

ООО «КРИПТО-ПРО»

Аннотация

Настоящая инструкция предназначена для Пользователей сервиса электронной подписи ООО «КРИПТО-ПРО» на базе ПАКМ "КриптоПро HSM" (далее – СЭП) и определяет порядок использования Веб-интерфейса СЭП для осуществления операций по доступу и управлению сертификатами ключей проверки электронной подписи, созданию и проверке электронной подписи, шифрованию и расшифрованию электронных документов.

Информация о разработчике ПАКМ "КриптоПро HSM":

OOO «КРИПТО-ПРО» 127018, Москва, ул. Сущевский вал, 18 Телефон: (495) 995 4820 <u>http://www.CryptoPro.ru</u> <u>https://saas.cryptopro.ru/cryptoproidp/Users</u> E-mail: info@CryptoPro.ru

Содержание

Аннотация	2
Информация о разработчике ПАКМ "КриптоПро HSM":	2
1. Общие положения	5
1.1. Требования и подготовка рабочего места Пользователя	5
1.1.1. Настройка Internet Explorer	5
1.1.2. Настройка Яндекс-браузера	7
1.2. Первый вход в СЭП (аутентификация по паролю)	7
2. Настройка аутентификации	8
2.1. Настройка аутентификации по логину/паролю	8
2.2. Настройка аутентификации по сертификату	9
2.3. Настройка аутентификации с помощью мобильного приложения	10
2.4. Настройка доступа к операциям СЭП	15
3. Вход в веб-интерфейс СЭП	15
3.1. Вход в веб-интерфейс СЭП (аутентификация по паролю)	16
3.2. Вход в веб-интерфейс СЭП (аутентификация по сертификату)	17
3.3. Вторичная аутентификация	17
4. Меню интерфейса Пользователя СЭП	19
4.1. Раздел «Подписать»	19
4.2. Раздел «Усовершенствовать подпись»	23
4.3. Раздел «Зашифровать»	25
4.4. Раздел «Расшифровать»	26
4.5. Раздел «Проверить подпись»	27
4.6. Раздел «Проверить сертификат»	28
4.7. Раздел «Сертификаты»	29
4.7.1. Создание запроса на сертификат	30
4.7.2. Загрузка ключей из pfx	33
4.8. Раздел «Аудит»	34
5. Экспорт ключа электронной подписи и сертификата ключа проверки	
электронной подписи	34
5.1. OC Windows	34
5.2. OC Linux	37

5.3. OC macOS	
6. Использование «облачного» токена в СКЗИ «КриптоПро CSP 5.0»	
7. Работа с порталами органов государственной власти	
7.1. Установка КриптоПро ЭЦП Browser plug-in	
7.2. Работа с порталом nalog.ru	
7.3. Работа с порталом www.gosuslugi.ru	
8. Интеграция СЭП с использованием методов REST API	
9. Безопасность при работе в СЭП	
10. Перечень рисунков	50

1. Общие положения

Сервис электронной подписи ООО «КРИПТО-ПРО» на базе ПАКМ "КриптоПро HSM" версии 2.0 (далее – СЭП) предназначен для создания и хранения ключей электронной подписи, выполнения операций по созданию и проверке электронной подписи различного формата криптографических сообщений, шифрования и расшифрования электронных документов.

Настоящая инструкция определяет порядок действия Пользователя СЭП (далее – Пользователь) при выполнении операций формирования, усовершенствования и проверки электронной подписи, шифрования и расшифрования электронных документов.

1.1. Требования и подготовка рабочего места Пользователя

На рабочем месте Оператора под управлением MS Windows 7 или выше, macOS версии 10.10 и выше, *Unix-системы (совместимые OC см. формуляр СКЗИ Криптопро CSP ЖТЯИ.00087-03 30 01) должен быть установлен СКЗИ «КриптоПро CSP» версии 4.0 или выше. Для подключения к СЭП необходимо использовать Интернет-браузер с поддержкой ГОСТ-TLS: Яндекс-браузер, Chromium-GOST, Internet Explorer. Для использования модуля Cloud необходимо установить СКЗИ «КриптоПро CSP» версии 5.0.

1.1.1. Настройка Internet Explorer

Для корректной работы с СЭП необходимо добавить адрес в доверенные сайты в настройках браузера. Для этого в свойствах браузера выбрать вкладку «*Безопасность*», в список надежных сайтов добавить узел <u>https://saas.cryptopro.ru/</u>и сохранить изменения свойств (см. Рисунок 1 – Добавление сайта в зону надежных сайтов).

зойства браузера ? × Содержание Полключения Поогранны Дополнительно Общие Безопасность Конфиденциальность 2	~ ≙ С Пои	ск	۰ م	
Выберите зону для параметры на параматоря безопасности. интернет интерн		Настройка	Завести почту	Почта
Надежные сайты Зона для надежных сайтов, которые не приченят вреда вашених колтыотеру или данным. В этой зоне есть веб-сайты.	Надежные сайты Х		Пароль	?
Уровень безопасности для этой зоны Разрешенные уровни: любые - Средний - Запрос перед окачиванием опасного содерживого - Капортигивные запечиты Астич и социального	Вы можете добавлять в эту зону веб-сайты и удалять их из нее. Заданные для зоны паранетры безопасности будут использоваться для всех ее сайтов.		B f ¥ …	Войти
	Добавить в зону следующий узел: https://saas.cryptopro.ru/ Добавить			
Включить защищенный режим (потребуется перезапуск	Веб-сайты: 5	1		
Internet Explorer) Другой По унолчанию	https://www.cryptopro.ru	H	айти	
Выбрать уровень безопасности по умолчанию для всех зон		Y Скачайте Яндекс Бр	раузер	
	Для всех сайтов этой зоны требуется проверка серверов (https:)			
ОК Отнена Применить	Закрыть			

Рисунок 1 – Добавление сайта в зону надежных сайтов

В разделе "Элементы ActiveX и модуль подключения" проверить состояние настройки "Использование элементов управления ActiveX, не помеченных как безопасные для использования" - должно быть "Включить" (см. Рисунок 2 – Включение ActiveX). Для этого зайти в Internet Explorer меню «Сервис» - «Свойства обозревателя» – «Безопасность» - для зоны "Надежные узлы" нажать кнопку "Другой".

Параметры	Параметры
Предлагать Запуск элементов АсtiveX и модулей подключения Включить Отключить Предлагать Запускать антивредоносное ПО для элементов управления Включить Отключить Отключить Отключить Предлагать Поредлагать Поредлагать Поредлагать Попинамые з лементов управления ActiveX, не помечени Поредлагать Попинамые з лементов управления ActiveX, не помечени Попинамые з лементов управления ActiveX, не помечени Октоке и помена и и и и и и и и и и и и и и и и и и и	Предлагать Запуск элементов АсtiveX и модулей подключения Эключить Допущенных администратором Отключить Предлагать Запускать антивредоносное ПО для элементов управления Включить Отключить Отключить Предлагать Поведение злементов управления ActiveX, не помечени Включить Предлагать Поведение двоичного кодов и сценариев Включить Полинации запиванистовтором Использование запиванистов тором Использование запиванистов тором Использование запивание после перезапуска компьютера Сброс особых параметров На уровень: Средний (по умолчанию) ОК Отмена

Рисунок 2 – Включение ActiveX

1.1.2. Настройка Яндекс-браузера

Перейдите в «Настройки» - «Системные».

Убедитесь, что в разделе «Сеть» включена опция «Подключаться к сайтам,

использующим шифрование по ГОСТ. Требуется КриптоПро СЅР».



Рисунок 3 – Включение поддержки ГОСТ

1.2. Первый вход в СЭП (аутентификация по паролю)

Оператор СЭП после регистрации Пользователя выдает ему логин и пароль для входа.

Для работы в СЭП Пользователю требуется осуществить вход в веб-интерфейс Пользователя по адресу <u>https://saas.cryptopro.ru/cryptopro</u>

В окне аутентификации введите логин Пользователя, полученный от Оператора СЭП, и нажмите кнопку «Далее» (см. Рисунок 4 - Вход в СЭП. Окно ввода учётной записи)

КРИПТОПРО
Вход в
Веб-интерфейс Сервиса подписи
Ivanov
Далее
Ц Чужой компьютер
Вход по сертификату

Рисунок 4 - Вход в СЭП. Окно ввода учётной записи

Если имя учётной записи введено верно, появится форма для ввода пароля, выданного Пользователю Оператором СЭП при регистрации (см. Рисунок 5 - Вход в СЭП).

КРИПТОПРО
Вход в
Веб-интерфейс Сервиса подписи
К Иванов Иван Иванович
•••••
Войти
Запомнить пароль

Рисунок 5 - Вход в СЭП

2. Настройка аутентификации

Для редактирования параметров настроек аутентификации СЭП Пользователю требуется осуществить вход в веб-интерфейс Пользователя по адресу <u>https://saas.cryptopro.ru/cryptoproidp/Users</u>.

2.1. Настройка аутентификации по логину/паролю.

Для настройки аутентификации Пользователя по логину и паролю необходимо в группе «Методы вторичной аутентификации» раскрыть блок «*Аутентификация по паролю*» и нажать кнопку «*Изменить*». Новый пароль отобразится на экране (см. Рисунок 6 - Изменение пароля).



Рисунок 6 - Изменение пароля

2.2. Настройка аутентификации по сертификату

Для настройки первичной аутентификации пользователя по сертификату необходимо импортировать компоненты имени Пользователя из существующего сертификата с расширением *.cer/*.crt по кнопке «Заполнить компоненты имени из сертификата» (см. Ошибка! Источник ссылки не найден.).

Аутентификация по сертификату 👻	
Различительное имя субъекта: "G=Ivanov"	
🕼 Заполнить компоненты имени из сертификата	

Рисунок 7 - Загрузка сертификата

Для экспорта сертификата с расширением *.cer/*.crt/*.p7b откройте Криптопро CSP – «*Сервис*» - «*Просмотреть сертификаты в контейнере*» - «*Обзор*» выберите нужный контейнер и нажмите «*Далее*»

езопасность Winlogon Настройки TLS Криптопровайдеры Бщие Оборудование Сервис Дополнительно Алгоритмы	Контейнер закрытого ключа Введите или укажите контейнер закрытого ключа для просмотра сертификатов в этом контейнере
Контейнер закрытого ключа Эти мастера позволяют протестировать, скопировать или удалить контейнер закрытого ключа с носителя. Протестировать Удалить	
Сертификаты в контейнере закрытого ключа	Имя ключевого контейнера:
Этот мастер позволяет просмотреть сертификаты, находящиеся	Обзор
в контейнере закрытого ключа, и установить их в хранилище сертификатов.	
Просмотреть сертификаты в контейнере	Введенное имя задает ключевой контейнер: По сертификату
	О Компьютера
Личный сертификат	
контейнером закрытого ключа, установив этот сертификат в хранилище.	Выберите CSP для поиска ключевых контейнеров:
Установить личный сертификат	Все поддерживаемые криптопровайдеры 🗸
Пароли закрытых ключей	4
Эти мастера позволяют изменить пароли (ПИН-коды) закрытых ключей или удалить запомненные ранее пароли.	< Назад Далее > Отмена
Изменить пароль Удалить запомненные пароли	

Рисунок 8 - Импорт сертификата через КриптоПро CSP

В открывшемся окне сертификата нажмите кнопку «Свойства», перейдите во вкладку «Состав» и нажмите «Копировать в файл» (см. Рисунок 9 - Экспорт сертификата)



Рисунок 9 - Экспорт сертификата

На следующем шаге выберете «Нет, не экспортировать закрытый ключ».

Далее следуйте указаниям мастера импорта сертификатов, на этапе выбора места сохранения файла укажите удобную директорию и имя файла.

Сертификат должен быть установлен локально на компьютере пользователя, и требуется обеспечить доверие к данному сертификату со стороны сервера СЭП. Для этого отправьте цепочку сертификатов (выгруженный по инструкции сертификат в формате p7b) издателя на почту operdss@cryptopro.ru в формате zip/rar.

2.3. Настройка аутентификации с помощью мобильного приложения

Для настройки вторичной аутентификации Пользователя с помощью мобильного приложения «DSS Client» в группе «Методы вторичной аутентификации» раскройте блок «Аутентификация с помощью мобильного приложения» и нажмите кнопку «Добавить устройство» (см. Рисунок 10 - Аутентификация с помощью мобильного приложения).



Рисунок 10 - Аутентификация с помощью мобильного приложения

Выберите способ отправки кода активации и отсканировать QR-код в мобильном приложении (см. Рисунок 11 - QR-код для DSS Client).



Рисунок 11 - QR-код для DSS Client

Для обеспечения работоспособности вторичной аутентификации с помощью мобильного приложения Пользователю необходимо установить мобильное приложение «DSS Client» из магазина <u>Google Play</u>, <u>Apple App Store</u>, <u>AppGallery</u>.

В мобильном приложении выберите способ привязки «через QR-код» и введите имя учетной записи.

При первом запуске мобильное приложение запросит разрешение на отправку уведомлений и установку способа защиты приложения (см. Рисунок 12 - Первый запуск мобильного приложения).



Рисунок 12 - Первый запуск мобильного приложения

На следующем шаге мобильное приложение попросит отсканировать QR-код. Как только QR-код будет успешно отсканирован, Пользователь должен ввести полученный им ранее при регистрации код активации (см. Рисунок 13 - Регистрация учетной записи в DSS Client).



Рисунок 13 - Регистрация учетной записи в DSS Client

После ввода кода активации выберите способ защиты Вашей учетной записи и нажмите кнопку «Применить». Если Вы выбрали пункт «ПИН-код / Face ID», придумайте и введите в следующем окне ПИН-код. Данный ПИН-код необходимо будет вводить в дальнейшем при подтверждении операций, создании запросов на сертификаты, добавлении новых устройств и других действий, требующих аутентификации. Нажмите кнопку «Подтвердить». Если ранее в приложении не использовалась биометрия (например, при задании кода-пароля защиты приложения), разрешите приложению использовать биометрические данные (отпечаток пальца или скан формы лица). Биометрия может заменять ввод ПИНкода при подтверждении операций и прочих действий, требующих аутентификации (см. Рисунок 14 - Защита мобильного приложения).

16:29 7	16:30 -7 ап ≑ ■) Введите новый пароль	16:30 4
Выберите способ защиты учётной записи	Введите пароль для использования в случае ошибки TouchID	
ПИН-код / TouchID / FaceID	1 1	
Без ПИН-кода		
	1 1	
	Пароль	
	Полтвержление пароля	Хотите разрешить «КриптоПро DSS Client» использовать Face ID? Идентификация пользователя
		Запретить Разрешить
	I I	
	I I	
	I I	
	I I	
Применить	Подтвердить	

Рисунок 14 - Защита мобильного приложения

На экране мобильного устройства отобразится информация о Вашей учетной записи. Если данные верны, нажмите кнопку «Подтвердить», после чего привязка устройства будет завершена и его можно будет использовать для подтверждения подписи документов. В случае если данные не верны, следует отказаться от подтверждения привязки учетной записи и обратиться к Оператору. Если данные учётной записи верны, и Вы подтвердили привязку, на экране отобразится соответствующее информационное уведомление. Для перехода к подписи документов и подтверждению операций нажмите кнопку "Ок". Статус учетной записи в меню «Настройки» – «Учетные записи» изменится на «Используется по умолчанию» или «Активный», если Ваше мобильное устройство ранее уже привязывалось к другим учетным записям (см. Рисунок 15 - Информация об учетной записи пользователя).



Рисунок 15 - Информация об учетной записи пользователя

2.4. Настройка доступа к операциям СЭП

После успешной настройки параметров аутентификации Пользователя необходимо определить операции, которые Пользователь должен подтверждать выбранным методом вторичной аутентификации.

Можно настроить доступ к следующим операциям в СЭП:

- Подпись документа
- Шифрование/расшифрование документа
- Удаление сертификата
- Смена ПИН-кода закрытого ключа
- Создание запроса на сертификат

3. Вход в веб-интерфейс СЭП

Аутентификация Пользователя в СЭП происходит с использованием методов первичной и вторичной аутентификации в СЭП. Оператор СЭП назначает Пользователю как минимум один метод первичной аутентификации и как минимум один метод вторичной аутентификации. Заданные методы первичной и вторичной

аутентификации, а также перечень операций, подтверждаемых Пользователем с их помощью, сообщаются Пользователю Оператором СЭП, выполняющим регистрацию Пользователя в СЭП.

Возможные методы первичной аутентификации Пользователя:

• «Аутентификация по сертификату» – первичная аутентификация Пользователя происходит по сертификату, предоставленному Пользователем Оператору СЭП.

• «Аутентификация по паролю» – первичная аутентификация Пользователя происходит по паролю, выданному Пользователю Оператором СЭП.

Возможные методы вторичной аутентификации Пользователя:

•«Аутентификация с помощью мобильного приложения» – вторичная аутентификация Пользователя происходит в мобильном приложении DSS Client.

3.1. Вход в веб-интерфейс СЭП (аутентификация по паролю)

В случае если Оператором СЭП определен метод первичной аутентификации «*Аутентификация по паролю*», Пользователю необходимо ввести имя учётной записи (логин) в поле ввода и нажать кнопку «*Далее*» (см. Рисунок 16 - Вход в СЭП. Окно ввода учётной записи).

Для работы в СЭП Пользователю требуется осуществить вход в веб-интерфейс Пользователя по адресу <u>https://saas.cryptopro.ru/cryptopro</u>



Рисунок 16 - Вход в СЭП. Окно ввода учётной записи

Если имя учётной записи введено верно, появится форма для ввода пароля, выданного Пользователю Оператором СЭП при регистрации (см. Рисунок 17 - Вход в СЭП).

Вход в Вкод в Веб-интерфейс Сервиса подписи
🗲 Иванов Иван Иванович
•••••
Войти Запомнить пароль

Рисунок 17 - Вход в СЭП

3.2. Вход в веб-интерфейс СЭП (аутентификация по сертификату)

В случае если определен метод первичной аутентификации «Аутентификация по сертификату», Пользователю необходимо осуществить вход в веб-интерфейс Пользователя по адресу <u>https://saas.cryptopro.ru/cryptopro</u>, после чего выбрать «*Bxod no сертификату*» (см. Рисунок 18 – Вход по сертификату).

В появившемся окне подтверждения сертификата выбрать сертификат Пользователя и нажать кнопку «*ОК*».

	КРИПТОПРО	
	Вход в	
	SignServer	
Логин		
	Далее	
🗌 Чужой к	омпьютер	
	Вход по сертификату	
	вход по сертификату	

Рисунок 18 – Вход по сертификату

3.3. Вторичная аутентификация

Если Пользователю СЭП включено подтверждение операции входа в вебинтерфейс при помощи метода вторичной аутентификации – «Аутентификация с *помощью мобильного приложения*», Пользователь должен подтвердить операцию входа в мобильном приложении «DSS Client».

При необходимости подтверждения операции с помощью мобильного приложения DSS Client СЭП выдаст соответствующий запрос (см. Рисунок 19 - Запрос аутентификации с помощью мобильного приложения DSS Client).



Рисунок 19 - Запрос аутентификации с помощью мобильного приложения DSS Client

После получения PUSH-уведомления о подтверждении операции в мобильном приложении DSS Client выбрать операцию для подтверждения и нажать на нее.

В открывшемся окне просмотрите следующие параметры операции, полученные с сервера:

• Учётная запись. Убедитесь, что подтверждаете операцию для нужной учетной записи.

• Идентификатор сессии. Убедитесь, что идентификаторы в веб-интерфейсе и в мобильном приложении совпадают.

В случае успешного подтверждения операции в мобильном приложении появится уведомление "*Операция успешно подтверждена*" (см. Рисунок 20 - Подтверждение операции). Для продолжения работы с приложением нажмите на произвольной области экрана.



Рисунок 20 - Подтверждение операции

4. Меню web-интерфейса Пользователя СЭП

В меню web-интерфейса Пользователя доступны 8 разделов:

- Подписать
- Усовершенствовать подпись
- Зашифровать
- Расшифровать
- Проверить подпись
- Проверить сертификат
- Сертификаты
- Аудит

4.1. Раздел «Подписать»

Раздел предназначен для формирования электронной подписи электронных документов Пользователя. Для того, чтобы Пользователь мог подписывать

электронные документы, ему необходимо иметь хотя бы один действующий сертификат в СЭП.

Для формирования электронной подписи электронного документа перейдите в раздел «*Подписать*» и выполните следующие действия:

1) Загрузите электронный документ, который требуется подписать, в СЭП, нажав кнопку «*Выбрать*» в секции «*Документ*».

2) Выберите нужный формат электронной подписи в секции «Формат подписи».

3) Выберите параметры электронной подписи в секции «Параметры подписи».

- 4) Выберите нужный сертификат Пользователя в секции «Сертификат».
- 5) Нажмите кнопку «Подписать»
- 6) Подтвердите операцию выполнения подписи в мобильном приложении DSS Client.

7) Документ будет загружен после подтверждения (см. Рисунок 21 - Документ успешно подписан).

		🛔 testovii 👻
KPUITION PO	Сервер электронной подписи КриптоПро DSS	
Подписать	Создание подписи	Подписать
Усовершенствовать подпись	• Документ успешно подписан	
Зашифровать		
Расшифровать	Документ • Не задан	
Проверить подпись	Документ будет отправлен на сервер.	
Проверить сертификат	Выбрать	
Сертификаты	Получить исходный документ	
Аудит	Формат подписи - Электронная подпись в формате CMS	
	Параметры подписи - Отделённая Подпись данных	
	Сертификат - CN=test	
temp.txt.sig		Показать все

Рисунок 21 - Документ успешно подписан

Подтверждение операции подписи с помощью мобильного приложения

Если для Пользователя СЭП включено подтверждение операции подписи при помощи мобильного приложения, Пользователь должен подтвердить операцию подписи в мобильном приложении «DSS Client». При необходимости подтверждения операции с помощью мобильного приложения DSS Client СЭП выдаст соответствующий запрос (см. Рисунок 22 - Подтверждение операции подписи)



Рисунок 22 - Подтверждение операции подписи

После получения PUSH-уведомления о подтверждении операции в мобильном приложении DSS Client выберете операцию для подтверждения, нажав на нее.

В открывшемся окне просмотрите следующие параметры операции, полученные с сервера:

• Учётная запись. Убедитесь, что подтверждаете операцию для нужной учетной записи.

Сертификат. Убедитесь, что выбран верный сертификат, используемый при подписи документа.

•Сервер. Данный параметр заполняется автоматически и содержит адрес сервера, на котором производится подпись.

•Скачать документы. Переведите данный переключатель в активное положение, если требуется использовать офлайн-режим.

После того как Вы просмотрели все параметры операции, нажмите кнопку "Подтвердить" (см. Рисунок 23 - Информация об операции).



Рисунок 23 - Информация об операции

В открывшемся окне отобразится список документов, подпись которых требуется подтвердить. Ознакомьтесь с подписываемым документом(ами). После того как Вы ознакомились с документом, вернитесь назад и нажмите кнопку "Подтвердить". Если операцию необходимо отменить, нажмите кнопку "Отказаться". В случае успешного подтверждения операции документ будет подписан. В мобильном приложении появится уведомление "Операция успешно подтверждена" (см. Рисунок 24 - Подтверждение операции подписи). Для продолжения работы с приложением нажмите на произвольной области экрана.



Рисунок 24 - Подтверждение операции подписи

4.2. Раздел «Усовершенствовать подпись»

Раздел предназначен для усовершенствования (дополнения) электронной подписи документа до формата усовершенствованной электронной подписи: CAdES-T (добавление штампа времени к электронной подписи), CAdES-XLT1 (добавление статуса сертификата на момент подписания и штампа времени).

Для усовершенствования электронной подписи электронного документа необходимо перейти в раздел «Усовершенствовать» и выполнить следующие действия:

1) Загрузить файл подписи, которую необходимо усовершенствовать, в СЭП, нажав кнопку «*Обзор*» в секции «*Документ*».

2) Выбрать параметры электронной подписи в секции «*Параметры подписи*», экземпляр службы штампов времени (TSP).

3) Установить флажок «Удалить имеющиеся доказательства подлинности», в случае если есть необходимость удалить из подписи существующие штампы времени/статусы сертификатов.

4) Нажать кнопку «*Усовершенствовать*» (см. Рисунок 25 - Формирование усовершенствованной подписи).

5) Загрузить полученную усовершенствованную электронную подпись (см. Рисунок 26 - Загрузка файла усовершенствованной подписи документа).

	👗 testovii 👻			
KPUITIOI IPO	Сервер электронной подписи КриптоПро DSS			
Подписать	Усовершенствование подписи Усовершенствовать			
Усовершенствовать подпись	Документ			
Зашифровать	tauh wraid (swn)			
Расшифровать	Документ будет отправлен на сервер.			
Проверить подпись				
Проверить сертификат	Параметры подписи - Присоединенная			
Сертификаты	CAdES XLT1			
Аудит	Адрес TSP службы: http://testca2012.cryptopro.ru/tsp/tsp.srf			
	 В Присоединённая Отделённая САdES T САdES XLT1 Адрес службы штампов времени [tsp ▼ Удалить имеющиеся доказательства подписи 			

Рисунок 25 - Формирование усовершенствованной подписи

		🛔 testovii 👻
KPUITIOI IPO	Сервер электронной подписи КриптоПро DSS	
Подписать	Усовершенствование подписи	Усовершенствовать
Усовершенствовать подпись	• Документ успешно дополнен до усовершенствованной подписи	
Зашифровать		
Расшифровать	Документ 🔺 Не задан	
Проверить подпись	Документ будет отправлен на сервер.	
Проверить сертификат	Выбрать	
Сертификаты		
Аудит	Параметры подписи + Присоединённая CAdES T Адрес TSP службы: http://testca2012.cryptopro.ru/tsp/tsp.srf	
		Последние действия
temp.txt (1).sig		Показать все Х
temp.txt (1).sig		Последние действия ООО "Иринато проз Ф 2022 Показать все

Рисунок 26 - Загрузка файла усовершенствованной подписи документа

4.3. Раздел «Зашифровать»

Раздел предназначен для адресного шифрования электронных документов. Для шифрования нужен файл электронного документа и сертификат/сертификаты адресата/адресатов.

Для адресного шифрования электронного документа необходимо перейти в раздел «Зашифровать» и выполнить следующие действия:

1) Загрузить файл электронного документа, который требуется зашифровать, в СЭП, нажав кнопку «*Обзор*» в секции «*Документ*».

2) Загрузить сертификат/сертификаты адресата/адресатов, для которого/которых будет шифроваться электронный документ, в СЭП, нажав кнопку «*Обзор*» в секции «*Сертификаты получателей*».

3) Нажать кнопку «Зашифровать» (см. Рисунок 27 - Параметры шифрования).

	🛔 testovii 👻
KPUITIOI IPO	Сервер электронной подписи КриптоПро DSS
Подписать	Шифрование документа Зашифровать
Усовершенствовать подпись	Документ ▼
Зашифровать	temp.txt (1).sig (14AD)
Расшифровать	Формат шифрования. ▲ СМS шифрование (CMS Enveloped data)
Проверить подпись	СМЅ шифрование (CMS Enveloped data)
Проверить сертификат	○ XML шифрование (доступно только для сертификатов из файлов и из хранилища сертификатов)
Сертификаты	□ Документ ФСС □ Документ закодирован в Base64
Аудит	

Рисунок 27 - Параметры шифрования

4) Загрузить полученный зашифрованный электронный документ (см. Рисунок 28 -Шифрование электронного документа).

	🛔 testovii 🗸	
КРИПТОПРО	Сервер электронной подписи КриптоПро DSS	
Подписать	Шифрование документа Зашифровать	
Усовершенствовать подпись	• Документ успешно зашифрован	
Зашифровать		
Расшифровать	Документ • Не задан	
Проверить подпись	Документ будет отправлен на сервер.	
Проверить сертификат	Выбрать	
Сертификаты		
Аудит	Формат шифрования • СМS шифрование (CMS Enveloped data)	
	Сертификаты получателей -	
	Последние действии	1
	ດດດ. "ທຸກສາກາ ກາດາ" ຄ.ລາ.	12
temp.txt.sig.enc	Показать все	×

Рисунок 28 -Шифрование электронного документа

4.4. Раздел «Расшифровать»

Раздел предназначен для расшифрования электронных документов, зашифрованных для Пользователя. Для расшифрования электронного документа нужен зашифрованный файл электронного документа. 26

Для расшифрования электронного документа необходимо перейти в раздел «*Расшифровать*» и выполнить следующие действия:

1) Загрузить зашифрованный для Пользователя файл электронного документа, который требуется расшифровать, в СЭП, нажав кнопку «*Обзор*» в секции «*Документ*».

2) В поле сертификат автоматически будет отображён сертификат Пользователя, для которого зашифрован электронный документ.

3) Нажать кнопку «*Расшифровать*». (см. Рисунок 29 - Расшифрование электронного документа).

4) Загрузить расшифрованный электронный документ.

Сервер электронной подписи КриптоПро DSS				
Расшифрование документа				Расшифровате
Документ • Новый+текстовый+документ.td. enc (515Б)				
Документ будет отправлен на сервер.				
Новый+текстовый+документ.txt.enc	Изменить	Убрать		
Сертификат - Имя субъекта: С№Иванов Иван Иванович, С=RU, S=77 г. Москва, L=Москва, CDE7D0F921CC4A2A1B585FF37469526C81C4D568	0="000 ""КРИ	110-NPO-	, OU=Oтдел безопасности систем, T=Cneциалист по информационной безопасности, E=Inf@cryptopro.ru, Orneчаток :	

Рисунок 29 - Расшифрование электронного документа

4.5. Раздел «Проверить подпись»

Раздел предназначен для проверки подписи электронных документов. Для проверки подписи электронного документа нужен файл подписи электронного документа (для отсоединённой подписи).

Для проверки подписи электронного документа необходимо перейти в раздел «Проверить подпись» и выполнить следующие действия:

1) Загрузить файл подписи электронного документа в СЭП, нажав кнопку «*Обзор*» в секции «*Документ* для проверки».

2) Формат подписи будет определён автоматически.

3) В секции «*Параметры*» указать параметры подписи (присоединённая, подпись данных/подпись хэш-функции).

4) Для отсоединённой подписи загрузить файл электронного документа в СЭП, нажав кнопку «*Обзор*» в секции «*Исходный документ*».

5) Нажать кнопку «*Проверить*» (см. Рисунок 30 - Проверка подписи электронного документа).

6) Для присоединенной подписи также будет доступна кнопка «*Снять и проверить*», которая позволит получить исходный документ при корректной прохождении проверки.

7) Получить результат проверки подписи (см. Рисунок 31 - Результат проверки подписи).

← https://www.justsign.me	ryptopro/Veify/	- ≜ С Поиск	- D P・ 品 ☆ 隠
Сервер электронной подп × С	Center Spectrowing Romany KountoRoo DSS		🛔 Иванов Иван Иванович 👻
Подписать	Проверка подписи		Проверить
Усовершенствовать подпись	Документ для проверки ≁ Пезентация1 lies sis (14КБ)		
Зашифровать	Определён формат подписы: Подпись в формате CMS		
Расшифровать			
Проверить подпись	Формат подписи + Подпись в формате CMS		
Сертификаты	Параметры -		
Аудит	Отсоединізная подпись		
	Исходный документ - Презентацият (pg (38КБ)		
	🔓 Презентация1.jpg Изменить Убрать		

Рисунок 30 - Проверка подписи электронного документа

С Серер электронной подл., ×	yptopro/Verify/	- 📾 d) Tewc)☆®(
КРИПТОПРО	Сервер электронной подп	▲ Иеанов Иеан Иеа	840884 -
Подписать	Результат проверки		
Усовершенствовать подпись	Название документа	Tpeserrayert jøg sig	
Зашифровать	подпись т		
Расшифровать	Результат проверки	Подпись, денствительна	
Проверить подлись	Дополнительная информация	Отсулствует	
Проверить сертификат	Дополнительная информация о подписи		
Сертификаты	Формат	Dontaria a divoluate XI T1	
Аудит	подписи СА	ES	
	Время подля полученное штампа	кси, 05.04.2019.15.03.01 из	
	Время подля	кси 05.04.2019.15.03.00	
	Информация о сертификате		
	Субъект	СN=Иванов Иван Иванович, C=RU, S=77 г. Мосява, L=Mocява, O="000 "КРИПТО-ПР0"", CU=0тдел безопасности систем, T=Слециалист по информационной безопасности, E=Ist@cryptopro па	
	Издатель	CN+914 KPMITIC-TIPO (FOCT 2012), O+**000 "KPMITIC-TIPO"", L+Moceaa, S+Moceaa, C+RU, E+repca@cryptopro.ru	
	Серийный номер	014127A5000FAA2C8546EE8433DD63B968	
	Срок действ	ия 13.03.2019 12:51:19 - 13.03.2024 13.01:19	
	Отпечаток сертификата	CDE7D0F921CC4A2A18585FF37469528CB1C4D568	

Рисунок 31 - Результат проверки подписи

4.6. Раздел «Проверить сертификат»

Раздел предназначен для проверки статуса сертификатов. Для проверки статуса сертификата нужен файл сертификата.

Для проверки статуса сертификата необходимо перейти в раздел «*Проверить сертификат*» и выполнить следующие действия:

1) Загрузить файл сертификата в СЭП, нажав кнопку «Обзор» в секции «Файл сертификата».

2) Нажать кнопку «Проверить» (см. Рисунок 32 - Проверка статуса сертификата).

Получить результат проверки статуса сертификата (см. Рисунок 33 - Результат проверки статуса сертификата)

	🛓 testovii 👻
KPUI ITOI IPO	Сервер электронной подписи КриптоПро DSS
Подписать	Проверка сертификата Проверить
Усовершенствовать подпись	
Зашифровать	Файл сертификата:
Расшифровать	Выбрать
Проверить подпись	Дополнительные проверки:
Проверить сертификат	☐ Проверка на соответствие требованиям к квалифицированным сертификатам
Сертификаты	
Аудит	

Рисунок 32 - Проверка статуса сертификата

		å te	estovii 👻
KPUITIOTIPO	Сервер электронной	подписи КриптоПро DSS	
Подписать	Результат проверк	и	
Усовершенствовать подпись	Название документа	минцифры.cer	
Зашифровать	Результат проверки	Сертификат прошел проверку	
Расшифровать		Consistencies.	
Проверить подпись	информация	Отсутствува	
Проверить сертификат	Информация о		
Сертификаты	сертификате		
Аудит	Субъект	CN=Минцифры России, ИНН ЮЛ=7710474375, ОГРН=1047702026701, О=Минцифры России, STREET="Пресненская набережная, дом 10 строение 2", L=r. Москва, S=77 Москва, C=RU, E=dit@digital.gov.ru	0,
	Издатель	CN=Минцифры России, ИНН ЮЛ=7710474375, ОГРН=1047702026701, О=Минцифры России, STREET="Пресненская набережная, дом 10 строение 2", L=r. Москва, S=77 Москва, C=RU, E=dit@digital.gov.ru	0,
	Серийный номер	00951FA3477C61043AADFA858627823442	
	Срок действия	08.01.2022 16:32:39 - 08.01.2040 16:32:39	
	Отпечаток сертификат	2F0CB09BE3550EF17EC4F29C90ABD18BFCAAD63A a	

Рисунок 33 - Результат проверки статуса сертификата

4.7. Раздел «Сертификаты»

Раздел предназначен для создания запросов на сертификат, управления сертификатами Пользователя.

4.7.1. Создание запроса на сертификат

Для создания запроса на новый/первый сертификат Пользователя необходимо перейти в раздел «*Сертификаты*» и нажать кнопку «*Создать запрос на сертификат*» (см. Рисунок 34 – Вкладка «Сертификаты»).

	👗 testovii 🛩					
KPUITIONPO	Сервер электронной подписи КриптоПро DSS					
Подписать	Сертификаты 😂	+ Создать запрос на сертификат	Установить сертификат			
Усовершенствовать подпись	Сертификаты отсутствуют.					
Зашифровать						
Расшифровать						
Проверить подпись						
Проверить сертификат						
Сертификаты						
Аудит						

Рисунок 34 – Вкладка «Сертификаты»

Далее необходимо отредактировать данные Пользователя и нажать кнопку «*Создать запрос*» (см. Рисунок 35 - Создание запроса на сертификат), задать ПИН-код к ключу в СЭП и нажать кнопку «*ОК*».

🗲 Сервер электронной подп 🛛 🎦			
КРИПТОПРО	Сервер электронной подписи КриптоПро DSS		🛔 rakort 👻 🤸
Подписать	Создание запроса на сертификат		
Усовершенствовать подпись	Выберите шаблон сертификата	Сертификат пользователя DSS -	
Зашифровать		🗌 Неподписанный запрос	
Расшифровать	Компоненты имени сертификата		
Проверить подпись	Параметры времени действия сертификата 👻		
Проверить сертификат	Тип идентификации заявителя 🗸		
Сертификаты		Создать запрос	
Аудит			
		Последние действия 20	323-01-16 17:21:10
		000 *KPi	ипто-про* © 2023 🗸

Рисунок 35 - Создание запроса на сертификат

При установке чекбокса «*Henodnucaнный запрос*» ключи пользователя будут храниться в мобильном устройстве.

После создания такого запроса его статус изменится на «*Ожидает подписи*» (см. Рисунок 36 - Неподписанный запрос).

🧖 Информация о запросе 😂	
Субъект Издатель Статус	CN=test, C=RU Тестовый УЦ 2.0 ГОСТ 2012 (Основной) Ожидает подписи
🕹 Скачать 🖨 Печать 🗎 Удалить	

Рисунок 36 - Неподписанный запрос

Дальнейшие действия выполняются в мобильном приложении.

Необходимо открыть DSS Client перейти в «*Настройки*» - «*Сертификаты*» и нажать на созданный запрос со статусом «*Запрос на сертификат не подписан*».

Откроется информация о запросе, в данном окне нажмите кнопку «*Подписать запрос*». На следующем этапе откроется датчик случайных чисел, нажимайте на экран телефона для генерации ключей до тех пор, пока шкала в нижней части экране

не будет заполнена (см. Рисунок 37 - Подписание запроса в мобильном приложении).

11:25	al 🗢 📶	11:26	al 🗢 🔟	11:25	al 🕈 💋
← Иванов Иван Иванович Запрос ка сертификат не подгисан Аvdeeva Outo/Band		← Иванов Иван Иванович Отправлен запрос Аvdeeva Outo/Band		Нажимайте для ген	ерации случайных данных
Расширенная информация	~	Расширенная информация	~	_	
Подписать запрос		Установить сертификат			
Удалить		Скачать запрос на сертифика	т		
					Этмена

Рисунок 37 - Подписание запроса в мобильном приложении

После появления сообщения «Запрос успешно подписан» запрос перейдет в мобильном приложении перейдет в статус «Отправлен запрос», а в веб-интерфейсе на «Обрабатывается» (см. Рисунок 38 - Информация о статусе запроса).



Рисунок 38 - Информация о статусе запроса

Данный запрос на сертификат можно:

- Скачать
- Распечатать
- Удалить

Полписать	Запрос на сертификат						
//	🙆 Информация о запросе 🗧						
усовершенствовать подпись							
Зашифровать	Субъект	CN=test					
Расшифровать	Издатель	OutOfBand					
Проверить подпись	Статус	Обрабатывается					
Проверить сертификат							
Сертификаты	🛓 Скачать 🖨 Печать 🗎 Удалить						
Аудит							

Рисунок 39 - Действия с запросом на сертификат

После получения сертификата его необходимо загрузить в СЭП. Для этого вернитесь на вкладку «*Сертификаты*» и нажмите кнопку «*Установить сертификат*» (см. Рисунок 34 – Вкладка «Сертификаты»).

В открывшемся окне нажмите «*Выбрать*» - выбрать файл сертификата на компьютере пользователя и нажмите «*Загрузить сертификат*» (см. Рисунок 40 - Загрузка нового сертификата).

KPURTORPO				
	Сервер электронной подписи КриптоПро DSS	3		
	0			
Подписать	Загрузка нового сертификата			
Усовершенствовать подпись	Из файла	adfs_token_signing.cer	Изменить	Убрать
Зашифорать		Загрузить сертификат		
Расшифровать				
Проверить подпись				
Проверить сертификат				
Сертификаты				
Аудит				

Рисунок 40 - Загрузка нового сертификата

4.7.2. Загрузка ключей из pfx

Экспорт ключей в pfx описан в разделе 5 данной инструкции (см. Экспорт ключа электронной подписи и сертификата ключа проверки электронной подписи)

Для загрузки ключей из pfx во вкладке «*Сертификаты*» нажмите «*Загрузить сертификат*» - «*Выбрать*» - выберите файл pfx на компьютере пользователя и нажмите «*Загрузить сертификат*» (см. Рисунок 40 - Загрузка нового сертификата).

4.8. Раздел «Аудит»

Раздел предназначен для отображения журнала событий, связанных с действиями Пользователей и Операторов в СЭП, совершенных над Пользователем с возможностью фильтрации по типам событий (см. Рисунок 41 - Журнал Аудита).

+ https://www.justsign.me/	cryptopro/Audit	t/List/		т 🗎 С Поиск	e- 🕅 🕁 🕮 🥲
с Сервер электронной подп ×					🛔 Иванов Иван Иванович 👻 ,
КРИПТОПРО	Сервеј	р электронной подписи Криг	тоПро DSS		
Подписать	Журна	ал Аудита			Фильтр 🔻
Усовершенствовать поллись	Статус	Код события	Данные	Дат	a
	~	Получение политики сервиса (33)	Запрос политики сервиса подписи.	201	9-04-04 14:59:08
Зашифровать Расшифровать	*	Получение списка сертификатов (27)	Запрос списка сертификатов пользователя.	201	9-04-04 14:59:07
Проверить подпись	*	Получение списка сертификатов (27)	Запрос списка сертификатов пользователя.	201	9-04-04 14:59:07
Проверить сертификат	~	Получение политики сервиса (33)	Запрос политики сервиса подписи.	201	9-04-04 14:59:07
Comuturen	~	Получение списка запросов (25)	Получение списка запросов на сертификат.	201	9-04-04 14:59:07
Сертификаты	~	Получение политики сервиса (33)	Запрос политики сервиса подписи.	201	9-04-04 14:59:07
Аудит	1	Получение сертификата (28)	Запрос сертификата пользователя. Отпечаток сертификата: CDE7D0F921CC4A2A1B5B5FF37469526CB1C4D5	56B. 201	9-04-04 14:34:18
	*	Получение списка сертификатов (27)	Запрос списка сертификатов пользователя.	201	9-04-04 14:34:18
	~	Получение сертификата (28)	Запрос сертификата пользователя. Отпечаток сертификата: CDE7D0F921CC4A2A1B5B5FF37469526CB1C4D5	56B. 201	9-04-04 14:32:34
	~	Получение списка сертификатов (27)	Запрос списка сертификатов пользователя,	201	9-04-04 14:32:34
	~	Получение сертификата (28)	Запрос сертификата пользователя. Отпечаток сертификата: CDE7D0F921CC4A2A1B5B5FF37469526CB1C4D5	56B. 201	9-04-04 14:21:05
	~	Создание транзакции (160)	Создание токена транзакции. Идентификатор: 3ce5ce52-0f0d-4482-b1ed-00f5a34c3004. Операция: PrivateKeyA	ccess 201	9-04-04 14:20:47
	~	Получение сертификата (28)	Запрос сертификата пользователя. Отпечаток сертификата: CDE7D0F921CC4A2A1B5B5FF37469526CB1C4D5	56B. 201	9-04-04 14:20:47

Рисунок 41 - Журнал Аудита

5. Экспорт ключа электронной подписи и сертификата ключа проверки электронной подписи

Импорт pfx описан в разделе 4.7.2 данной инструкции (см. Загрузка ключей из pfx).

5.1. OC Windows

Для экспорта ключа подписи и сертификата ключа проверки электронной подписи необходимо запустить СКЗИ «КриптоПро CSP» перейти во вкладку «*Сервис*», нажать «*Просмотреть сертификаты в контейнере закрытого ключа*» (см. Рисунок 42 - Кнопка «Просмотреть сертификаты в контейнере»), через кнопку «*Обзор*» выбрать необходимый контейнер закрытого ключа (см. Рисунок 43 - Выбор ключевого контейнера).

⊵ КриптоПро	CSP		×			
Алгоритмы	Безопасность	Winlogon	Настройки TLS			
Общие	Оборудование	Сервис	Дополнительно			
Контейнер за Эти мастера удалить кон	акрытого ключа позволяют протести тейнер закрытого кл	ровать, скопи юча с носител	оовать или я.			
Протестиро	вать Скопире	овать	Удалить			
Личный серт Этот мастер	Просмотреть сертификаты в контейнере Личный сертификат Этот мастер позволяет связать сертификат из файла с					
хранилище.	закрытого ключа, у	становив этот	сертификат в			
	Установи	ть личный сер	тификат			
Пароли закры Эти мастера	ытых ключей	пароли (ПИН-+	(оды) закрытых			
ключей или	ключей или удалить запомненные ранее пароли.					
Измени	ть пароль	Удалить запом	ненные пароли			
	O	(Оті	применить			

Рисунок 42 - Кнопка «Просмотреть сертификаты в контейнере»



Рисунок 43 - Выбор ключевого контейнера

Нажать кнопку «*Свойства*», перейти во вкладку «*Состав*» и нажать «*Копировать в* файл» (см.Рисунок 44 - Экспорт ключа).

Prazathi (Praz		
CDCE>	~	
Поле	Значение	^
Версия	V3	
Серийный номер	014127a5000faa2c8546ee843	
🔄 Алгоритм подписи	FOCT P 34.11-2012/34.10-20	T
🕎 Хэш-алгоритм подписи	ГОСТ Р 34.11-2012 512 бит	
Издатель	УЦ КРИПТО-ПРО (ГОСТ 2012	
🛄 Действителен с	13 марта 2019 г. 12:51:19	
📴 Действителен по	13 марта 2024 г. 13:01:19	
CVADERT	MRAHOR MRAH MRAHORMU RII	~
	Свойства Копировать в файл	

Рисунок 44 - Экспорт ключа

На следующем шаге выбрать «Да, экспортировать закрытый ключ» (см. Рисунок 45 - Экспортирование закрытого ключа).



Рисунок 45 - Экспортирование закрытого ключа

На следующем шаге оставить все по умолчанию и нажать «Далее». Задать пароль, нажать «Далее». Выбрать директорию для сохранения файла (например, Рабочий стол) и задать имя файла, соглашаться с работой Мастера нажатием кнопки «Далее» (см. Рисунок 46 - Экспорт ключа подписи и сертификата ключа проверки электронной подписи).

		×
÷	🖑 Мастер экспорта сертификатов	
	Безопасность Для обеспечения безопасности вам необходимо защитить закрытый ключ для субъекта безопасности или воспользоваться паролем.	
	Группы или пользователи (рекомендуется)	
	Добавить	
	Удалить	
	✓ Пароль:	
	Подтверждение:	
	•••	
	Шифровани TripleDES-SHA1 V	
	Далее Отмена	

Рисунок 46 - Экспорт ключа подписи и сертификата ключа проверки электронной подписи

5.2. OC Linux

Для экспорта ключа подписи и сертификата ключа проверки электронной подписи необходимо запустить cptools («Инструменты КриптоПро»).



Рисунок 47 - Инструменты КриптоПро

Перейти во вкладку «*Сертификаты*» и выбрать нужный контейнер. Нажать кнопку «Экспортировать ключи».

	cptoo	ols - Инструменты Криг	тоПро		- • ×
	Сертификаты				
Общее	Личное				•
Облачный провайдер	Поиск серти	фиката			
Контейнеры	Имя субъекта User	Имя издателя CRYPTO-PRO Test Cent	Срок действия 16/08/2022	Экспорт ключа разрешен	Серийный 12005ed23l
Сертификаты					
Создание подписи					
Проверка подписи					
Зашифровать файл					
Расшифровать файл					
	Установи	іть сертификаты	Эн	сспортировать сертифик	аты
	Импорт	ировать ключи		Экспортировать ключи	1
Показать расширенные	Свойсте	за сертификата		Удалить сертификат	

Рисунок 48 - Экспортировать ключи

Далее задать пароль на pfx и выбрать «Экспортировать pfx в файл» (см. Рисунок 49 - Параметры экспорта ключа)

Экспортировать ключи	×
Введите пароль на PFX:	
 Экспортировать PFX в файл Экспортировать PFX в QR-код 	
Экспортировать с цепочкой сертификатов Уменьшить размер QR-кодов (при проблемах со сканированием	٩)
Выберите приложение:	
NGate Клиент	-
CRYPTOPRO://CSP/PFX/ADD/	
ОК	Cancel

Рисунок 49 - Параметры экспорта ключа

На последнем этапе выберите место сохранения файла и имя.

5.3. OC macOS

Необходимо использовать Криптопро CSP 5.0.

Для экспорта ключа подписи и сертификата ключа проверки электронной подписи необходимо последовательно открыть «Finder -> Программы -> Инструменты КриптоПро». Открыть вкладку «*Сертификаты*» и нажать кнопку «*Экспортировать ключи*» (см. Рисунок 50 - Экспортировать ключи).

•••	cptools - Инструменты КриптоПро					
Q Поиск	Сертификаты					
Общее Облачный провайдер	Личное Q Поиск сертифи	ката				0
Контейнеры	Имя субъекта	Субъект	Имя издателя	Срок действия	Отпечаток	
Сертификаты	Тестовый оператор	0="000 ""КРИПТО	Тестовый подчиненн	30/06/2021	3429F153F66FAEE01	
Создание подписи						
Проверка подписи						
Зашифровать файл						
Расшифровать файл						
	У	становить сертифика	аты		Экспортировать сертификаты	
		Импортировать ключ	чи		Экспортировать ключи	
Показать расширенные		Свойства сертифика	та		Удалить сертификат	

Рисунок 50 - Экспортировать ключи

Далее задать пароль на pfx и выбрать «Экспортировать pfx в файл» (см. Рисунок 51 - Меню экспорта)

$\bullet \ \bigcirc \ \bigcirc$	Экспортировать ключи	
Введите пароль на	a PFX:	
••••		
 Экспортироват Экспортироват Экспортироват 	ть PFX в файл гь PFX в QR-код гь PFX в глубинную ссылку	
 Экспортироват Уменьшить раз 	т ь с цепочкой сертификатов мер QR-кодов (при проблемах со сканирование	em)
Выберите прилож	ение:	
NGate Клиент		\$
CRYPTOPRO://CSP	P/PFX/ADD/	
	C	ОК Отмена

Рисунок 51 - Меню экспорта

Указать место сохранения и имя файла и нажать кнопку «*Save*» (см. Рисунок 52 - Сохранение pfx).

		Save	
		Экспорт ключей	
	Save As:	test)
	Tags:)
	Where:	Desktop 📀 🗸)
File type:	Транспо	ортный ключевой контейнер PKCS #1	2 (*.pfx) ᅌ
		Cancel	Save

Рисунок 52 - Сохранение pfx

Экспорт успешно выполнен.

6. Использование «облачного» токена в СКЗИ «КриптоПро CSP 5.0»

Пользователи могут использовать «облачные» ключи, хранящиеся в СЭП, в приложениях, в которые встроено СКЗИ «КриптоПро CSP» (например, программы шифрования электронной подписи файлов, системы электронного И документооборота И др.), В которых используются механизмы аутентификации/электронной подписи, порталы органов государственной власти (www.nalog.ru, www.gosuslugi.ru)).

Импорт «облачных» ключей из СЭП доступен в СКЗИ «КриптоПро CSP» версии 5.0 и выше. Для импорта «облачного» ключа необходимо выполнить следующие действия на АРМ Пользователя СЭП:

1) Открыть приложение «Инструменты КриптоПро» (по умолчанию «Пуск» -> «Все программы» -> «КРИПТО-ПРО» -> «Инструменты КриптоПро»).

2) Выбрать пункт «*Облачный провайдер*» в меню приложения «*Инструменты КриптоПро*» и указать следующие параметры (например, для экземпляра СЭП с идентификатором «saas.cryptopro.ru»):

3) Сервер авторизации: https://saas.cryptopro.ru:4433/cryptoproidp/oauth;

4) Сервер DSS: https://saas.cryptopro.ru:4433/cryptopross/rest (см. Рисунок 53 - Настройки облачного провайдера), после чего нажать кнопку «Установить сертификаты».





 \times

📀 CryptoPro We	eb Authentication	×
	Вход в SignServer	
	Ivanov ×	
	Далее	
	Ц Чужой компьютер	
	Вход по сертификату	

Рисунок 54 - Ввод учетной записи пользователя

Теперь необходимо пройти аутентификацию в СЭП. В окне «*CryptoPro Web Authentication*» для этого понадобится указать имя Пользователя в экземпляре СЭП и нажать кнопку «*Далее*» (см. Рисунок 54 - Ввод учетной записи пользователя).

После этого в появившуюся форму ввести пароль Пользователя и нажать

кнопку «Войти» (см. Рисунок 55 - Ввод пароля пользователя).

В случае если для Пользователя установлены вторичные методы аутентификации при входе в Центр идентификации СЭП, необходимо подтвердить операцию соответствующим методом.

На следующем шаге будет отображено сообщение об успешной установке сертификатов Пользователя.

×



Рисунок 55 - Ввод пароля пользователя

«Облачный» ключевой контейнер можно увидеть во вкладке «Контейнеры» (см. Рисунок 56 - «Облачный» контейнер).

Далее «облачный» ключевой контейнер можно использовать так же, как и локальный, во всех приложениях, в которые встроено СКЗИ «КриптоПро CSP» (при каждом обращении к данному контейнеру необходимо будет проходить аутентификацию Пользователя в СЭП, как указано выше), в том числе, вебпорталах, информационных системах и т.д.

КриптоПро CSP			-	o x	
Q Поиск	Контейнеры				
05.000	Выберите CSP для	а операций с контейнерами			
Оощее	Все контейнеры (выбрать CSP автоматически)				
Облачный провайдер	Q Поиск контей	і́нера			
Контойноры	Считыватель	Контейнер	Имя субъекта		
Контемперы	CLOUD	DSS-0b566eaa-5e6b-473	Иванов Иван Иванович		

Рисунок 56 - «Облачный» контейнер

7. Работа с порталами органов государственной власти

7.1. Установка КриптоПро ЭЦП Browser plug-in

Необходимо перейти на страницу:

https://www.cryptopro.ru/products/cades/plugin

и скачать актуальную версию КриптоПро ЭЦП Browser plug-in.

Далее перейти на тестовую страницу:

<u>https://www.cryptopro.ru/sites/default/files/products/cades/demopage/main.html</u> и попробовать подписать данные.

Информация о сертификате								
Владолоц: СМ=Иванов Иван Ивановии								
Излатель: СN=УШ КРИПТО-ПРО (ГОСТ 2012)								
Выдан: 13.03.2019 09:51:19 UTC								
Действителен до: 13.03.2024 10:01:19 UTC								
Криптопровайдер: Crypto-Pro GOST R 34.10-2 Provider	012	Cŋ	/pto	gra	phic	Ser	vice	
Алгоритм ключа: ГОСТ Р 34.10-2012 256 бит								
Статус: Действителен								
Установлен в хранилище: Да								

Данные для подписи:

Hello World	^
icito ioria	~
Полянсать	

Рисунок 57 - Подпись данных

Далее необходимо пройти аутентификацию в СЭП. В окне «*CryptoPro Web Authentication*» укажите имя Пользователя в экземпляре СЭП и нажмите кнопку «*Далее*» (см. Рисунок 54 - Ввод учетной записи пользователя).

После этого в появившуюся форму введите пароль Пользователя и нажмите кнопку «Войти» (см. Рисунок 55 - Ввод пароля пользователя).

В случае если для Пользователя установлены вторичные методы аутентификации при входе в Центр идентификации СЭП, необходимо подтвердить операцию соответствующим методом (см Рисунок 15 - Информация об учетной записи пользователя).

Результатом является успешное подписание данных (см. Рисунок 58 - Результат подписи данных).

CN=Иванов Иван Иванович; Выдан: 13.03.2019 09:51:19



Данные для подписи:

Hello World

Подписать

Подпись сформирована успешно:



Рисунок 58 - Результат подписи данных

7.2. Работа с порталом nalog.ru

Необходимо перейти по адресу https://lkfl2.nalog.ru/lkfl/login, выбрать «*Войти с помощью ЭП*».

Выполнить все рекомендации, приведенные на странице «*Bxod в Личный кабинет*». Выбрать сертификат и нажать «*Войти*».



Вход в Личный кабинет

Доступ к сервису Личный кабинет налогоплательщика возможен с помощью ЭП без посещения инспекции.

Квалифицированный сертификат ключа проверки ЭП налогоплательщик может получить в Удостоверяющем центре, аккредитованном Минкомсвязи России. С

Для доступа к сервису налогоплательщик, используя ЭП, заполняет в электронном виде заявление на подключение со стартовой страницы сервиса. При этом необходимые для идентификации пользователя реквизиты считываются с носителя ЭП и автоматически подгружаются в форму заявления, дополнительные необязательные реквизиты «Номер телефона», «Электронная почта» вводятся вручную.

Для получения доступа к сервису Личный кабинет налогоплательщика для физических лиц с помощью ЭП необходимо обеспечить выполнение ряда технических условий:

1. Операционная система Microsoft Windows версий XP SP3 и выше (например, Windows 7)

- 2. Веб-браузер одной из поддерживаемых версий:
 - Microsoft Edge
 - Google Chrome 48+
 - Mozilla Firefox 45+
 - Yandex Browser 14+
 - Safari 9.0+

3. Крипто ПРО CSP 3.6 или выше с действующей лицензией (скачать с официального сайта компании «Крипто-Про», заполнив форму регистрации);

4. Драйверы ключевых носителей (eToken, RuToken и т.п.).

Установить корневой сертификат УЦ ФНС России 🖒

іберите сертификат *	
	~
	Отменить Войти

Рисунок 59 - Вход в личный кабинет nalog.ru

Далее необходимо пройти аутентификацию в СЭП. В окне «*CryptoPro Web Authentication*» для этого укажите имя Пользователя в экземпляре СЭП и нажмите кнопку «*Далее*» (см. Рисунок 54 - Ввод учетной записи пользователя).

После этого в появившуюся форму введите пароль Пользователя и нажмите кнопку «Войти» (см. Рисунок 55 - Ввод пароля пользователя).

В случае если для Пользователя установлены вторичные методы аутентификации при входе в Центр идентификации СЭП, необходимо подтвердить операцию соответствующим методом (см. Рисунок 60 - Вход в личный кабинет gosuslugi.ru).

7.3. Работа с порталом www.gosuslugi.ru

Необходимо перейти на страницу <u>www.gosuslugi.ru</u>, перейти в раздел «Личный кабинет», выбрать «*Bxod с помощью электронной подписи*» -> «Готово».

Для входа в личный кабинет необходимо установить плагин:

https://ds-plugin.gosuslugi.ru/plugin/upload/Index.spr

Если плагин установлен, то появится окно выбора сертификата (см. Рисунок 60 - Вход в личный кабинет gosuslugi.ru).

- 🗋 C

ГОСУСЛУГИ Единая система идентификации и аутентификации	
Выбор сертификата ключа проверки электронной подписи	×
Иванов Иван Иванович Издатель: УЦ КРИПТО-ПРО (ГОСТ 2012) Кому выдан: Действителен: с 13.03.2019 по 13.03.2024	

Рисунок 60 - Вход в личный кабинет gosuslugi.ru

Далее необходимо пройти аутентификацию в СЭП. В окне «*CryptoPro Web Authentication*» для этого укажите имя Пользователя в экземпляре СЭП и нажмите кнопку «*Далее*» (см. Рисунок 54 - Ввод учетной записи пользователя).

После этого в появившуюся форму введите пароль Пользователя и нажмите кнопку «Войти» (см. Рисунок 55 - Ввод пароля пользователя).

В случае если для Пользователя установлены вторичные методы аутентификации при входе в Центр идентификации СЭП, необходимо подтвердить операцию соответствующим методом.

8. Интеграция СЭП с использованием методов REST API

Для обеспечения возможности интеграции с СЭП сторонних прикладных систем, с использованием методов REST API, необходимо отправить запрос на почту operdss@cryptopro.ru, в котором требуется перечислить список методов, планируемых к использованию. С полным списком можно ознакомиться в руководстве разработчика КриптоПро DSS: https://dss.cryptopro.ru/docs/articles/intro.html

9. Безопасность при работе в СЭП

Для создания квалифицированной электронной подписи Пользователем УЦ используется СЭП на базе ПАМК «КриптоПро HSM» версии 2.0.

Ключи электронной подписи Пользователя УЦ формируются и хранятся в СЭП в неизвлекаемом формате, т.е. недоступном для выгрузки и сохранения на съемные носители, мобильные устройства и рабочие места Пользователя УЦ.

При создании ключа электронной подписи в СЭП Пользователем УЦ может быть установлен индивидуальный PIN-код доступа к ключевому контейнеру, содержащему ключ электронной подписи.

Использование ключа электронной подписи должно подтверждаться владельцем соответствующего сертификата ключа проверки электронной подписи (Пользователем УЦ) с помощью:

• ключа аутентификации в мобильном приложении DSS Client из состава ПО «Модуль аутентификации DSS Client для ПАК «КриптоПро DSS» версии 2.0 (далее – Мобильное приложение) на мобильном устройстве Пользователя УЦ;

• а также (опционально) индивидуальным PIN-кодом доступа к ключевому контейнеру, содержащему используемый ключ электронной подписи Пользователя УЦ.

Работа Мобильного приложения обеспечивается при соответствии мобильного устройства Пользователя УЦ следующим техническим требованиям:

- операционная система iOS версий: 8/9/10/11 и выше;
- операционная система Android версий: 7.0 и выше.

Мобильное приложение должно устанавливаться из официальных источников:

- для OC iOS: магазин приложений «App Store»;
- для ОС Huawei магазин приложений «AppGallery»;
- для OC Android: магазин приложений «Google Play».

В целях исключения доступа посторонних лиц к Мобильному приложению Пользователям УЦ рекомендуется установить пароль для доступа к мобильному устройству и разблокировки экрана. В случае наличия в мобильном устройстве функции распознавания отпечатка пальца, ее также рекомендуется включить.

Для обеспечения безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи Пользователь УЦ должен:

• Хранить в тайне индивидуальный PIN-код доступа к ключевому контейнеру, аутентификационную информацию для доступа к СЭП, обеспечить сохранность персональных мобильных устройств, используемых для подтверждения использования ключа электронной подписи при подписании

электронного документа, принимать все возможные меры для предотвращения их потери, раскрытия и несанкционированного использования.

• Применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи (в расширениях Extended Key Usage, Application Policy сертификата ключа проверки электронной подписи), если такие ограничения были установлены.

• Немедленно обратиться в Удостоверяющий центр с заявлением на прекращение действия соответствующего сертификата ключа проверки электронной подписи и не применять данный ключ электронной подписи:

- 1) при наличии оснований полагать, что конфиденциальность данного ключа нарушена;
- 2) в случае компрометации аутентификационной информации и утраты мобильных устройств, на которых установлено мобильное приложения DSS Client;
- 3) в случае, если Пользователю УЦ стало известно, что этот ключ электронной подписи используется или использовался ранее другими лицами, в том числе если Пользователь УЦ получил сообщение от СЭП о выполнении каких-либо операций от его имени в, то время, когда он их не выполнял.

• Использовать и регулярно обновлять средства антивирусной защиты в мобильных устройствах и на рабочих местах Пользователя УЦ.

10. Перечень рисунков

Рисунок 1 – Добавление сайта в зону надежных сайтов	6
Рисунок 2 – Включение ActiveX	6
Рисунок 3 – Включение поддержки ГОСТ	7
Рисунок 4 - Вход в СЭП. Окно ввода учётной записи	8
Рисунок 5 - Вход в СЭП	8
Рисунок 6 - Изменение пароля	9
Рисунок 7 - Загрузка сертификата	9
Рисунок 8 - Импорт сертификата через КриптоПро CSP	9
Рисунок 9 - Экспорт сертификата	10
Рисунок 10 - Аутентификация с помощью мобильного приложения	11
Рисунок 11 - QR-код для DSS Client	11
Рисунок 12 - Первый запуск мобильного приложения	12
Рисунок 13 - Регистрация учетной записи в DSS Client	13
Рисунок 14 - Защита мобильного приложения	14
Рисунок 15 - Информация об учетной записи пользователя	15
Рисунок 16 - Вход в СЭП. Окно ввода учётной записи	16
Рисунок 17 - Вход в СЭП	17
Рисунок 18 – Вход по сертификату	17
Рисунок 10 - Запрос аутентификации с помощью мобильного приложения DSS Client	18
Рисунок 19 - Полтверждение операции	19
Рисунок 20 - Подперядение операции	20
Рисунок 21 – Долумент успешно подписа	21
Рисунок 23 - Информация об операции	21
Рисунок 23 - Понтрерудение операции полниси	22
Рисунок 24 - Подльсрждение операции подписи	23 24
Писунок 25 - Формирование усовершенствованной подписи	24
Рисунок 20 - Загрузка фамла усовершенствованной подписи документа	25
Гисунок 2/ - Параметры шифрования.	20
Рисунок 28 - Шифрование электронного документа	20
Рисунок 29 - Расшифрование электронного документа	21 20
Рисунок 50 - Проверка подписи электронного документа	20
Рисунок 31 - Результат проверки подписи	28
Рисунок 32 - Проверка статуса сертификата	29
Рисунок 33 - Результат проверки статуса сертификата	29
Рисунок 34 – Вкладка «Сертификаты»	
Рисунок 35 - Создание запроса на сертификат	31
Рисунок 36 - Неподписанный запрос	31
Рисунок 37 - Подписание запроса в мобильном приложении	32
Рисунок 38 - Информация о статусе запроса	32
Рисунок 39 - Действия с запросом на сертификат	33
Рисунок 40 - Загрузка нового сертификата	33
Рисунок 41 - Журнал Аудита	34
Рисунок 42 - Кнопка «Просмотреть сертификаты в контейнере»	35
Рисунок 43 - Выбор ключевого контейнера	35
Рисунок 44 - Экспорт ключа	36
Рисунок 45 - Экспортирование закрытого ключа	36
Рисунок 46 - Экспорт ключа подписи и сертификата ключа проверки электронной подписи	37
Рисунок 47 - Инструменты КриптоПро	38
50	

Рисунок 48 - Экспортировать ключи	
Рисунок 49 - Параметры экспорта ключа	
Рисунок 50 - Экспортировать ключи	
Рисунок 51 - Меню экспорта	
Рисунок 52 - Сохранение pfx	41
Рисунок 53 - Настройки облачного провайдера	
Рисунок 54 - Ввод учетной записи пользователя	
Рисунок 55 - Ввод пароля пользователя	
Рисунок 56 - «Облачный» контейнер	
Рисунок 57 - Подпись данных	
Рисунок 58 - Результат подписи данных	
Рисунок 59 - Вход в личный кабинет nalog.ru	
Рисунок 60 - Вход в личный кабинет gosuslugi.ru	47
· · · ·	