



РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ ПО КЛИЕНТ АИС 'ГУЦ'



Цифровая подпись
любых файлов и данных



Верификация
файлов и контейнеров файлов



Управление
реестрами цифровых объектов



Поддержка
современных стандартов ГОСТ 34.11 2012
и ГОСТ 34.10 2012



Генерация
штампа времени цифровой подписи



Кроссплатформенность
программного обеспечения

СОДЕРЖАНИЕ

1	Подготовка к работе с программой.....	5
1.1	Подготовка к работе под Windows	5
1.2	Подготовка к работе под Linux.....	8
1.3	Быстрый старт.....	11
1.4	Резервное копирование	11
2	Операции с заявками.....	12
2.1	Описание экрана	12
2.2	Создание заявки на выдачу сертификата	14
	Выбор типа заявки	14
	Создание или выбор ключевой пары	15
	Выбор шаблона заявки	18
	Ввод атрибутов заявки.....	18
	Ввод капчи	20
2.3	Создание заявки на отзыв сертификата.....	21
	Выбор типа заявки	21
	Выбор сертификата на отзыв	22
	Выбор причины отзыва.....	23
	Ввод капчи	23
3	Операции с сертификатами.....	24
3.1	Описание экрана	24
3.2	Создание сертификата	25
3.3	Создание самоподписного сертификата.....	26
	Выбор периода действия сертификата	26
3.4	Экспорт и импорт	27
	Экспорт сертификата.....	27
	Импорт сертификата	29
4	Работа с электронной подписью.....	33
4.1	Создание электронной подписи	33
	Выбор алгоритма подписи	33
	Включение исходных данных	34

Создание штампа времени	34
Выбор директории для сохранения результатов	34
Выбор сертификата для подписи.....	34
Выбор файла для подписи.....	37
Подпись документа.....	37
4.2 Проверка электронной подписи	38
Выбор сертификата для проверки подписи.....	38
Проверка штампа времени	39
Просмотр результатов	39
5 Шифрование данных	41
5.1 Шифрование	41
Выбор алгоритма.....	42
Выбор директории для сохранения файлов.....	42
Выбор ключа шифрования (для симметричных алгоритмов).....	42
Выбор сертификата (для асимметричных алгоритмов).....	42
Выбор файлов.....	42
Запуск шифрования.....	43
5.2 Расшифрование	43
Выбор алгоритма.....	43
Выбор директории для сохранения файлов.....	43
Выбор ключа шифрования (для симметричных алгоритмов).....	43
Выбор сертификата (для асимметричных алгоритмов).....	43
Выбор файлов.....	44
Запуск расшифрования	44
6 Операции с ключами	45
6.1 Создание ключей	47
6.2 Экспорт ключей	47
6.3 Импорт ключей.....	48
7 Операции с сервисами.....	49
8 Настройки.....	50
8.1 Операции с удостоверяющими центрами	50
Добавление удостоверяющего центра	51
Удаление удостоверяющего центра.....	53

8.2	API Сервис	54
	Защищенный режим	55
8.3	Обновление	56
8.4	Сервер обновлений.....	57
9	Общие принципы	58
9.1	Главный экран	58
9.2	Меню	59

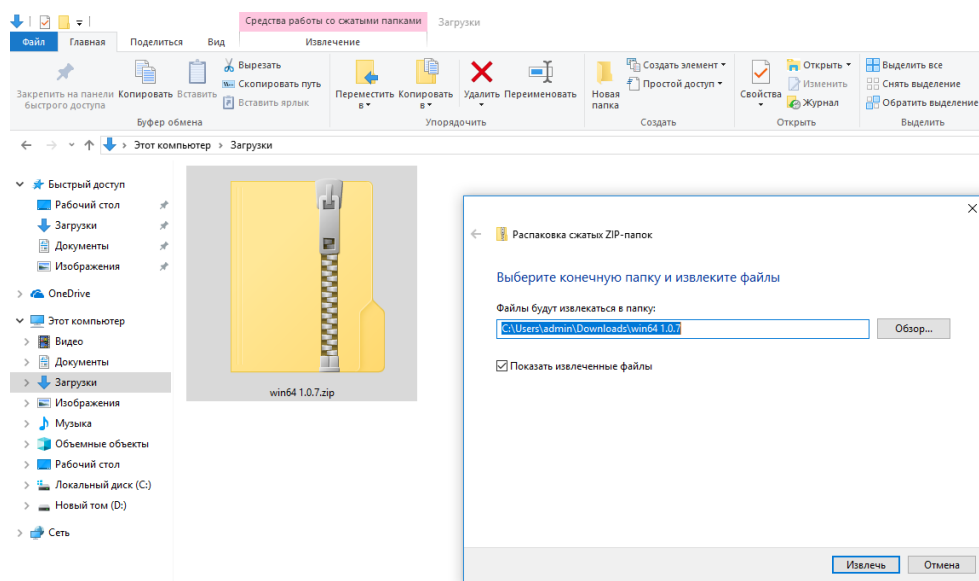
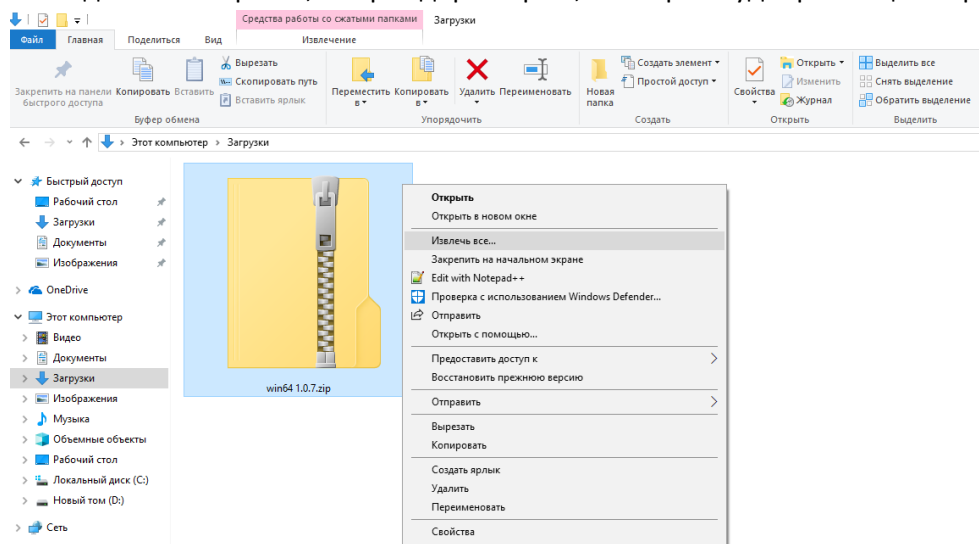
1 ПОДГОТОВКА К РАБОТЕ С ПРОГРАММОЙ

Данное программное обеспечение поставляется в виде сборок для операционных систем Windows (Windows 7 и выше) и Linux.

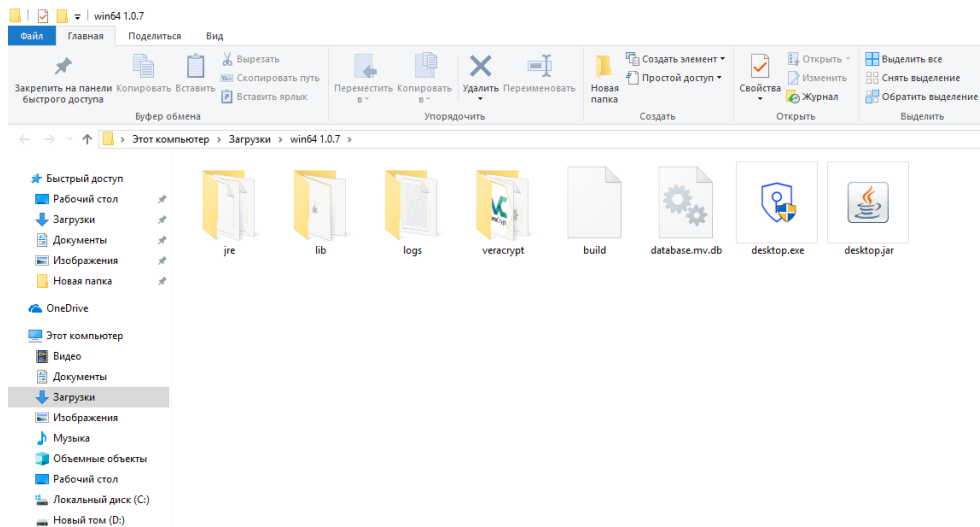
1.1 ПОДГОТОВКА К РАБОТЕ ПОД WINDOWS

Для запуска приложения на платформе Windows, необходимо сделать следующее:

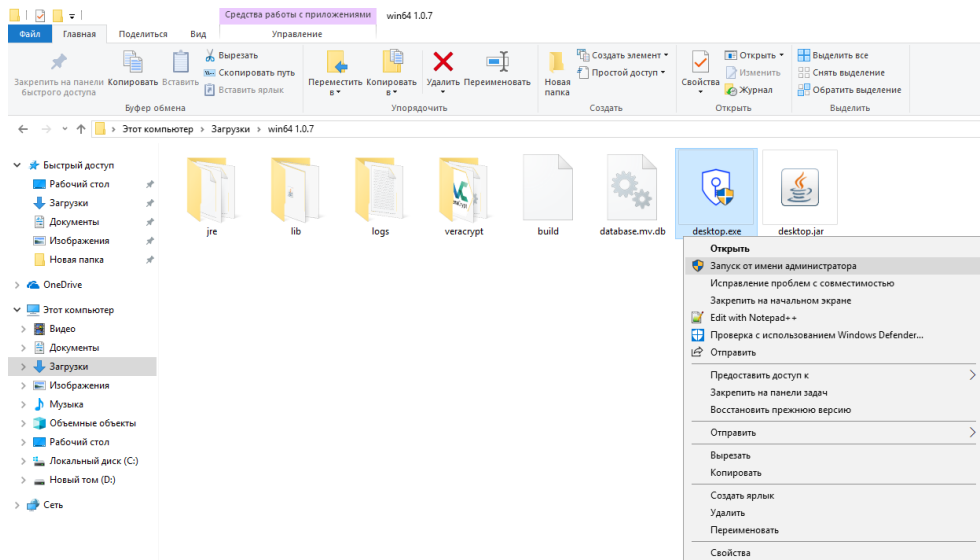
1. Открыть директорию со скачанным архивом в Проводнике.
2. Извлечь данные из архива, выбрав директорию, в которой будет размещено приложение.



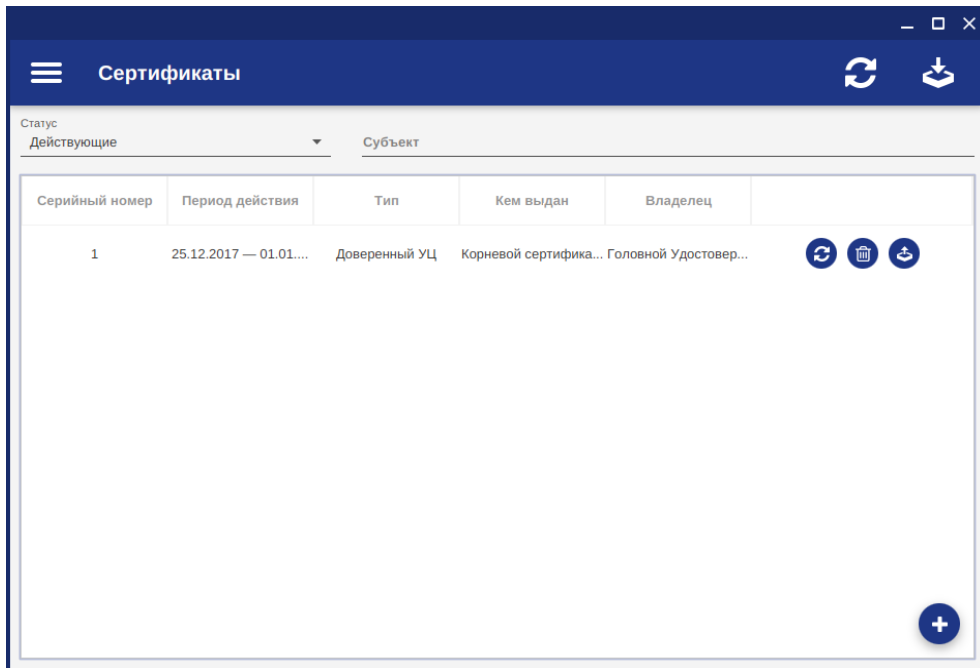
3. На следующем шаге следует открыть директорию, в которую было распаковано приложение. Её содержимое будет выглядеть следующим образом:



4. Для того чтобы запустить приложение, следует нажать правой кнопкой мыши по файлу desktop.exe и выбрать пункт «Запуск от имени администратора».



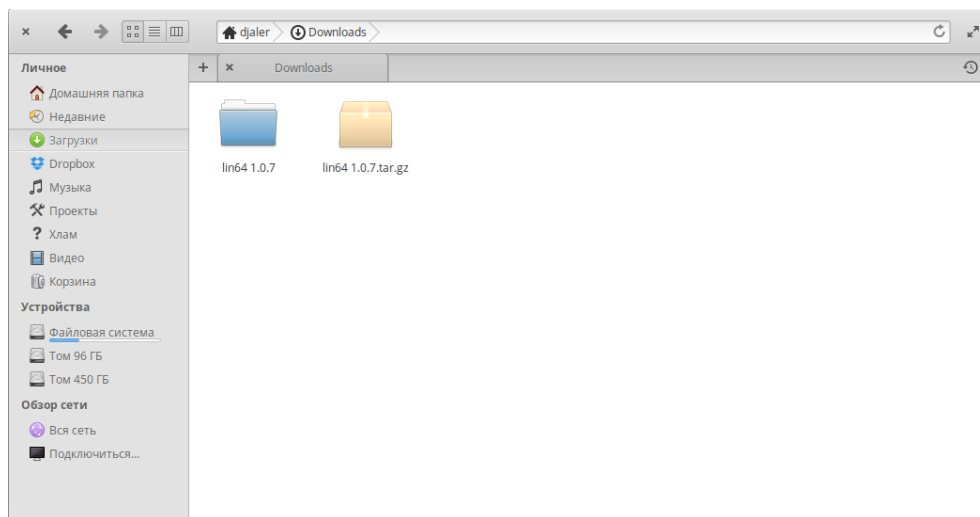
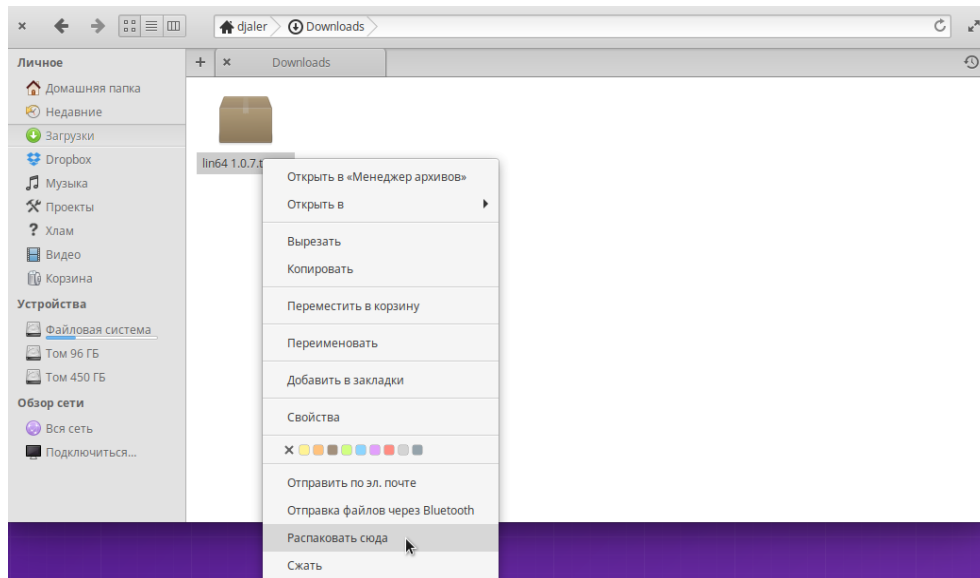
5. После процесса загрузки Вы увидите стартовое окно «Сертификаты».



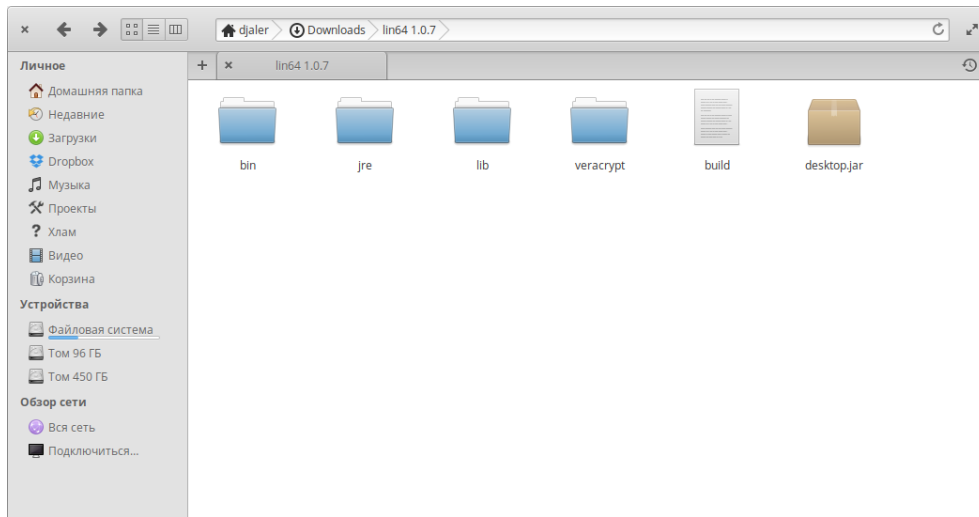
1.2 ПОДГОТОВКА К РАБОТЕ ПОД LINUX

Для запуска приложения на Linux необходимо сделать следующее:

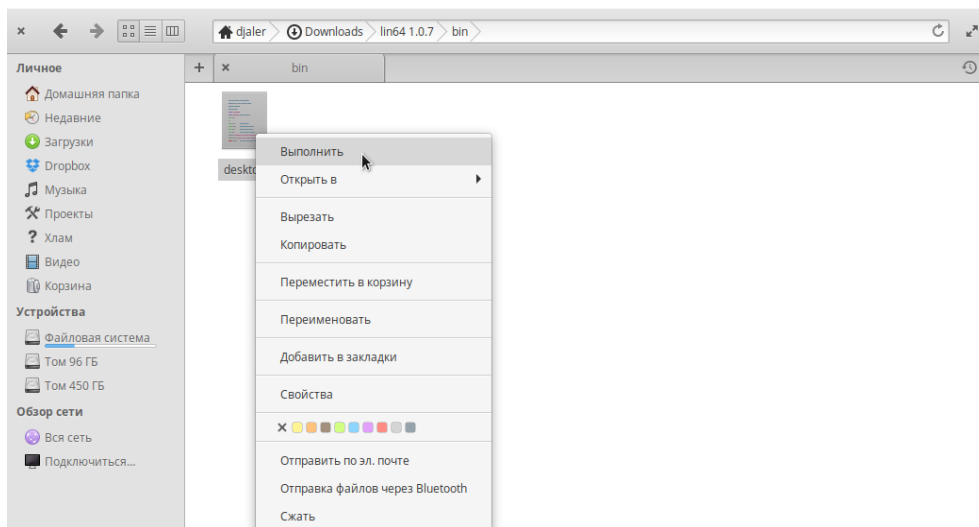
1. Открыть директорию со скачанным архивом в любом файловом менеджере.
2. Далее следует извлечь (распаковать) файлы из архива.



3. На следующем шаге следует открыть директорию, в которую было распаковано приложение. Её содержимое будет выглядеть следующим образом:



4. Для того чтобы запустить приложение, необходимо перейти в папку bin, в которой находится файл desktop, после чего нажать правой кнопкой мыши по файлу и выбрать пункт «Выполнить».



5. После процесса загрузки Вы увидите стартовое окно «Сертификаты».



Сертификаты

Статус: Действующие

Субъект

Серийный номер	Период действия	Тип	Кем выдан	Владелец	
1	25.12.2017 — 01.01....	Доверенный УЦ	Корневой сертифика...	Головной Удостовер...	

+

1.3 БЫСТРЫЙ СТАРТ

Для работы с основным функционалом приложения, созданием и проверкой цифровой подписи, пользователь должен иметь действующий сертификат. При первом запуске приложения откроется экран сертификатов. Существуют следующие варианты получения сертификата:

- Создание заявки на получение сертификата;
- Создание самоподписного сертификата;
- Импорт существующего сертификата.

Подробное описание этих вариантов доступно в разделе 2 - «Операции с заявками».

После получения сертификата одним из этих способов пользователю станет доступна работа с цифровыми подписями, а экран цифровой подписи будет открываться первым при старте приложения.

1.4 РЕЗЕРВНОЕ КОПИРОВАНИЕ

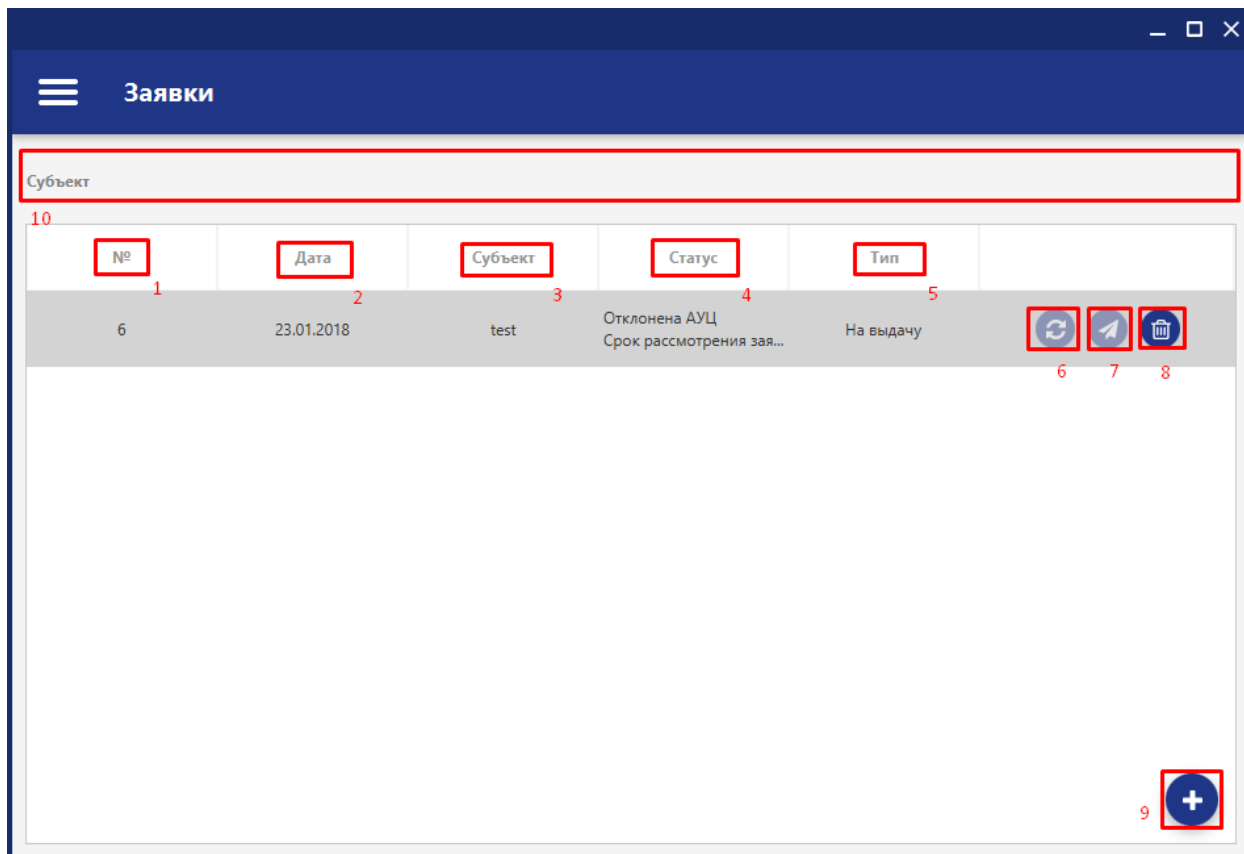
Для резервного копирования ключей и сертификатов предусмотрен экспорт/импорт данной информации в файл либо на токен. Процесс импорта/экспорта описан в соответствующих разделах данного документа.

Внимание! Все данные приложения хранятся в файле `database.mv.db`, который находится в папке с приложением.

2 ОПЕРАЦИИ С ЗАЯВКАМИ

2.1 ОПИСАНИЕ ЭКРАНА

Чтобы просмотреть все заявки, необходимо выбрать в меню пункт «Заявки». Будет открыто окно с заявками, которые были созданы ранее с помощью данного приложения.



Информация о заявках представлена в виде таблицы следующего содержания:

- Номер заявки (1);
- Дата создания заявки (2);
- Субъект заявки (3);
- Статус заявки (4). Предусмотрено 6 статусов заявок:
 - Новая
 - Не обработана
 - Проверена АУЦ
 - Отклонена АУЦ
 - Принята ГУЦ
 - Отклонена ГУЦ
- Тип заявки (5). Предусмотрено 2 типа заявок:
 - На выдачу
 - На отзыв.

Напротив каждой заявки находятся кнопки для работы с ней.

При нажатии на кнопку 6 будет обновлён статус соответствующей ей заявки. Данная кнопка может быть заблокирована, если обновление запущено в данный момент или заявка уже обработана. Если заявка на выдачу получает статус «Принята ГУЦ», значит сертификат сформирован и доступен на экране сертификатов.

При нажатии на кнопку 7 заявка будет отправлена. Данная кнопка может быть заблокирована, если заявка была отправлена ранее или отправляется в данный момент. После успешной отправки заявки она получает статус «Не обработана». Если тип заявки — «На отзыв», то она сразу переходит в статус «Принята ГУЦ», а сертификат становится отозванным.

При нажатии на кнопку 8 заявка будет удалена.

При нажатии на кнопку 9 будет открыто окно с первым этапом создания заявки.

Строка 10 предназначена для быстрого поиска заявки. Пользователь может ввести несколько символов имени субъекта и заявки будут отфильтрованы по этому полю.

2.2 СОЗДАНИЕ ЗАЯВКИ НА ВЫДАЧУ СЕРТИФИКАТА

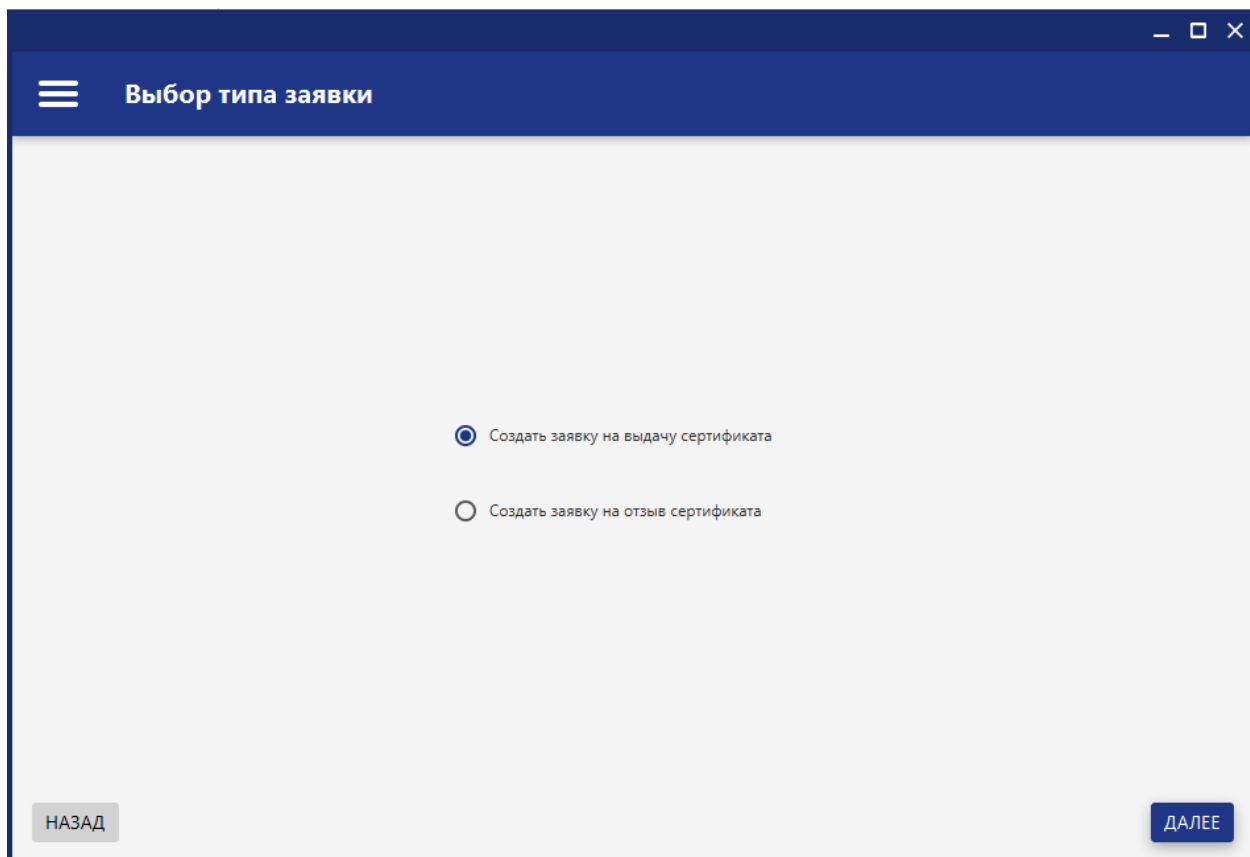
Для того, чтобы создать новую заявку, необходимо нажать кнопку добавления заявки (9) на экране «Заявки».

Процесс создания заявки состоит из следующих этапов:

- Выбор типа заявки;
- Создание или выбор ключевой пары;
- Выбор шаблона заявки;
- Ввод атрибутов заявки;
- Ввод капчи.

ВЫБОР ТИПА ЗАЯВКИ

Для создания заявки на выдачу сертификата на первом этапе пользователь должен выбрать соответствующий тип. Данный экран может быть пропущен, если у пользователя отсутствуют активные сертификаты.



Выбор типа заявки

Создать заявку на выдачу сертификата

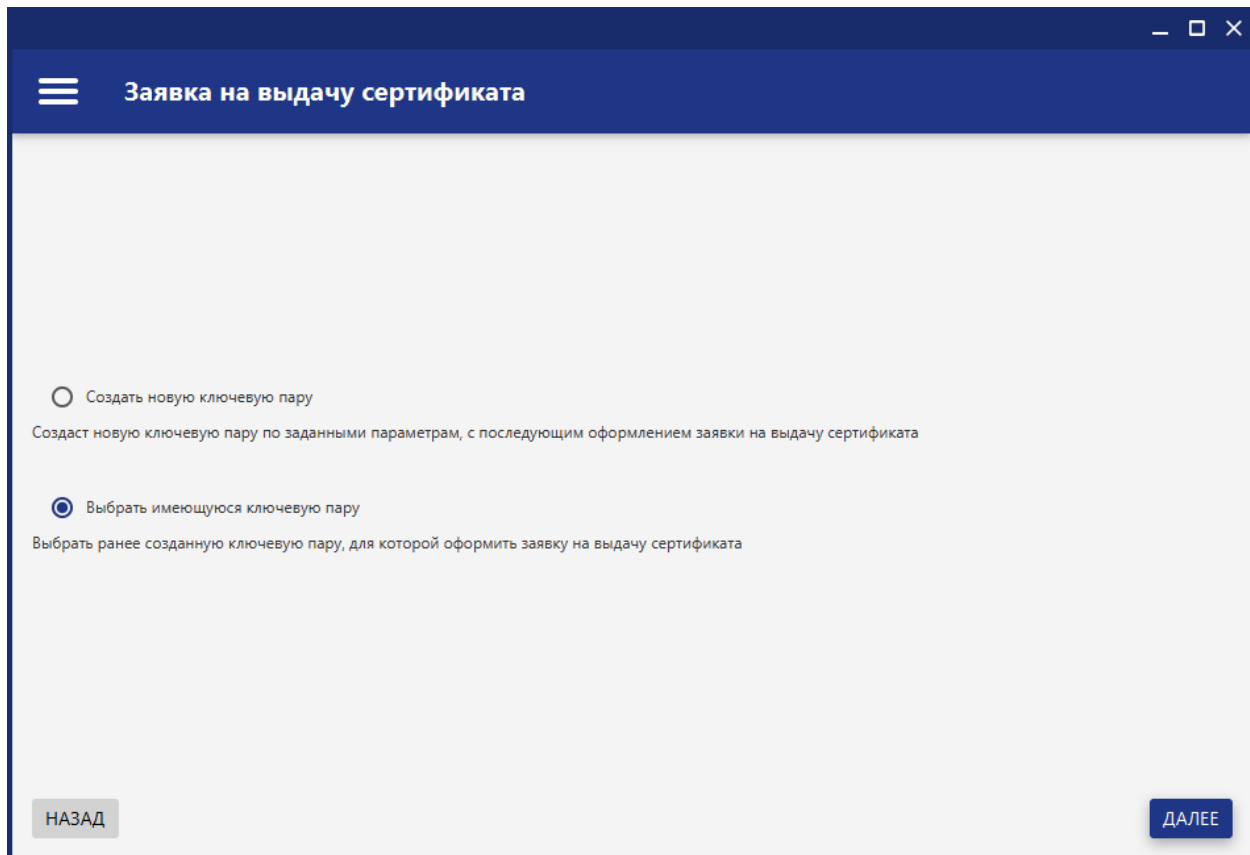
Создать заявку на отзыв сертификата

НАЗАД ДАЛЕЕ

После выбора типа заявки следует нажать кнопку «Далее».

СОЗДАНИЕ ИЛИ ВЫБОР КЛЮЧЕВОЙ ПАРЫ

На этом этапе пользователь должен выбрать существующую ключевую пару либо создать новую.



Заявка на выдачу сертификата

Создать новую ключевую пару
Создаст новую ключевую пару по заданным параметрам, с последующим оформлением заявки на выдачу сертификата

Выбрать имеющуюся ключевую пару
Выбрать ранее созданную ключевую пару, для которой оформить заявку на выдачу сертификата

НАЗАД

ДАЛЕЕ

СОЗДАНИЕ КЛЮЧЕВОЙ ПАРЫ

Для того чтобы создать ключевую пару, необходимо:

- Ввести корректное название нового ключа (допустим ввод латинских символов нижнего регистра, цифр и знака подчеркивания);
- Выбрать алгоритм генерации ключа и конфигурацию ключа (рекомендуется использовать значения по умолчанию);
- Нажать кнопку «Далее».

Создание ключевой пары необходимо, если ключевые пары отсутствуют.

Создание ключей

Название ключа

Алгоритм ключа
ГОСТ34.10 2012 512

Конфигурация ключа
ГОСТ34.10 2012 A 512

НАЗАД

ДАЛЕЕ

ВЫБОР СУЩЕСТВУЮЩЕЙ КЛЮЧЕВОЙ ПАРЫ

Если в системе уже существуют ключевые пары, пользователь может выбрать, какую именно следует использовать для формирования заявки.

Выбор ключей

Фильтр

Метка	Тип	Длина	Добавлен
test1	ГОСТ34.10 2012 512	512	23.01.2018 10:56:46

НАЗАД ДАЛЕЕ

ВЫБОР ШАБЛОНА ЗАЯВКИ

Для того, чтобы выбрать шаблон заявки, необходимо:

- Выбрать тип собственности субъекта в выпадающем списке «Тип заявки» (1);
- Ознакомиться с Соглашением на обработку персональных данных и отметить пункт «Я принимаю условия» (2);
- Нажать кнопку «Далее» (3). Кнопка не будет активна, пока предыдущий пункт не будет выполнен.

На любом этапе оформления заявки доступна кнопка «Назад», при нажатии на которую будет отображен предыдущий шаг создания заявки.

Выбор шаблона заявки

Тип заявки
Физическое лицо 1

СОГЛАСИЕ на обработку персональных данных

В соответствии с п. 1 ст. 9 закона ДНР от 09.06.2015 № 61-ІНС «О персональных данных» даю Государственному предприятию «Почта Донбасса», согласие на обработку моих персональных данных.

Перечень персональных данных, на обработку которых дается согласие субъекта персональных данных:
фамилия, имя, отчество; дата рождения; место рождения; адрес регистрации; фактический адрес проживания; тип и наименование основного документа, удостоверяющего личность; номер, серия, кем, когда выдан документ, удостоверяющий личность субъекта персональных данных; гражданство субъекта обращения; идентификационный номер налогоплательщика (ИНН); телефонный номер; адрес электронной почты, фотографическое изображение, социальное и имущественное положение, семейное положение, занимаемая должность, результат предоставления административной услуги/отказ в ее предоставлении.

Обработка данных осуществляется с целью:

- 1) Обеспечения соблюдения требований законодательства Донецкой Народной Республики.
- 2) Предоставления услуг Удостоверяющего Центра по изготовлению и верификации сертификата ключа электронной подписи.

Обработка вышеуказанных персональных данных будет осуществляться путем смешанной обработки персональных данных (сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение персональных данных при автоматизированной и без использования средств автоматизации обработке; запись на электронные носители и их хранение).

Настоящее согласие действительно с дня его подписания до дня отзыва в письменной форме.

Я принимаю условия 2

НАЗАД ДАЛЕЕ 3

ВВОД АТРИБУТОВ ЗАЯВКИ

На этапе ввода атрибутов, необходимо:

- Корректно заполнить поля с персональной информацией (1);
- Выбрать действие для сохранения заявки 5 - «Сохранить» или 6- «Сохранить и отправить».

Пользователь имеет возможность управлять вариантами использования сертификата с помощью галочек «Для подписи» (2) и «Для шифрования» (3), а также дополнительных настроек (4). Изменение параметров использования сертификата не рекомендуется.

При нажатии на кнопку «Сохранить» (5) заявка будет проверена на корректность ввода атрибутов, и, при корректном вводе атрибутов, сохранена. В дальнейшем заявка будет доступна на экране заявок, откуда её можно будет отправить.

При нажатии на кнопку «Сохранить и отправить» (6) заявка будет отправлена на сервер удостоверяющего центра, после чего заявка будет доступна в разделе заявок, а также в разделе сертификатов (как ещё не полученный сертификат).

Ввод атрибутов заявки

1

2

3

4

5

6

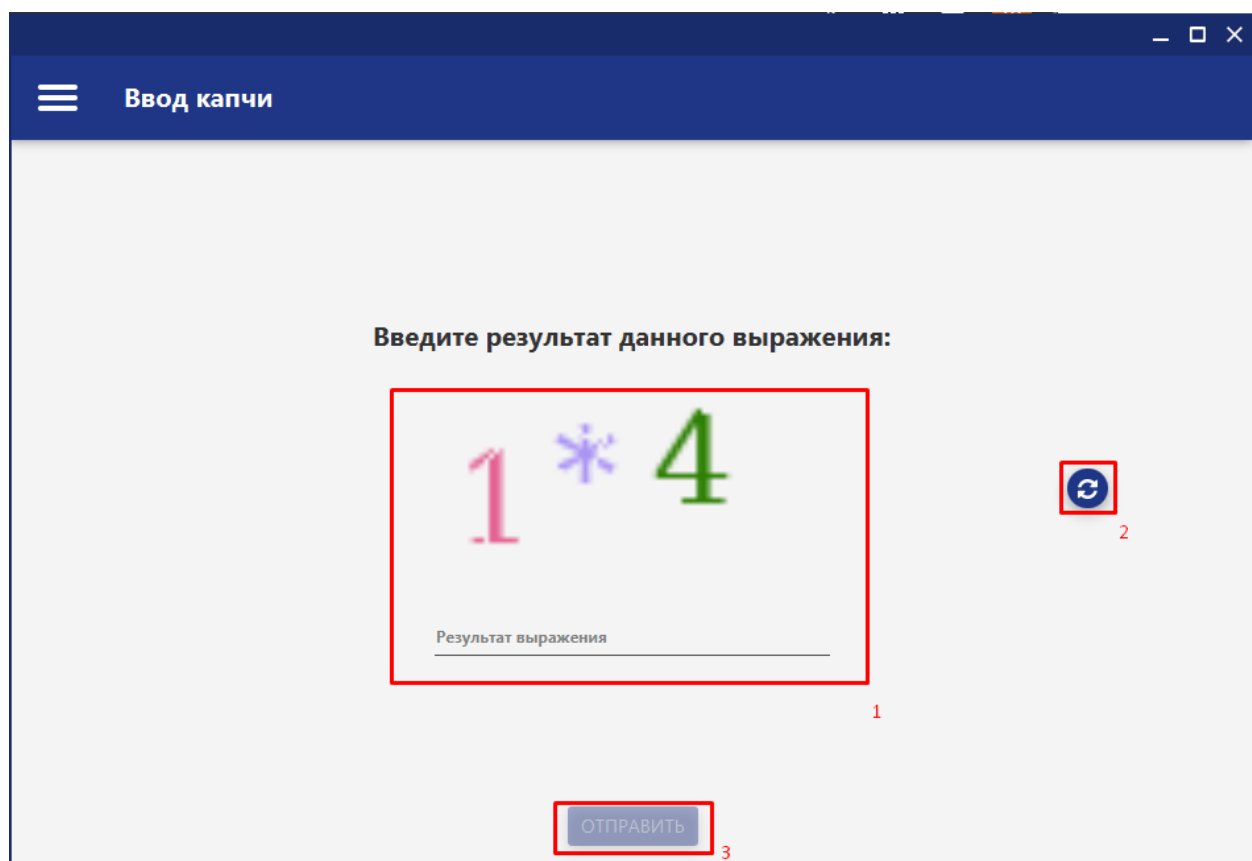
ВВОД КАПЧИ

Данный этап является последним перед отправкой заявки.

Капча представляет собой арифметическое выражение, результат которого необходимо ввести в поле «Результат выражения» под номером 1.

Если капча выглядит неразборчиво, пользователь может обновить её, нажав на кнопку «Обновить» под номером 2.

Для завершения работы с заявкой следует нажать кнопку «Отправить» (3), после чего будет открыт раздел заявок. Если при отправке заявки произошла какая-либо проблема, пользователь может повторить попытку, нажав на кнопку отправки.



The screenshot shows a web interface for entering a CAPTCHA. At the top, there is a blue header with a menu icon and the text "Ввод капчи". The main content area has a light gray background. In the center, the instruction "Введите результат данного выражения:" is displayed. Below this, a red-bordered box contains the CAPTCHA expression: a pink number "1", a purple asterisk "*", and a green number "4". To the right of this box is a blue circular button with a refresh icon, labeled with a red "2". Below the CAPTCHA box is a text input field with the placeholder text "Результат выражения", labeled with a red "1". At the bottom center, there is a blue button with the text "ОТПРАВИТЬ", labeled with a red "3".

2.3 СОЗДАНИЕ ЗАЯВКИ НА ОТЗЫВ СЕРТИФИКАТА

Отзыв сертификата доступен, если у пользователя существуют действующие сертификаты. Для создания заявки на отзыв сертификата пользователю необходимо перейти на экран заявок и нажать на кнопку создания заявки.

Создание заявки на отзыв сертификата состоит из следующих этапов:

- Выбор типа заявки;
- Выбор сертификата;
- Выбор причины отзыва заявки;
- Ввод капчи.

ВЫБОР ТИПА ЗАЯВКИ

Для создания заявки на выдачу сертификата на первом этапе пользователь должен выбрать соответствующий тип.

После выбора типа заявки следует нажать кнопку «Далее».

Скриншот экрана «Выбор типа заявки». В верхней части экрана (темно-синий заголовок) находится меню (три горизонтальные линии) и заголовок «Выбор типа заявки». В центре экрана расположены две опции с радиокнопками:

- Создать заявку на выдачу сертификата
- Создать заявку на отзыв сертификата

В нижней части экрана (серый фон) расположены две кнопки: «НАЗАД» (слева) и «ДАЛЕЕ» (справа).

ВЫБОР СЕРТИФИКАТА НА ОТЗЫВ

На данном этапе пользователю необходимо выбрать сертификат, который будет отозван и нажать кнопку «Далее».

Выбор сертификата

Субъект

Серийный номер	Период действия	Кем выдан	Владелец
7	24.01.2018 — 23.01.2023	Тестовый сертификат ГУЦ	Martin Kepta

НАЗАД

ДАЛЕЕ

ВЫБОР ПРИЧИНЫ ОТЗЫВА

На этом этапе пользователю необходимо:

- Выбрать причину отзыва заявки в списке (1);
- Выбрать действие для сохранения заявки - «Сохранить» (2) или «Сохранить и отправить» (3).

Ввод причины отзыва

Причина отзыва сертификата
Скомпрометирован ключ

1

2 3

НАЗАД СОХРАНИТЬ СОХРАНИТЬ И ОТПРАВИТЬ

ВВОД КАПЧИ

Пользователь должен ввести капчу и нажать кнопку «Отправить» (3), после чего откроется раздел заявок. Шаг с вводом капчи подробно описан в разделе 2.2 «Создание заявки на выдачу сертификата».

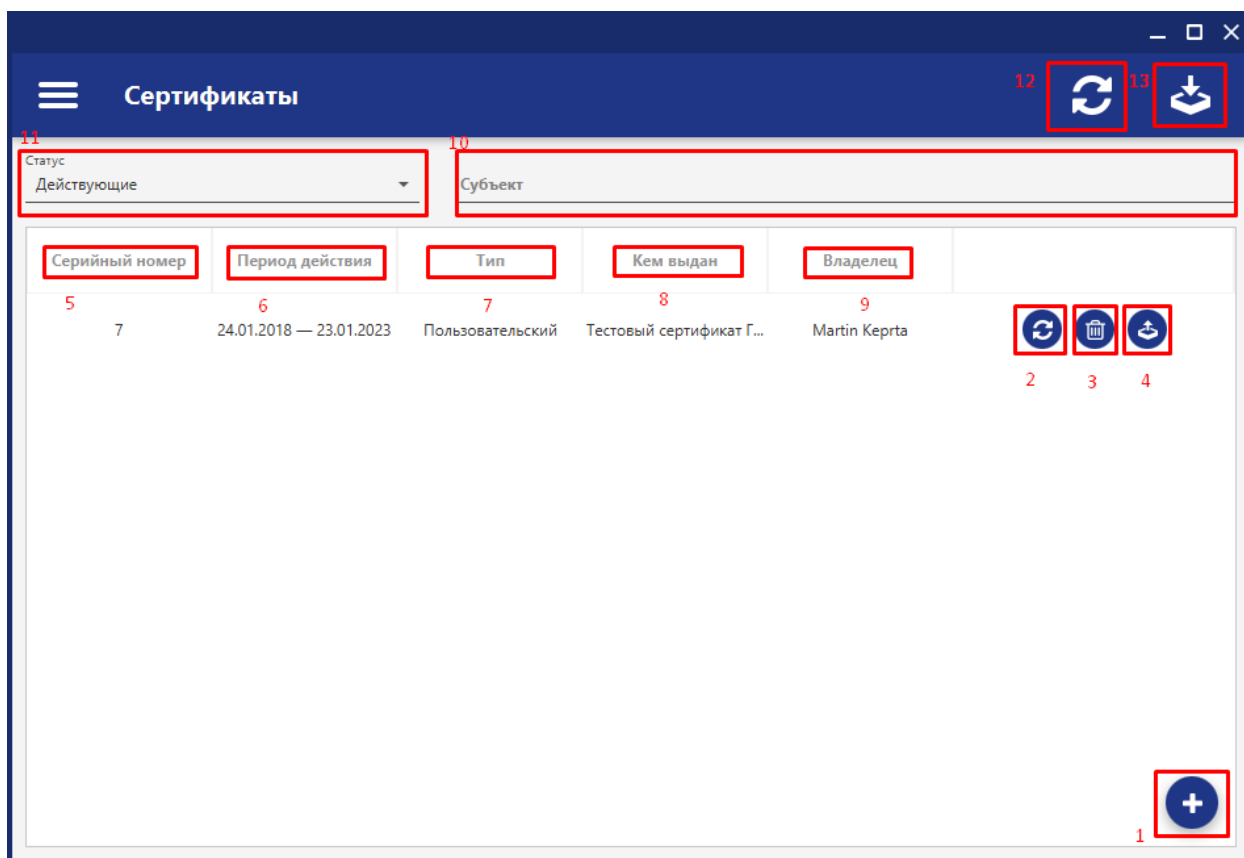
Если при отправке заявки произошла какая-либо проблема, можно повторить попытку, нажав на кнопку отправки.

3 ОПЕРАЦИИ С СЕРТИФИКАТАМИ

3.1 ОПИСАНИЕ ЭКРАНА

Чтобы просмотреть все сертификаты, необходимо выбрать в меню пункт «Сертификаты». Будет открыто окно с сертификатами, которые были созданы ранее. Информация о сертификатах представлена в виде таблицы следующего содержания:

- Серийный номер сертификата (5);
- Период действия сертификата (6);
- Тип сертификата (7);
- Кем выдан сертификат (8);
- Владелец сертификата (9).



Напротив каждого сертификата находятся кнопки для работы с ним.

При нажатии на кнопку 2 статус соответствующего сертификата будет обновлён. Данная кнопка заблокирована, если обновление запущено на данный момент.

При нажатии на кнопку 3 сертификат будет удалён.

При нажатии на кнопку под номером 4 сертификат будет экспортирован в файловую систему.

При нажатии на кнопку под номером 1 будет открыто окно добавления следующего сертификата.

Строка 10 предназначена для быстрого поиска сертификата. Пользователь может ввести несколько первых символов имени субъекта и сертификаты будут отфильтрованы по этому полю.

Список под номером 11 предназначен для фильтрации сертификатов по статусу. Для этого необходимо выбрать один из элементов списка, и таблица с сертификатами будет обновлена в соответствии с выбранным статусом.

При нажатии на кнопку 12 список сертификата будет обновлён.

При нажатии на кнопку 13 будет открыто окно для импорта сертификата.

3.2 СОЗДАНИЕ СЕРТИФИКАТА

Для создания заявки на сертификат вам необходимо нажать на кнопку создания сертификата, а затем выбрать «Создать заявку на выдачу сертификата». Этот процесс описан в разделе 2.2 - «Создание заявки на выдачу сертификата».

Создание сертификата

Создать заявку на выдачу сертификата

Создать самоподписной сертификат

НАЗАД

ДАЛЕЕ

3.3 СОЗДАНИЕ САМОПОДПИСНОГО СЕРТИФИКАТА

Для создания самоподписного сертификата пользователю нужно выбрать пункт «Создать самоподписной сертификат» после нажатия на кнопку создания сертификата.

Процесс создания самоподписного сертификата практически идентичен процессу создания заявки на получение сертификата. К нему добавляется шаг выбора периода действия сертификата.

ВЫБОР ПЕРИОДА ДЕЙСТВИЯ СЕРТИФИКАТА

На данном шаге пользователь должен выбрать дату окончания действия сертификата в календаре под номером 2, по достижении которой он будет считаться более не действительным.

Для того, чтобы завершить процедуру создания сертификата, следует нажать кнопку «Далее» под номером 1.

Выбор периода действия сертификата

Дата окончания действия 1/24/2019

2

НАЗАД

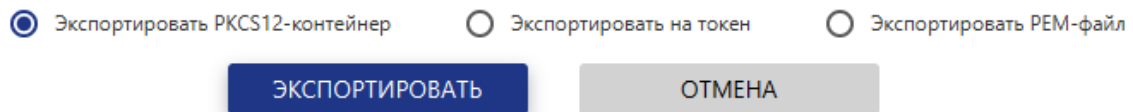
ДАЛЕЕ

1

3.4 ЭКСПОРТ И ИМПОРТ

ЭКСПОРТ СЕРТИФИКАТА

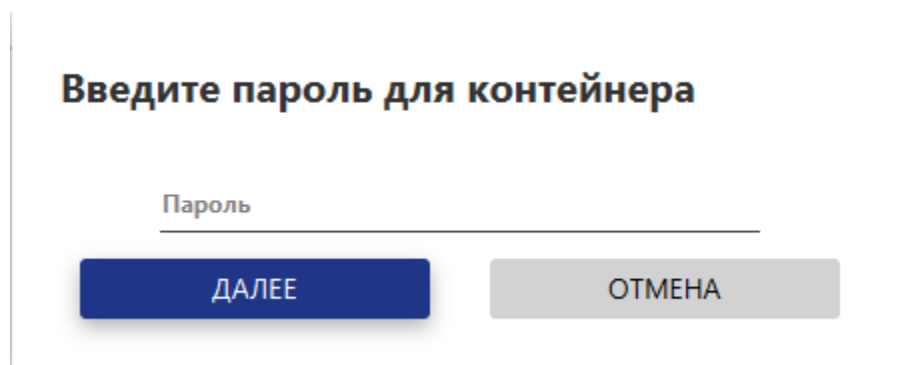
Для экспорта сертификата пользователь должен нажать на кнопку экспорта у соответствующего сертификата на экране сертификатов. В появившемся диалоге необходимо выбрать вариант экспорта.



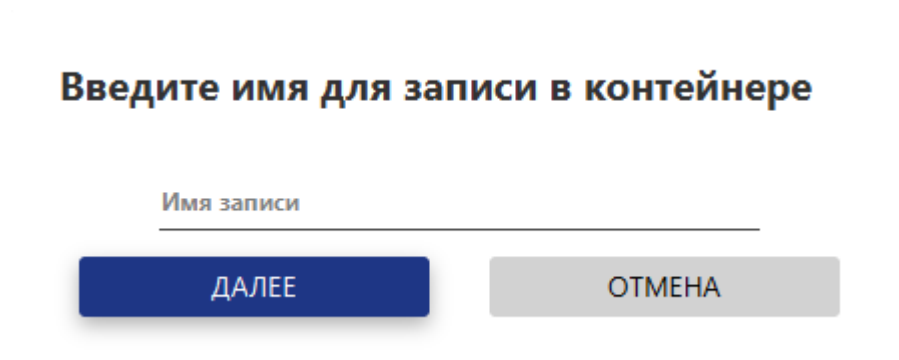
ЭКСПОРТ PKCS12

Для экспорта сертификата и ключевой пары в PKCS12-контейнер необходимо выбрать соответствующий пункт и нажать кнопку «Экспортировать».

На следующем шаге необходимо ввести пароль для доступа к контейнеру с сертификатом и нажать кнопку «Далее».



Далее необходимо ввести имя записи в контейнере, в которой будет сохранен сертификат, и нажать кнопку «Далее».



После этого пользователю необходимо выбрать место, в которое будет сохранен файл PKCS12-контейнера.

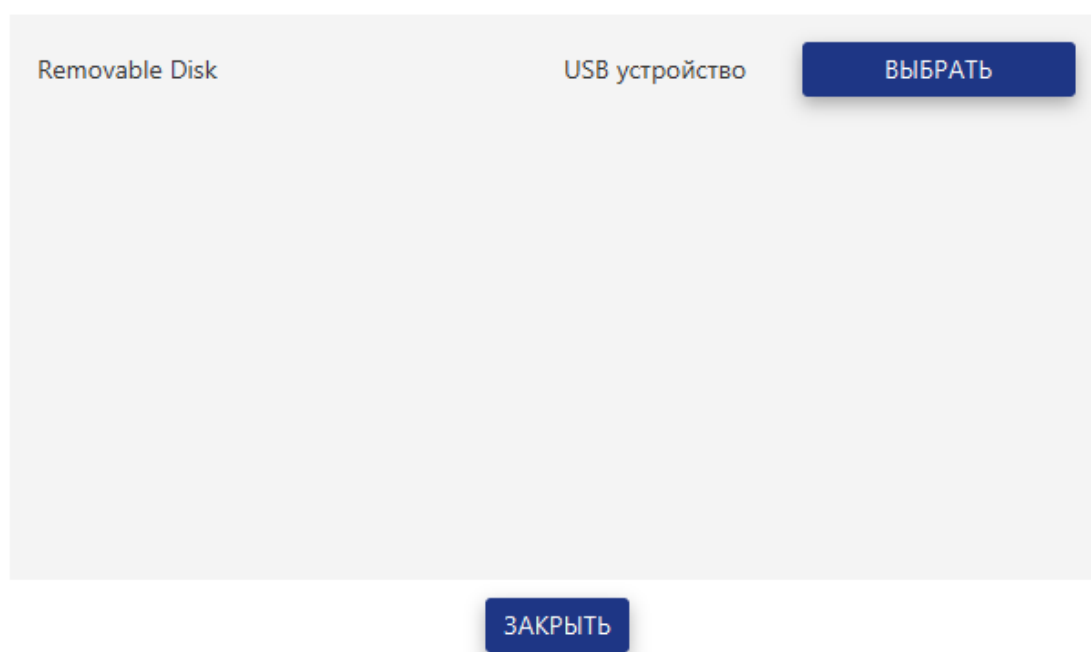
ЭКСПОРТ НА ТОКЕН

Токен представляет собой USB-носитель, хранящий сертификаты и ключи в зашифрованном формате. Токеном может стать любой USB-носитель. При первом экспорте на нём автоматически будет сформировано защищенное хранилище.

Для экспорта на токен необходимо выбрать соответствующую опцию (она может быть скрыта, если отсутствуют подходящие USB-носители).

На первом шаге пользователю необходимо выбрать целевой USB-носитель и нажать кнопку «Выбрать» напротив него.

Подключенные токены



Далее пользователь должен ввести PIN для доступа к токену и нажать кнопку «Далее».

Если на данный момент на этом устройстве отсутствует защищенное хранилище (это первый экспорт), пользователь может ввести любой желаемый PIN. При последующих попытках доступа к токену будет необходимо вводить выбранный на данном этапе PIN.

Введите PIN для доступа к токenu

PIN

ДАЛЕЕ ОТМЕНА

Далее пользователь должен ввести имя записи на токене и нажать кнопку «Далее». Токен будет автоматически создан на USB-носителе.

Введите имя для записи на токене

Имя записи

ЭКСПОРТИРОВАТЬ ОТМЕНА

ЭКСПОРТ В PEM

В данном формате экспортируется только сам сертификат, без соответствующей ему ключевой пары.

Для экспорта сертификата в PEM-формате, пользователь должен выбрать соответствующую опцию. Далее пользователю будет предложено выбрать место для сохранения PEM-файла.

ИМПОРТ СЕРТИФИКАТА

Для импорта сертификата необходимо нажать на кнопку импорта на экране сертификатов. В появившемся диалоге необходимо выбрать вариант импорта.

ИМПОРТ PKCS12

Для импорта из PKCS12-контейнера необходимо выбрать первый пункт в окне импорта сертификата и нажать кнопку «Импортировать».

Импортировать PKCS12-контейнер Импортировать из токена Импортировать PEM-файл

ИМПОРТИРОВАТЬ ОТМЕНА

В открывшемся диалоге следует выбрать файл, содержащий PKCS12-контейнер.

Далее необходимо ввести пароль от выбранного контейнера и нажать кнопку далее.

Введите пароль от контейнера

Пароль

ДАЛЕЕ

ОТМЕНА

На следующем этапе пользователь должен ввести желаемое имя для ключевой пары импортируемого сертификата, а затем нажать на кнопку «Импортировать». После загрузки сертификат будет импортирован и появится в списке.

Введите имя для импортируемого ключа

Имя ключа

ИМПОРТИРОВАТЬ

ОТМЕНА

ИМПОРТ PEM

В данном формате импортируется только сам сертификат, без соответствующей ему ключевой пары.

Импортировать PKCS12-контейнер

Импортировать из токена

Импортировать PEM-файл

ИМПОРТИРОВАТЬ

ОТМЕНА

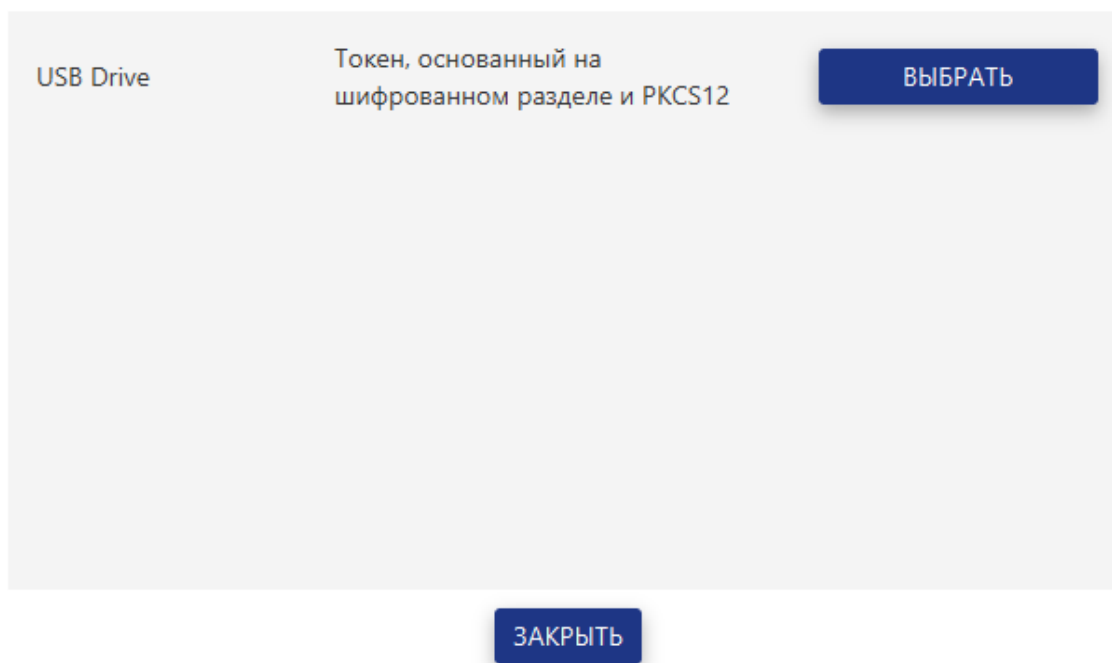
Для импорта PEM-файла пользователю будет предложено выбрать файл. После импорта сертификат будет отображен в списке.

ИМПОРТ ИЗ ТОКЕНА

Для импорта сертификата из токена пользователь должен выбрать соответствующую опцию в окне импорта (она может быть скрыта, если отсутствуют подходящие USB-носители).

На следующем шаге должно быть выбрано устройство из предложенного списка с помощью кнопки «Выбрать».

Подключенные токены



Далее пользователю необходимо ввести PIN для доступа к токenu и нажать кнопку «Далее».

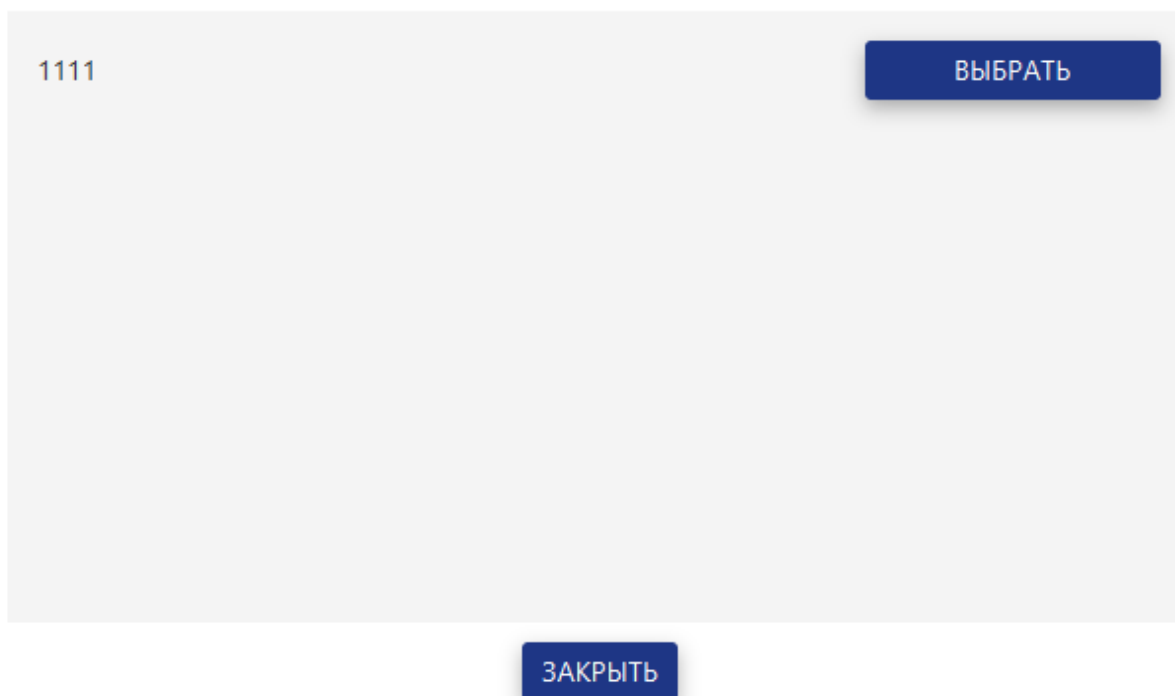
Введите PIN для доступа к токenu

PIN

ДАЛЕЕ ОТМЕНА

Далее пользователю необходимо выбрать необходимую запись из предложенного списка, используя кнопку «Выбрать» напротив записи. После загрузки сертификата будет импортирован и появится в списке.

Содержимое



1111

ВЫБРАТЬ

ЗАКРЫТЬ

На этом этапе пользователю необходимо ввести желаемое имя для ключевой пары импортируемого сертификата и нажать на кнопку «Импортировать».

Введите имя для импортируемого ключа



Имя ключа

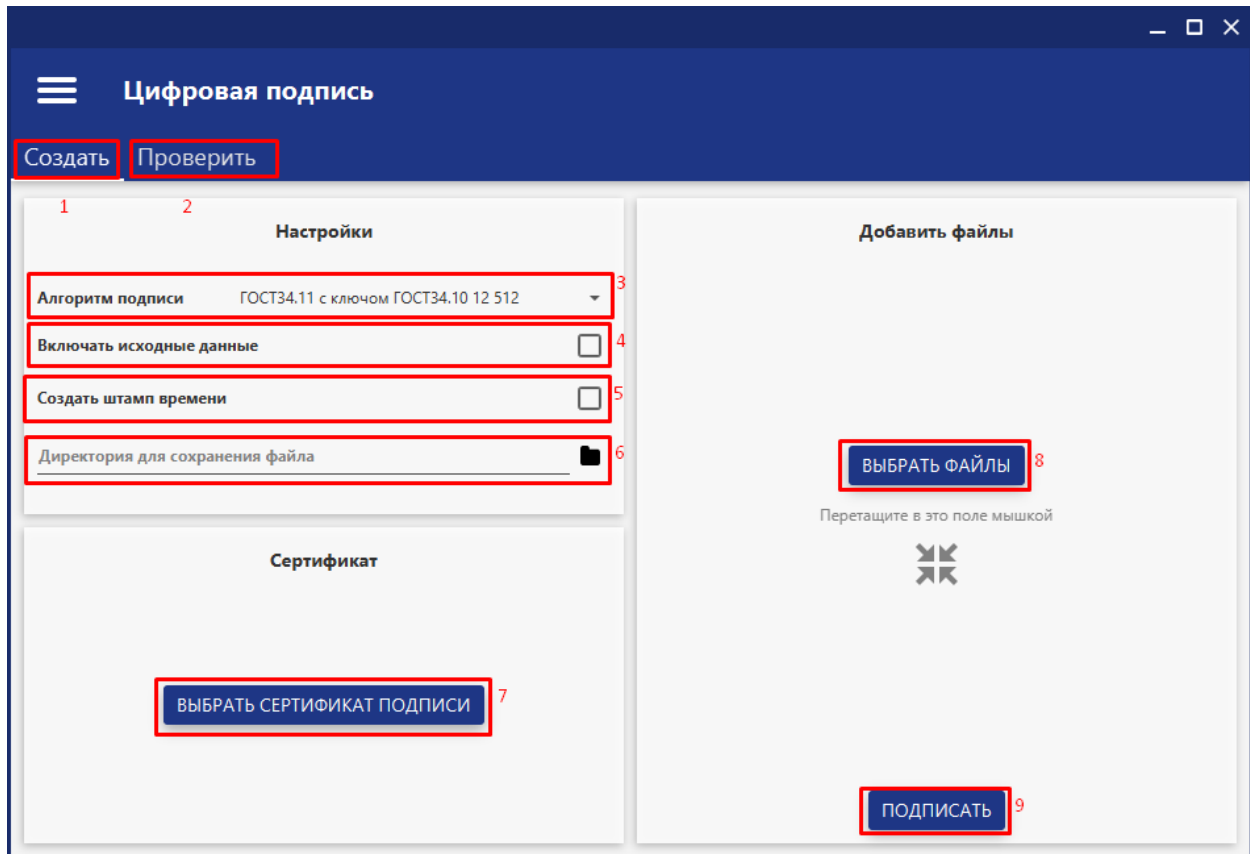
ИМПОРТИРОВАТЬ

ОТМЕНА

После загрузки сертификат будет импортирован и появится в списке.

4 РАБОТА С ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Для работы с электронной цифровой подписью пользователю нужно перейти на экран «Цифровая подпись» через одноименный пункт меню.



4.1 СОЗДАНИЕ ЭЛЕКТРОННОЙ ПОДПИСИ

Для подписи файлов пользователю необходимо нужно перейти на вкладку «Создать» (1) в окне «Цифровая подпись», а затем выполнить следующие шаги:

- Выбор алгоритма подписи(3);
- Включение исходных данных (4);
- Создание штампа времени (5);
- Выбор директории для сохранения результатов (6).
- Выбор сертификата для подписи (7);
- Выбор файла для подписи (8);
- Создание подписи документа (9).

ВЫБОР АЛГОРИТМА ПОДПИСИ

Для выбора алгоритма подписи пользователю необходимо выбрать из выпадающего списка требуемый алгоритм (3). Рекомендуется использовать алгоритм, установленный по умолчанию.

ВКЛЮЧЕНИЕ ИСХОДНЫХ ДАННЫХ

Для включения исходных данных в контейнер с подписями пользователь должен поставить соответствующий флажок (4).

СОЗДАНИЕ ШТАМПА ВРЕМЕНИ

Для добавления штампов времени к подписям пользователю необходимо соответствующий флажок (5).

ВЫБОР ДИРЕКТОРИИ ДЛЯ СОХРАНЕНИЯ РЕЗУЛЬТАТОВ

Для выбора директории пользователь должен нажать на кнопку 6. Пользователю будет предложено выбрать путь, где будет сохранен контейнер с подписью.

ВЫБОР СЕРТИФИКАТА ДЛЯ ПОДПИСИ

Для создания подписи пользователь должен загрузить сертификат, нажав на кнопку «Выбрать сертификат подписи» (7) и выбрав желаемый сертификат из списка. Список сертификатов может варьироваться в зависимости от выбранного алгоритма подписи.

Окно с выбором сертификата разделено на 2 части: слева представлен список сертификатов, справа – информация о сертификате, который выбран в списке на текущий момент. Для того, чтобы был использован текущий сертификат, необходимо нажать клавишу «Выбрать».

Сертификаты

Серийный номер	8
Владелец	test
Кем выдан	Тестовый сертификат ГУЦ
Период действия	24.01.2018 — 24.01.2019
Статус	Действующий

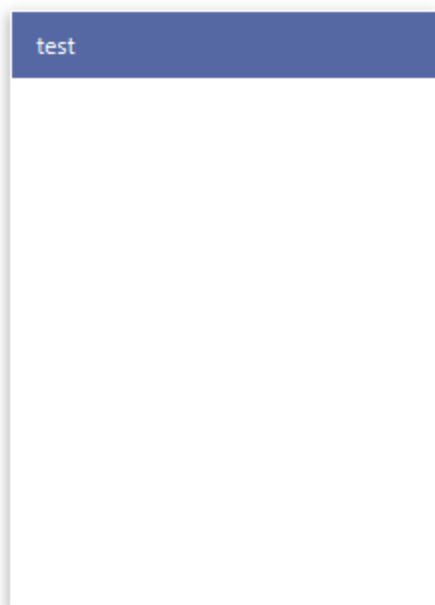
test

ЗАГРУЗИТЬ ИЗ ТОКЕНА **ВЫБРАТЬ** ОТМЕНА

ЗАГРУЗКА СЕРТИФИКАТА ИЗ ТОКЕНА

Для загрузки сертификата из токена необходимо предварительно вставить USB-носитель (токен), в компьютер, затем нажать на кнопку «Загрузить из токена».

Сертификаты



Серийный номер

8

Владелец

test

Кем выдан

Тестовый сертификат ГУЦ

Период действия

24.01.2018 — 24.01.2019

Статус

Действующий

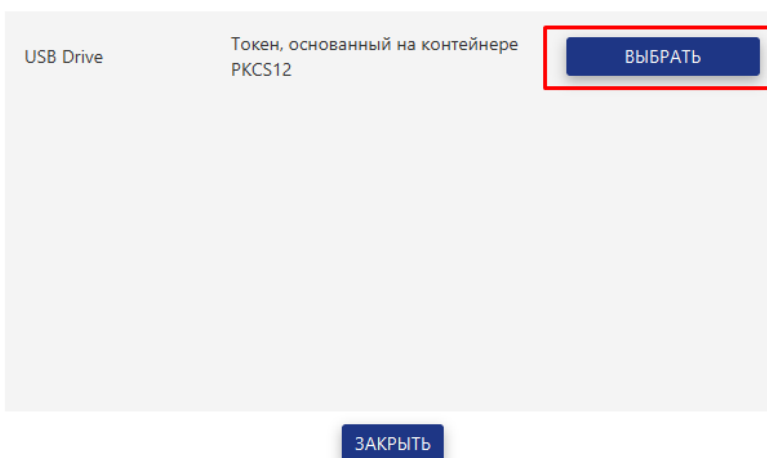
ЗАГРУЗИТЬ ИЗ ТОКЕНА

ВЫБРАТЬ

ОТМЕНА

Далее следует выбрать необходимый USB-носитель и нажать кнопку «Выбрать» напротив него.

Подключенные токены



На следующем этапе необходимо ввести PIN для доступа к токenu и нажать кнопку «Далее».

Введите PIN для доступа к токену

PIN

ДАЛЕЕ

ОТМЕНА

После успешного ввода PIN необходимо выбрать желаемую запись и нажать кнопку «Выбрать» напротив него.

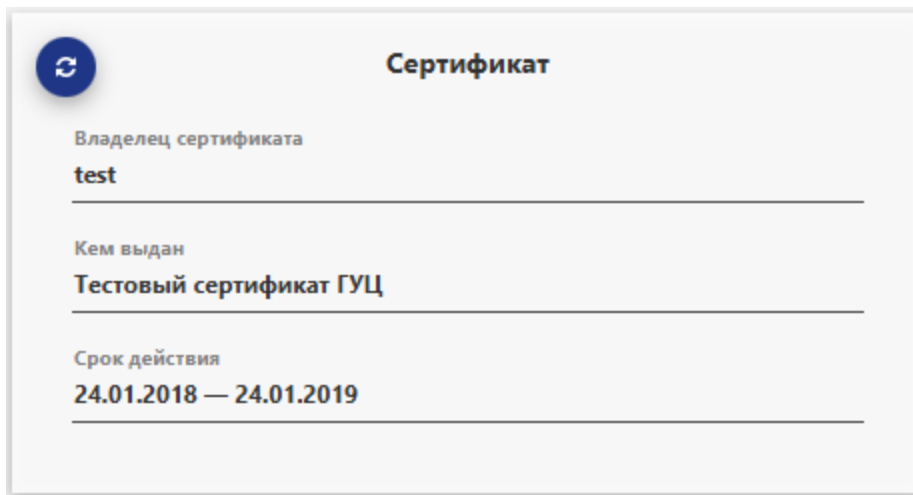
Содержимое

1111

ВЫБРАТЬ

ЗАКРЫТЬ

После загрузки сертификат будет отображен на экране.



ВЫБОР ФАЙЛА ДЛЯ ПОДПИСИ

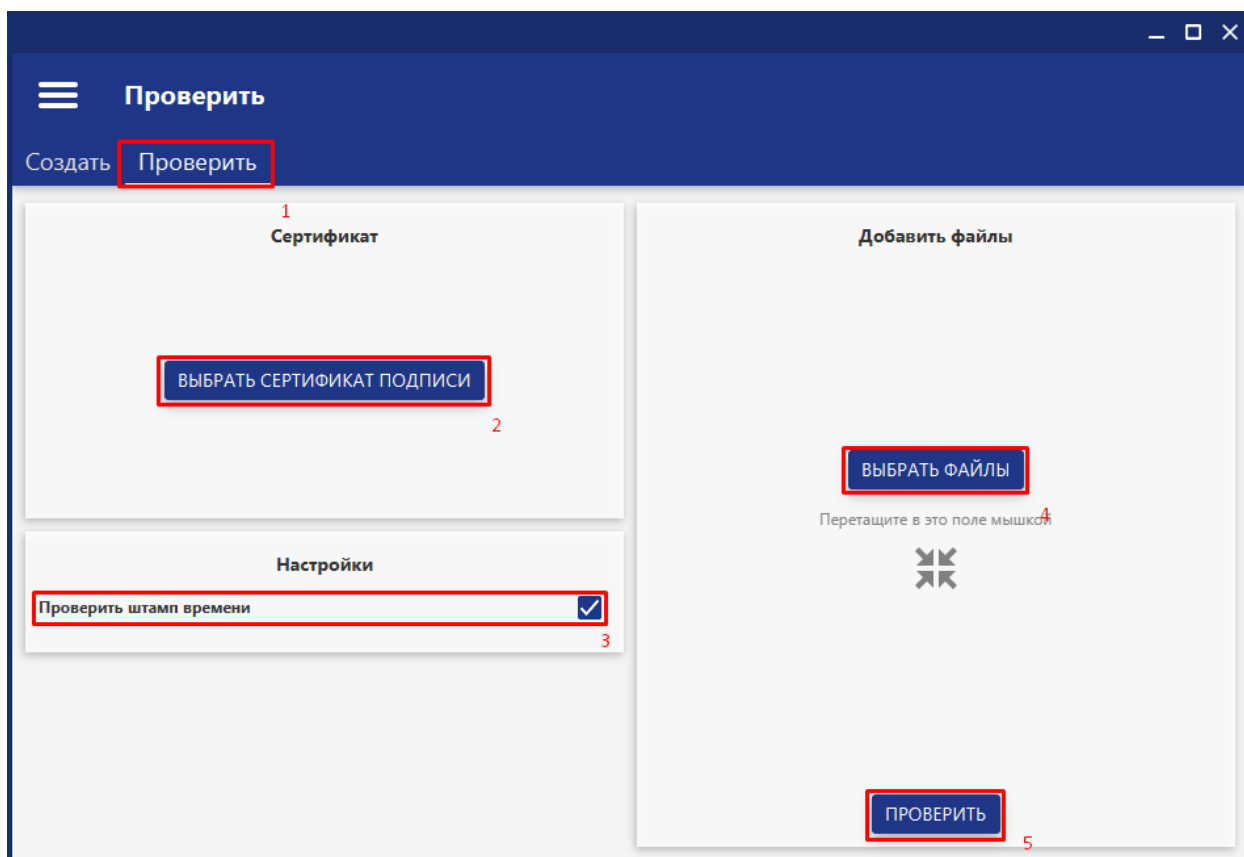
Для выбора файлов, которые должны быть подписаны, пользователь может перетащить файлы в соответствующий элемент окна либо нажать на кнопку «Выбрать файлы» и выбрать файлы из файловой системы.

ПОДПИСЬ ДОКУМЕНТА

После установки пользовательских настроек, выбора файлов и сертификата, следует нажать кнопку «Подписать». Подписанные документы будут сохранены в виде архива в директории, которую пользователь указал на первом шаге.

4.2 ПРОВЕРКА ЭЛЕКТРОННОЙ ПОДПИСИ

Для проверки подписи пользователю нужно перейти на вкладку «Проверить» (1) на экране «Цифровая подпись».



Для проверки подписей необходимо выполнить следующие шаги:

- Выбор сертификата для проверки (2). Может быть пропущено, если добавлен контейнер;
- Добавление контейнера с подписями и файлов, которые необходимо проверить, если файлы включены в контейнер (4).

Также пользователь может управлять опцией проверки штампа времени (3). Рекомендуется использовать значение по умолчанию.

ВЫБОР СЕРТИФИКАТА ДЛЯ ПРОВЕРКИ ПОДПИСИ

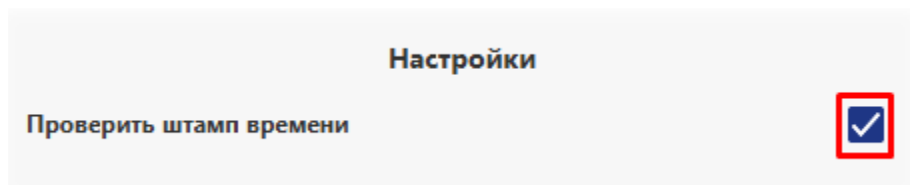
При добавлении контейнера с подписью, из него автоматически будет загружен сертификат, с помощью которого была сформирована эта подпись. Для того, чтобы выбрать сертификат, следует нажать на кнопку «Выбрать сертификат для подписи» под номером 2.

ВЫБОР СЕРТИФИКАТА

Для проверки подписей вне контейнера пользователь можете загрузить сертификат, нажав на кнопку «Выбрать сертификат подписи» под номером 2 и выбрав желаемый сертификат из списка.

ПРОВЕРКА ШТАМПА ВРЕМЕНИ

Для проверки штампов времени, которые установлены вместе с подписью, пользователю необходимо поставить соответствующий флажок.



После выбора всех необходимых файлов и настроек пользователь должен нажать на кнопку «Проверить» (5). Пользователю будут представлены результаты проверки электронной цифровой подписи в виде таблицы.

ПРОСМОТР РЕЗУЛЬТАТОВ

Результаты проверки

Исходные данные	Файл подписи	Результат	
1_без дубликатов.txt	4a79338e-ac00-48ae-bde7-fc732cdfa52d.p7s	✓	
1	2	3	4

В данном окне пользователь можете просмотреть результаты проверки подписи. Окно содержит информацию в следующем формате:

- проверяемый файл (1);
- файл подписи (2);
- результат проверки (3);
- кнопка для открытия лога операций(4).

Для просмотра подробной информации о проверке подписи пользователь может нажать соответствующую кнопку в нужной строке, после чего будет открыт лог операций.

Лог операций представляет собой последовательность шагов, которые могут иметь следующие результаты:

- Успех;
- Ошибка;
- Пропущен.

Лог операций

Шаг	Результат	Сообщения
Проверка подписи ЭЦП	✓	ЭЦП прошла проверку подписи
Проверка статуса сертификата подписи по OCSP	?	Шаг пропущен
Проверка статуса сертификата подписи по CRL	?	Шаг пропущен
Проверка сертификата подписи	✓	Самоподписной сертификат Сертификат является доверенным
Проверка штампа времени	?	Проверка штампа времени пропущена
Проверка времени создания ЭЦП	?	Шаг пропущен

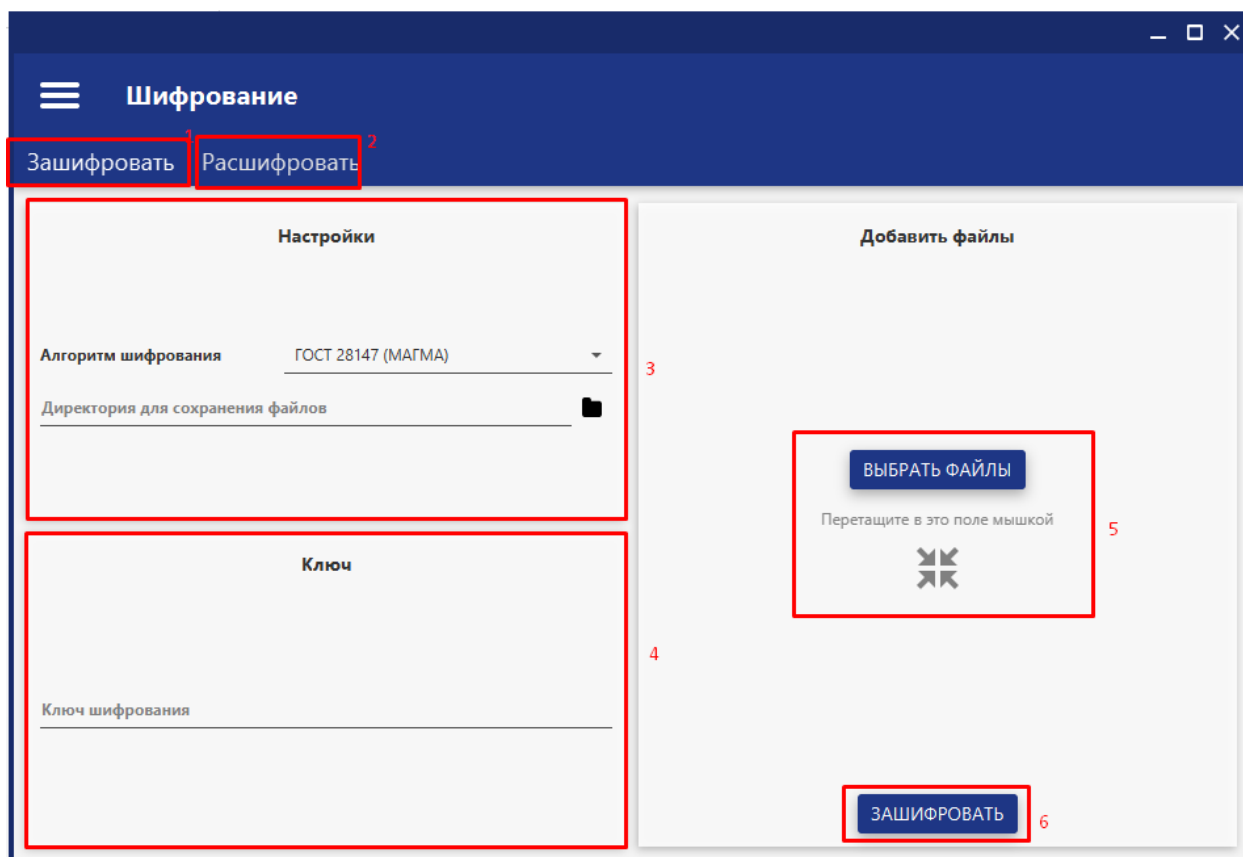
НАЗАД

5 ШИФРОВАНИЕ ДАННЫХ

Для шифрования и расшифрования файлов пользователь должен перейти на экран «Шифрование» через одноименный пункт меню.

5.1 ШИФРОВАНИЕ

Для шифрования файлов пользователь должен перейти на вкладку «Зашифровать» экрана шифрования с помощью кнопки под номером 1.



Для того чтобы выполнить шифрование файлов, необходимо выполнить следующие шаги:

- Выбрать алгоритм;
- Выбрать директорию для сохранения файлов;
- Выбрать ключ шифрования;
- Выбрать файл;
- Запустить шифрование.

ВЫБОР АЛГОРИТМА

Для выбора алгоритма подписи пользователю необходимо выбрать из выпадающего списка требуемый алгоритм (3).

ВЫБОР ДИРЕКТОРИИ ДЛЯ СОХРАНЕНИЯ ФАЙЛОВ

После нажатия на кнопку выбора директории пользователю будет предложено выбрать путь, по которому будут сохранены зашифрованные файлы (3).

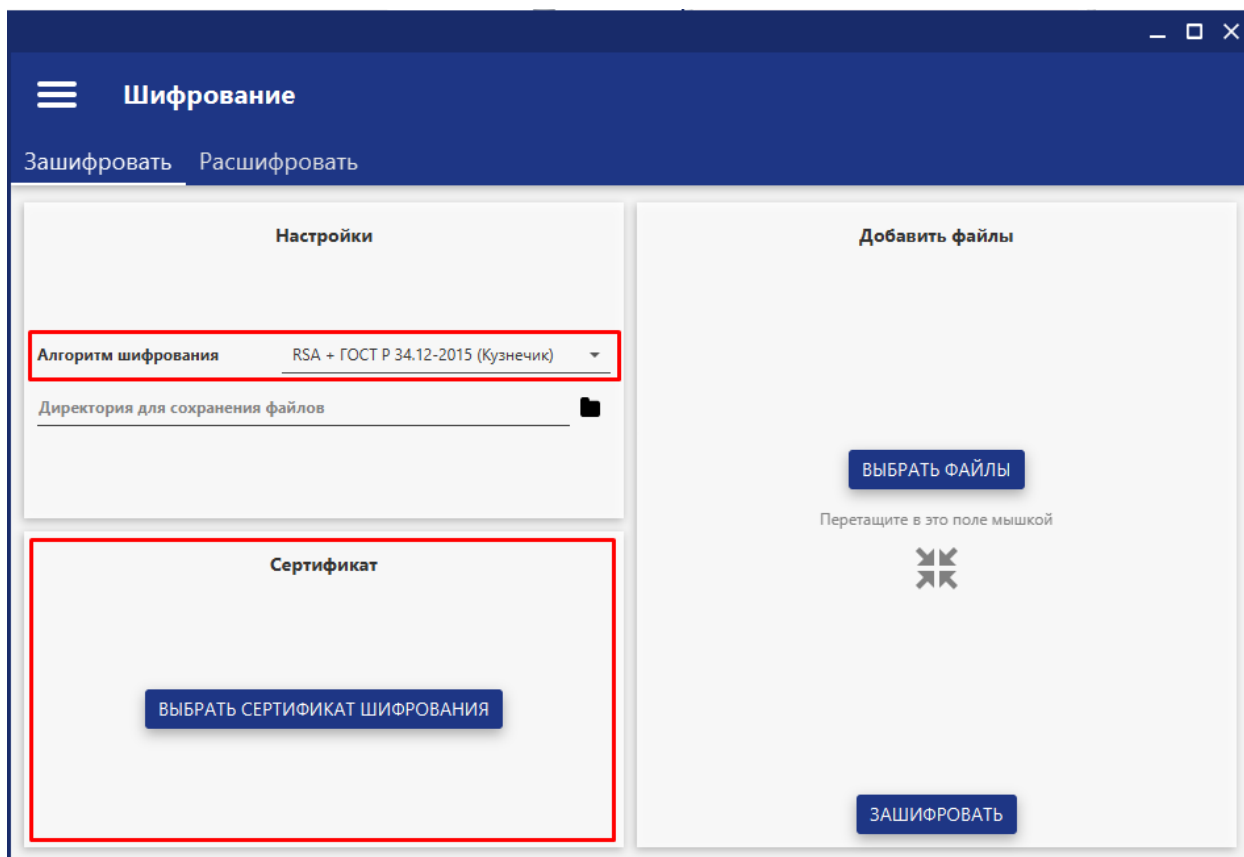
Следующий шаг зависит от выбранного алгоритма шифрования.

ВЫБОР КЛЮЧА ШИФРОВАНИЯ (ДЛЯ СИММЕТРИЧНЫХ АЛГОРИТМОВ)

Пользователю необходимо ввести ключ, с использованием которого будут зашифрованы файлы (4).

ВЫБОР СЕРТИФИКАТА (ДЛЯ АСИММЕТРИЧНЫХ АЛГОРИТМОВ)

Пользователю необходимо выбрать сертификат, с помощью которого будут зашифрованы файлы. Более подробно процесс выбора сертификата рассмотрен в разделе 4.1 (Создание электронной подписи).



ВЫБОР ФАЙЛОВ

На следующем этапе пользователю необходимо выбрать файлы, которые будут зашифрованы с помощью кнопки «Выбрать файлы» под номером 5.

ЗАПУСК ШИФРОВАНИЯ

Для запуска шифрования необходимо нажать на кнопку «Зашифровать» под номером 6. По окончании процесса зашифрованные файлы будут помещены в выбранную директорию.

5.2 РАСШИФРОВАНИЕ

Для расшифрования файлов вам нужно перейти на вкладку «Расшифровать» экрана шифрования и выполнить следующие шаги:

- Выбор алгоритма;
- Выбор директории для сохранения файлов;
- Выбор ключа;
- Выбор файлов;
- Запуск расшифрования.

ВЫБОР АЛГОРИТМА

Для выбора алгоритма подписи пользователю необходимо выбрать из выпадающего списка требуемый алгоритм (1). Рекомендуется использовать алгоритм, установленный по умолчанию.

ВЫБОР ДИРЕКТОРИИ ДЛЯ СОХРАНЕНИЯ ФАЙЛОВ

После нажатия на кнопку выбора директории пользователю будет предложено выбрать путь, по которому будут сохранены расшифрованные файлы (2).

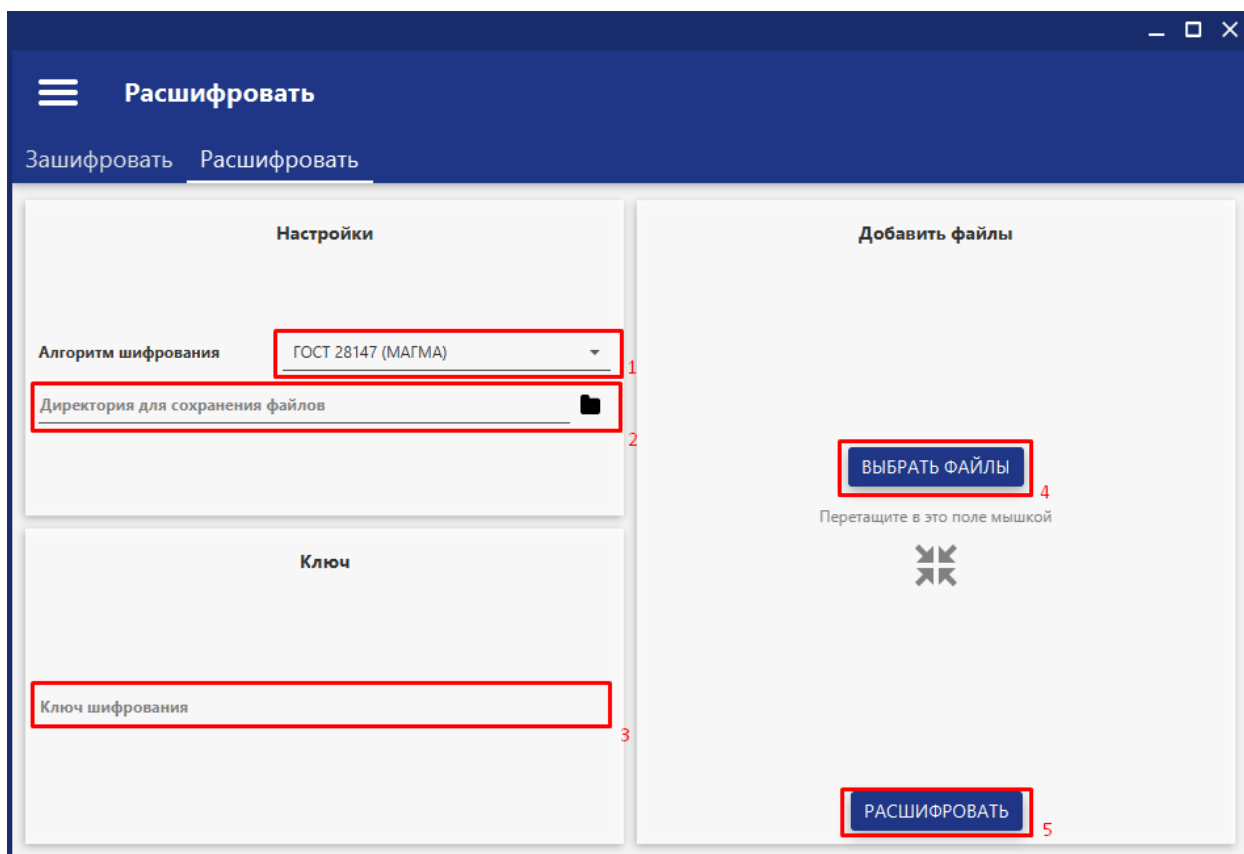
Следующий шаг зависит от выбранного алгоритма шифрования.

ВЫБОР КЛЮЧА ШИФРОВАНИЯ (ДЛЯ СИММЕТРИЧНЫХ АЛГОРИТМОВ)

Пользователю необходимо ввести ключ, с использованием которого будут расшифрованы файлы (3).

ВЫБОР СЕРТИФИКАТА (ДЛЯ АСИММЕТРИЧНЫХ АЛГОРИТМОВ)

Пользователю необходимо выбрать сертификат, с помощью которого будут расшифрованы файлы. Более подробно процесс выбора сертификата рассмотрен в разделе 4.1 (Создание электронной подписи).



ВЫБОР ФАЙЛОВ

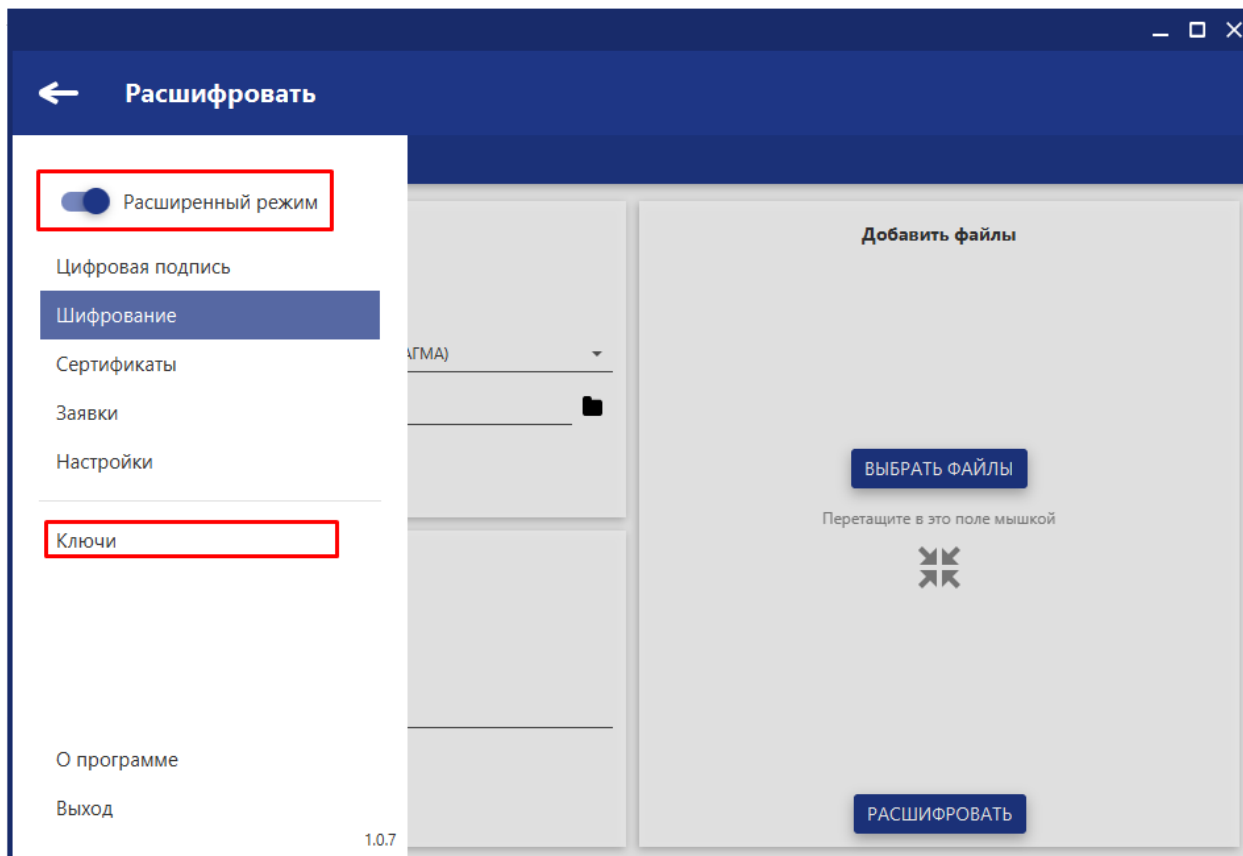
На следующем этапе пользователю необходимо выбрать файлы, которые будут расшифрованы с помощью кнопки «Выбрать файлы» под номером 4.

ЗАПУСК РАСШИФРОВАНИЯ

Для запуска расшифрования необходимо нажать на кнопку «Расшифровать» под номером 5. По окончании процесса расшифрованные файлы будут помещены в выбранную директорию.

6 ОПЕРАЦИИ С КЛЮЧАМИ

Для доступа к управлению ключами пользователю необходимо активировать «Расширенный режим» в меню приложения.



Чтобы просмотреть все ключи, необходимо выбрать в меню пункт «Ключи». Будет открыто окно с ключами, которые были добавлены ранее. О каждом ключе представлена следующая информация:

- Метка (4);
- Тип ключа (5);
- Длина ключевой пары (6);
- Дата создания (7).

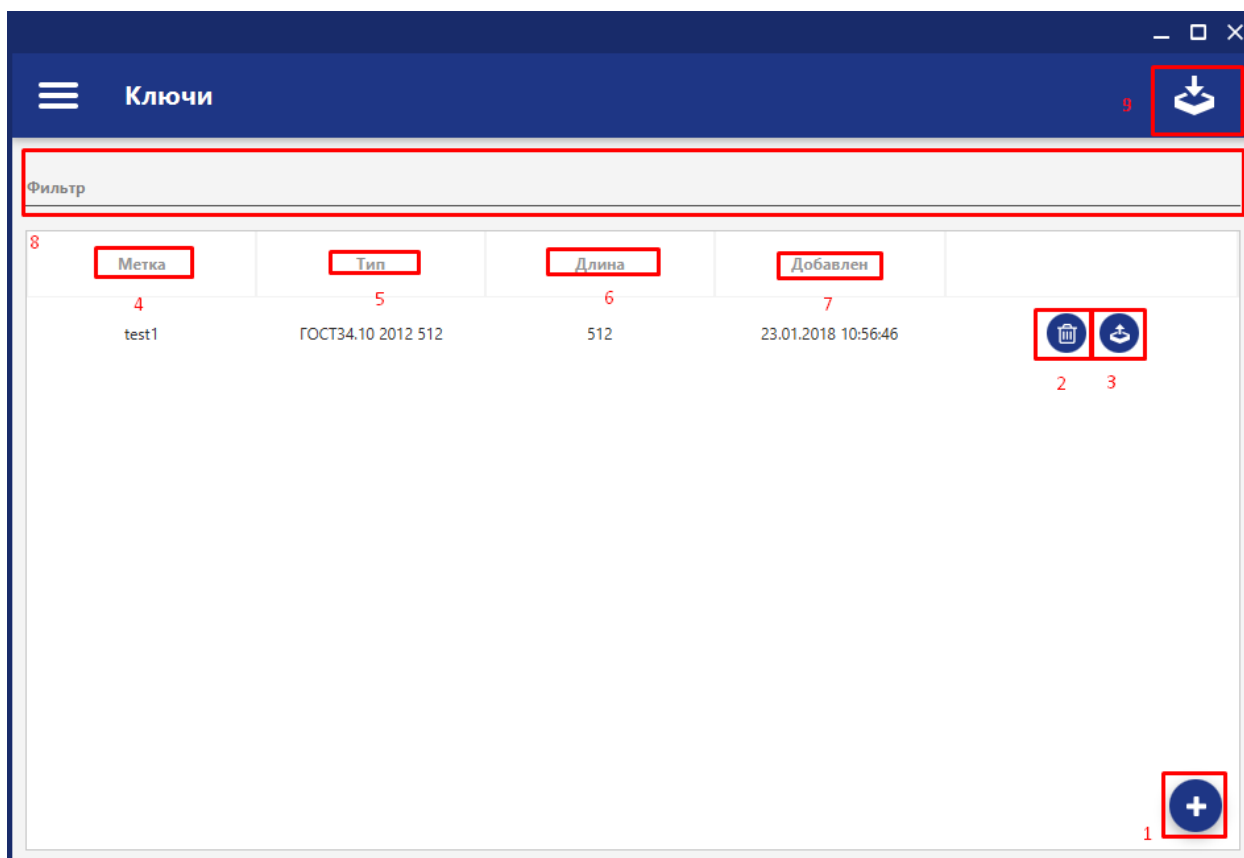
Напротив каждого ключа находятся кнопки для работы с ним.

При нажатии на кнопку 1 будет открыто окно для добавления нового ключа.

При нажатии на кнопку 2 ключ будет удалён.

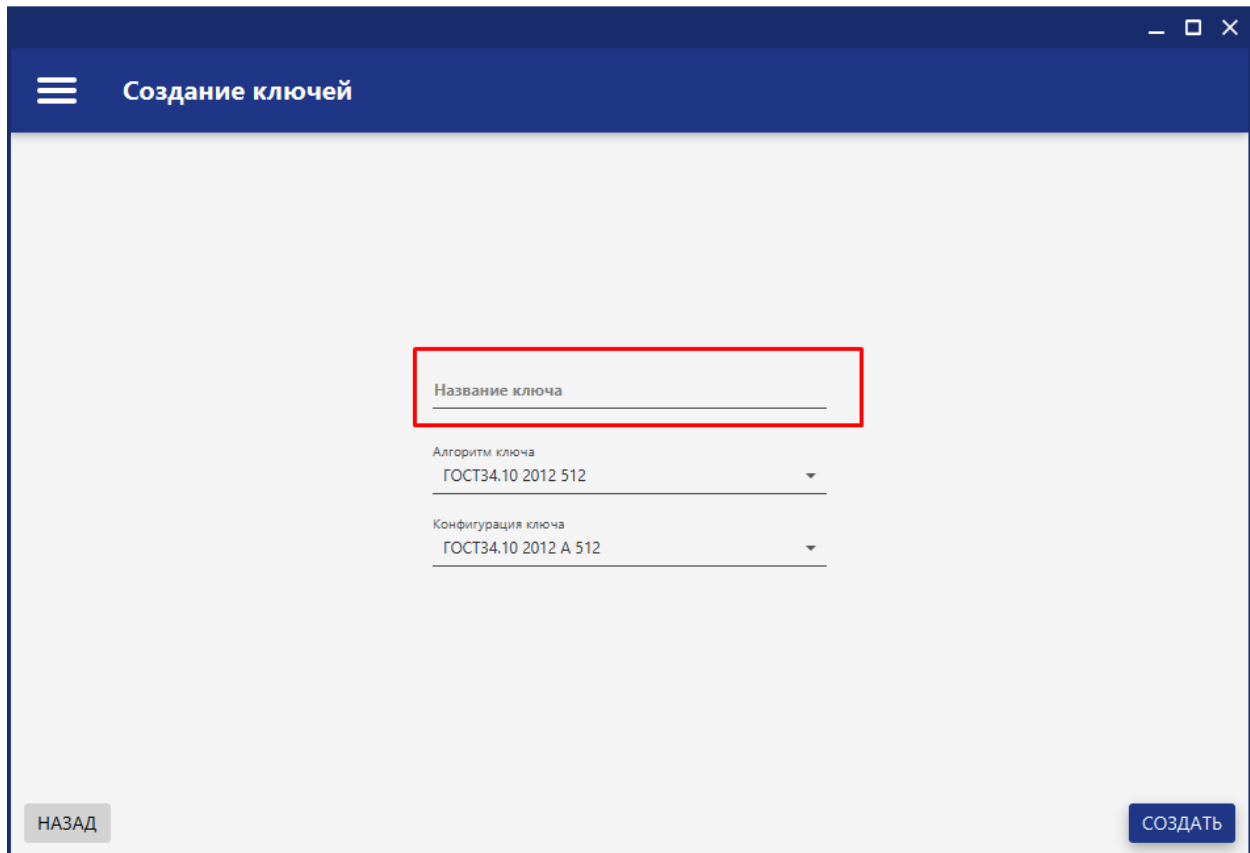
При нажатии на кнопку 3 будет осуществлён экспорт соответствующего ключа.

Строка 8 предназначена для быстрого поиска ключа. Пользователь может ввести несколько первых символов метки и ключи будут отфильтрованы по этому полю.



6.1 СОЗДАНИЕ КЛЮЧЕЙ

Для создания новой ключевой пары пользователю необходимо нажать на кнопку 1 в окне «Ключи».



Создание ключей

Название ключа

Алгоритм ключа
ГОСТ34.10 2012 512

Конфигурация ключа
ГОСТ34.10 2012 А 512

НАЗАД СОЗДАТЬ

Для создания ключевой пары пользователь должен выполнить следующие шаги:

- Ввод желаемого названия (допустимы латинские буквы в нижнем регистре, цифры и знак подчёркивания);
- Выбор алгоритма ключа;
- Выбор конфигурации ключа;
- Запуск генерации ключа с помощью кнопки «Создать».

После этого новая ключевая пара будет отображена в списке ключей.

6.2 ЭКСПОРТ КЛЮЧЕЙ

Для экспорта ключевой пары вам необходимо нажать на кнопку экспорта напротив желаемого ключа. Будет отображен диалог для сохранения двух файлов:

- public.pem — публичный ключ;
- private.pem — приватный ключ.

6.3 ИМПОРТ КЛЮЧЕЙ

Для импорта ключевой пары пользователю необходимо нажать на кнопку импорта в окне «Ключи» под номером 9.

Будет отображен диалог для выбора файла, содержащего публичный ключ.

Затем будет отображен диалог для выбора файла, содержащего приватный ключ.

После этого пользователю будет предложено ввести желаемое имя для ключевой пары.

Введите имя для импортируемого ключа

Имя ключа

ИМПОРТИРОВАТЬ ОТМЕНА

После нажатия кнопки «Импортировать» ключ появится в списке доступных ключей.

7 ОПЕРАЦИИ С СЕРВИСАМИ

Для доступа к управлению сервисами пользователю необходимо активировать «Расширенный режим» в меню приложения, а затем выбрать в меню пункт «Сервисы».

О каждом зарегистрированном сервисе представлена следующая информация:

- Имя (2);
- Дата регистрации (3);
- Дата последней активности (4);
- Статус (5).

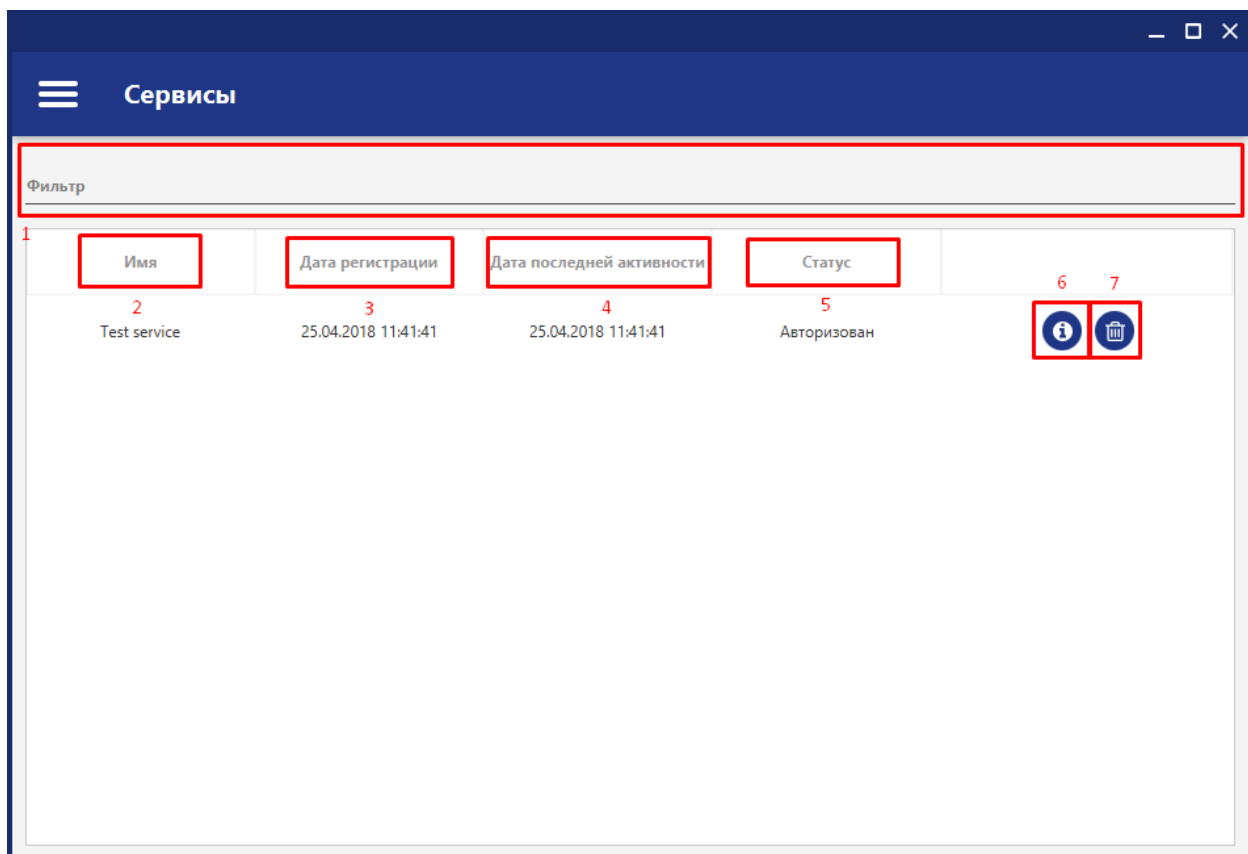
Статус сервиса может быть сменен на «Авторизован» или «Заблокирован» с помощью соответствующего поля в строке сервиса.

Напротив каждого сервиса находятся кнопки для работы с ним.

При нажатии на кнопку 6 будет открыто окно с описанием сервиса.

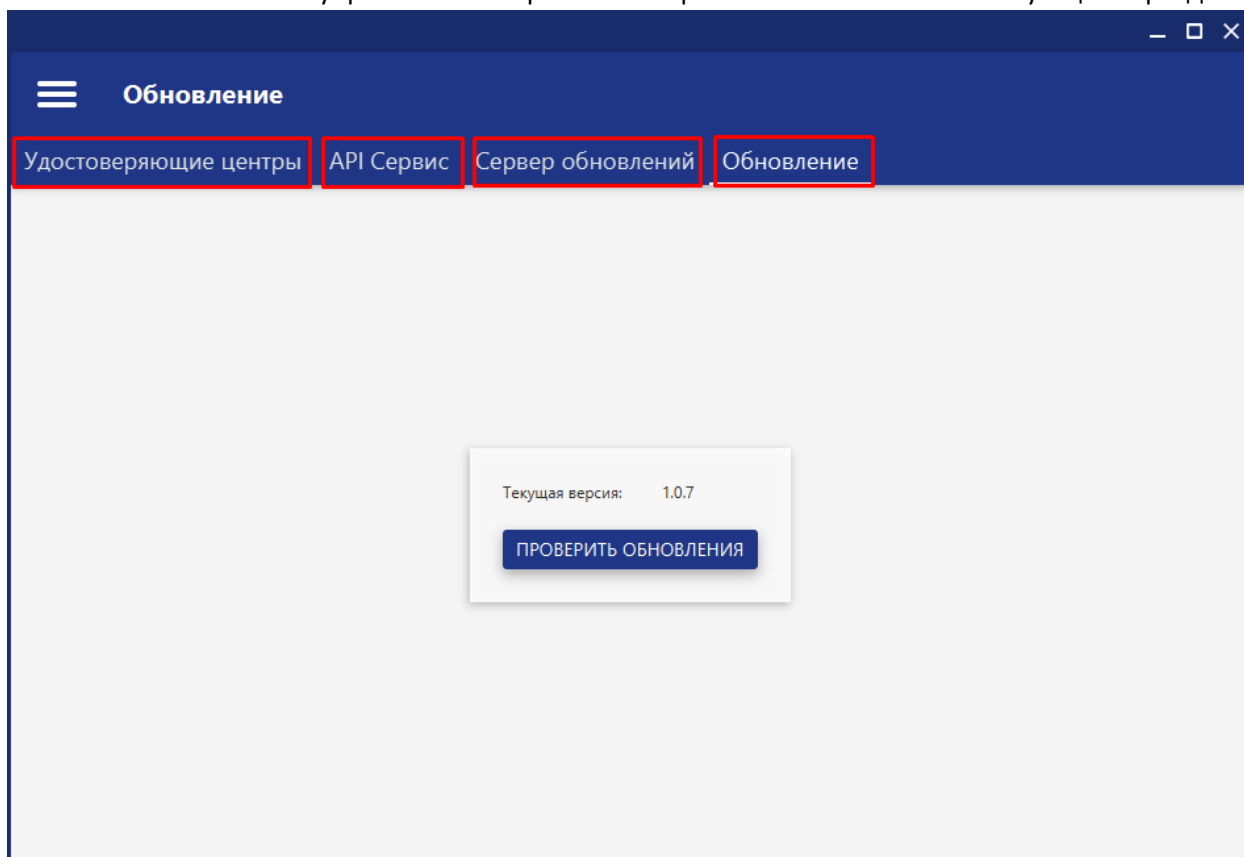
При нажатии на кнопку 7 сервис будет удален из списка зарегистрированных.

Строка 1 предназначена для быстрого поиска сервиса. Пользователь может ввести несколько символов имени, и сервисы будут отфильтрованы по этому полю.



8 НАСТРОЙКИ

Пользователь может управлять настройками приложения в соответствующем разделе.



8.1 ОПЕРАЦИИ С УДОСТОВЕРЯЮЩИМИ ЦЕНТРАМИ

Для управления удостоверяющими центрами пользователю необходимо перейти на соответствующую вкладку в окне настроек.

Окно «Удостоверяющие центры» содержит информацию о созданных удостоверяющих центрах в следующем формате (1):

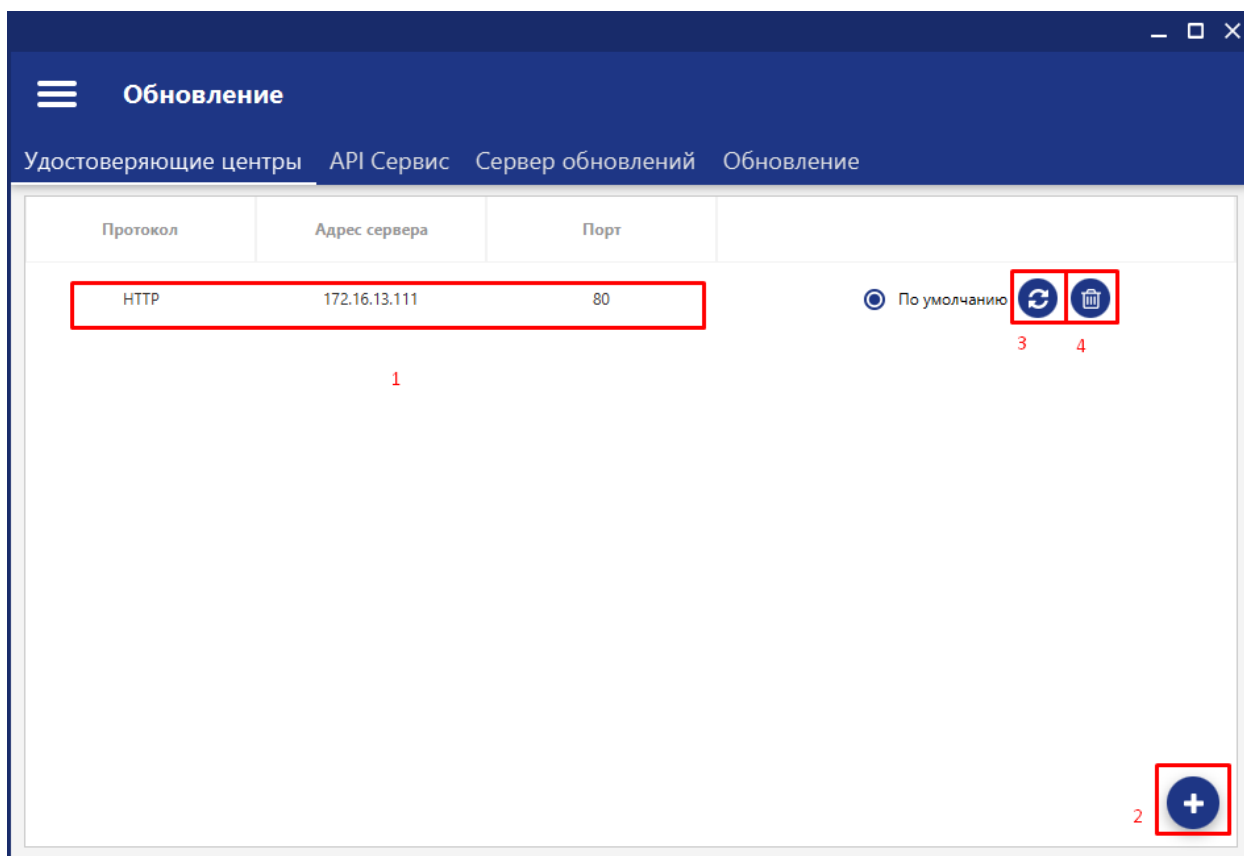
- Протокол доступа;
- Адрес сервера;
- Порт.

Напротив каждого удостоверяющего центра находятся кнопки для работы с ним.

При нажатии на кнопку 3 будет выполнена проверка подключения соответствующего ему центра.

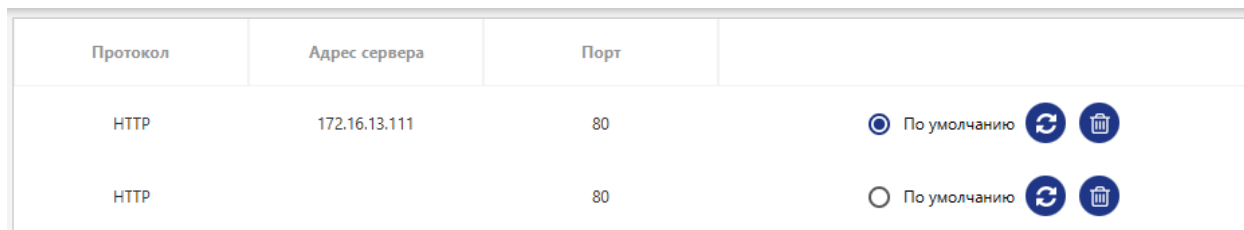
При нажатии на кнопку 4 удостоверяющий центр будет удалён из списка.

Напротив одного из удостоверяющих центров будет активна радиокнопка «По умолчанию». Это значит, что на данный момент соответствующий удостоверяющий центр выбран по умолчанию.



ДОБАВЛЕНИЕ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Для добавления удостоверяющего центра необходимо нажать на кнопку 2.



После этого в списке появится новый удостоверяющий центр, параметры подключения которого необходимо ввести пользователю. После ввода параметров следует нажать на кнопку проверки подключения под номером 3.

Если параметры введены корректно и у вас есть доступ к указанному адресу, на экране будет отображена информация о сертификате данного удостоверяющего центра.

Сертификат

Серийный номер

1

Владелец

Тестовый сертификат ГУЦ

Кем выдан

Тестовый Корневой сертификат ГУЦ

Период действия

21.12.2017 — 01.01.2099

ЗАКРЫТЬ

После закрытия данного окна, если данный сертификат не находится списке доверенных для текущего пользователя, будет предложено добавить его. Для корректной работы приложения с данным удостоверяющим центром следует добавить его сертификат в список доверенных.

Добавить данный сертификат в список доверенных?

ДА

НЕТ

После этого сертификат удостоверяющего центра будет добавлен в раздел сертификатов.

Серийный номер	Период действия	Тип	Кем выдан	Владелец	
8	24.01.2018 — 24.01.2019	Пользовательский	Тестовый сертификат Г...	test	
1	21.12.2017 — 01.01.2099	Доверенный УЦ	Тестовый Корневой се...	Тестовый сертификат Г...	

УДАЛЕНИЕ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Для удаления удостоверяющего центра необходимо нажать на кнопку удаления напротив соответствующего удостоверяющего центра.

8.2 API СЕРВИС

API позволяет сторонним сервисам подключаться к данному приложению с целью формирования и проверки подписи, а также шифрования и расшифрования файлов.

Для того чтобы включить API, следует активировать переключатель 1.

Если пользователю необходимо, чтобы API включался всегда при старте приложения, следует изменить положение переключателя 2.

При необходимости, можно активировать защищенный режим, при котором сторонним сервисам необходимо предварительно регистрироваться для работы с API. Для этого следует изменить положение переключателя 3.

Пользователь может изменить порт при необходимости в поле под номером 4. Если в момент изменения порта API было активировано, необходимо его деактивировать и активировать заново.

Для изменения максимального размера запроса в формате form-encoded необходимо задать новое значение в поле под номером 5. Рекомендуется оставить значение по умолчанию.

В случае передачи больших данных в формате multipart/form-data, они сохраняются во временные файлы. Для изменения минимального размера данных, которые будут сохранены во временные файлы, пользователю нужно установить значение в поле 6. Рекомендуется оставить значение по умолчанию.

The image shows a settings panel for the API service. It contains six numbered callouts pointing to specific controls:

- 1: A toggle switch labeled "Активация" (Activation), currently turned off.
- 2: A toggle switch labeled "Запуск при старте" (Start on launch), currently turned off.
- 3: A toggle switch labeled "Защищенный режим" (Protected mode), currently turned off.
- 4: A text input field labeled "Порт" (Port) with the value "8088".
- 5: A text input field labeled "Максимальный размер запроса form-encoded (МБ) *" (Maximum request size form-encoded (MB) *) with the value "10".
- 6: A text input field labeled "Создавать временные файлы при превышении размера (МБ) *" (Create temporary files when exceeding size (MB) *) with the value "10".

At the bottom of the panel, there is a note: "* 0 - неограниченно" (0 - unlimited).

ЗАЩИЩЕННЫЙ РЕЖИМ

При активном защищенном режиме сторонние сервисы имеют возможность отправлять запрос на регистрацию в API. При получении такого запроса будет отображено окно с информацией об этом сервисе.

У пользователя есть возможность авторизовать работу с этим сервисом (1), заблокировать его (2), либо проигнорировать этот запрос с помощью кнопки «Заккрыть» (3).

Дальнейшее управление зарегистрированными сервисами возможно в разделе «Сервисы», работа с которым описана в пункте 7.

Запрос на регистрацию сервиса

API-токен

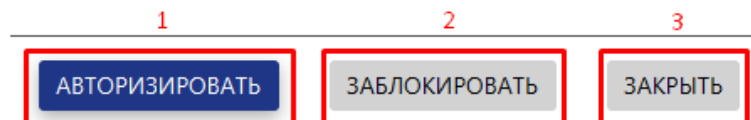
1e87ccbc-ca98-49ed-8064-e57f831f0a3f

Имя

Test service

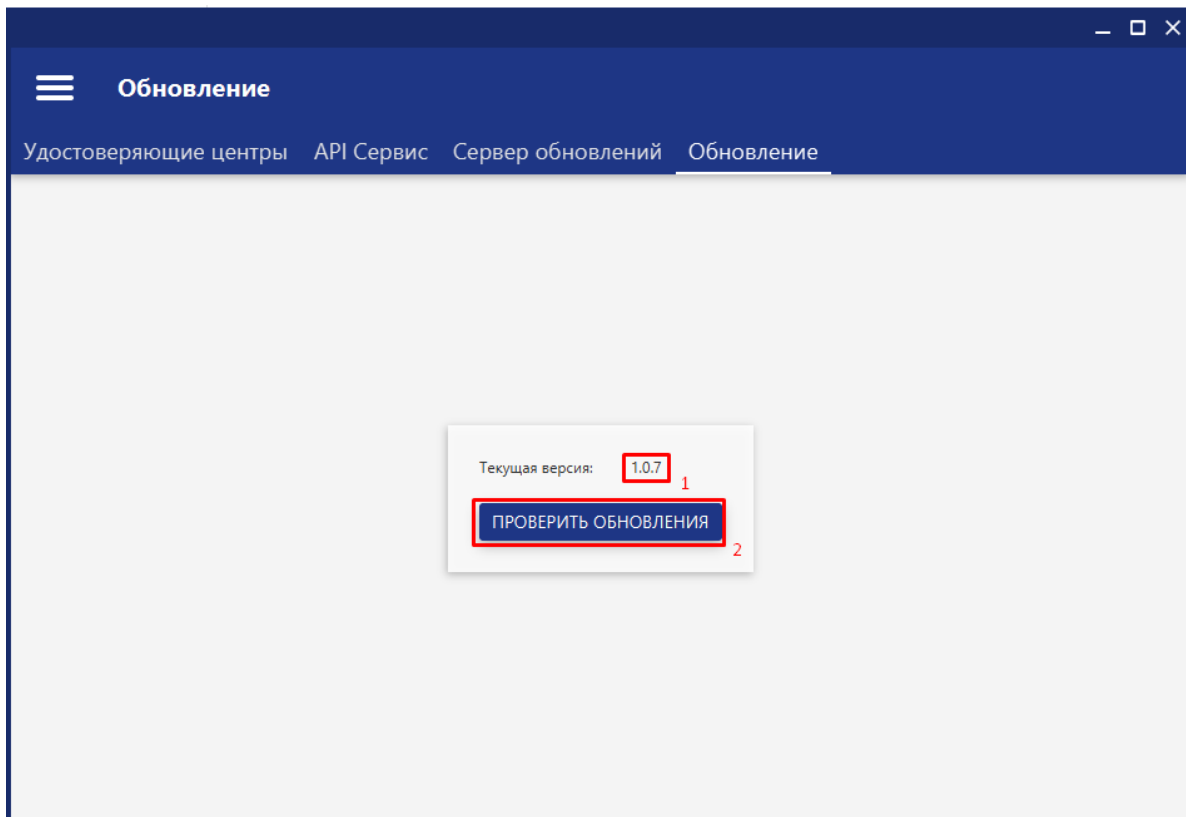
Описание

Test service

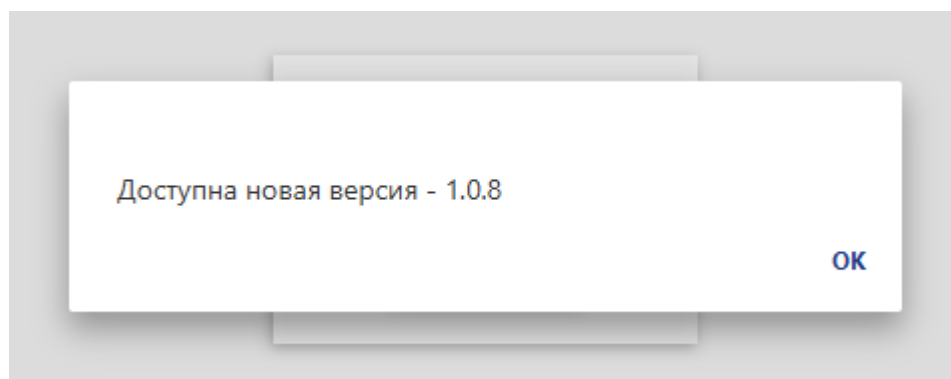


8.3 ОБНОВЛЕНИЕ

Для проверки обновлений необходимо перейти на вкладку «Обновление» экрана настроек, после чего нажать на кнопку «Проверка обновлений» (2).



Если для приложения существуют обновления, пользователь увидит окно с информацией о новой версии.



После этого вам необходимо нажать на кнопку «Обновить». Это запустит процесс обновления, по завершении которого приложение автоматически перезапустится.

8.4 СЕРВЕР ОБНОВЛЕНИЙ

Для смены адреса сервера обновлений необходимо перейти на вкладку «Сервер обновлений» экрана настроек.

Далее пользователь должен выбрать из предложенных списков протокол (1), адрес сервера (2) и ввести порт (3). Для сохранения следует нажать кнопку под номером 4.

Сервер обновлений

Удостоверяющие центры API Сервис Сервер обновлений Обновление

Протокол
HTTPS

Адрес сервера
guc-dnr.ru/updater

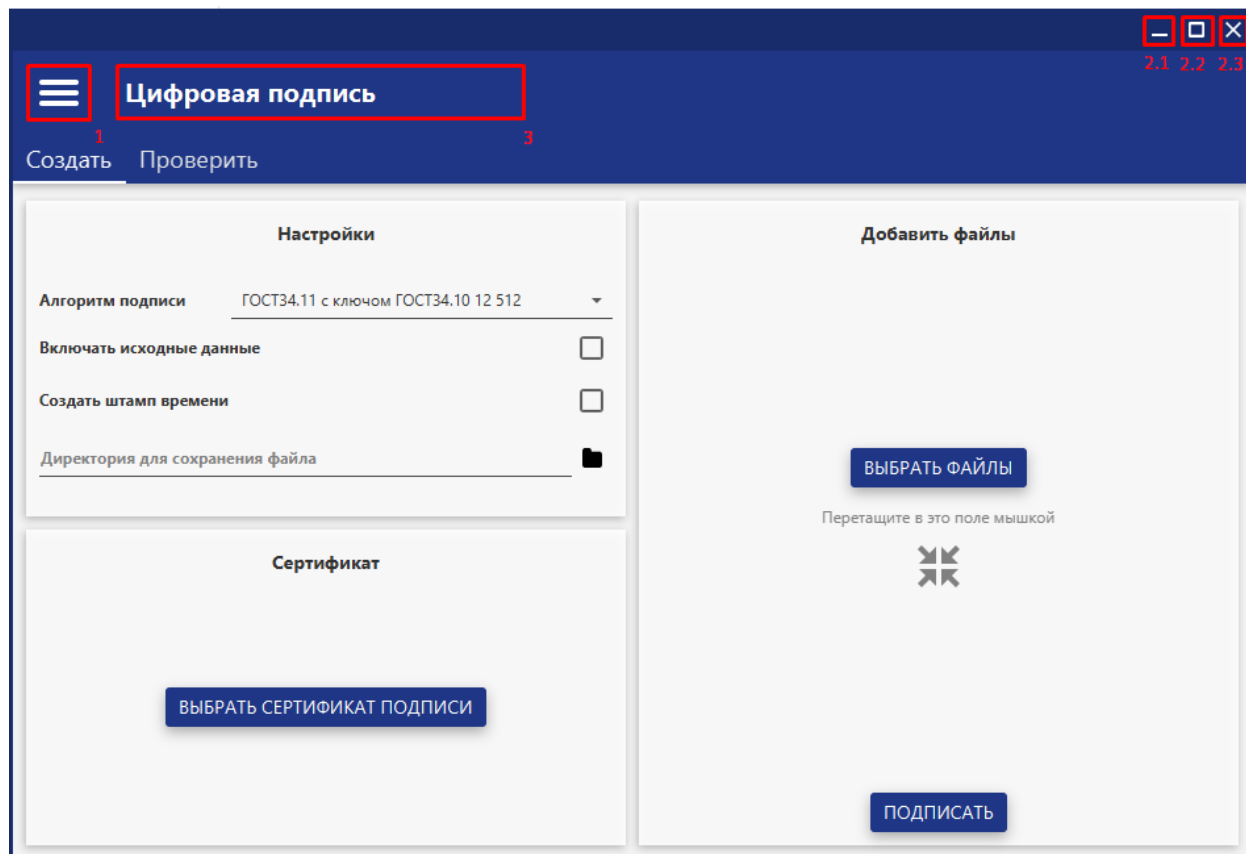
Порт
443

1 2 3 4

9 ОБЩИЕ ПРИНЦИПЫ

9.1 ГЛАВНЫЙ ЭКРАН

После запуска приложения отображается главный экран, название которого расположено вверху окна (3).



С помощью меню (1) можно осуществлять навигацию по другим разделам приложения.

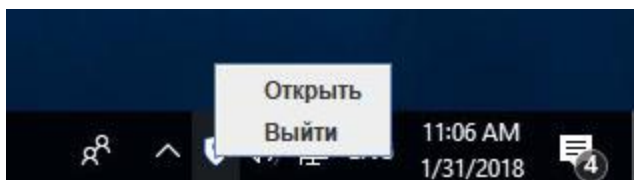
Для того, чтобы свернуть приложение, необходимо нажать кнопку «Свернуть» в правом верхнем углу (2.1). При последующем нажатии на иконку на панели задач приложение продолжит работу.

При нажатии на кнопку «Развернуть» 2.2 приложение будет развернуто на весь экран. При повторном нажатии окно свернется до исходного размера.

При нажатии на кнопку «Закреть» 2.3 окно приложения будет закрыто, однако само приложение не завершит своё выполнение, находясь в трее.

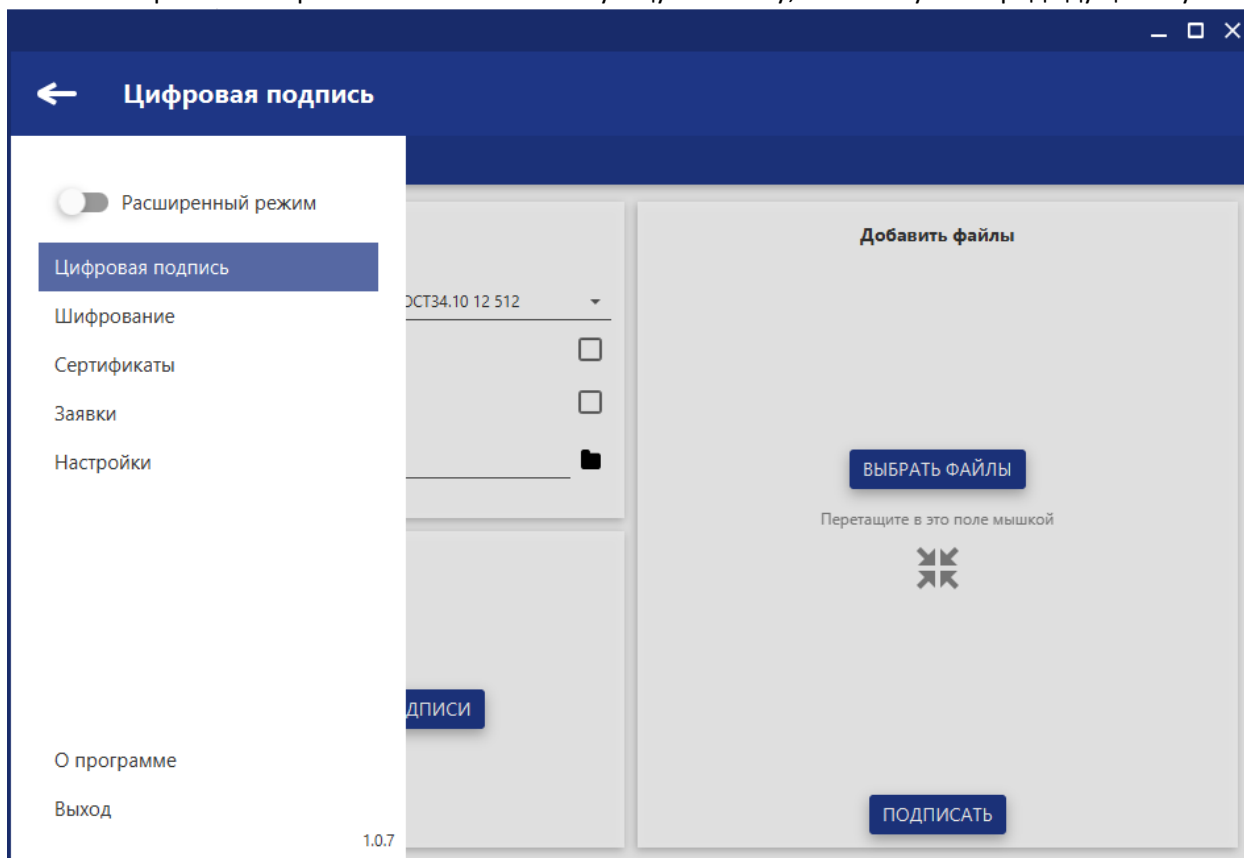


Для того, чтобы продолжить работу с приложением, необходимо нажать на иконку приложения в трее и выбрать пункт «Открыть». При выборе пункта «Выйти» приложение полностью завершит работу.



9.2 МЕНЮ

Меню отображается при клике на соответствующую иконку, описанную в предыдущем пункте.



РАСШИРЕННЫЙ РЕЖИМ

При изменении положения переключателя «Расширенный режим» пользователь получит доступ к пункту меню «Ключи».

ЦИФРОВАЯ ПОДПИСЬ

При выборе пункта меню «Цифровая подпись» будет открыт экран, где пользователь может подписывать документы и проверять электронные подписи.

ШИФРОВАНИЕ

При выборе пункта меню «Шифрование» будет открыт экран на экран, где пользователь может шифровать и расшифровать файлы.

СЕРТИФИКАТЫ

При выборе пункта меню «Сертификаты» будет открыт экран, где пользователь может работать с сертификатами.

ЗАЯВКИ

При выборе пункта меню «Заявки» будет открыт экран, где пользователь может просматривать, создавать, удалять и отправлять заявки, а также проверять их статус.

НАСТРОЙКИ

При выборе пункта меню «Настройки» будет открыт экран, где пользователь может управлять удостоверяющими центрами, сервисом API и обновлениями.

О ПРОГРАММЕ

При выборе пункта меню «Настройки» будет открыт экран, где пользователь может просмотреть информацию о программе.

КЛЮЧИ

При выборе пункта меню «Ключи» будет открыт экран, где пользователь может просматривать, создавать и удалять ключи.

СЕРВИСЫ

При выборе пункта меню «Сервисы» будет открыт экран, где пользователь может управлять зарегистрированными сервисами.

ВЫХОД

При выборе пункта меню «Выход» приложение завершит работу.