QIWI ЗАЩИТА
вер. 3.0

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ
вер. 3.0

МОСКВА
8-495-783-5959

РОССИЯ
8-800-200-0059

ФАКС
8-495-926-4619

WEB
WWW.QIWI.RU

СОДЕРЖАНИЕ

1. ГЛОССАРИЙ

Термин	Определение
Агентский сайт	Личный кабинет агента в системе QIWI, содержащий данные агента и различные сервисы, предоставляемые агенту системой.
Агентская персона	Учетная запись, зарегистрированная на агентском сайте для сотрудника агента, работающего с системой QIWI. Персона имеет определенный набор прав доступа к системе.
Сертификат	Цифровой документ, используемый для идентификации персоны на агентском сайте.
Логин	Имя пользователя, отображаемое при авторизации в приложениях QIWI.
Пароль	Секретный набор символов, используемый совместно с *логином* для авторизации пользователя.
Системное хранилище ОС	Защищенное от случайного доступа хранилище сертификатов в составе операционной системы.

2. ВВЕДЕНИЕ

Данный документ представляет собой руководство по установке и использованию приложения *QIWI Защита*.

2.1. Назначение приложения

ПО *QIWI Защита* управляет сертификатами безопасности для продуктов QIWI

ВНИМАНИЕ

Для повышения уровня безопасности авторизационные данные рекомендуется хранить на eToken.

2.2. Технические требования

Для работы приложения на локальном компьютере необходимо выполнение следующих требований к программному и аппаратному обеспечению:

- не менее 100 МБ свободного дискового пространства;
- не менее 2 ГБ оперативной памяти;
- операционная система Windows 7 и выше;
- наличие подключения к сети Интернет;
- драйверы для работы с eToken (в случае необходимости сохранения сертификатов в хранилище eToken).

3. БЫСТРЫЙ СТАРТ

3.1. Создание сертификата

Для создания сертификата выполните следующие действия:

1. Выберите пункт **Получить доступ на агентский сайт**.
2. Введите авторизационные данные персоны (**логин** и **одноразовый пароль для сертификата**).
3. Выберите тип хранилища.

СОВЕТ

Наиболее рекомендуемым хранилищем по соображениям безопасности является **eToken**.

4. Сохраните сертификат в хранилище.

ПРИМЕЧАНИЕ

Процесс создания сертификата подробно описан в разделе 6.

3.2. Создание сертификата для ПО QIWI Кассир

Для создания сертификата выполните следующее:

1. Выберите пункт **Создать сертификат для QIWI Кассира**.
2. Выберите тип хранилища.

СОВЕТ

Наиболее рекомендуемым хранилищем по соображениям безопасности является **eToken**.

3. Введите авторизационные данные персоны (**псевдоним**, **логин**, **одноразовый пароль для сертификата** и **ID терминала**).
4. Сохраните информацию в хранилище.

ПРИМЕЧАНИЕ

Процесс управления сертификатами подробно описан в разделе 7.

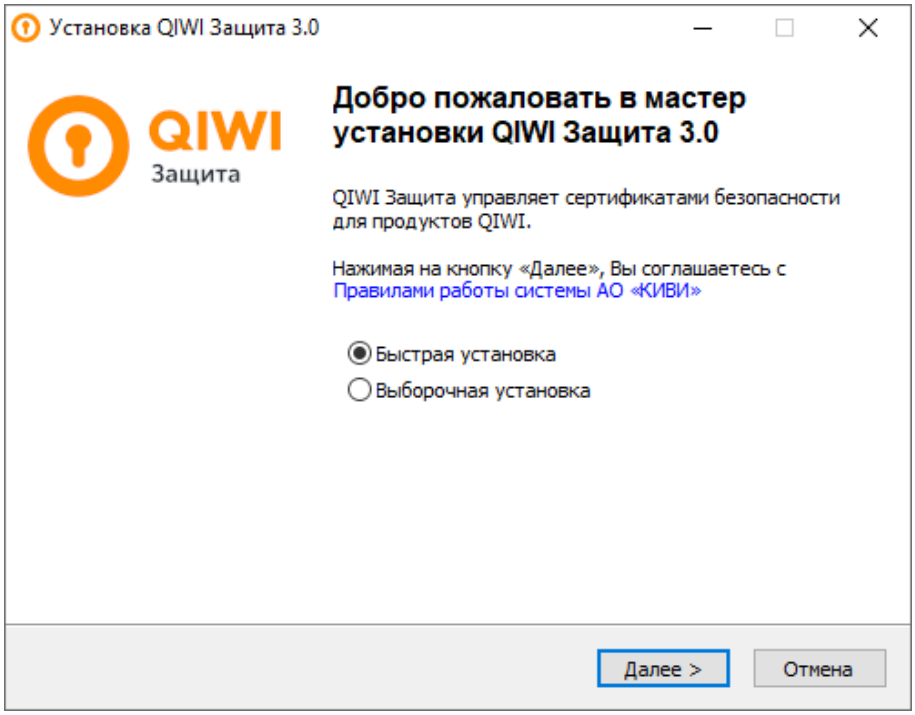
4. УСТАНОВКА И ГЛАВНОЕ ОКНО ПРИЛОЖЕНИЯ

4.1. Установка приложения

Для установки приложения выполните следующее:

1. Скачайте последнюю версию приложения с сайта qiwi.com, раздел **Бизнесу→Агентам→Скачать ПО и документацию**.
2. Запустите файл qiwiguard-x.x-win.exe (x.x – номер версии приложения) (Рис. 1).

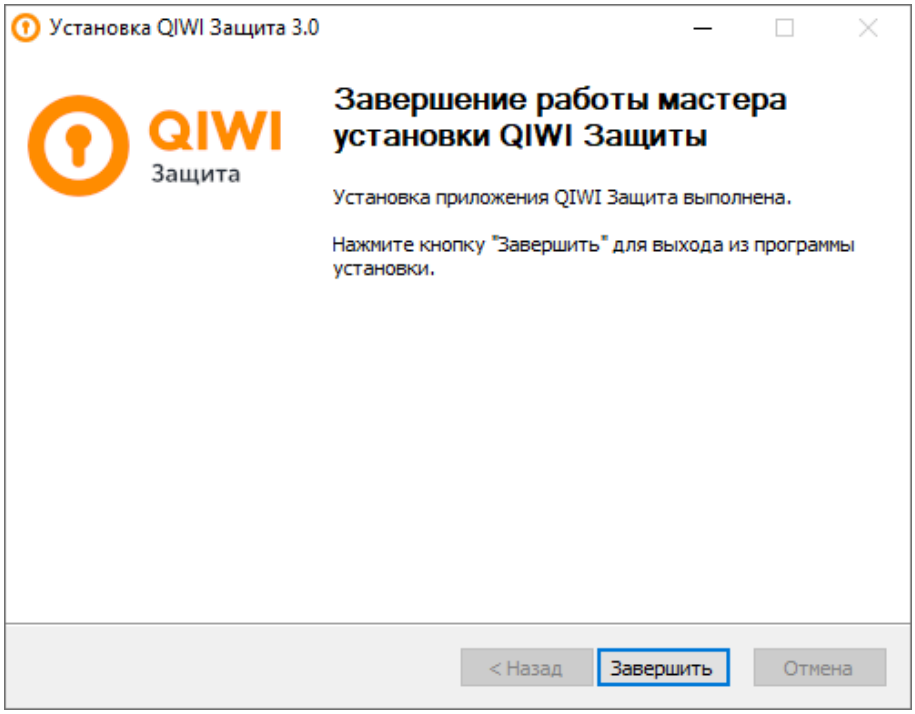
Рис. 1. Мастер установки



3. Выберите тип установки:
   - **Быстрая установка** – будет выполнена автоматическая установка приложения, и вы перейдете к финальному шагу (Рис. 2).
   - **Выборочная установка** – вам будет предложено:
     - выбрать папку для установки;
     - выбрать папку в меню *Пуск* для размещения ярлыков программы.

     После чего вы перейдете к финальному шагу установки (Рис. 2).

Рис. 2. Финальный шаг установки



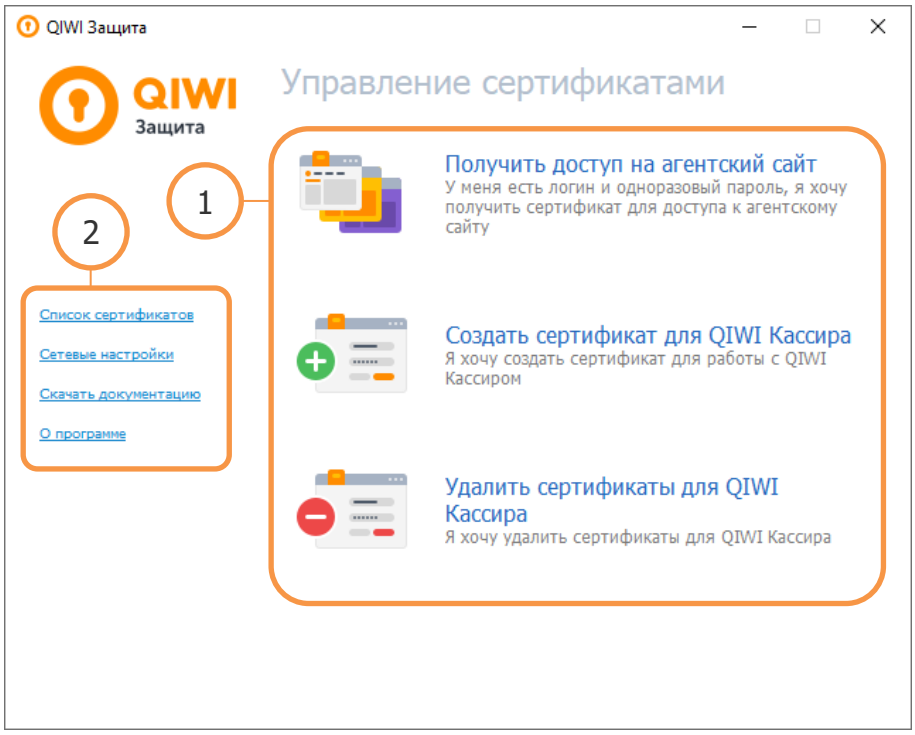
4. Для завершения работы мастера нажмите кнопку **Завершить**.

Приложение будет установлено. На рабочем столе и в меню **Пуск** будут расположены соответствующие ярлыки.

4.2. Главное окно приложения

Главное окно приложения показано на Рис. 3.

Рис. 3. Главное окно приложения



Главное окно приложения состоит из двух областей:

- **1 – Список основных задач**:
  - **Получить доступ на агентский сайт** – получение сертификата для доступа к агентскому сайту. Подробнее см. в разделе 6.
  - **Создать сертификат для QIWI Кассира** – создание сертификата для работы с ПО *QIWI Кассир*. Подробнее см. в разделе 7.
  - **Удалить сертификаты для QIWI Кассира** – удаление сертификата для ПО *QIWI Кассир.*
- **2 – Список дополнительных возможностей:**
  - Список сертификатов – открывает системное хранилище сертификатов;
  - Сетевые настройки – открывает меню настроек параметров сети для доступа к Интернету;
  - Скачать документацию – открывает раздел **Бизнесу→Агентам→Скачать ПО и документацию** на сайте qiwi.com, откуда можно скачать последнюю версию руководства пользователя;
  - О программе – открывает окно с информацией о приложении.

5. ПРЕДВАРИТЕЛЬНАЯ ПОДГОТОВКА

На агентском сайте необходимо зарегистрировать:

- для получения доступа на агентский сайт – персону;
- для создания персоны для ПО «QIWI Кассир» – персону и терминал;
- задать **Логин персоны**;
- сгенерировать **пароль**.

Логин и пароль персоны будут отправлены в SMS на мобильный телефон персоны, создающей данную персону (т.е. той, с данными которой вы авторизовались на агентском сайте для создания новой персоны).

ПРИМЕЧАНИЕ

Одноразовый пароль в процессе генерации сертификата можно использовать только один раз, после чего он блокируется сервером. Если процесс был завершен ошибкой, вам будет необходимо сгенерировать новый одноразовый пароль.

ВНИМАНИЕ

Для роли «Главный менеджер» и некоторых других сертификат разрешается сохранять только в хранилище eToken.

Подробнее о создании персон, терминалов и генерации одноразового пароля см. в Руководстве пользователя агентского сайта.

6. ПОЛУЧЕНИЕ ДОСТУПА НА АГЕНТСКИЙ САЙТ

ВНИМАНИЕ

Перед работой с ПО QIWI Защита рекомендуется выполнить синхронизацию даты и времени.

Перед генерацией сертификата с помощью ПО QIWI Защита прочтите раздел 5.

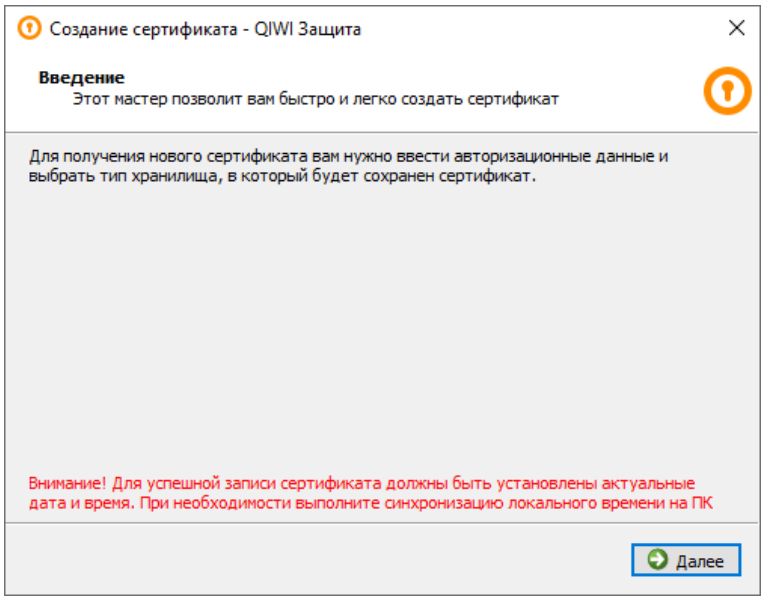
Для роли «Главный менеджер» и некоторых других сертификат разрешается сохранять только в хранилище eToken.

Для получения доступа на агентский сайт необходимо сгенерировать сертификат. Для этого:

1. В главном окне приложения выберите действие **Получить доступ на агентский сайт** (см. Рис. 3).

   Будет открыт *Мастер создания сертификатов* (Рис. 4).

Рис. 4. Мастер создания сертификатов



2. Укажите данные персоны для генерации сертификата (Рис. 5):
   - **Логин** – логин персоны;
   - **Пароль** – одноразовый пароль для сертификата;
   - **Показать пароль** – проставьте флаг, если необходимо отобразить значение поля **Пароль**.

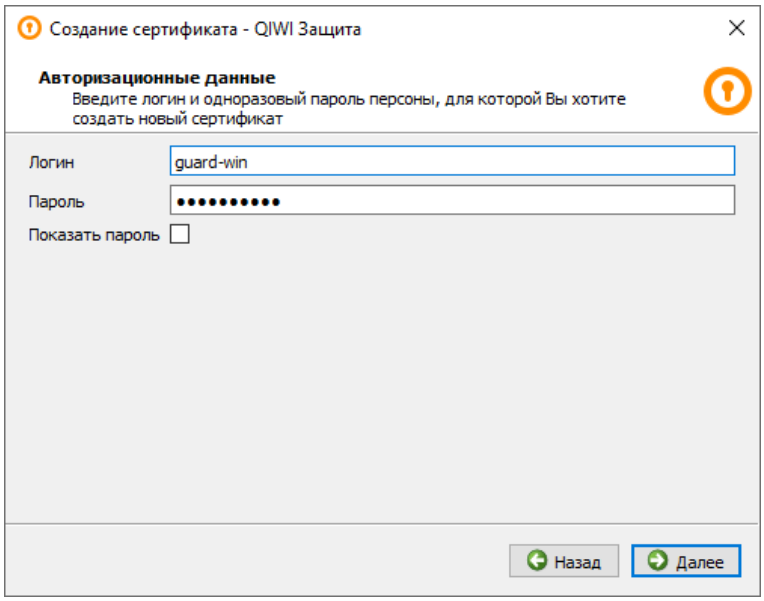
ПРИМЕЧАНИЕ

Далее описаны шаги генерации сертификата с типом хранилища eToken, т.к. он является наиболее рекомендуемым хранилищем по соображениям безопасности.

Процесс сохранения сертификата в другое хранилище описан в приложениях:

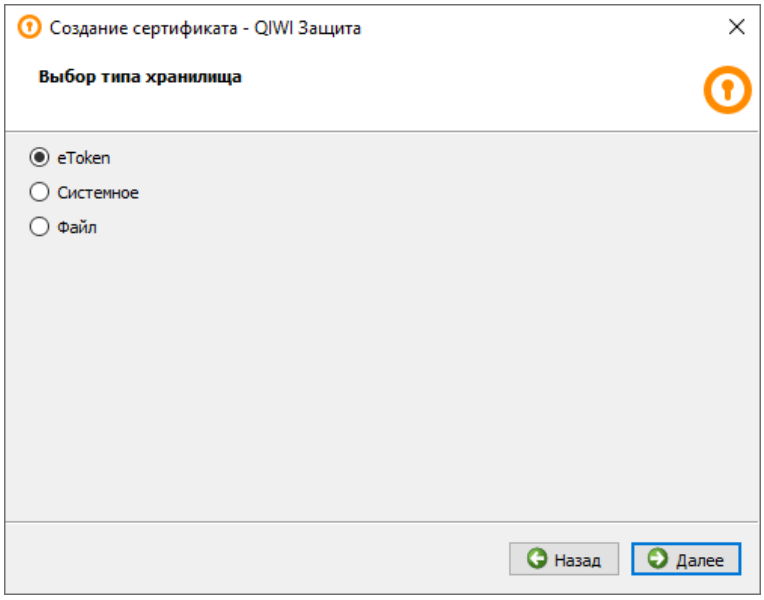
- Системное хранилище – Приложение Б;
- Файл – Приложение В.

Рис. 5. Ввод авторизационных данных



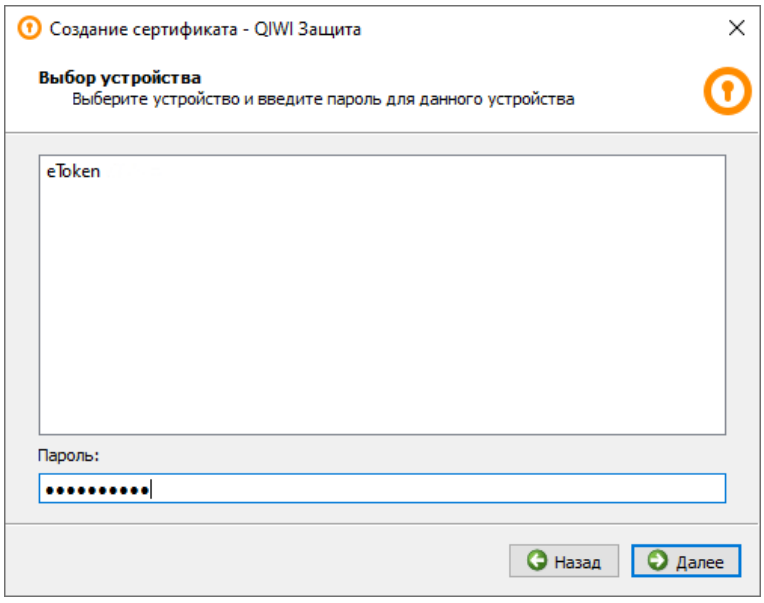
3. Выберите тип хранилища **eToken** (Рис. 6).

Рис. 6. Выбор хранилища сертификата



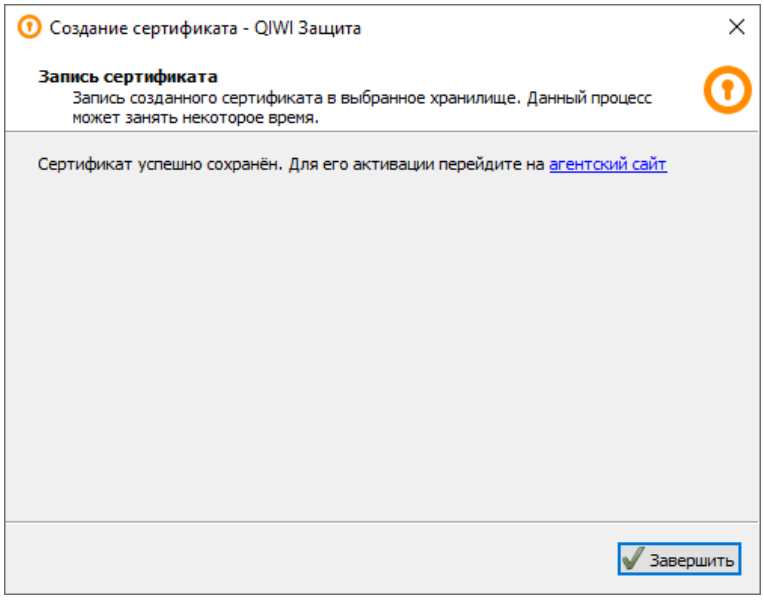
4. Выберите необходимое устройство из списка eToken и укажите пароль для него (Рис. 7).

Рис. 7. Выбор устройства хранения информации



5. Дождитесь сообщения «*Сертификат успешно сохранен*» и нажмите кнопку **Завершить** (Рис. 8).

Рис. 8. Запись сертификата



Сертификат сохранен на eToken, его можно использовать для входа на сайт.

Подробнее об авторизации на агентском сайте с помощью сертификата см. в Приложении А.

7. СОЗДАНИЕ/УДАЛЕНИЕ СЕРТИФИКАТА ДЛЯ QIWI КАССИР/QIWI КАССИР ДЛЯ 1С:ПРЕДПРИЯТИЯ

ПО *QIWI Защита* позволяет сгенерировать (а также удалить ранее созданный) сертификат для работы с ПО *QIWI Кассир.*

7.1. Создание сертификата

ВНИМАНИЕ

Перед работой с ПО QIWI Защита рекомендуется выполнить синхронизацию даты и времени.

Перед созданием сертификата с помощью ПО QIWI Защита прочтите раздел 5.

Для создания сертификата выполните следующее:

1. В главном окне приложения выберите **Создать сертификат для QIWI Кассира** (см. Рис. 3). Будет открыт *Мастер создания сертификатов для QIWI Кассира.*

ВНИМАНИЕ

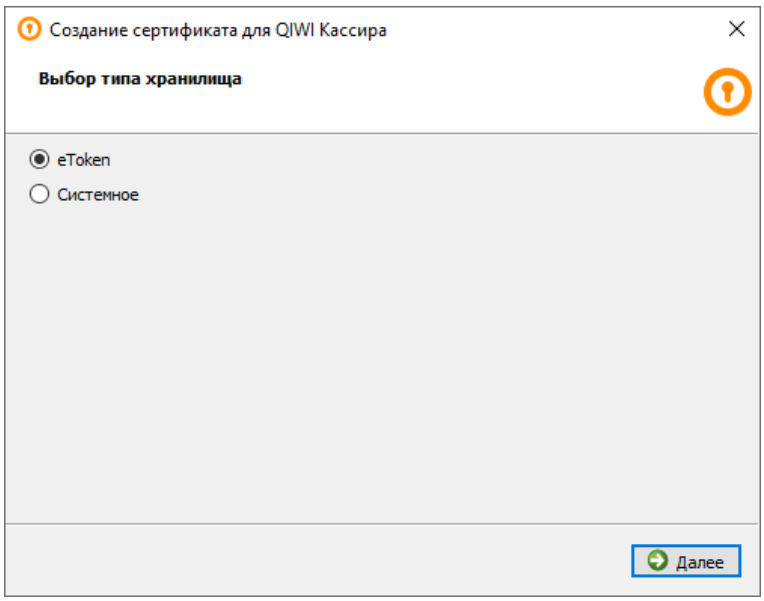
Далее описаны шаги при выборе типа хранилища **eToken**, т.к. это хранилище является наиболее безопасным.

Процесс сохранения сертификата в другое хранилище описан в приложениях:

- Системное хранилище – Приложение Б;
- Файл – Приложение В.

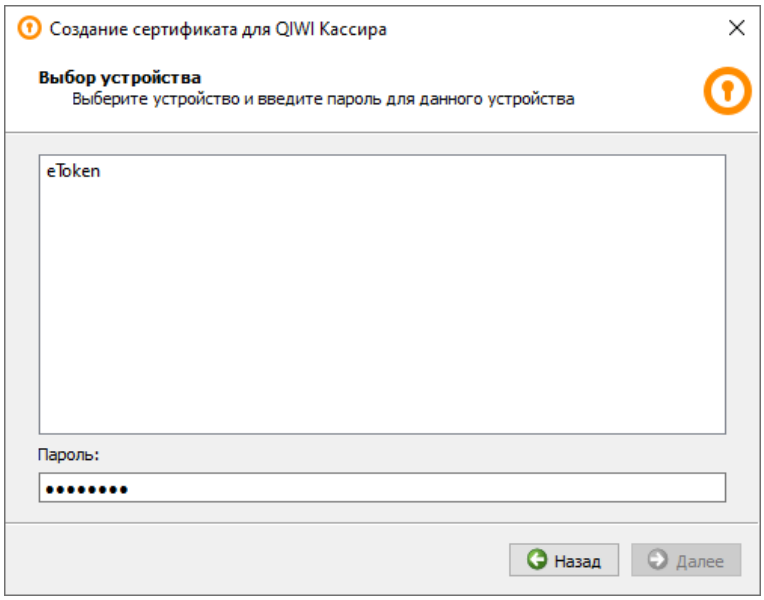
2. Выберите тип хранилища **eToken** (Рис. 9).

Рис. 9. Выбор устройства хранения информации о персонах



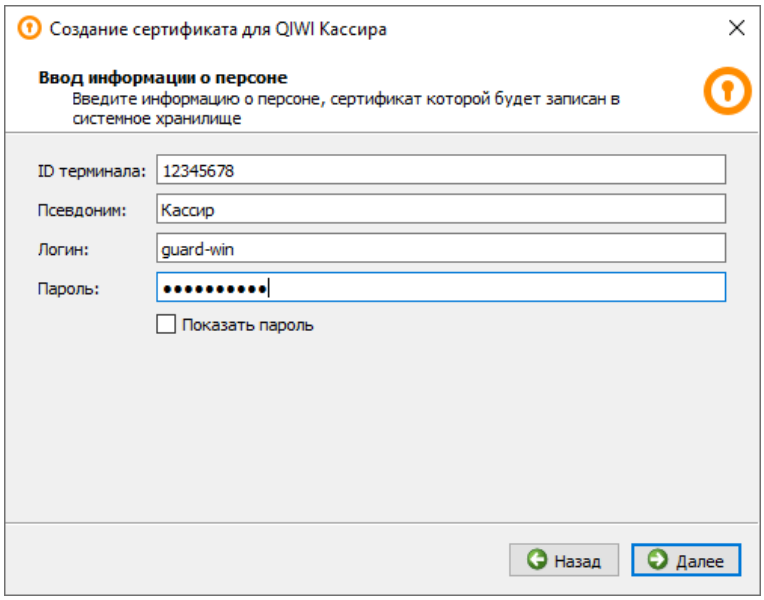
3. Выберите необходимый eToken и укажите пароль для него (Рис. 10).

Рис. 10. Выбор устройства хранения информации



4. Введите данные персоны и нажмите кнопку **Далее** (Рис. 11):

Рис. 11. Ввод информации о персоне

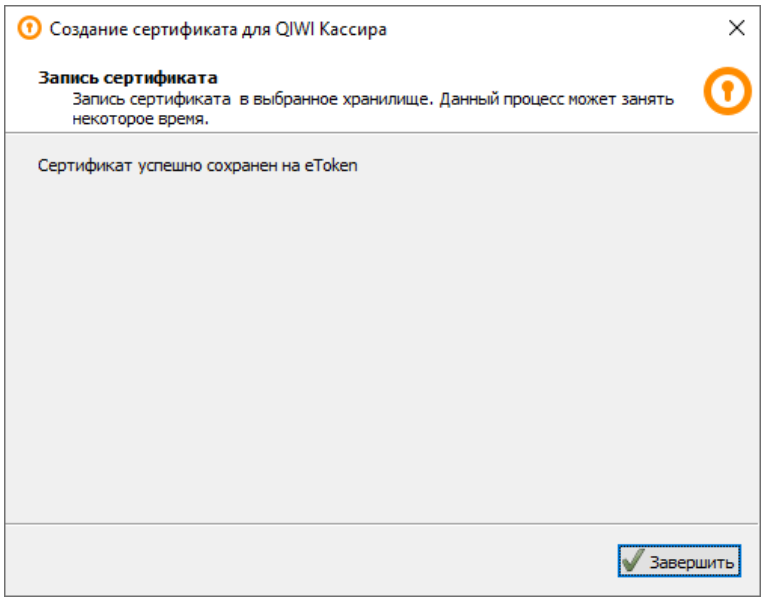


- **Псевдоним** – введите любое имя учетной записи, которое в дальнейшем будет использоваться для авторизации в ПО *QIWI Кассир*;
- **Логин** – логин персоны;

- **ID терминала** – номер терминала;
- **Пароль** – одноразовый пароль для сертификата;
- **Показать пароль** – проставьте флаг, если необходимо отобразить значение поля **Пароль**.

5. Дождитесь сообщения «*Сертификат успешно сохранен на eToken*» и нажмите кнопку **Завершить** (Рис. 12).

Рис. 12. Успешная запись данных



Авторизационные данные персоны сохранены на eToken.

7.2. Удаление сертификата

Для удаления сертификата в главном окне приложения выберите **Удалить сертификат для QIWI Кассира** (см. Рис. 3).

С помощью мастера управления персонами выполните следующее:

1. Выберите тип хранилища:
   - **eToken**;

ПРИМЕЧАНИЕ

Вам будет предложено выбрать необходимый **eToken** и указать пароль к нему.

   - **Системное хранилище**;
2. Выберите сертификаты, которые необходимо удалить;
3. Нажмите кнопку **Далее.**

Сертификаты будут удалены.

8. ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

Приложение реализует следующие дополнительные возможности:

- Список сертификатов – открывает системное хранилище сертификатов;
- Сетевые настройки – открывает меню настроек параметров сети для доступа к Интернету;
- Скачать документацию – открывает раздел **Бизнесу→Агентам→Скачать ПО и документацию** на сайте qiwi.com, откуда можно скачать последнюю версию руководства пользователя;
- О программе – открывает окно с информацией о приложении.

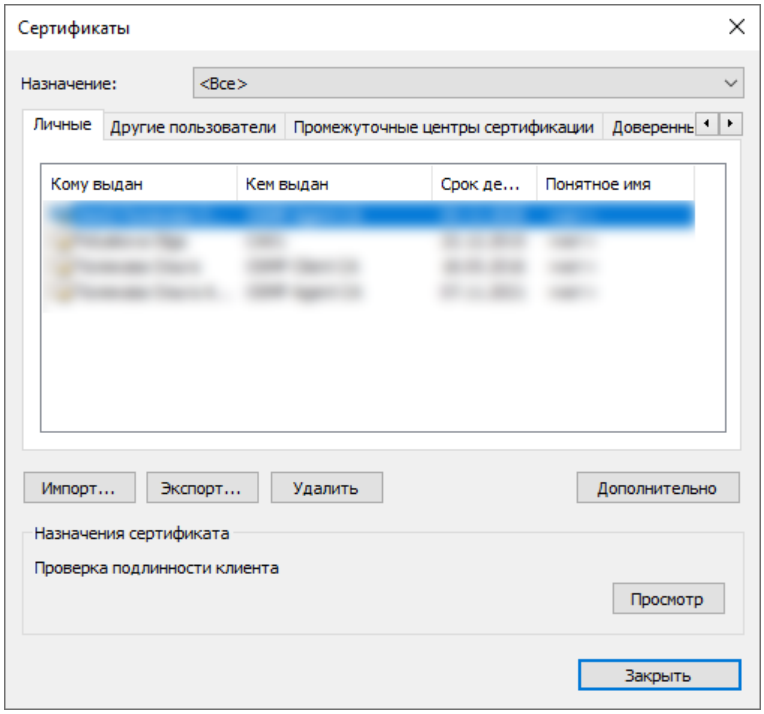
8.1. Список сертификатов

Для просмотра сертификатов, установленных в системе, выберите **Список сертификатов** в главном окне приложения (см. Рис. 3). Будет открыто окно **Сертификаты** (Рис. 13).

ПРИМЕЧАНИЕ

На вкладке **Личные** отображаются сертификаты, выданные данному пользователю ОС.

Рис. 13. Системные сертификаты



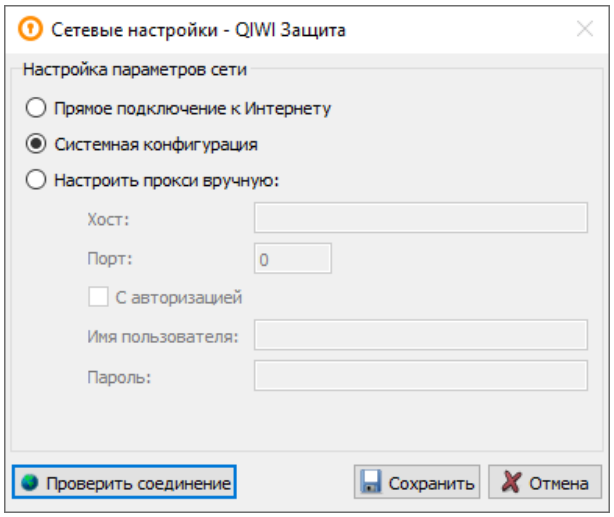
8.2. Сетевые настройки

Для изменения сетевых настроек выполните следующее:

1. В главном окне приложения выберите **Сетевые настройки** (см. Рис. 3).

   Будет открыто диалоговое окно **Сетевые настройки** (Рис. 14).

Рис. 14. Установки прокси



2. Задайте необходимые настройки:

   – **Прямое подключение к Интернету** – соединение с сетью Интернет без прокси-сервера.

   – **Системная конфигурация** – при подключении будут использованы настройки свойств обозревателя.

ВНИМАНИЕ

Для использования данного типа подключения в *Свойствах обозревателя* должен быть установлен флаг **Автоматическое определение параметров.**

Проверить флаг можно, выполнив переход **Пуск→Панель управления→Свойства обозревателя→Подключения→Настройка сети.**

   – **Настроить прокси вручную –** позволяет задать следующие настройки прокси:

ПРИМЕЧАНИЕ

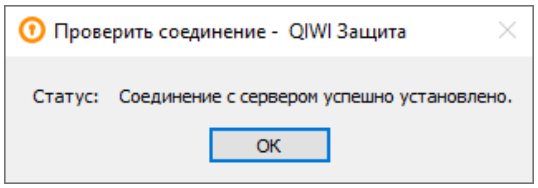
Информацию о прокси-сервере запросите у вашего системного администратора.

   - **Хост** – адрес прокси-сервера.
   - **Порт** – порт подключения к прокси-серверу.
   - **С авторизацией** – установите флаг, если на прокси-сервере используется авторизация:
     - **Имя пользователя** и **Пароль** – укажите авторизационные данные подключения к прокси-серверу (если требуется).

3. Нажмите кнопку **Сохранить**.
4. Нажмите кнопку **Проверить соединение**.

Если все настройки были заданы правильно, вы увидите сообщение (Рис. 15).

Рис. 15. Успешное соединение с сервером



8.3. Загрузка документации

Для получения руководства пользователя к текущей версии ПО:

1. Выберите пункт **Скачать документацию** в главном окне приложения (Рис. 3).
2. С помощью окна проводника укажите место, куда будет сохранен документ.
3. Нажмите кнопку **Сохранить**.

Документ будет загружен.

ПРИЛОЖЕНИЕ А: Авторизация на сайте

ВНИМАНИЕ

При первой авторизации вам будет необходимо пройти процедуру подтверждения сертификата. Подробнее см. в Руководстве по работе с сайтом (раздел «Активация сертификата»).

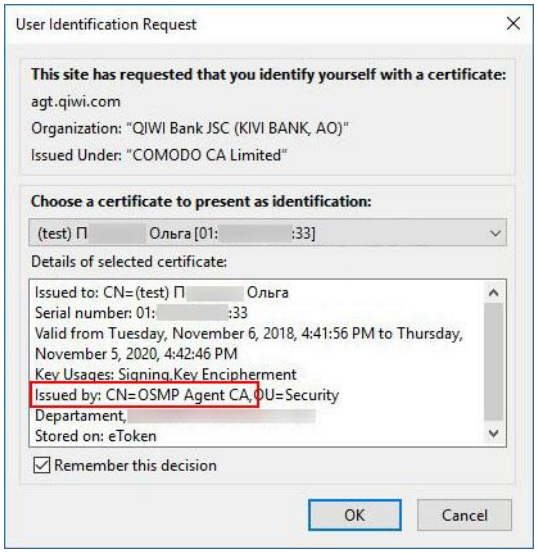
Для авторизации на агентском сайте QIWI выполните следующее:

1. Установите ключ eToken в USB порт компьютера (пропустите этот пункт, если сертификат находится в хранилище сертификатов компьютера).
2. В браузере введите адрес agt.qiwi.com или agent.qiwi.com.
3. Если установлен ключ eToken, браузер запросит пароль от него. Введите пароль и нажмите ОК.

Рис. 16. Ввод пароля от eToken

4. Будет открыто окно выбора сертификта (Рис. 17). Выберите сертификат, выпущенный *OSMP Agent CA*, и нажмите **ОК**.

Рис. 17. Выбор сертификата



ПРИМЕЧАНИЕ

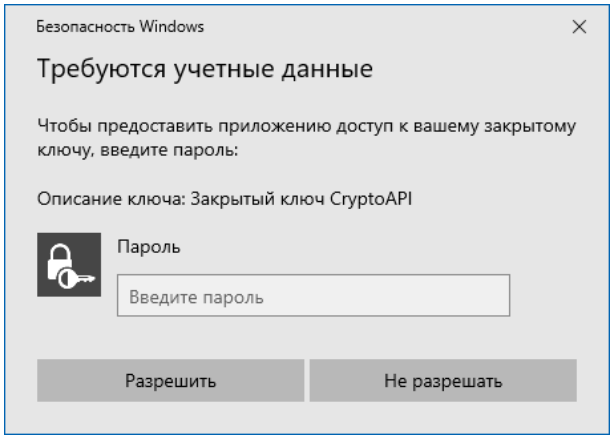
Сертификаты различаются по имени владельца, которое было задано при создании персоны на агентском сайте (в полях **Фамилия, Имя и Отчество**).

При необходимости вы можете хранить на eToken несколько сертификатов.

В зависимости от используемого браузера очередность пунктов 3 и 4 может меняться.

5. Если сертификат находится в системном хранилище и при создании сертификата был установлен высокий уровень безопасности, введите пароль для ключа (Рис. 18).

Рис. 18. Ввод пароля для закрытого ключа в системном хранилище



После этого вы перейдете на сайт и получите доступ ко всем функциям в соответствии с ролью персоны.

ПРИЛОЖЕНИЕ Б: Сохранение в системное хранилище

ВНИМАНИЕ

Системное хранилище является менее защищенным, чем eToken. Использовать сертификат вы сможете только на том локальном компьютере, на котором он был сгенерирован.

Для роли «Главный менеджер» и некоторых других сертификат разрешается сохранять только в хранилище eToken.

Для сохранения в системное хранилище вам необходимо выполнить следующие шаги:

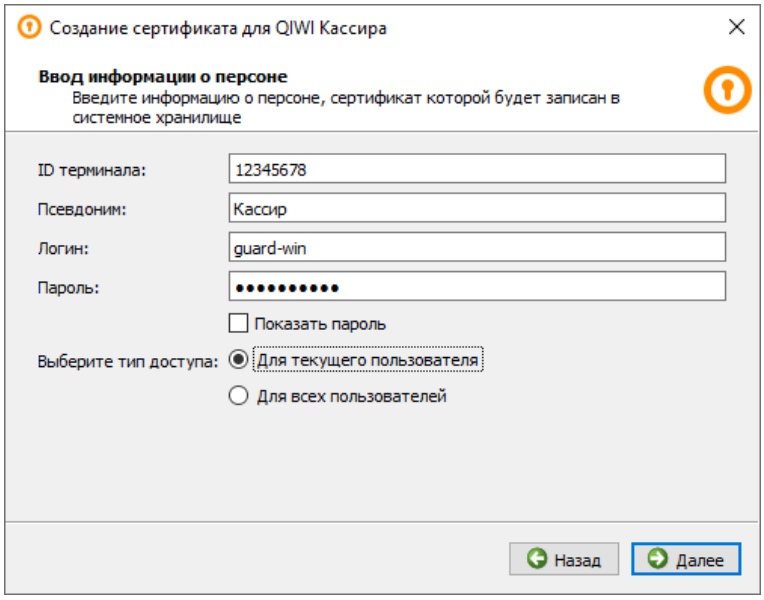
1. Указать данные персоны в ПО QIWI Защита.
2. Сгенерировать ключ подписи RSA.
3. Завершить генерацию сертификата/создания персоны в ПО QIWI Защита.

ШАГ 1. Ввод данных персоны

В зависимости от выполнения типа операции выполните следующее:

- **Получение доступа на агентский сайт:**
  - Выберите пункт **Получить доступ на агентский сайт**.
  - Введите авторизационные данные персоны (**логин** и **одноразовый пароль**).
  - Выберите тип хранилища **Системное**.
  - Перейдите к ШАГУ 2.
- **Создание сертификата для QIWI Кассира**:
  - Выберите пункт **Создать сертификат для QIWI Кассира**.
  - Выберите тип хранилища **Системное**.

Рис. 19. Ввод информации о персоне



– Введите данные персоны (Рис. 19):
  - **Псевдоним** – введите любое имя учетной записи, которое в дальнейшем будет использоваться для авторизации в ПО QIWI Кассир;
  - **Логин** – логин персоны;
  - **ID терминала** – номер терминала;
  - **Пароль** – одноразовый пароль;
  - **Показать пароль** – проставьте флаг, если необходимо отобразить значение поля **Пароль**.

ПРИМЕЧАНИЕ

На данном шаге указываются данные персоны и терминала, ранее зарегистрированных на агентском сайте.

– Выберите тип доступа:
  - **Для текущего пользователя** – авторизационные данные персоны сможет использовать только тот пользователь операционной системы Windows, под которым был выполнен вход в Систему.
  - **Для всех пользователей** – авторизационные данные персоны сможет использовать любой пользователь операционной системы Windows.

ВНИМАНИЕ

Сохранить авторизационные данные для всех пользователей можно только под учетной записью с правами Администратора.

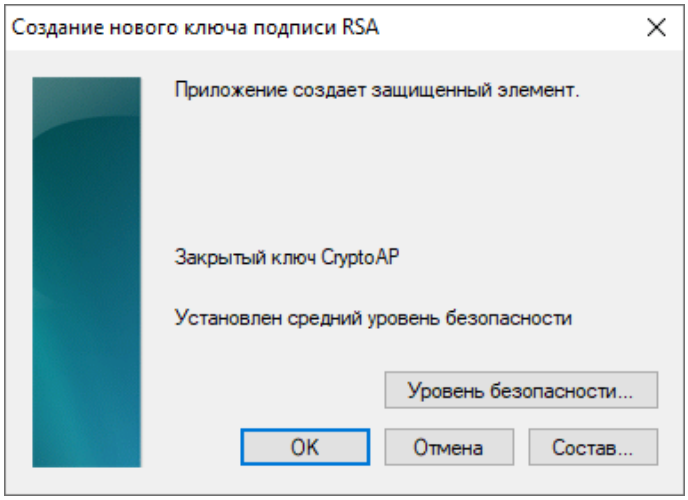
– Нажмите кнопку **Далее**.

– Перейдите к ШАГУ 2.

ШАГ 2. Генерация ключа подписи RSA

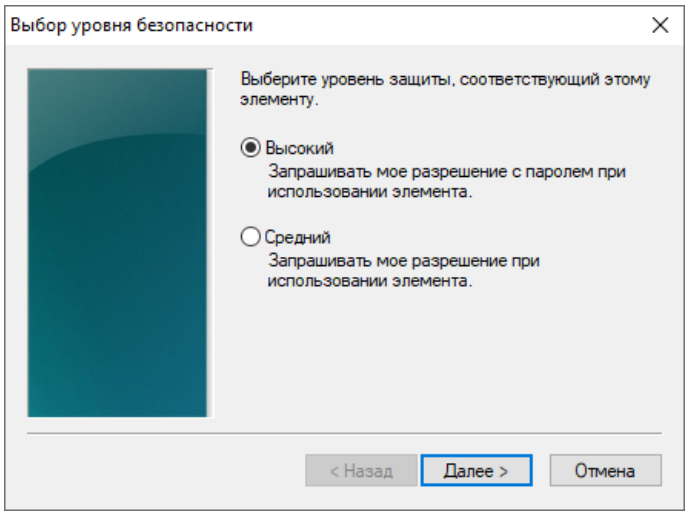
1. Нажмите кнопку **Уровень безопасности** (Рис. 20).

Рис. 20. Создание нового ключа подписи RSA



2. Выберите уровень защиты и нажмите кнопку **Далее** (Рис. 21):

Рис. 21. Выбор уровня защиты

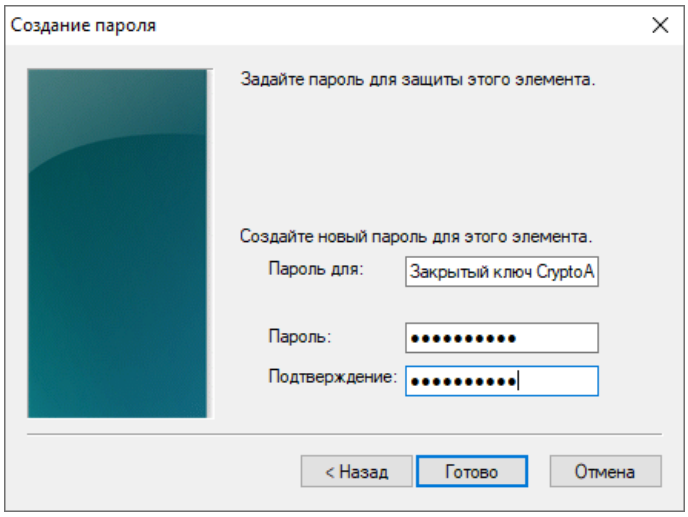


ПРИМЕЧАНИЕ

Рекомендованный уровень защиты - **Высокий.**

– **Высокий уровень** – задайте пароль для сертификата и нажмите кнопку **Готово** (Рис. 22):

Рис. 22. Установка пароля сертификата

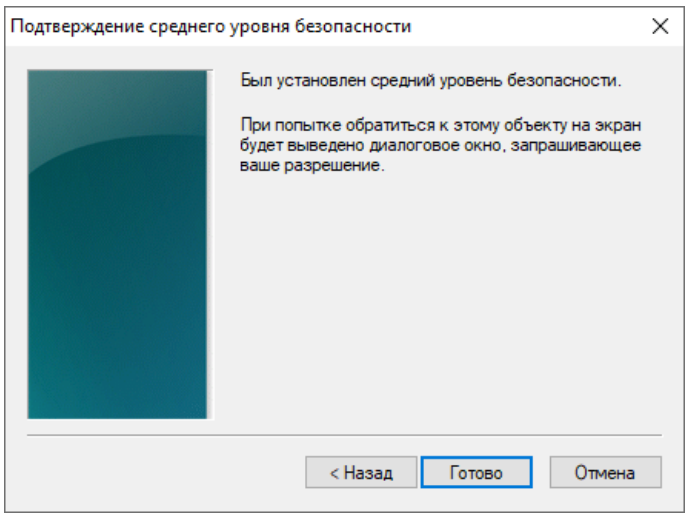


ПРИМЕЧАНИЕ

Данный пароль необходимо будет вводить при авторизации на сайте QIWI. Подробнее об авторизации на сайте см. в Приложении А.

– **Средний уровень** – прочитайте информацию о процессе авторизации и нажмите кнопку **Готово** (Рис. 23):

Рис. 23. Информация об авторизации при среднем уровне безопасности системного хранилища



Вы будете возвращены к первому шагу *Мастера создания нового ключа подписи RSA* (см. Рис. 20).

3. Нажмите кнопку **ОК**.

Вы будете возвращены в главное окно ПО *QIWI Защита*.

ШАГ 3. Завершение генерации сертификата/создания персоны

Дождитесь отображения информации об окончании записи сертификата и нажмите кнопку **Завершить** (см. Рис. 8).

ПРИЛОЖЕНИЕ В: Работа с «Файлом» сертификата

ВНИМАНИЕ

Файл служит только для переноса файла сертификата. Данная процедура не является безопасной и не рекомендована для использования. В процессе переноса файл может попасть к злоумышленникам, что может привести к значительному материальному ущербу и невозможности работы с Системой.

Приложение содержит инструкцию по следующим действиям:

1. Сохранение сертификата в «Файл».
2. Экспорт сертификата в системное хранилище.

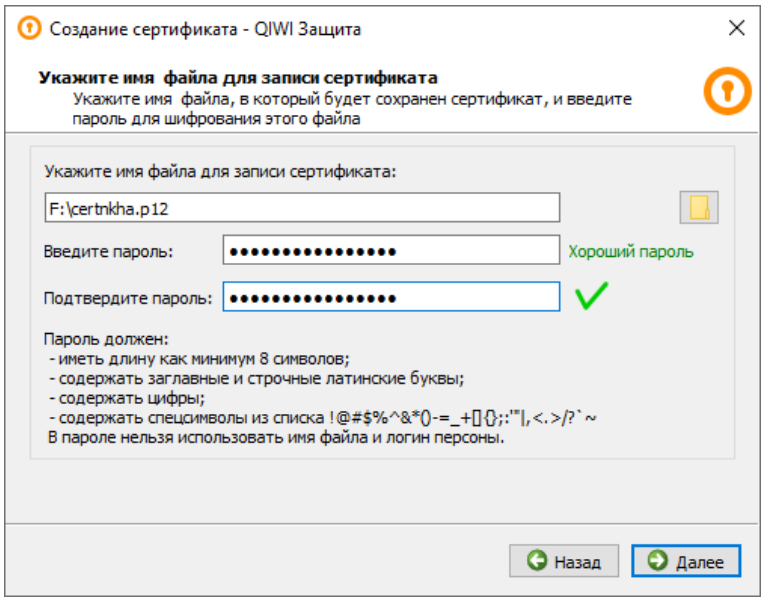
1. Сохранение сертификата в «Файл»

Для сохранения сертификата в **Файл** выполните следующее:

1. Пройдите шаги с 1 по 4, описанные в разделе 6.
2. Выберите тип хранилища **Файл**.
3. Выберите файл для записи сертификата и придумайте пароль. Этот пароль необходимо будет ввести при импорте сертификата в системное хранилище.

   Приложение оценивает надежность пароля по мере ввода символов. Для сохранения сертификата в файл пароль должен получить оценку **Хороший пароль** (Рис. 24).

Рис. 24. Выбор файла для записи сертификата



ПРИМЕЧАНИЕ

В первый раз приложение предложит сохранить сертификат в файл с названием `certnkha.p12` в системную папку `C:\Users\Имя_пользователя`.

Если необходимо сохранить сертификат под другим именем или в другой папке, укажите путь к файлу, используя кнопку или вручную, и имя файла. В дальнейшем приложение будет предлагать последние указанные имя файла и папку для сохранения новых сертификатов.

Изменяемая часть имени сертификата – `certnkha` (.p12 расширение файла, менять его нельзя).

ВНИМАНИЕ

Если вы решили изменить имя файла, убедитесь что расширение осталось без изменения.

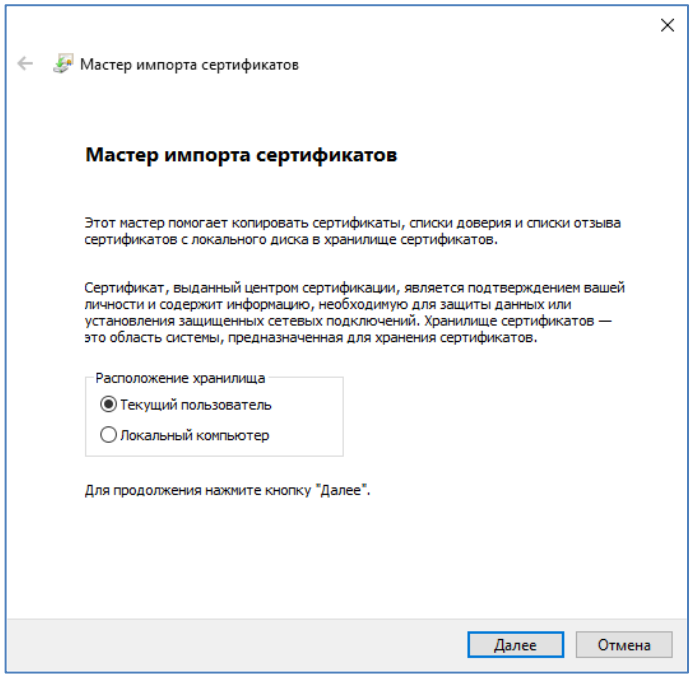
4. Нажмите кнопку **Далее**. Вы будете возвращены в *Мастер создания сертификатов*.
5. Дождитесь, пока *Мастер создания сертификатов* отобразит информацию об окончании записи сертификата, и нажмите кнопку **Завершить** (см. Рис. 8). Сертификат будет сохранен в файле.

2. Импорт сертификата

Для импорта файла сертификата в системное хранилище выполните следующее:

1. Щелкните дважды левой кнопкой мыши по файлу сертификата. Будет запущен *Мастер импорта сертификатов* (Рис. 25). Укажите расположение хранилища и нажмите **Далее**.

Рис. 25. Мастер импорта сертификатов

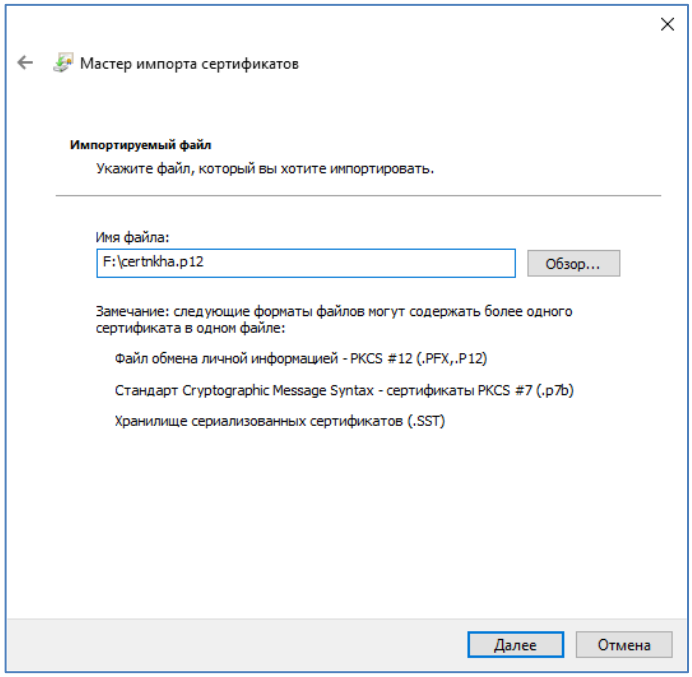


2. Подтвердите или укажите расположение файла сертификата. Нажмите кнопку **Далее** (Рис. 26).

ПРИМЕЧАНИЕ

По умолчанию указан файл сертификата, с помощью которого был запущен *Мастер импорта сертификатов.*

Рис. 26. Импортируемый файл



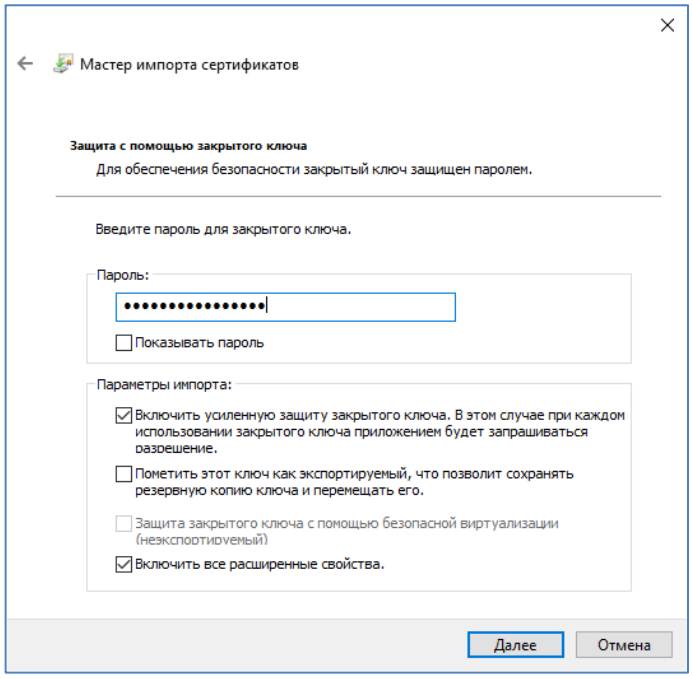
3. Установите флаги **Включить усиленную защиту закрытого ключа, Включить все расширенные свойства** (Рис. 27).

ПРИМЕЧАНИЕ

Установка данных флагов необходима в целях повышения уровня защиты.

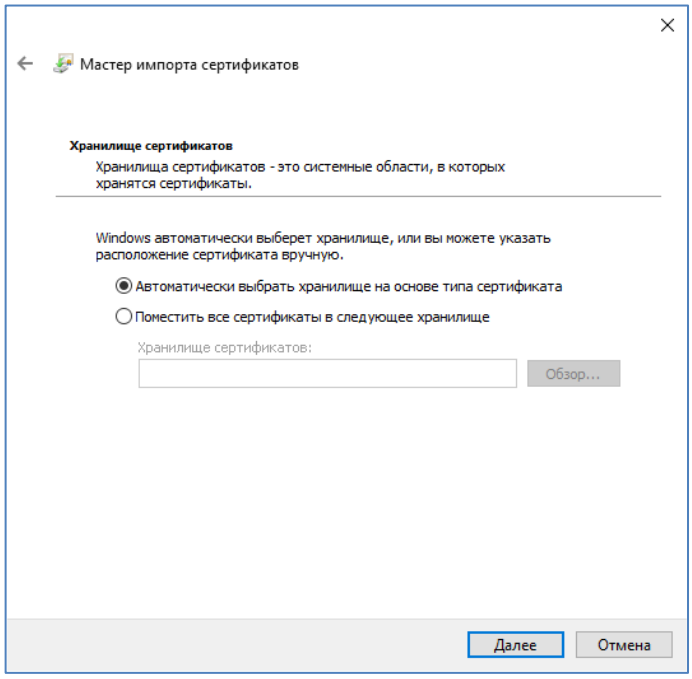
4. Введите пароль для доступа к файлу сертификата и нажмите кнопку **Далее**

Рис. 27. Ввод пароля для файла сертификата



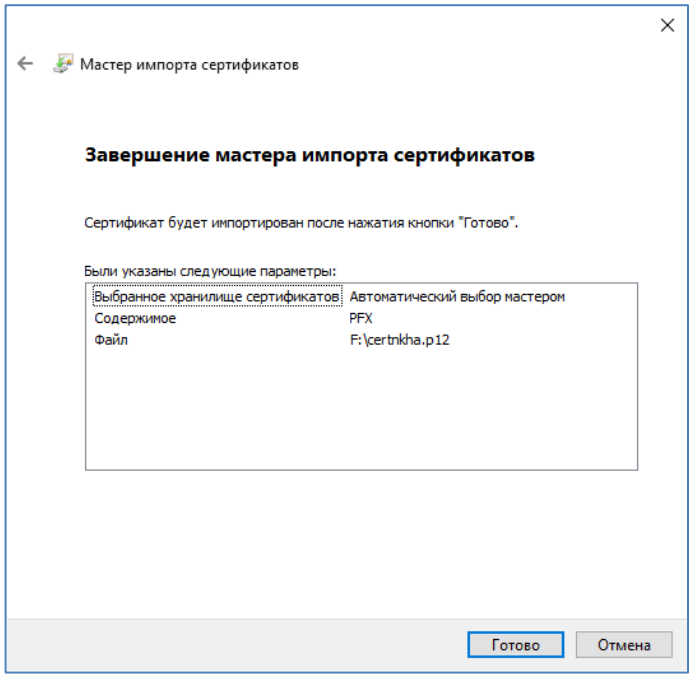
5. Выберите **Автоматически выбрать хранилище на основе типа сертификата** и нажмите кнопку **Далее** (Рис. 28).

Рис. 28. Выбор размещения сертификата



Будет выполнен импорт сертификата, и *Мастер импорта сертификатов* отобразит параметры импорта (Рис. 29).

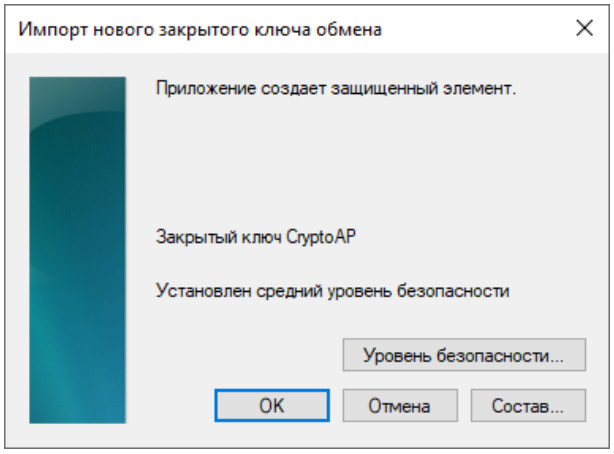
Рис. 29. Параметры импорта сертификата



6. Нажмите кнопку **Готово**.

   Импорт сертификата в системное хранилище будет завершен и вам будет предложено задать уровень безопасности сертификата (Рис. 30).

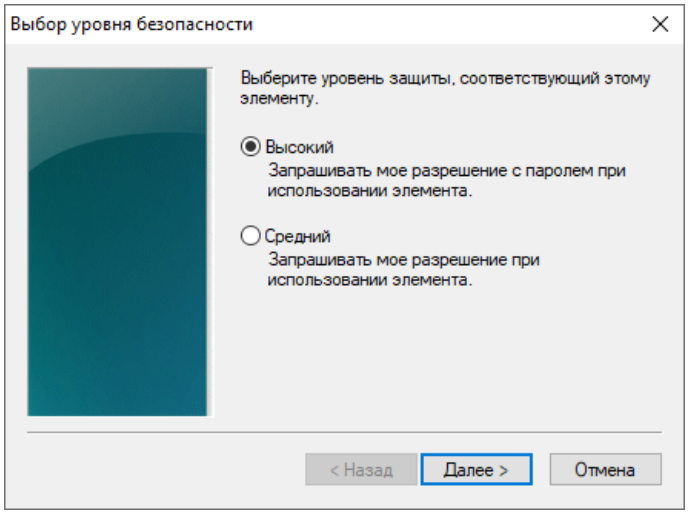
Рис. 30. Создание защищенного элемента



7. Нажмите кнопку **Уровень безопасности**.

   Будет открыто диалоговое окно с выбором уровня защиты (Рис. 31).

Рис. 31. Выбор уровня безопасности



8. Выберите уровень безопасности и нажмите кнопку **Далее**.

ПРИМЕЧАНИЕ

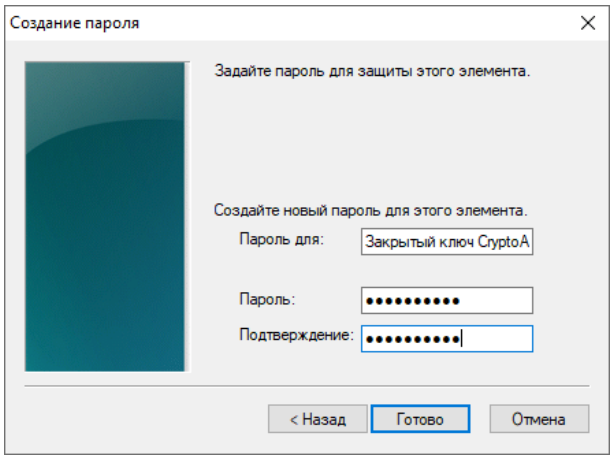
Рекомендованный уровень защиты - **Высокий.**

– **Высокий уровень** – задайте пароль для сертификата и нажмите кнопку **Готово** (Рис. 32).

ПРИМЕЧАНИЕ

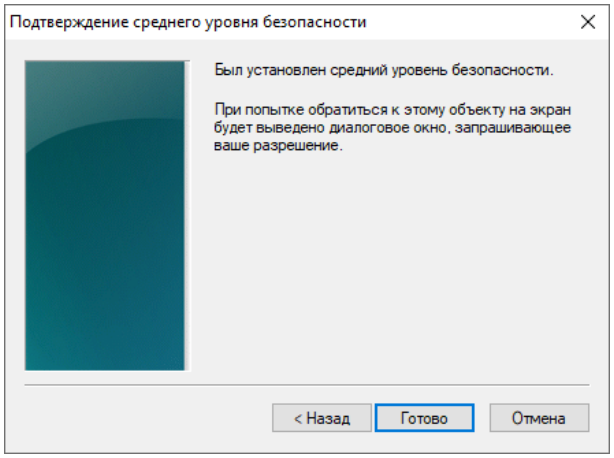
Данный пароль необходимо будет вводить при авторизации на сайте КИВИ. Подробнее об авторизации на сайте см. в Приложении А.

Рис. 32. Установка пароля сертификата



– **Средний уровень** – прочитайте информацию о процессе авторизации и нажмите кнопку **Готово** (Рис. 33).

Рис. 33. Информация об авторизации при среднем уровне безопасности системного хранилища

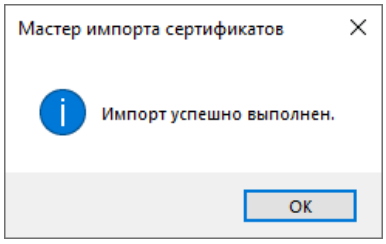


Вы будете возвращены к первому шагу *Мастера создания нового ключа подписи RSA* (см. Рис. 30).

9. Нажмите кнопку **OK**.

   Будет открыто диалоговое окно, информирующее об успешном импорте сертификата (Рис. 34).

Рис. 34. Успешный импорт сертификата



10. Нажмите кнопку **OK**.

Настройки сертификата будут заданы.

СПИСОК РИСУНКОВ