

QIWI ЗАЩИТА вер. 3.2

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ вер. 3.2

MOCKBA 8-495-783-5959 РОССИЯ 8-800-200-0059 ФАКС 8-495-926-4619 WEB WWW.QIWI.RU

СОДЕРЖАНИЕ

4	глосси	йиа		2
1.	THOLE	арии		3
2.	ВВЕДЕН	ИЕ		4
	2.1.	Назначени	1Е ПРИЛОЖЕНИЯ	4
	2.2.	Техническ	ИЕ ТРЕБОВАНИЯ	4
3.	БЫСТРЫ	ЫЙ СТАРТ .		5
	3.1.	Создание	СЕРТИФИКАТА	5
	3.2.	Создание	сертификата для ПО QIWI Кассир	5
	3.3.	Создание	платежного сертификата для Рапиды	6
4.	УСТАНС	ОВКА И ГЛИ	АВНОЕ ОКНО ПРИЛОЖЕНИЯ	7
	4.1.	Установка	ПРИЛОЖЕНИЯ	7
	4.2.	Главное о	КНО ПРИЛОЖЕНИЯ	9
5.	ПРЕДВА	РИТЕЛЬНИ	АЯ ПОДГОТОВКА	. 11
6.	ПОЛУЧ	ЕНИЕ ДОС	ГУПА НА АГЕНТСКИЙ САЙТ	. 12
7.	СОЗДАН	НИЕ/УДАЛЕ	ЕНИЕ СЕРТИФИКАТА ДЛЯ QIWI КАССИР/QIWI КАССИР ДЛЯ 1С:ПРЕДПРИЯТИЯ	. 16
	7.1.	Создание	СЕРТИФИКАТА	. 16
	7.2.	Удаление	СЕРТИФИКАТА	. 18
8.	СОЗДАН	НИЕ ПЛАТЕ	ЖНОГО СЕРТИФИКАТА ДЛЯ РАПИДЫ	. 19
9.	допол	НИТЕЛЬНЕ	JE ВОЗМОЖНОСТИ	. 22
	9.1.	Список се	РТИФИКАТОВ	. 22
	9.2.	Сетевые н.	астройки	. 22
	9.3.	Загрузка д	ОКУМЕНТАЦИИ	. 24
ПРИЛ	ОЖЕНИЕ	A:	АВТОРИЗАЦИЯ НА САЙТЕ	. 25
ПРИЛ	ОЖЕНИЕ	Б:	СОХРАНЕНИЕ В СИСТЕМНОЕ ХРАНИЛИЩЕ	. 27
ПРИЛ	ОЖЕНИЕ	B:	РАБОТА С «ФАЙЛОМ» СЕРТИФИКАТА	. 32
ПРИЛ	ОЖЕНИЕ	Г:	СЕРТИФИКАТ С ГОСТ-ШИФРОВАНИЕМ	. 39
ПРИЛ	ОЖЕНИЕ	Д:	коды ошибок	41
СПИС	ОК РИСУ	НКОВ		. 42

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 <i>логином</i> 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).
- Выберите тип хранилища.



Процесс создания сертификата подробно описан в разделе <u>6</u>.

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.



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



ПРИМЕЧАНИЕ

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.

Наиболее	рекомендуемым	хранилишем	ПО	соображениям	безопасности	является	внеш
зашишенн	ый носитель.	L					

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



4. УСТАНОВКА И ГЛАВНОЕ ОКНО ПРИЛОЖЕНИЯ

4.1. Установка приложения

Для установки приложения выполните следующее:

- 1. Скачайте последнюю версию приложения с сайта <u>qiwi.com</u>, 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

2 – 🗆 X
Добро пожаловать в мастер установки QIWI Защита 3.2
QIWI Защита управляет сертификатами безопасности для продуктов QIWI.
Нажимая на кнопку «Далее», Вы соглашаетесь с Правилами работы системы АО «КИВИ»
Быстрая установка Выбороцияя установка
Далее > Отмена

- 3. Выберите тип установки:
 - Быстрая установка будет выполнена автоматическая установка приложения, и вы перейдете к финальному шагу (<u>Рис. 2</u>).
 - 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 <u>6</u>.
 - Создать сертификат для QIWI Кассира создание сертификата для работы с ПО QIWI Кассир. Подробнее см. в разделе <u>7</u>.
 - Платежный сертификат Рапиды создание платежного сертификата для Рапиды.
 Подробнее см. в разделе <u>8</u>.
 - Удалить сертификаты для QIWI Кассира удаление сертификата для ПО QIWI Кассир.
- 2 Список дополнительных возможностей:
 - <u>Список сертификатов</u> открывает системное хранилище сертификатов;
 - <u>Сетевые настройки</u> открывает меню настроек параметров сети для доступа к Интернету;

- <u>Скачать документацию</u> открывает раздел Бизнесу→Действующим агентам→Скачать ПО и документацию на сайте <u>qiwi.com</u>, 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).

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.



1

ПРИМЕЧАНИЕ

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 <u>qiwi.com</u>.

6. ПОЛУЧЕНИЕ ДОСТУПА НА АГЕНТСКИЙ САЙТ

Перед работой с ПО *QIWI Защита* рекомендуется выполнить синхронизацию даты и времени. Перед генерацией сертификата с помощью ПО *QIWI Защита* прочтите раздел <u>5</u>. 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:

 В главном окне приложения выберите действие Сертификат для доступа на агентский сайт (см. <u>Рис. 3</u>).

Будет открыт Мастер создания сертификатов (Рис. 4).

Рис. 4. Мастер создания сертификатов

🕕 Создание сертификата - QIWI Защита	Х
Введение Этот мастер позволит вам быстро и легко создать сертификат	•
• Агент АО "КИВИ"	
Агент АО "КИВИ Банк" (агент Рапиды)	
Для получения нового сертификата вам нужно ввести авторизационные данные и выбрать тип хранилища, в который будет сохранен сертификат.	
Внимание! Для успешной записи сертификата должны быть установлены актуальные дата и время. При необходимости выполните синхронизацию локального времени на компьютере	
Ода	алее

- 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.

Ω

ВНИМАНИЕ

ПРИМЕЧАНИЕ

ß

Далее описаны шаги генерации сертификата с типом хранилища eToken.

Процесс сохранения сертификата в другое хранилище описан в приложениях:

- Системное хранилище <u>Приложение Б</u>;
- Файл <u>Приложение В</u>.

Рис. 5. Ввод авторизационных данных

🛈 Создание се	ртификата - QIWI Защита	×
Авторизации Введите л создать н	инные данные огин и одноразовый пароль персоны, для которой Вы хотите звый сертификат	0
Логин	guard-win	
Пароль	•••••	
Показать парол	ь <u> </u>	
	О Назад	🕽 Далее

4. Выберите тип хранилища еТокеп (Рис. 6).

Рис. 6. Выбор хранилища сертификата

О Создание сертификата - QIWI Защита	×
Выбор типа хранилища	0
(i) eToken	
О Системное	
🔿 Файл	
	🗘 Назад 😧 Далее

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

Рис. 7. Выбор устройства хранения информации

зыбор устройства			
Выберите устройство	и введите пароль для да	нного устройства	
eToken			
ароль:			
•••••			

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

Рис.	8.	Данные	сертификата	для	агентов	Рапиды
------	----	--------	-------------	-----	---------	--------

🕐 Создание с	ртификата - QIWI Защи	га		>
Данные сер Заполнит	ификата поля для создания серти	фиката		0
Страна				
Область				
Город				
Организация [
Отделение				
			🔾 Назад	🕑 Далее

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 <u>5</u>. Для создания сертификата выполните следующее:

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

Далее описаны шаги при выборе типа хранилища eToken.

Процесс сохранения сертификата в другое хранилище описан в приложениях:

- Системное хранилище <u>Приложение Б</u>;
- Файл <u>Приложение В</u>.
- 2. Выберите тип хранилища еТокеп (Рис. 10).

Рис. 10. Выбор устройства хранения информации о персонах

О Создание сертификата для QIWI Кассира	×
Выбор типа хранилища	0
() eToken	
О Системное	
[🕤 Далее

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

внимание

Рис. 11. Выбор устройства хранения информации

) Создание сертификата для QIWI Кассира	
Выбор устройства Выберите устройство и введите пароль для данного устройства	0
eToken	
Пароль:	
• Назад	🔾 Далее

- 4. Введите данные персоны и нажмите кнопку Далее (Рис. 12):
- Рис. 12. Ввод информации о персоне

Осоздание сер Осоздание сер	этификата для QIWI Кассира	>
Ввод информ Введите ин системное	ации о персоне нформацию о персоне, сертификат которой будет записан в хранилище	0
ID терминала:	12345678	
Псевдоним:	Кассир	
Логин:	guard-win	
Пароль:	••••••	
	🗌 Показать пароль	

- 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 еToken*» и нажмите кнопку **Завершить** (<u>Рис. 13</u>).

Рис. 13. Успешная запись данных

Осоздание сертификата для QIWI Кассира	×
Запись сертификата Запись сертификата в выбранное хранилище. Данный процесс может занять некоторое время.	0
Сертификат успешно сохранен на eToken	
🗸 Заве	ршить

Авторизационные данные персоны сохранены на eToken.

7.2. Удаление сертификата

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

С помощью мастера управления персонами выполните следующее:

- 1. Выберите тип хранилища:
 - eToken;

примечание (1)

Вам будет предложено выбрать необходимый еТокеп 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

Перед работой с ПО *QIWI Защита* рекомендуется выполнить синхронизацию даты и времени. Перед созданием сертификата с помощью ПО *QIWI Защита* прочтите раздел <u>5</u>.

Для создания сертификата выполните следующее:

- 1. В главном окне приложения выберите **Платежный сертификат для Рапиды** (см. <u>Рис. 3</u>). 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.

Далее описаны шаги генерации сертификата с типом хранилища eToken.

Процесс сохранения сертификата в другое хранилище описан в приложениях:

- Системное хранилище Приложение Б;
- Файл <u>Приложение В</u>;
- ГОСТ Приложение Г

Рис. 14. Ввод авторизационных данных для сертификата Рапиды

🛈 Создание пла	тежного сертификата Рапиды	Х
Авторизацион Введите лог создать нов	ные данные ин и одноразовый пароль персоны, для которой Вы хотите ый сертификат	0
Логин Пароль Показать пароль		
		🕗 Далее

A

ВНИМАНИЕ

ПРИМЕЧАНИЕ

3. Выберите тип хранилища **еТокеп** (<u>Рис. 15</u>).

Рис. 15. Выбор хранилища сертификата

 Создание платежного сертификата Рапиды 	×
Выбор типа хранилища.	0
eTaken	
Осистемное	
О Файл	
О гост	
	🔾 Назад 📀 Далее

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

Рис. 16. Выбор устройства хранения информации

ыбор устройства			
вырерите устроиство и вве	дите пароль для данног	го устроиства	
eToken			
ароль:			
•••••			
		🔾 Назад 🚺	🕽 Дал

- 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

Данные сер Заполните	г ификата е поля для о	создания	сертифик	ата		(
Страна						
Область						
Город						
Организация						
Отделение						

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

Рис. 18. Запись сертификата

Осоздание платежного сертификата Рапиды	×
Запись сертификата Запись созданного сертификата в выбранное хранилище. Данный процесс может занять некоторое время.	•
Сертификат успешно сохранён.	
🗸 Зав	ершить

9. ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

Приложение реализует следующие дополнительные возможности:

- <u>Список сертификатов</u> открывает системное хранилище сертификатов;
- <u>Сетевые настройки</u> открывает меню настроек параметров сети для доступа к Интернету;
- <u>Скачать документацию</u> открывает раздел Бизнесу->Агентам->Скачать ПО и документацию на сайте <u>qiwi.com</u>, 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. <u>Рис. 3</u>). Будет открыто окно **Сертификаты** (<u>Рис. 19</u>).

	ПРИМЕЧАНИЕ
На вкладке Личные отображаются сертификаты, выданные дан	ному пользователю ОС.

Рис. 19. Системные сертификаты

ичные	Другие г	юльзова	атели	Промежуточн	ые центры серти	фикации	Довереннь
Кому в	зыдан		Кем вь	ыдан	Срок де	Понятн	юе имя
1мпорт	Эt	кспорт	•	Удалить			Дополнительн
Импорт азначе	Эн	кспорт фиката		Удалить			Дополнительн

9.2. Сетевые настройки

Для изменения сетевых настроек выполните следующее:

H)

В главном окне приложения выберите Сетевые настройки (см. <u>Рис. 3</u>).
 Будет открыто диалоговое окно Сетевые настройки (<u>Рис. 20</u>).

Рис. 2	20.	Установки	прокси
--------	-----	-----------	--------

🕐 Сетевые настройки - Q	IWI Защита X
Настройка параметров сети	
Прямое подключение к І	Интернету
Осистемная конфигураци	я
🔘 Настроить прокси вручн	ую:
Хост:	
Порт:	0
С авторизацией	
Имя пользователя:	
Пароль:	
Проверить соединение	🔚 Сохранить 🛛 💥 Отмена

- 2. Задайте необходимые настройки:
 - Прямое подключение к Интернету соединение с сетью Интернет без проксисервера.
 - 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:



Информацию о прокси-сервере запросите у вашего системного администратора.

- ↔ Хост адрес прокси-сервера.
- Савторизацией 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

🛈 Прове	ерить соединение - QIWI Защита	\times
Статус:	Соединение с сервером успешно установле	но.
	OK	

9.3. Загрузка документации

Для получения руководства пользователя к текущей версии ПО:

- 1. Выберите пункт Скачать документацию в главном окне приложения (<u>Рис. 3</u>).
- 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 <u>Процедура активации персоны на сайте</u> 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 <u>aqt.qiwi.com</u>или <u>agent.qiwi.com</u>.
- 3. Браузер может запросить пароль от носителя сертификатов. Введите пароль и нажмите ОК.

Рис. 22. Ввод пароля от носителя сертификатов

Passwo	rd Required		×
?	Please enter the mast	er password for the e	Token.
	ОК	Cancel	

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

Рис. 23. Выб	ор сертификата
--------------	----------------

This site has	requested that y	ou identify yourself	with a certificate
Organization	"OIWI Bank ISC		
Issued Under	"COMODO CA L	imited"	
Choose a cer	tificate to prese	nt as identification:	
(test) ∏	Ольга [01:	:33]	~
Details of sele	ected certificate:		
Issued to: CN Serial numbe Valid from T November 5 Key Usages: Issued by: CI Departamen Stored on: e	I=(test) Π er: 01: :: 2020, 4:42:46 PM Signing,Key Encip N=OSMP Agent C t, Foken	Ольга 33 rr 6, 2018, 4:41:56 PM herment A. OU=Security	to Thursday,
Remembe	er this decision		

 $(\mathbf{1})$



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 (<u>Рис. 24</u>). Пропустите этот пункт, если сертификат находится на внешнем защищенном носителе.



Рис. 24. Одноразовый код подтверждения

Пол	ТВЕРДИТЕ ВХОД
Введите	код из приложения для одноразовых кодов
1. Открой	те на своем смартфоне приложение для одноразовых кодов
2. Войдит	е в аккаунт QIWI
Создать н	овый безопасный ключ

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.
- 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.
- 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.

Системное хранилище является менее защищенным, чем внешний защищенный носитель (смарткарта, usb-ключ и др.). Использовать сертификат вы сможете только на том локальном компьютере, на котором он был сгенерирован.

ВНИМАНИЕ

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. <u>Указать данные персоны в ПО QIWI Защита</u>.
- 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 <u>ШАГУ 2</u>.
- Создание сертификата для Рапиды:
 - Выберите пункт Платежный сертификат для Рапиды.
 - Введите авторизационные данные персоны (логин и одноразовый пароль).
 - Выберите тип хранилища Системное.

- Перейдите к <u>ШАГУ 2</u>.
- Создание сертификата для QIWI Кассира:
 - Выберите пункт Создать сертификат для QIWI Кассира.
 - Выберите тип хранилища Системное.
 - Введите данные персоны (<u>Рис. 25</u>):

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

ПРИМЕЧАНИЕ

- 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

Введите информаци системное хранили	ю о персоне, сертификат которой будет записан в це
D терминала:	12345678
Севдоним:	Кассир
Логин:	guard-win
Пароль:	•••••
	Показать пароль
Выберите тип доступа:	• Для текущего пользователя
	Для всех пользователей

- 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.



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

- Нажмите кнопку Далее.
- Перейдите к <u>ШАГУ 2</u>.

ШАГ 2. Генерация ключа подписи RSA

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

Рис. 26. Создание нового ключа подписи RSA

Создание ново	ого ключа подписи RSA	Х
	Приложение создает защищенный элемент.	
	Закрытый ключ CryptoAP Установлен средний уровень безопасности	
	Уровень безопасности ОК Отмена Состав	

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

Рис. 27. Выбор уровня защиты

Выбор уровня безопасно	сти	X
Выбор уровня безопасно	сти Выберите уровень защиты, соответствующий этом элементу. Высокий Запрацивать мое разрешение с паролем при использовании элемента. Средний Запрашивать мое разрешение при использовании элемента.	× y
	< Назад Далее > Отмена	



Рис. 28. Установка пароля сертификата

<u>28</u>):

Создание пароля		×
	Задайте пароль для защиты этого элемента.	
	Создайте новый пароль для этого элемента. Пароль для: Закрытый ключ CryptoA]
	Пароль: Подтверждение:	
	< Назад Готово От	мена



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 (<u>Рис. 29</u>):

Был	і установлен с	редний уро	вень безог	асности.
При буде ваш	і попытке обра ет выведено ді је разрешение	атиться к эт иалоговое (гому объек окно, запр	ту на экран ашивающее

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

Вы будете возвращены к первому шагу *Мастера создания нового ключа подписи RSA* (см. <u>Рис.</u> 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. <u>Рис. 9</u>).

ПРИЛОЖЕНИЕ В: Работа с «Файлом» сертификата



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 <u>6</u>.
- 2. Выберите тип хранилища Файл.
- 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** (<u>Рис. 30</u>).

Рис. 30. Выбор файла для записи сертификата

0	Осоздание сертифика	та - QIWI Защита	×
	Укажите имя файла Укажите имя файл пароль для шифров	для записи сертификата а, в который будет сохранен сертификат, и зания этого файла	и введите
	Укажите имя файла дл	я записи сертификата:	
	F:\certnkha.p12		
	Введите пароль:	•••••	Хороший пароль
	Подтвердите пароль:	•••••	
	Пароль должен: - иметь длину как мин - содержать заглавны - содержать цифры; - содержать спецсимы В пароле нельзя испол	имум 8 символов; е и строчные латинские буквы; элы из списка !@#\$%^&*0-=_+[]{;:" ,<.> ьзовать имя файла и логин персоны.	>/?`~
		G	Назад 🔾 Далее

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).



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. <u>Рис. 9</u>). 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* (<u>Рис. 31</u>). Укажите расположение хранилища и нажмите **Далее**.

Рис. 31. Мастер импорта сертификатов

÷ 🛃	Мастер импорта сертификатов	×
	Мастер импорта сертификатов	
	Этот мастер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов с локального диска в хранилище сертификатов.	
	Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит инфорнацию, необходимую для защиты данных или установления защищенных сетевых подключений. Хранилище сертификатов — это область системы, предназначенная для хранения сертификатов.	
	Расположение хранилища • Текущий пользователь О Локальный компьютер	
	Для продолжения нажните кнопку "Далее".	
	Далее Отмена	

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



Рис. 32. Импортируемый файл

и	мпортируемый файл
	Укажите файл, который вы хотите импортировать.
	Има файла-
	F:\certnkha.p12 O6sop
	Замечание: следующие форматы файлов могут содержать более одного сертификата в одном файле:
	Файл обмена личной информацией - PKCS #12 (.PFX,.P12)
	Стандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b)
	Хранилище сериализованных сертификатов (.SST)

3. Установите флаги Включить усиленную защиту закрытого ключа, Включить все расширенные свойства (<u>Рис. 33</u>).



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

Рис. 33. Ввод пароля для файла сертификата

Защита с помощью закрытого ключа
Для обеспечения безопасности закрытый ключ защищен паролем.
Введите пароль для закрытого ключа.
•••••
Показывать пароль
Параметры импорта:
Включить усиленную защиту закрытого ключа. В этом случае при каждом
использовании закрытого ключа приложением будет запрашиваться разрешение.
Пометить этот ключ как экспортируемый, что позволит сохранять резервную копию ключа и перемещать его.
Защита закрытого ключа с помощью безопасной виртуализации (неэкспоотируемый)
Включить все расширенные свойства.

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

Рис. 34. Выбор размещения сертификата

Windows pacnond accord At C Tr X	ища сертифика ся сертификат в автоматичес ожение сертиф втоматически юместить все о ранилища сер	атов - это сист гы. ски выберет хр фиката вручнун выбрать хран сертификаты в	анилище, и ю. илище на ос з следующе	или вы мож снове типа се хранили	ете указать сертификата це	
Windows pacnond Ar Dr X	s автоматичес ожение сертиф втоматически юместить все с ранилище сер	ски выберет хр фиката вручну выбрать хран сертификаты в	анилище, и ю. илище на ос 3 следующе	пли вы мож снове типа е хранили	ете указать сертификата ще	
A ا الم	втоматически оместить все о ранилище сер	і выбрать хран сертификаты в	илище на ос 3 следующе	снове типа е хранили	сертификата це	
	оместить все о (ранилище сер	сертификаты в	з следующе	е хранили	це	
×	(ранилище сер	тификатов				
		iniquica robi				
					Обзор	
				ſ	Лалее От	Mer
					1	Далее От

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

Рис. 35. Параметры импорта сертификата

	-	
Сертифика	r будет импортирован после	е нажатия кнопки "Готово".
Были указа	ны следующие параметры:	
Выбранно	е хранилище сертификатов	Автоматический выбор мастером
Содержим	oe	PFX
Файл		F:\certnkha.p12

6. Нажмите кнопку Готово.

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

Рис. 36. Создание защищенного элемента

Импорт ново	ого закрытого ключа обмена	\times
	Приложение создает защищенный элемент.	
	Закрытый ключ CryptoAP Установлен средний уровень безопасности	
	Уровень безопасности ОК Отмена Состав	

7. Нажмите кнопку Уровень безопасности.

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

Рис. 37. Выбор уровня безопасности

ыбор уровня без	опасности >
	Выберите уровень защиты, соответствующий этому элементу.
	Высокий Запрашивать мое разрешение с паролем при использовании элемента.
	Средний Запрашивать мое разрешение при использовании элемента.
	< Назад Далее > Отмена

8. Выберите уровень безопасности и нажмите кнопку Далее.

	ПРИМЕЧАНИЕ	
Рекомендованный уровень защиты - Высокий.		
сомендованный уровень защиты - высокий.		

– Высокий уровень – задайте пароль для сертификата и нажмите кнопку Готово (<u>Рис. 38</u>).

		ПРІ	ИМЕЧАНИЕ	1
Данный пароль необходимо будет вводит авторизации на сайте см. в <mark>Приложении А</mark>	ь при авторизации	на сайте КИ	ИВИ. Подробнее	об

Рис. 38. Установка пароля сертификата

Создание пароля		×
	Задайте пароль для	защиты этого элемента.
	Создайте новый пар Пароль для:	ооль для этого элемента. Закрытый ключ CryptoA
	Пароль: Подтверждение:	••••••
	< Назад	Готово Отмена

 Средний уровень – прочитайте информацию о процессе авторизации и нажмите кнопку Готово (<u>Рис. 39</u>).

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

Подтверждение среднего	уровня безопасности	×
	Был установлен средний уровень безопасности. При попытке обратиться к этому объекту на экран будет выведено диалоговое окно, запрашивающее ваше разрешение.	
	< Назад Готово Отмена	

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

9. Нажмите кнопку ОК.

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

Рис. 40. Успешный импорт сертификата



10. Нажмите кнопку ОК.

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. <u>Рис. 3</u>). 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 (<u>Рис. 41</u>).

Рис. 41. Выбор хранилища сертификата - ГОСТ

 Создание платежного сертификата Рапиды 	×
Выбор типа хранилища.	0
() eToken	
О Системное	
🔘 Файл	
● [FOCT]	
Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider	
	🕒 Назад 🖸 Далее

- 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

Данные серт Заполните	ификата поля для создания се	тификата	0
Страна			
Область			
ород			
Организация			
Отделение			
			🔾 Назал 🖸 Лапее

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

Рис. 1. Мастер установки	7
Рис. 2. Финальный шаг установки	8
Рис. 3. Главное окно приложения	9
Рис. 4. Мастер создания сертификатов	12
Рис. 5. Ввод авторизационных данных	13
Рис. 6. Выбор хранилища сертификата	13
Рис. 7. Выбор устройства хранения информации	14
Рис. 8. Данные сертификата для агентов Рапиды	14
Рис. 9. Запись сертификата	15
Рис. 10. Выбор устройства хранения информации о персонах	16
Рис. 11. Выбор устройства хранения информации	17
Рис. 12. Ввод информации о персоне	17
Рис. 13. Успешная запись данных	
Рис. 14. Ввод авторизационных данных для сертификата Рапиды	19
Рис. 15. Выбор хранилища сертификата	20
Рис. 16. Выбор устройства хранения информации	20
Рис. 17. Данные сертификата	21
Рис. 18. Запись сертификата	21
Рис. 19. Системные сертификаты	22
Рис. 20. Установки прокси	23
Рис. 21. Успешное соединение с сервером	24
Рис. 22. Ввод пароля от носителя сертификатов	25
Рис. 22. Ввод пароля от носителя сертификатов Рис. 23. Выбор сертификата	
Рис. 22. Ввод пароля от носителя сертификатов Рис. 23. Выбор сертификата Рис. 24. Ввод пароля для закрытого ключа в системном хранилище Ошибка! Заки	25 25 1адка не
Рис. 22. Ввод пароля от носителя сертификатов Рис. 23. Выбор сертификата Рис. 24. Ввод пароля для закрытого ключа в системном хранилище Ошибка! Закл определена.	25 25 1адка не
Рис. 22. Ввод пароля от носителя сертификатов Рис. 23. Выбор сертификата Рис. 24. Ввод пароля для закрытого ключа в системном хранилище Ошибка! Закл определена. Рис. 25. Ввод информации о персоне	25 25 1адка не 28
Рис. 22. Ввод пароля от носителя сертификатов Рис. 23. Выбор сертификата Рис. 24. Ввод пароля для закрытого ключа в системном хранилище Ошибка! Закл определена. Рис. 25. Ввод информации о персоне Рис. 26. Создание нового ключа подписи RSA	25 25 1адка не 28 28
Рис. 22. Ввод пароля от носителя сертификатов Рис. 23. Выбор сертификата Рис. 24. Ввод пароля для закрытого ключа в системном хранилище Ошибка! Закл определена. Рис. 25. Ввод информации о персоне Рис. 26. Создание нового ключа подписи RSA Рис. 27. Выбор уровня защиты	25 25 адка не 28 29 29
Рис. 22. Ввод пароля от носителя сертификатов Рис. 23. Выбор сертификата Рис. 24. Ввод пароля для закрытого ключа в системном хранилище Ошибка! Закл определена. Рис. 25. Ввод информации о персоне Рис. 26. Создание нового ключа подписи RSA Рис. 27. Выбор уровня защиты Рис. 28. Установка пароля сертификата	25 25 адка не 28 29 29
 Рис. 22. Ввод пароля от носителя сертификатов	25 1адка не 28 29 29 29 30 иища31
 Рис. 22. Ввод пароля от носителя сертификатов Рис. 23. Выбор сертификата Рис. 24. Ввод пароля для закрытого ключа в системном хранилище Ошибка! Заклопределена. Рис. 25. Ввод информации о персоне	25 1адка не 28 29 29 29 30 ища31 32
 Рис. 22. Ввод пароля от носителя сертификатов	25 1адка не 28 29 29 30 іища31 32 33
 Рис. 22. Ввод пароля от носителя сертификатов	25 1адка не 28 29 29 30 іища31 32 33 34
 Рис. 22. Ввод пароля от носителя сертификатов	25 1адка не 28 29 30 ища31 32 33 34 35
 Рис. 22. Ввод пароля от носителя сертификатов	25 1адка не 28 29 29 30 ища31 32 33 35 35
 Рис. 22. Ввод пароля от носителя сертификатов	25 1адка не 28 29 29 30 іища31 32 33 34 35 36
 Рис. 22. Ввод пароля от носителя сертификатов	25 • 25 • адка не 29 29 30 • ища31 32 33 34 35 36 36
 Рис. 22. Ввод пароля от носителя сертификатов	25 • 25 • адка не 29 29 30 • ища31 32 33 34 35 36 36 37
 Рис. 22. Ввод пароля от носителя сертификатов	25 1адка не 28 29 30 иища31 32 33 34 35 35 36 36 37 37
 Рис. 22. Ввод пароля от носителя сертификатов	25 1адка не 28 29 29 29 30 ища 31 32 33 34 35 35 35 35 36 36 37 37 ища 38
 Рис. 22. Ввод пароля от носителя сертификатов	25 1адка не 28 29 29 29 30 ища 31 32 33 34 35 35 35 36 36 37 37 ища 38 37 ища 38 38
 Рис. 22. Ввод пароля от носителя сертификатов	25 1адка не 28 29 30 ища31 32 33 34 35 36 36 37 ища38 38 38 38 39