# QIWI ЗАЩИТА
вер. 3.2

## РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ
вер. 3.2


**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 сертификаты доступа на сайт желательно хранить на внешнем криптографическом носителе (смарт-карта, usb-ключ и др.).

## 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;
- наличие программного обеспечения и драйверов для работы с внешним защищенным носителем сертификатов (если для хранения сертификатов используется внешний носитель).

# 3. БЫСТРЫЙ СТАРТ

## 3.1. Создание сертификата

Для создания сертификата выполните следующие действия:

1. Выберите пункт **Сертификат для доступа на агентский сайт**.
2. Выберите тип агента – агент АО КИВИ или АО КИВИ Банк (агент Рапиды).
3. Введите авторизационные данные персоны (**логин** и **одноразовый пароль для сертификата**).
4. Выберите тип хранилища.

**СОВЕТ**

Наиболее рекомендуемым хранилищем по соображениям безопасности является внешний защищенный носитель.

5. 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 внешний защищенный носитель.

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.

## 3.3. Создание платежного сертификата для Рапиды

Для создания сертификата выполните следующее:

1. Выберите пункт **Платежный сертификат для Рапиды**.
2. Введите авторизационные данные персоны (**логин** и **одноразовый пароль для сертификата**).
3. Выберите тип хранилища.

**СОВЕТ**

Наиболее рекомендуемым хранилищем по соображениям безопасности является внешний защищенный носитель.

4. Введите данные организации – владельца сертификата.
5. Сохраните сертификат в хранилище.

**ПРИМЕЧАНИЕ**

Процесс управления сертификатами подробно описан в разделе 8.

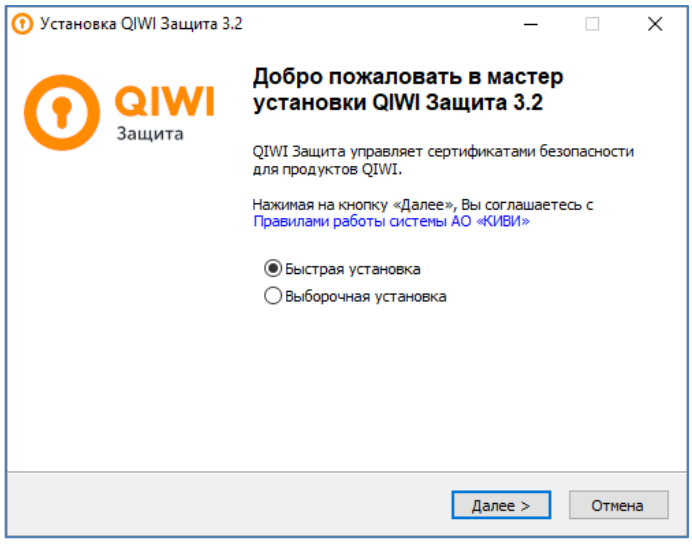
# 4. УСТАНОВКА И ГЛАВНОЕ ОКНО ПРИЛОЖЕНИЯ

## 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).

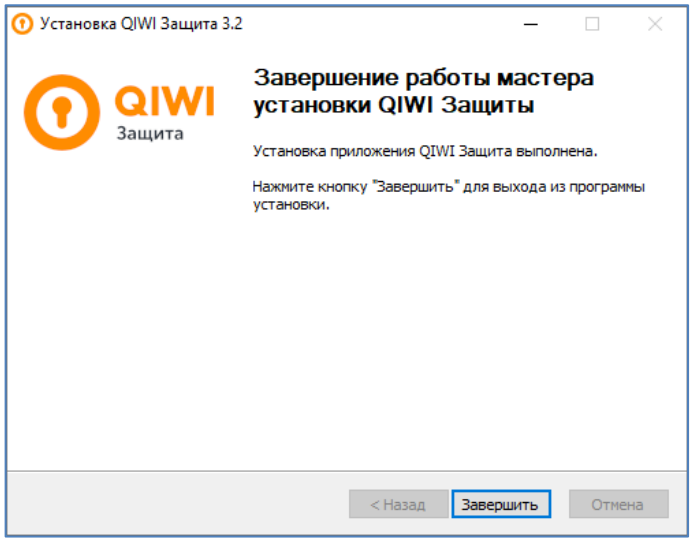
Рис. 1. Мастер установки




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



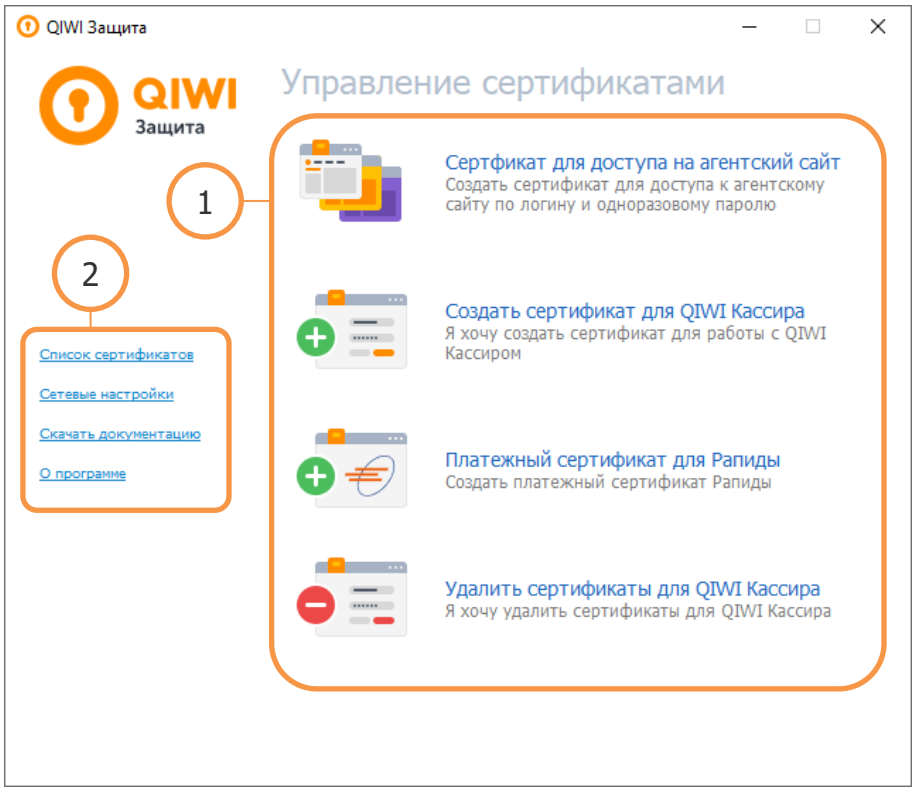

4. Для завершения работы мастера нажмите кнопку **Завершить**.

Приложение установлено, на рабочем столе и в меню **Пуск** размещены ярлыки для запуска.

## 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**:
  - **Сертификат для доступа 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.
  - **Платежный сертификат Рапиды** – создание платежного сертификата для Рапиды. Подробнее см. в разделе 8.
  - **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→Действующим агентам→Скачать ПО и документацию** на сайте qiwi.com, откуда можно скачать руководство пользователя;
- О программе – открывает окно с информацией о приложении.

# 5. ПРЕДВАРИТЕЛЬНАЯ ПОДГОТОВКА

Перед началом работы с ПО *QIWI Защита* рекомендуется установить актуальные дату и время.

На агентском сайте необходимо выполнить следующие действия:

- для получения доступа на агентский сайт – создать персону, задать для неё логин и сгенерировать одноразовый пароль;
- для создания сертификата для ПО *QIWI Кассир* – зарегистрировать терминал (персона для этого терминала будет создана и привязана к нему автоматически);
- для создания платежного сертификата Рапиды – создать персону, установить для неё роль 22 Продавец, задать логин и сгенерировать одноразовый 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, необходимо сгенерировать новый одноразовый пароль.

**ВНИМАНИЕ**

Для роли «Главный менеджер» и некоторых других сертификат разрешается сохранять только на внешний защищенный носитель.

Подробнее о создании персон, терминалов и генерации одноразового пароля см. в Руководстве пользователя агентского сайта, размещенном в разделе **Бизнесу→Действующим агентам→Скачать ПО и документацию** на сайте qiwi.com.

# 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.

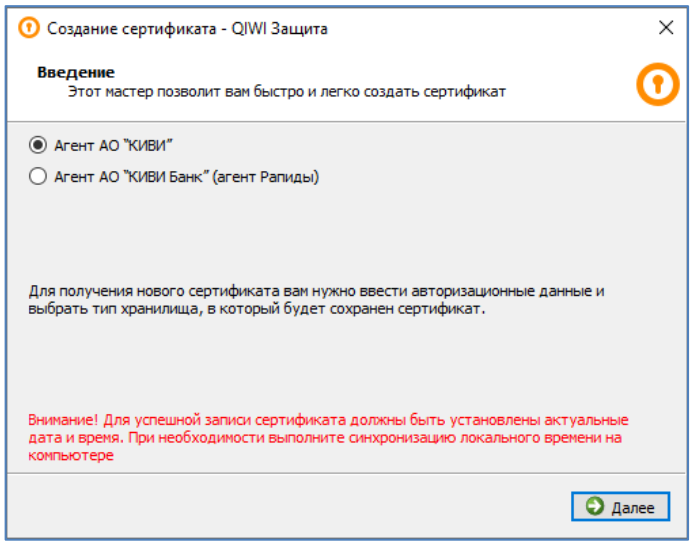
Для роли «Главный менеджер» и некоторых других сертификат разрешается сохранять только на внешний защищенный носитель.

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

1. В главном окне приложения выберите действие **Сертификат для доступа на агентский сайт** (см. Рис. 3).

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

Рис. 4. Мастер создания сертификатов



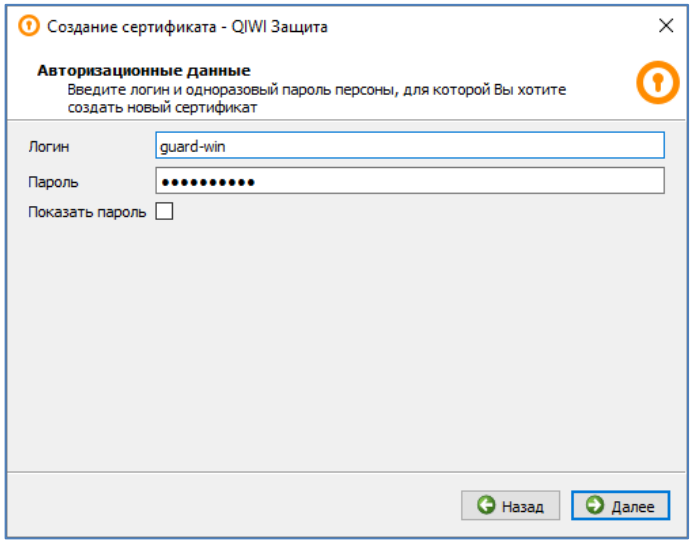

2. Выберите тип агента:
   - **Агент АО «КИВИ Банк» (агент Рапиды)** – если агент работает через адаптер протокола Рапиды;
   - **Агент АО «КИВИ»** - в прочих случаях;
3. Укажите данные персоны для генерации сертификата (Рис. 5):
   - **Логин** – логин персоны;
   - **Пароль** – одноразовый пароль для сертификата;
   - **Показать пароль** – проставьте флаг, если необходимо отобразить значение поля **Пароль**.

**ПРИМЕЧАНИЕ**

Далее описаны шаги генерации сертификата с типом хранилища eToken.
Процесс сохранения сертификата в другое хранилище описан в приложениях:

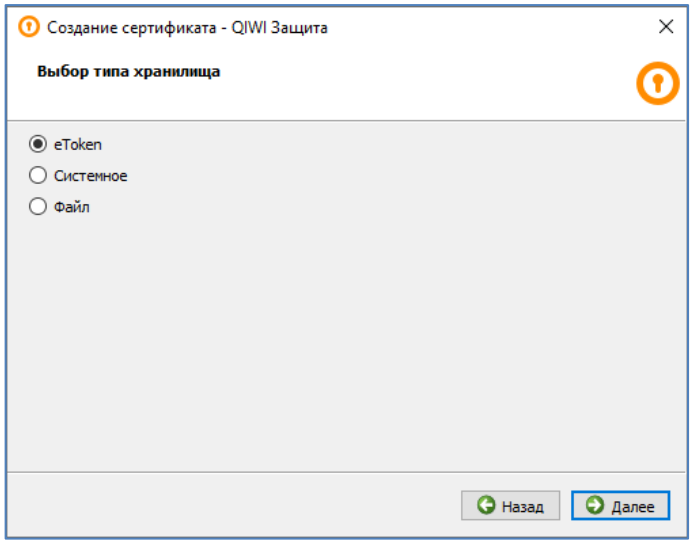
- Системное хранилище – Приложение Б;
- Файл – Приложение В.

Рис. 5. Ввод авторизационных данных



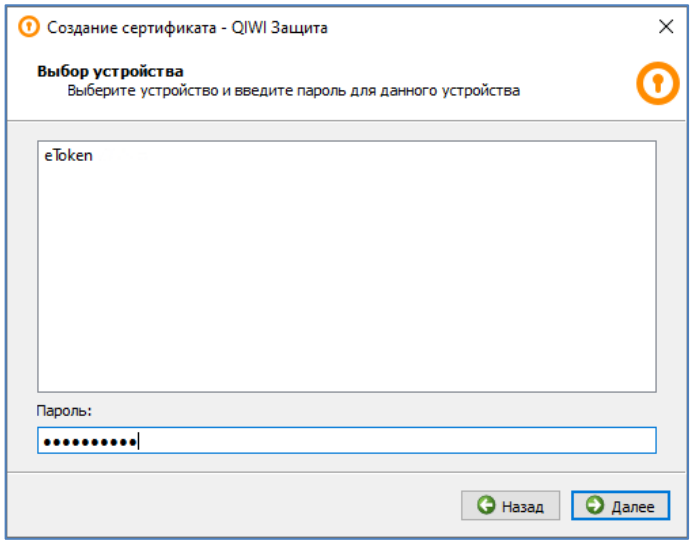

4. Выберите тип хранилища **eToken** (Рис. 6).

Рис. 6. Выбор хранилища сертификата



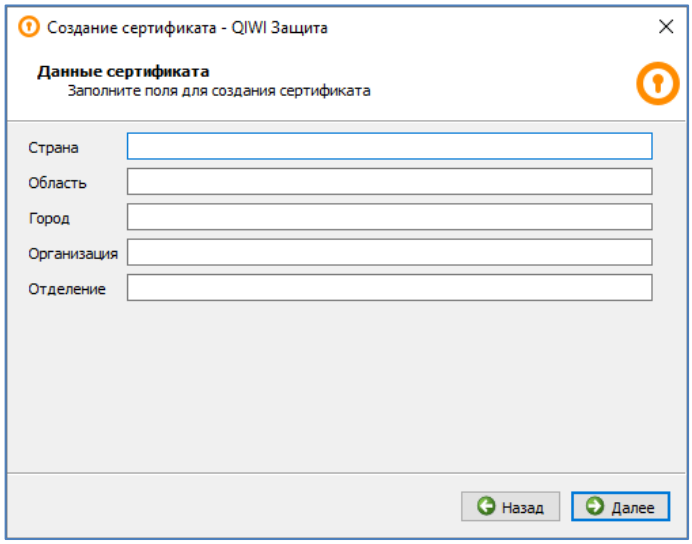

5. Выберите необходимое устройство из списка eToken и укажите пароль для него (Рис. 7).

Рис. 7. Выбор устройства хранения информации



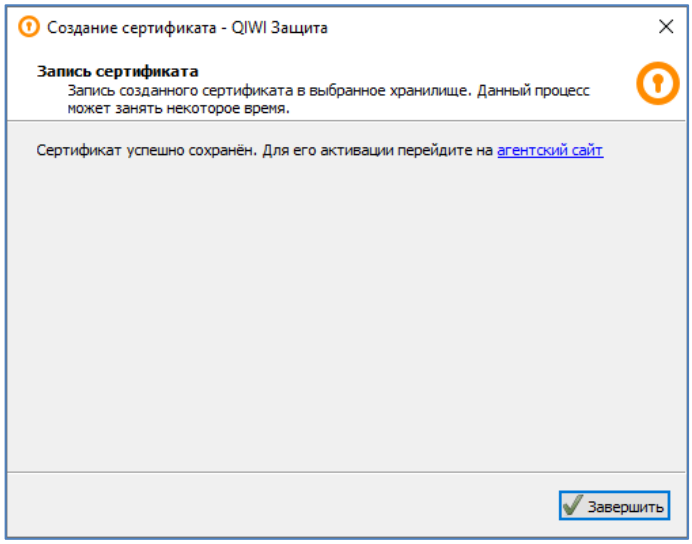

6. Если на первом шаге выбрали тип агента **Агент АО «КИВИ Банк» (агент Рапиды)**, введите данные организации – владельца сертификата на следующем экране (Рис. 8).

Рис. 8. Данные сертификата для агентов Рапиды




7. Дождитесь сообщения «*Сертификат успешно сохранен*» и нажмите кнопку **Завершить** (Рис. 9).

Рис. 9. 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* помогает 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**

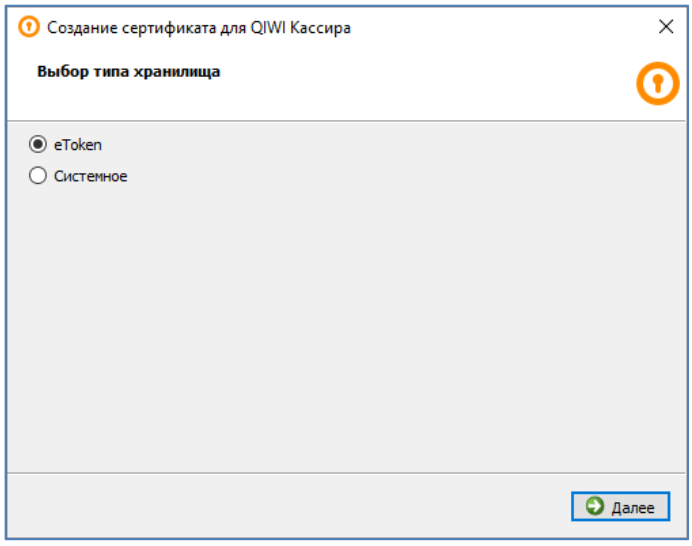
Далее описаны шаги при выборе типа хранилища eToken.

Процесс сохранения сертификата в другое хранилище описан в приложениях:

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

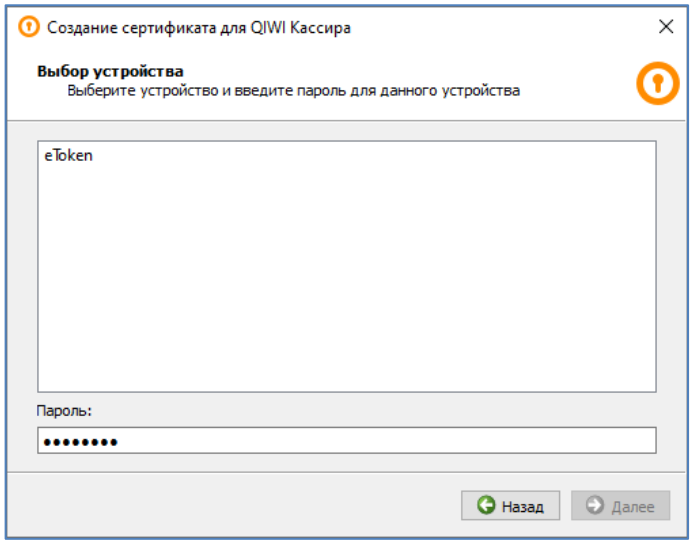
2. Выберите тип хранилища **eToken** (Рис. 10).

Рис. 10. Выбор устройства хранения информации о персонах



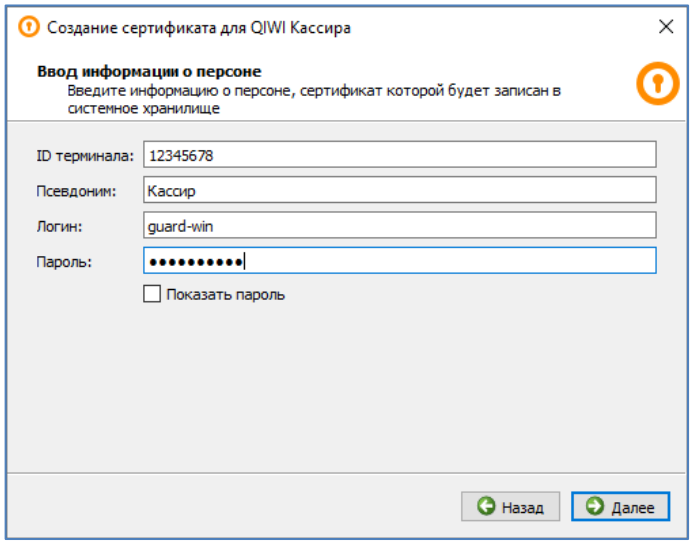

3. Выберите необходимый eToken и укажите пароль для него (Рис. 11).

Рис. 11. Выбор устройства хранения информации




4. Введите данные персоны и нажмите кнопку **Далее** (Рис. 12):

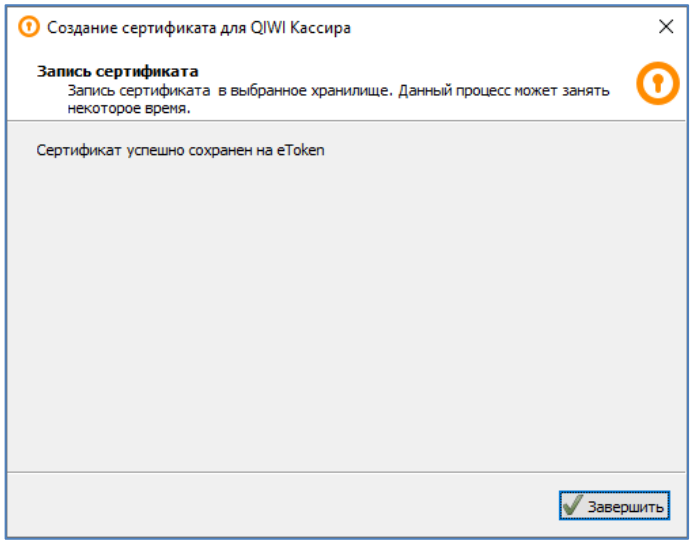
Рис. 12. Ввод информации о персоне




- **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. 13).

Рис. 13. 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. СОЗДАНИЕ ПЛАТЕЖНОГО СЕРТИФИКАТА ДЛЯ РАПИДЫ

**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 **Платежный сертификат для Рапиды** (см. Рис. 3). Будет открыт *Мастер создания сертификатов для Рапиды.*
2. Укажите данные персоны для генерации сертификата (Рис. 14):
   - **Логин** – логин персоны;
   - **Пароль** – одноразовый пароль для сертификата;
   - **Показать пароль** – проставьте флаг, если необходимо отобразить значение поля **Пароль**.

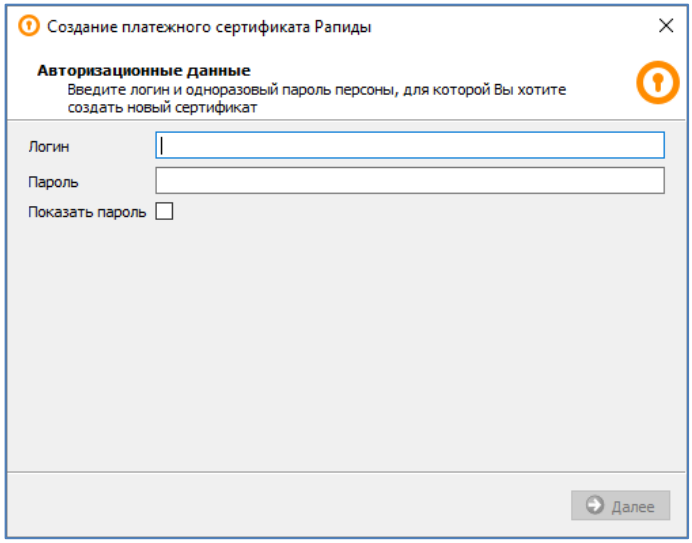
**ПРИМЕЧАНИЕ**

Далее описаны шаги генерации сертификата с типом хранилища eToken.

Процесс сохранения сертификата в другое хранилище описан в приложениях:

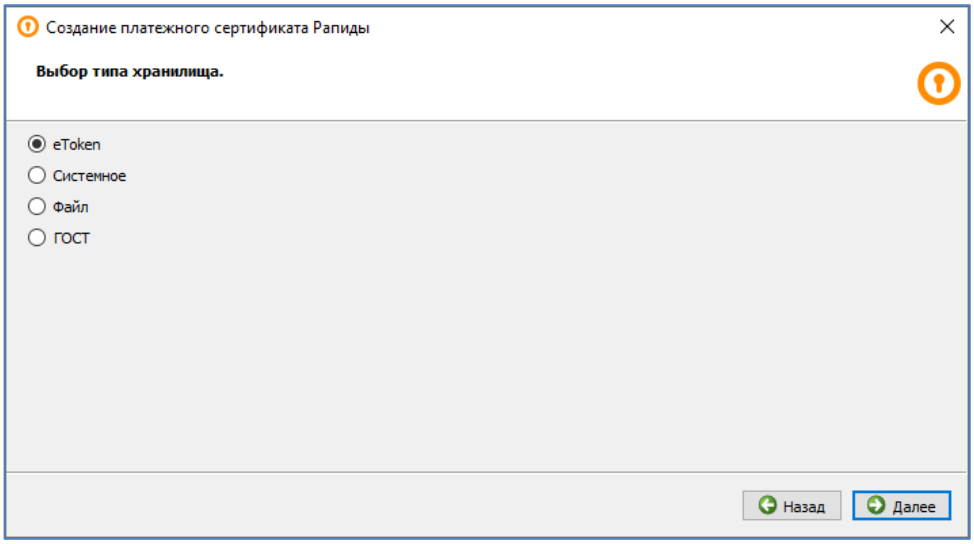
- Системное хранилище – Приложение Б;
- Файл – Приложение В;
- ГОСТ - Приложение Г

Рис. 14. Ввод авторизационных данных для сертификата Рапиды



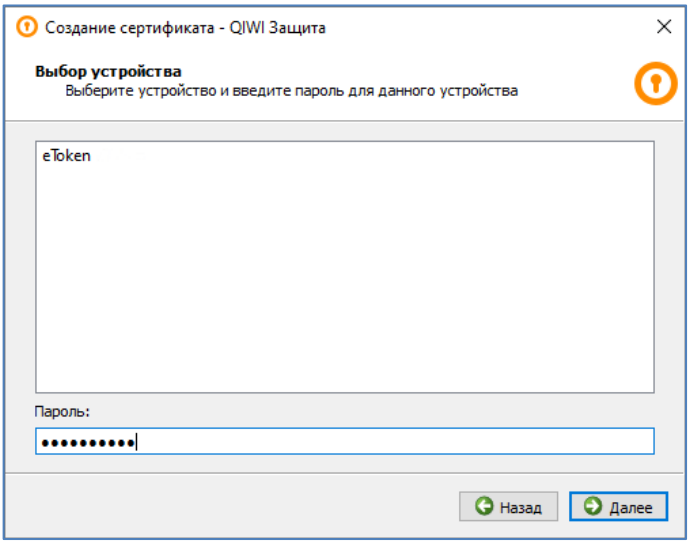
3. Выберите тип хранилища **eToken** (Рис. 15).

Рис. 15. Выбор хранилища сертификата



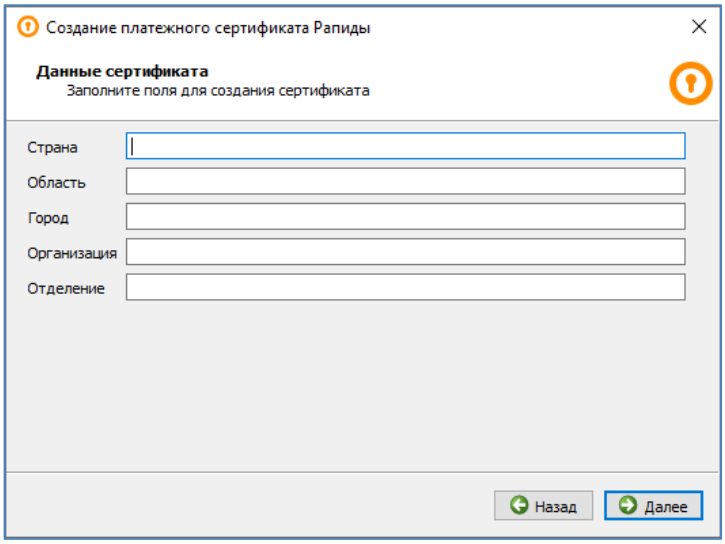

4. Выберите необходимое устройство из списка eToken и укажите пароль для него (Рис. 16).

Рис. 16. Выбор устройства хранения информации



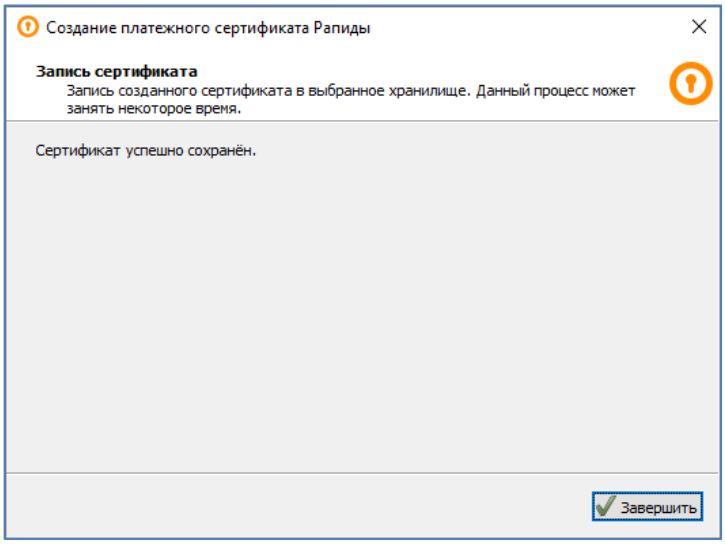

5. Введите данные организации – владельца сертификата (Рис. 17):
   - **Страна, Область, Город** – страна нахождения организации, к которой относится персона;
   - **Организация** – название организации;
   - **Отделение** – название отделения.

Рис. 17. Данные сертификата




6. Дождитесь сообщения «*Сертификат успешно сохранен*» и нажмите кнопку **Завершить** (Рис. 18).

Рис. 18. Запись сертификата



# 9. 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.

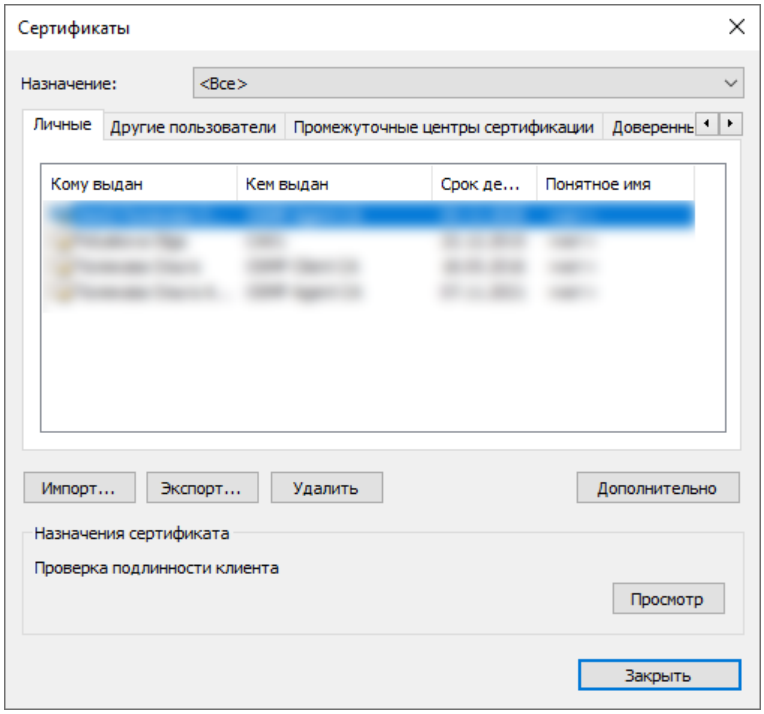
## 9.1. Список сертификатов

Для просмотра сертификатов, установленных в системе, выберите **Список сертификатов** в главном окне приложения (см. Рис. 3). Будет открыто окно **Сертификаты** (Рис. 19).

**ПРИМЕЧАНИЕ**

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

Рис. 19. Системные сертификаты



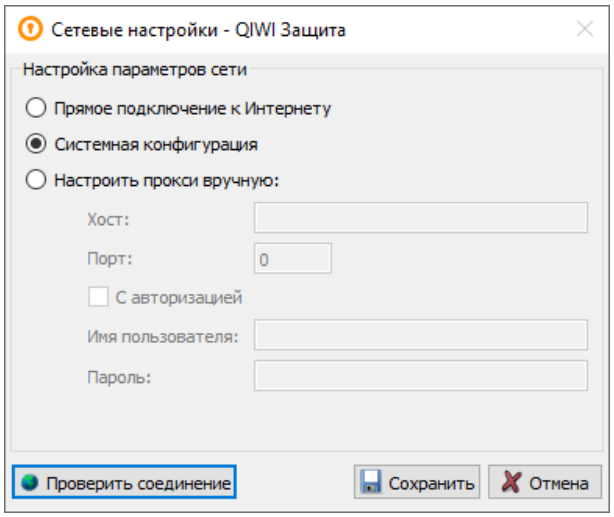

## 9.2. Сетевые настройки

Для изменения сетевых настроек выполните следующее:

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

   Будет открыто диалоговое окно **Сетевые настройки** (Рис. 20).

Рис. 20. 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**

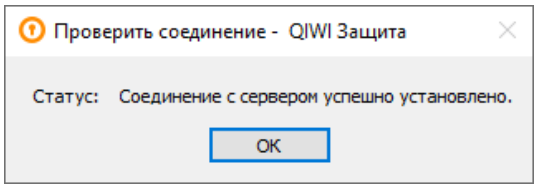
Информацию о прокси-сервере запросите у вашего системного администратора.

   - **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. 21).

Рис. 21. Успешное соединение с сервером




## 9.3. 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 необходимо пройти процедуру подтверждения контактных данных и активации сертификата. Подробнее см. в документе Процедура активации персоны на сайте agt.qiwi.com

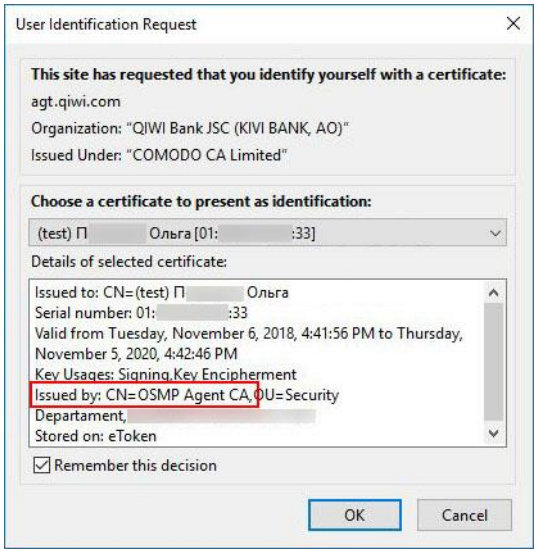
Для авторизации на агентском сайте QIWI выполните следующее:

1. Установите носитель с сертификатом 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. Браузер может запросить пароль от носителя сертификатов. Введите пароль и нажмите OK.

Рис. 22. Ввод пароля от носителя сертификатов


4. Будет открыто окно выбора сертификта (Рис. 23). Выберите сертификат, выпущенный *OSMP Agent CA*, и нажмите **OK**.

Рис. 23. 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 внешнем защищенном носителе несколько сертификатов.

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

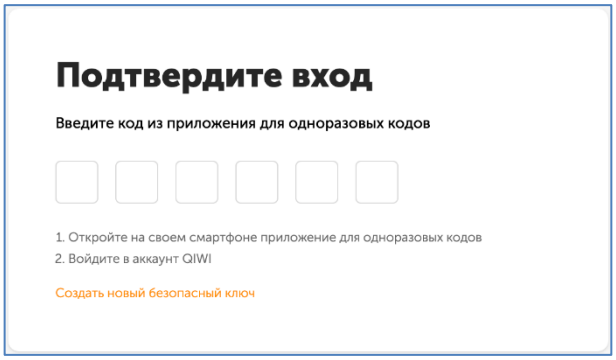
5. Введите одноразовый код подтверждения из приложения для одноразовых кодов (Рис. 24). Пропустите этот пункт, если сертификат находится на внешнем защищенном носителе.

**ПРИМЕЧАНИЕ**

Приложение для одноразовых кодов должно быть привязано к контактным данным персоны, которая авторизуется на сайте. Подробнее см. в документе Процедура активации персоны на сайте agt.qiwi.com.

Вход с помощью одноразового кода считается подтвержденным в течение 24 часов. Чтобы войти на сайт по истечении этого срока, нужно будет заново подтвердить вход одноразовым кодом.

Рис. 24. Одноразовый код подтверждения




Вход в систему будет осуществлён.

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

# ПРИЛОЖЕНИЕ Б: Сохранение в системное хранилище

Агенту по согласованию с курирующим менеджером может быть предоставлена возможность сохранять сертификаты для доступа к агентскому сайту в системном хранилище компьютера (без использования внешних защищенных носителей).

Чтобы получить такую возможность, выполните действия:

1. Отправьте курирующему менеджеру запрос на сохранение сертификатов доступа к агентскому сайту в системное хранилище. В ответном сообщении менеджер передаст шаблон документа для заполнения, подписания и последующей передачи в QIWI.
2. Предоставьте запрошенный курирующим менеджером документ в электронном и в бумажном виде по адресу, предоставленному менеджером.
3. Дождитесь подтверждения от курирующего менеджера о том, что возможность использовать для хранения сертификатов хранилище сертификатов компьютера предоставлена.
4. Добавьте персоне, сертификат которой должен быть сохранен на компьютере, роль 8000. Теперь для этой персоны с помощью ПО QIWI Защита можно выпустить сертификат доступа к агентскому сайту и сохранить его на компьютер.

**ВНИМАНИЕ**

Системное хранилище является менее защищенным, чем внешний защищенный носитель (смарт-карта, usb-ключ и др.). 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 на внешний защищенный носитель.

Для сохранения сертификата в системное хранилище выполните 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 выбранного типа операции выполните следующее:

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

– Перейдите к ШАГУ 2.

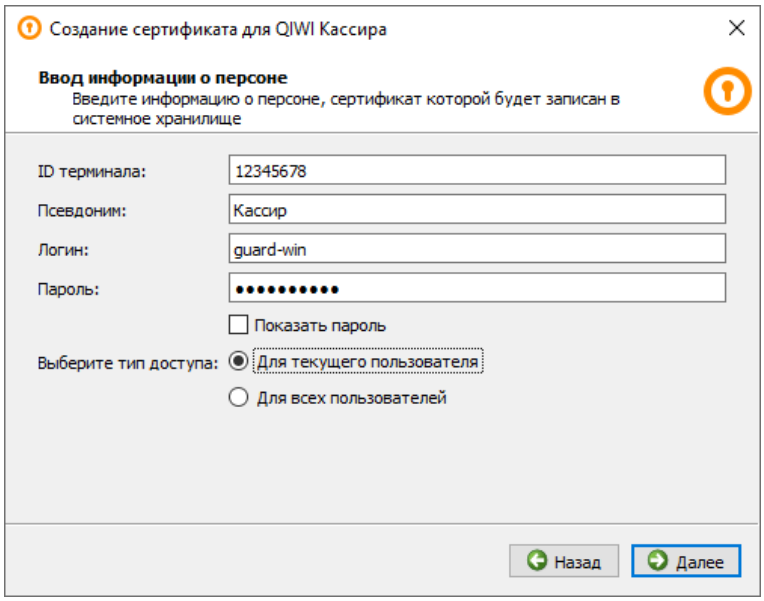
- **Создание сертификата для QIWI Кассира**:
  – Выберите пункт **Создать сертификат для QIWI Кассира**.
  – Выберите тип хранилища **Системное**.
  – Введите данные персоны (Рис. 25):

**ПРИМЕЧАНИЕ**

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

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

Рис. 25. Ввод информации о персоне




– 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.

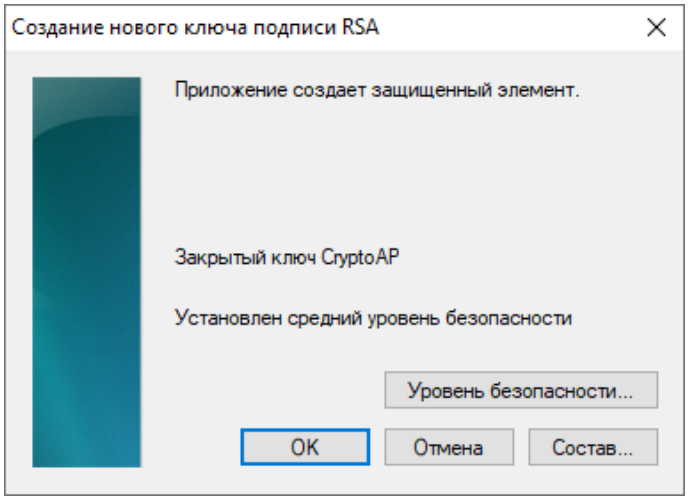
– Нажмите кнопку **Далее**.

– Перейдите к ШАГУ 2.

### ШАГ 2. Генерация ключа подписи RSA

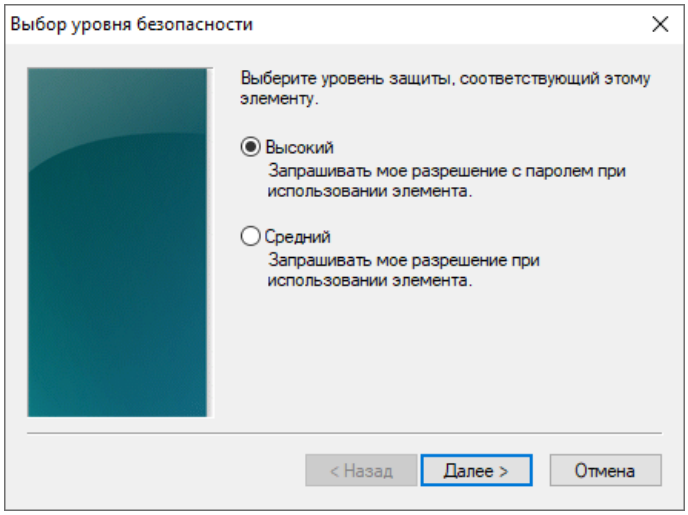
1. Нажмите кнопку **Уровень безопасности** (Рис. 26).

Рис. 26. Создание нового ключа подписи RSA




2. Выберите уровень защиты и нажмите кнопку **Далее** (Рис. 27):

Рис. 27. Выбор уровня защиты

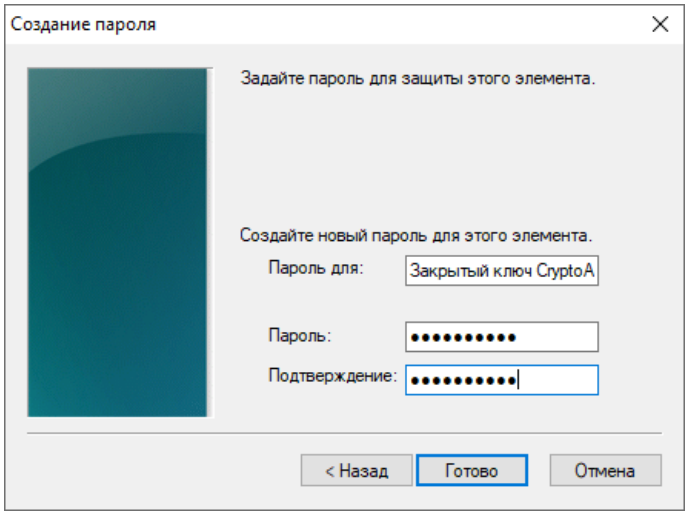


**ПРИМЕЧАНИЕ**

Рекомендованный уровень защиты - **Высокий.**

– **Высокий уровень** – задайте пароль для сертификата и нажмите кнопку **Готово** (Рис. 28):

Рис. 28. Установка пароля сертификата

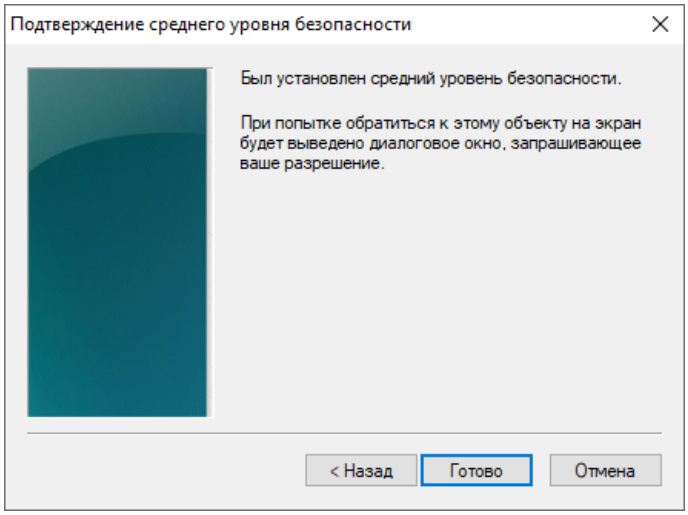



**ПРИМЕЧАНИЕ**

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. 29):

Рис. 29. Информация об авторизации при среднем уровне безопасности системного хранилища




Вы будете возвращены к первому шагу *Мастера создания нового ключа подписи RSA* (см. Рис. 26).

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. 9).

# 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. Импорт сертификата в системное хранилище.

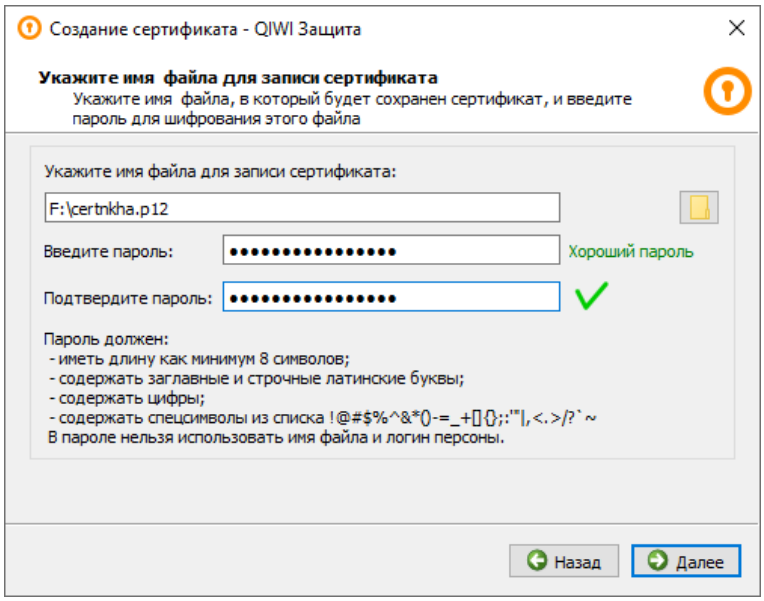
## 1. Сохранение сертификата в «Файл»

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. 30).

Рис. 30. 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.

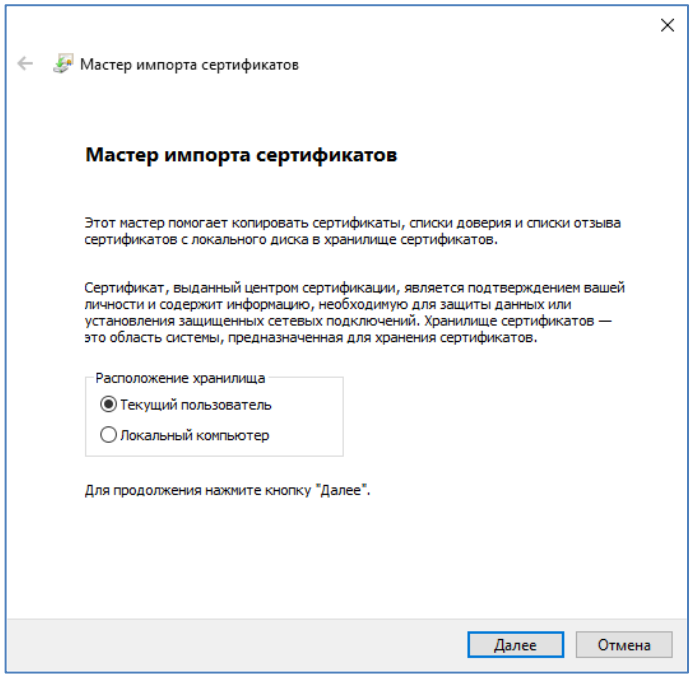
4. Нажмите кнопку **Далее**. Вы будете возвращены в *Мастер создания сертификатов*.
5. Дождитесь, пока *Мастер создания сертификатов* отобразит информацию об окончании записи сертификата, и нажмите кнопку **Завершить** (см. Рис. 9). Сертификат будет сохранен в файле.

## 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. 31). Укажите расположение хранилища и нажмите **Далее**.

Рис. 31. Мастер импорта сертификатов

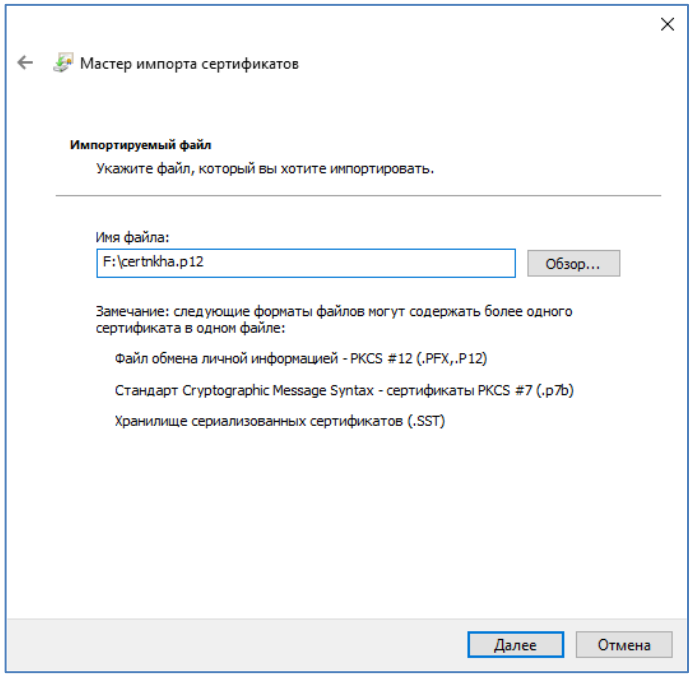


2. Подтвердите или укажите расположение файла сертификата. Нажмите кнопку **Далее** (Рис. 32).

**ПРИМЕЧАНИЕ**

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

Рис. 32. Импортируемый файл



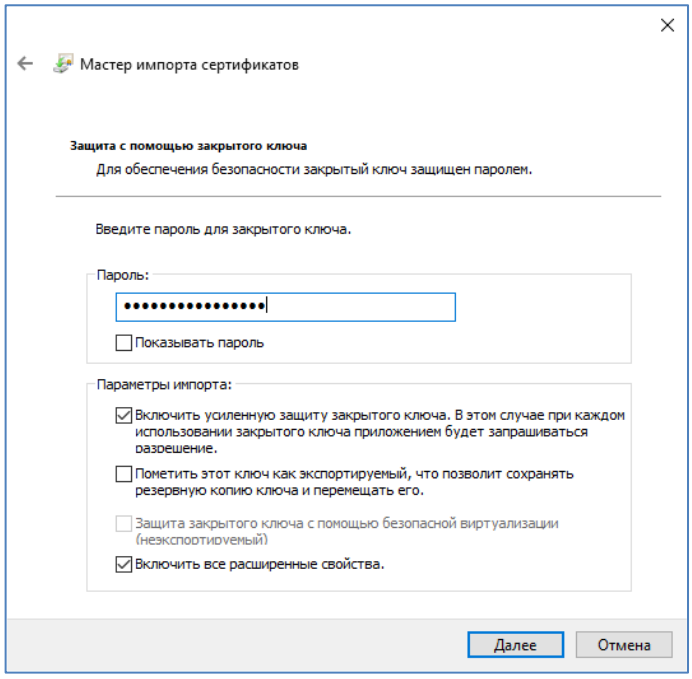

3. Установите флаги **Включить усиленную защиту закрытого ключа, Включить все расширенные свойства** (Рис. 33).

**ПРИМЕЧАНИЕ**

Установка данных флагов необходима в целях повышения уровня защиты.

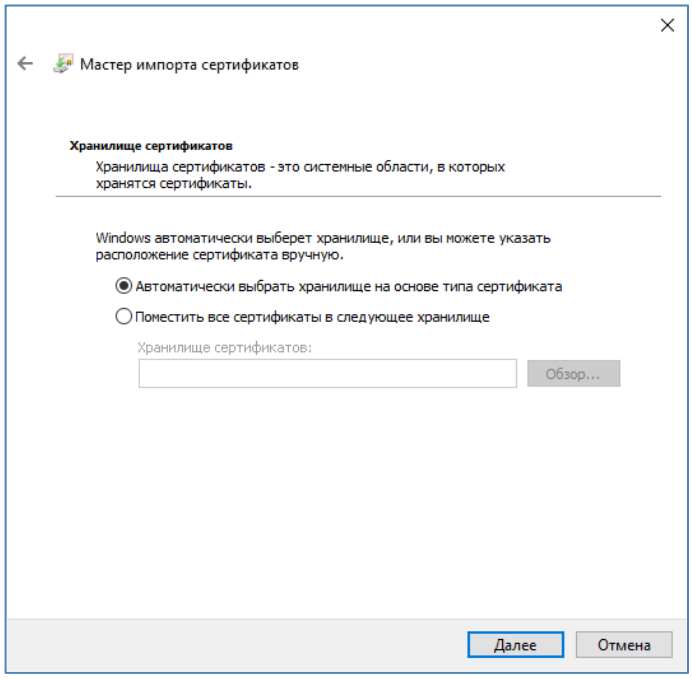
4. Введите пароль для доступа к файлу сертификата и нажмите кнопку **Далее**

Рис. 33. Ввод пароля для файла сертификата



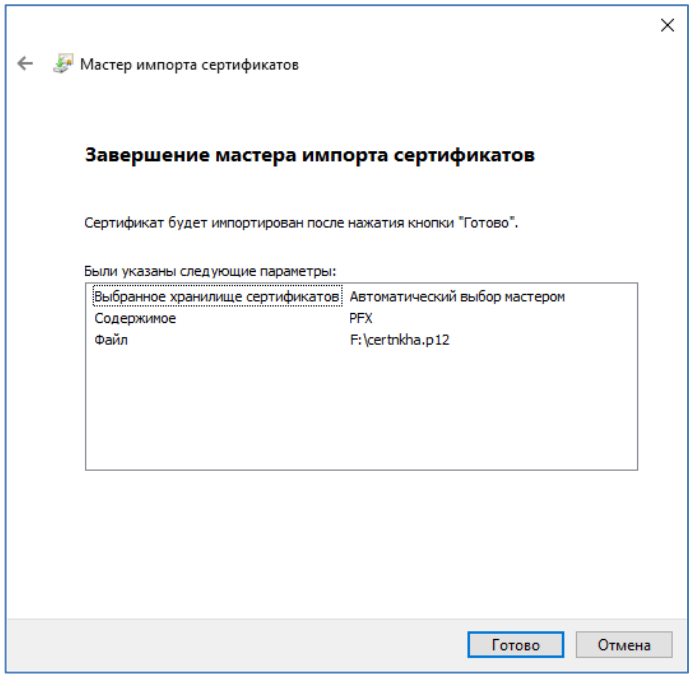

5. Выберите **Автоматически выбрать хранилище на основе типа сертификата** и нажмите кнопку **Далее** (Рис. 34).

Рис. 34. Выбор размещения сертификата



Будет выполнен импорт сертификата, и *Мастер импорта сертификатов* отобразит параметры импорта (Рис. 35).

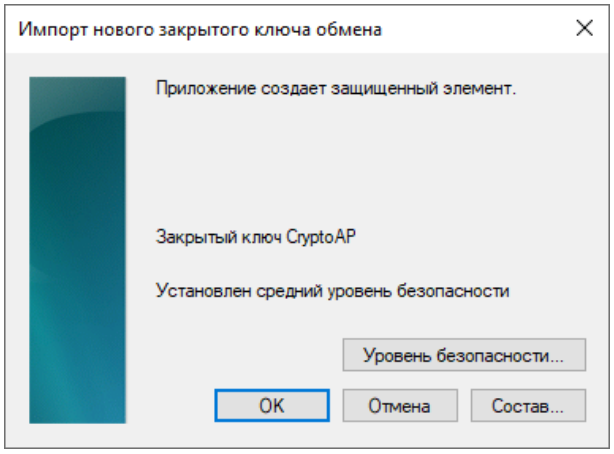
Рис. 35. Параметры импорта сертификата




6. Нажмите кнопку **Готово**.

   Импорт сертификата в системное хранилище будет завершен и вам будет предложено задать уровень безопасности сертификата (Рис. 36).

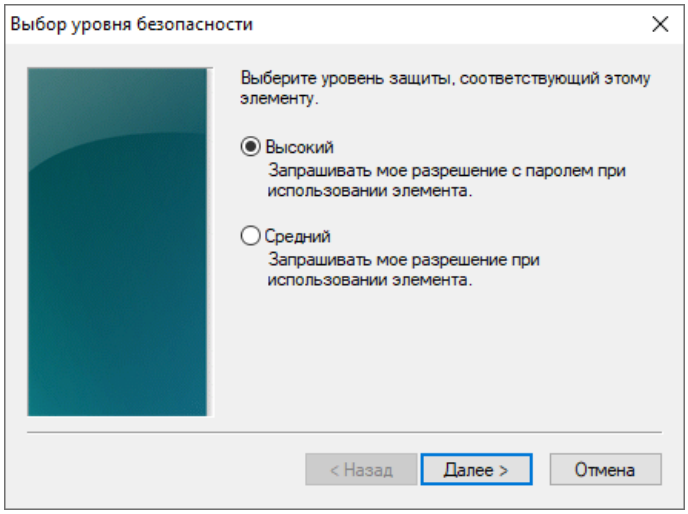
Рис. 36. Создание защищенного элемента




7. Нажмите кнопку **Уровень безопасности**.

   Будет открыто диалоговое окно с выбором уровня защиты (Рис. 37).

Рис. 37. Выбор уровня безопасности




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

**ПРИМЕЧАНИЕ**

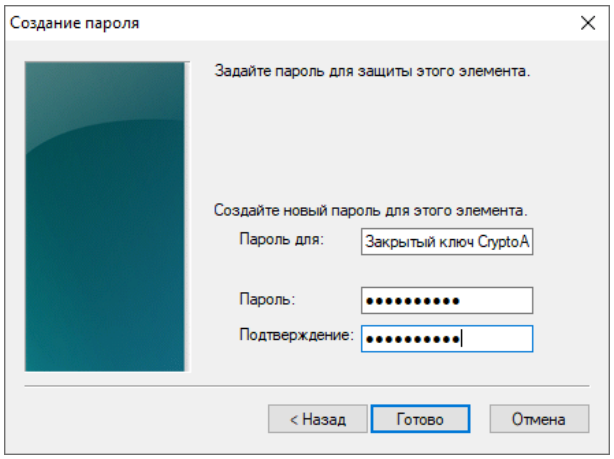
Рекомендованный уровень защиты - **Высокий.**

– **Высокий уровень** – задайте пароль для сертификата и нажмите кнопку **Готово** (Рис. 38).

**ПРИМЕЧАНИЕ**

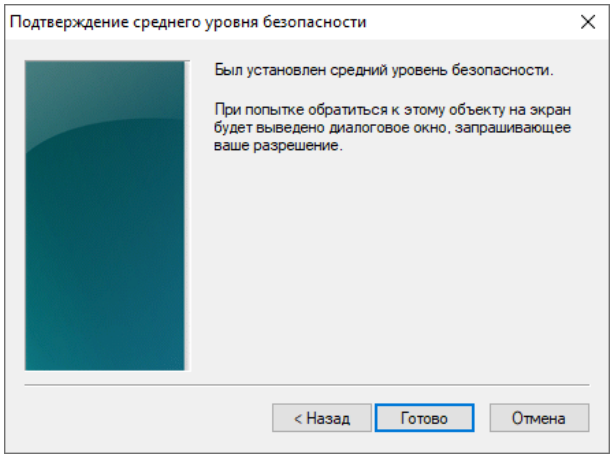
Данный пароль необходимо будет вводить при авторизации на сайте КИВИ. Подробнее об авторизации на сайте см. в Приложении А.

Рис. 38. Установка пароля сертификата



– **Средний уровень** – прочитайте информацию о процессе авторизации и нажмите кнопку **Готово** (Рис. 39).

Рис. 39. Информация об авторизации при среднем уровне безопасности системного хранилища

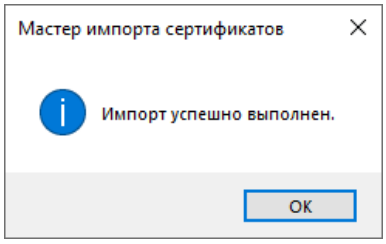



Вы будете возвращены к первому шагу *Мастера создания нового ключа подписи RSA* (см. Рис. 36).

9. Нажмите кнопку **OK**.

   Будет открыто диалоговое окно, информирующее об успешном импорте сертификата (Рис. 40).

Рис. 40. Успешный импорт сертификата




10. Нажмите кнопку **OK**.

Настройки сертификата будут заданы.

# ПРИЛОЖЕНИЕ Г: Сертификат с ГОСТ-шифрованием

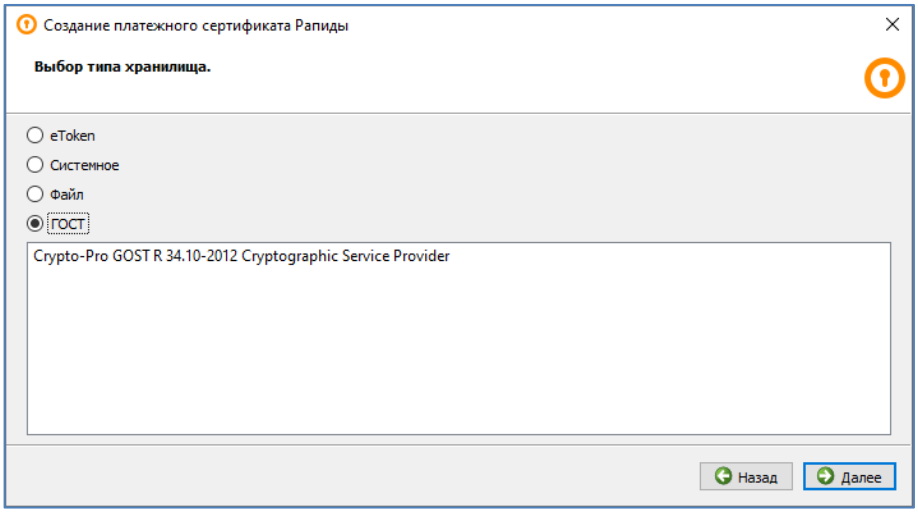
**ВНИМАНИЕ**

Для генерации сертификата с ГОСТ-шифрованием на компьютере должно быть установлено ПО крипто-провайдера, напр. Crypto-Pro.

Чтобы сгенерировать платежный сертификат Рапиды с ГОСТ-шифрованием выполните следующие действия:

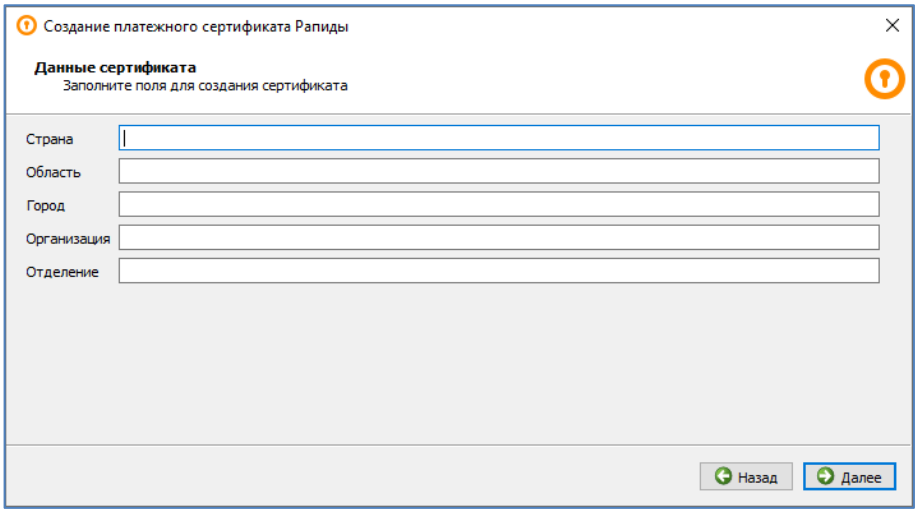
1. Запустите приложение QIWI Защита от имени администратора.
2. В главном окне приложения выберите **Платежный сертификат для Рапиды** (см. Рис. 3). Будет открыт *Мастер создания сертификатов для Рапиды.*
3. Укажите данные персоны для генерации сертификата (Рис. 14):
   - **Логин** – логин персоны;
   - **Пароль** – одноразовый пароль для сертификата;
   - **Показать пароль** – проставьте флаг, если необходимо отобразить значение поля **Пароль**.
4. Выберите тип хранилища **ГОСТ** и выберите ПО крипто-провайдера из списка установленных на вашем компьютере (Рис. 41).

Рис. 41. Выбор хранилища сертификата - ГОСТ




5. Введите данные организации – владельца сертификата (Рис. 42):
   - **Страна, Область, Город** – страна нахождения организации, к которой относится персона;
   - **Организация** – название организации;
   - **Отделение** – название отделения.

Рис. 42. Данные сертификата




Дальнейшие действия будут выполняться выбранным ПО крипто-провайдера.

Дождитесь сообщения «*Сертификат успешно сохранен*» и нажмите кнопку **Завершить.**

# ПРИЛОЖЕНИЕ Д: Коды ошибок

| Код ошибки | Описание |
|---|---|
| 516 | Отсутствует e-mail для персоны, введите его на сайте agt.qiwi.com |
| 518 | Указанный для данной персоны e-mail уже используется. Смените его на сайте agt.qiwi.com |
| 519 | Вы не можете выпускать данный сертификат |

# СПИСОК РИСУНКОВ