС1 КРИПТО-ПРО, Все права защищены.
Стурного ССР Алгоритмы Бе Общие Обор СтурноРго СС С Компания Запустить с прав	зопасность Winlogon Настройки TLS удование Сервис Дополнительно В Версия продукта: 4.0.9708 Версия ядра СКЗИ: 4.0.9006 КС1 КРИПТО-ПРО. Все права защищены. ами администратора
риптоцро ССР Алгоритмы Бе Общие Обор СтуртоРго СС С Компания Запустить с прав	зопасность Winlogon Настройки TLS кудование Сервис Дополнительно В Версия продукта: 4.0.9708 Версия ядра СКЗИ: 4.0.9006 КС1 КРИПТО-ПРО. Все права защищены. ами администратора
риптоПро ССР Алгоритмы Бе Общие Обор СтурtоPro СС СтурtоPro СС С Компания Запустить с прав Лицензия Серийный номер:	зопасность Winlogon Настройки TLS удование Сервис Дополнительно В Версия продукта: 4.0.9708 Версия ядра СКЗИ: 4.0.9006 КС1 КРИПТО-ПРО. Все права защищены. ами администратора
риптоцро ССР Алгоритмы Бе Общие Обор СтурtоPro СС © Компания Запустить с прав Лицензия Серийный номер: Владелец:	езопасность Winlogon Настройки TLS кудование Сервис Дополнительно 29 Версия продукта: 4.0.9708 Версия ядра СКЗИ: 4.0.9006 КС1 КРИПТО-ПРО. Все права защищены. ами администратора User
риптоцро ССР Алгоритмы Бе Общие Обор СтурtоPro СС СтурtоPro СС С Компания Запустить с прав Лицензия Серийный номер: Владелец: Организация:	зопасность Winlogon Настройки TLS удование Сервис Дополнительно В Версия продукта: 4.0.9708 Версия ядра СКЗИ: 4.0.9006 КС1 КРИПТО-ПРО. Все права защищены. ами администратора
риптоцро ССР Алгоритмы Бе Общие Обор СтурtоPro СС С Компания Запустить с прав Лицензия Серийный номер: Владелец: Организация: Срок действия	зопасность Winlogon Настройки TLS кудование Сервис Дополнительно P Версия продукта: 4.0.9708 Версия ядра СКЗИ: 4.0.9006 КС1 КРИПТО-ПРО. Все права защищены. ами администратора User Истекла Покупка
риптоцро ССР Алгоритмы Бе Общие Обор СтурtоPro СС СтурtоPro СС С Компания Запустить с прав Лицензия Серийный номер: Владелец: Организация: Срок действия Тип лицензии:	езопасность Winlogon Настройки TLS кудование Сервис Дополнительно Версия продукта: 4.0.9708 Версия ядра СКЗИ: 4.0.9006 КС1 КРИПТО-ПРО. Все права защищены. ами администратора User Истекла Покупка Серверная

Please enter your personal information.

User Name:	
i Ser	
Organization:	
Raffeserbark	
Serial Number:	
East to be a second	
Input serial number from the license agreement.	
	ОК

Рис. 8.16 — Стурто Pro CSP. Ввод серийного номера

8.7 Ошибка «Данный сертификат не содержит все обязательные параметры».

Данная ошибка (Рис.8.17) отображается пользователю при регистрации на портале АИС НГС, если в сертификате не указаны все необходимые параметры.



Рис. 8.17 — Ошибка: Данный сертификат не содержит все обязательные параметры

Для устранения ошибки, необходимо проверить наличие обязательных параметров сертификата УКЭП пользователя, которые перечислены в разделе №7 <u>«Требования к составу и содержанию обязательных параметров сертификата УКЭП»</u> данного документа.

В случае несоответствия требованиям сертификата УКЭП, необходимо обратиться в Удостоверяющий Центр, издавшего сертификат УКЭП и запросить корректные данные.