

# **QIWI ЗАЩИТА** вер. 2.1

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ вер. 1.9

MOCKBA 8-495-783-5959 РОССИЯ 8-800-200-0059 ФАКС 8-495-926-4615 WEB WWW.QIWI.RU

# СОДЕРЖАНИЕ

1.	ГЛОССА	АРИЙ	4
2.	ВВЕДЕ⊦	НИЕ	5
	2.1.	Назначение приложения	5
	2.2.	Технические требования	5
3.	БЫСТРЫ	ЫЙ СТАРТ	6
	3.1.	Создание сертификата	6
	3.2.	Создание персоны для ПО QIWI Кассир	6
	3.3.	Электронный документооборот	7
4.	УСТАНС	ОВКА И ВНЕШНИЙ ВИД ПРИЛОЖЕНИЯ	8
	4.1.	Установка приложения	8
	4.2.	Главное окно приложения	10
5.	ПРЕДВА	АРИТЕЛЬНАЯ ПОДГОТОВКА	12
	5.1.	Получение доступа на агентский сайт	12
	5.2.	Создание персоны для ПО «QIWI Кассир»	12
6.	ПОЛУЧ	ІЕНИЕ ДОСТУПА НА АГЕНТСКИЙ САЙТ	14
7.	СОЗДА	.НИЕ/УДАЛЕНИЕ ПЕРСОНЫ ДЛЯ QIWI КАССИР/QIWI КАССИР 1С	18
	7.1.	Создание персоны	18
	7.2.	Удаление персоны ПО QIWI Кассир	22
8.	HACTPO	ОИТЬ ЭТОТ КОМПЬЮТЕР ДЛЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА	23
9.	СЕРТИФ	ФИКАТЫ ЭЛЕКТРОННО-ЦИФРОВОЙ ПОДПИСИ	26
	9.1.	Создание заявки на сертификат ЭЦП	26
	9.2.	Установка сертификата	35
10.	допол	ПНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ	37
	10.1.	Список сертификатов	37
	10.2.	Сетевые настройки	38
	10.3.	Загрузка драйверов	39
	10.4.	Загрузка документации	39
	10.5.	О ПРОГРАММЕ	40
11.	ЧАСТО	ЗАДАВАЕМЫЕ ВОПРОСЫ	41
ПРИЛ	ОЖЕНИЕ	Е А: РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ	43
ПРИЛ	ОЖЕНИЕ	Е Б: ПОДГОТОВКА ЕТОКЕN К РАБОТЕ	44
ПРИЛ	ОЖЕНИЕ	Е В: АВТОРИЗАЦИЯ НА САЙТЕ	48
ПРИЛ	ОЖЕНИЕ	Е Г: СОХРАНЕНИЕ В СИСТЕМНОЕ ХРАНИЛИЩЕ	50
ПРИЛ	ОЖЕНИЕ	Е Д: РАБОТА С «ФАЙЛОМ» СЕРТИФИКАТА	55
ПРИЛ	ОЖЕНИЕ	Е Е: СИНХРОНИЗАЦИЯ ВРЕМЕНИ	63

ПРИЛОЖЕНИЕ Ж:	ПОЛУЧЕНИЕ СЕРТИФИКАТА ЭЦП	64
СПИСОК РИСУНКОВ		65

# 1. ГЛОССАРИЙ

Термин	Определение
Авторизация	Проверка прав персоны и предоставление доступа к ресурсам в соответствии с ними.
Персона	Учетная запись, зарегистрированная на сайте для сотрудника агента, работающего с системой ОСМП. Персона имеет определенный набор прав доступа к системе.
Псевдоним	Имя пользователя, отображаемое при авторизации в приложениях ОСМП (например, в ПО <i>QIWI Кассир</i> ).
Сертификат	Цифровой документ, используемый для идентификации персоны.

### 2. ВВЕДЕНИЕ

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

### 2.1. Назначение приложения

ПО *QIWI Защита* предназначено для повышения уровня безопасности при работе с *Системой ОСМП*. Приложение позволяет:

- Сгенерировать сертификат для авторизации на сайтах ОСМП:
  - агентский <u>agent.qiwi.com</u> (<u>portal.qiwi.com</u>);
  - провайдерский <u>prov.osmp.ru</u>.
- Сгенерировать авторизационные данные персоны для ПО QIWI Кассир.



Для повышения уровня безопасности авторизационные данные рекомендуется хранить на eToken/

• Создать электронно-цифровую подпись и настроить электронный документооборот с Системой ОСМП.

### 2.2. Технические требования

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

- не менее 21 Мб свободного дискового пространства;
- разрешение экрана 1024х768 в режиме High/True Color;
- оперативной памяти не менее 64 Мб (рекомендуется 128 Мб);
- частота процессора не ниже 233 МГц;
- наличие подключения к сети Интернет;
- операционная система Microsoft Windows 9x, ME, 2000, XP, 2003, Vista, 7;
- драйвера для работы с ключом eToken версии 4.55 или выше.

# 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 еТокел. 4. Сохраните сертификат в хранилище. ПРИМЕЧАНИЕ Процесс создания сертификата подробно описан в разделе <u>6</u>.

# 3.2. Создание персоны для ПО QIWI Кассир

Для создания авторизационных данных персоны выполните следующее:

- 1. Выберите пункт Создание/удаление персоны для QIWI Кассир/QIWI Кассир 1С.
- 2. Установите переключатель в положение Создание.
- 3. Выберите тип хранилища.



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



Процесс управления авторизационными данными персон подробно описан в разделе 7.1.

# 3.3. Электронный документооборот

Для настройки электронного документооборота выполните следующее:

- 1. Если на вашем компьютере отсутствует ПО *КриптоПро CSP* или *ЭЦП Browser Plug-in*, выберите пункт **Настроить этот компьютер для электронного документооборота**.
- 2. Будет запущен мастер установки ПО *КриптоПро CSP* и *ЭЦП Browser Plug-in*, необходимых для получения и установки сертификата электронно-цифровой подписи (ЭЦП).
- 3. Выполните все шаги мастера.



- Оформите заявку на сертификат ЭЦП: в главном окне программы выберите действие Сертификаты электронно-цифровой подписи → Заявка на сертификат и следуйте дальнейшим указаниям мастера.
- 5. После того как сертификат ЭЦП получен, установите сертификат на компьютер: в главном окне программы выберите действие **Сертификаты электронно-цифровой подписи** → **Установка сертификата**.



Процесс получения и установки сертификата ЭЦП подробно описан в разделе 9.

# 4. УСТАНОВКА И ВНЕШНИЙ ВИД ПРИЛОЖЕНИЯ

### 4.1. Установка приложения

Для установки приложения выполните следующее:

- 1. Скачайте последнюю версию приложения с сайта <u>www.qiwi.ru</u>, раздел **Бизнесу→Агентам→Скачать ПО**.
- 2. Запустите файл qiwiguard-x.x-ru-win.exe (x.x номер версии приложения) (Рис. 1).

#### Рис. 1. Мастер установки

🧍 Установка QIWI Защита Х.Х			
	Добро пожаловать в мастер установки QIWI Защита X.X		
	Программа QIWI Защита представляет собой удобный инструмент для управления сертификатами, позволяющими сделать работу в системе ОСМП более безопасной.		
OIWI	Нажмите кнопку 'Далее' для продолжения.		
защита	<ul> <li>Быстрая установка</li> <li>Выборочная установка</li> </ul>		
	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:
    - 🔶 ознакомиться с лицензионным соглашением;
    - выбрать папку установки;
    - выбрать папку в меню Пуск.

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

#### Рис. 2. Финальный шаг установки

🧍 Установка QIWI Защита	X.X	
	Завершение работы мастера установки QIWI Защита	
	Установка QIWI Защита выполнена.	
	Нажмите кнопку "Готово" для выхода из программы установки.	
OIWI	🗹 Запустить QIWI Защита	
🔪 защита	Рекомендации по безопасности	
	Полная информация о продуктах на нашем сайте.	
	< Назад Готово Отмена	

- 4. Снимите флаги, если вы не желаете выполнить данные действия:
  - Запустить QIWI Защита запустить приложение сразу после установки.
  - Рекомендации по безопасности ознакомиться с рекомендациями по обеспечению безопасности при работе с Системой.



5. Для завершения работы мастера нажмите кнопку Готово.

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

🎢 QIWI Защита	
O	Управление сертификатами и персонами
QIWI	Выбор задачи
2	Получить доступ на агентский сайт У меня есть логин и одноразовый пароль, я хочу получить сертификат для доступа к сайту agent.qiwi.ru
<ul> <li>Список сертификатов</li> <li>Сетевые настройки</li> </ul>	Создание/удаление персоны для QIWI Кассир/QIWI Кассир 1С Я хочу создать/удалить персону для работы с программами QIWI Кассир/QIWI Кассир 1С
<ul> <li>Загрузить драйверы</li> <li>Загрузить документаци о</li> <li>О программе</li> </ul>	Настройка компьютера для электронного документооборота (ЭЦП) Дает возможность подписывать документы Вашей электронной подписью
	Часто задаваемые вопросы Откуда скачать последнюю версию ПО? Как получить логин и одноразовый пароль?

Главное окно приложения состоит из двух областей:

- 1 Список основных задач:
  - Получить доступ на агентский сайт позволяет создать сертификат для доступа на сайты <u>portal.qiwi.com</u>, <u>agent.qiwi.com</u> и <u>prov.osmp.ru</u>. Подробнее о генерации сертификата см. в разделе <u>6</u>.
  - Создание/удаление персоны для QIWI Кассир/QIWI Кассир 1С позволяет создавать авторизационные данные персоны для работы с ПО *QIWI Кассир*, а также удалять их. Подробнее об управлении персонами см. в разделе <u>7</u>.
  - Настроить этот компьютер для электронного документооборота позволяет загрузить и установить ПО *КриптоПро CSP* или ЭЦП Browser Plug-in для получения возможности работать с электронной цифровой подписью (ЭЦП). Подробнее о настройке ПО для электронного документооборота см. в разделе <u>8</u>.

Если ПО *КриптоПро CSP* и ПО *ЭЦП Browser Plug-in* установлены на компьютере пользователя, на месте пункта **Настроить этот компьютер для электронного документооборота** отображается пункт **Сертификаты электронно-цифровой подписи.** 

- Сертификаты электронно-цифровой подписи позволяет создать запрос на сертификат ЭЦП и установить полученный сертификат на компьютер пользователя.
   Сертификат необходим для подписания актов агента с помощью ЭЦП. Подробнее о работе с сертификатами ЭЦП см. в разделе <u>9</u>.
- **Часто задаваемые вопросы** список ответов на часто задаваемые вопросы.
- 2 Список дополнительных возможностей:
  - <u>Список сертификатов</u> открывает системное хранилище сертификатов;
  - <u>Сетевые настройки</u> позволяет задать сетевые настройки для доступа к Интернету;
  - <u>Загрузить драйверы</u> позволяет загрузить драйверы, необходимые для работы с eToken в различных OC;
  - Загрузить документацию позволяет загрузить последнюю версию руководства пользователя;
  - <u>О программе</u> открывает окно с информацией о приложении.

### 5. Предварительная подготовка

Перед работой с ПО QIWI Защита рекомендуется выполнить синхронизацию даты и времени (подробнее см. <u>Приложение E</u>).

На agent.giwi.com вам необходимо зарегистрировать:

- для получения доступа на агентский сайт персону.
- для создания персоны для ПО «QIWI Кассир» персону и терминал.

Данный раздел содержит требования к персонам и терминалам. Подробнее о создании персон, терминалов и генерации одноразового пароля см. в Руководстве пользователя сайта <u>agent.qiwi.com</u>.

### 5.1. Получение доступа на агентский сайт

Для генерации сертификата вам потребуется зарегистрировать на сайте agent.qiwi.com персону:

- Роль персоны не должна быть Продавец или Автомат.
- Задать Логин персоны.
- Сгенерировать Одноразовый пароль.

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

### 5.2. Создание персоны для ПО «QIWI Кассир»

На сайте agent.giwi.com необходимо зарегистрировать:

- Персону:
  - Назначить роль Продавец
  - Задать Логин персоны
  - Сгенерировать Одноразовый пароль



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





 $(\mathsf{M})$ 

2.1

- Терминал:
  - Задать тип терминала **QIWI Кассир**
  - Указать Серийный номер ПО *QIWI Кассир*.

# 6. ПОЛУЧЕНИЕ ДОСТУПА НА АГЕНТСКИЙ САЙТ

Перед генерацией сертификата с помощью ПО QIWI Защита прочтите раздел <u>5</u>.

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

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

Будет открыт Мастер создания сертификатов (Рис. 4).

Рис. 4. Мастер создания сертификатов

🧍 Создание сертификата - QIWI Защита	
Введение Этот мастер позволит вам быстро и легко создать сертификат	
Для получения нового сертификата вам нужно ввести авторизационные данные и выбрать тип хранилища, в который будет сохранен сертификат.	
Примечание: Для успешной записи сертификата должны быть установлены актуа. дата и время. При необходимости выполните синхронизацию локального времени	льные на ПК.
٥	Далее

внимание

Рис. 5. Ввод авторизационных данных

🧍 Созда	ние сертификата - QIWI Защита	X
Автор Вв со:	<b>изационные данные</b> едите логин и одноразовый пароль персоны, для которой вы хотите здать новый сертификат	
Логин	Person	
Пароль	•••••	
	С Назад	Далее

- 2. Укажите данные персоны для генерации сертификата (Рис. 5):
  - Логин логин персоны;
  - Пароль одноразовый пароль для сертификата.
  - Показать пароль флаг позволяет отображать значение поля Пароль.

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

Процесс сохранения сертификата в другое хранилище описан в приложениях:

- Системное хранилище Приложение Г;
- Файл Приложение Д.

### Рис. 6. Выбор хранилища сертификата

🔒 Создание сертификата - QIWI Защита	X
Выбор типа хранилища	
💿 eToken	
О Системное	
🔘 Файл	
	🔾 Назад 🖸 Далее

- 3. Выберите тип хранилища **еТокеп** (<u>Рис. 6</u>).
- 4. Выберите необходимое устройство из списка eToken и укажите пароль для него (Рис. 7).

Рис. 7. Выбор устройства хранения информации

🔒 Создание сертификата - QIWI Защита	
Выбор устройства хранения информации о персонах Выберите устройство и введите пароль для данного устройства	
eToken AdditionalKev	
Пароль:	
••••••	
С Назад	🛛 Далее

### ПРИМЕЧАНИЕ

Если на eToken установлен пароль, требующий смены при первом использовании, вам будет предложено сменить его на постоянный (см. <u>Приложение Б</u>)

A

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

### Рис. 8. Запись сертификата

🧍 Создание сертификата - QIWI Защита	×
Запись сертификата Запись созданного сертификата в выбранное хранилище. Данный процесс может занять некоторое время.	QIWI
Сертификат успешно сохранен	
	✔ Завершить

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

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

# 7. СОЗДАНИЕ/УДАЛЕНИЕ ПЕРСОНЫ ДЛЯ QIWI КАССИР/QIWI КАССИР 1C

ПО *QIWI Защита* позволяет сгенерировать (а также удалить ранее созданные) авторизационные данные персоны для работы с ПО *QIWI Кассир.* 

### 7.1. Создание персоны



Для создания авторизационных данных персоны выполните следующее:

1. В главном окне приложения выберите **Создание/удаление персоны для QIWI Кассир/QIWI Кассир 1С** (см. <u>Рис. 3</u>).

Будет открыт Мастер управления персонами (Рис. 9).

#### Рис. 9. Мастер управления персонами

🔒 Создание/удаление персоны - QIWI Защита	
<b>Введение</b> Этот мастер представляет простой способ создать или удалить персону	QIWI
Выберите действие	
💿 Создание	
🔿 Удаление	
	🕽 Далее

2. Выберите Создание и нажмите кнопку Далее.

внимание

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

При сохранении авторизационных данных персоны в системном хранилище обязательно прочтите **Приложение Г**.

3. Выберите тип хранилища **еТокеп** (<u>Рис. 10</u>).

Рис. 10. Выбор устройства хранения информации о персонах

🖡 Создание персоны - QIWI Защита	X
Выбор типа хранилища	Q
💿 eToken	
О Системное	
	🕞 Назад 💽 Далее

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

### Рис. 11. Выбор устройства хранения информации

8	Создание	персоны - QIWI Защита	
I	<b>Выбор уст</b> Выбери	ройства хранения информации о персонах те устройство и введите пароль для данного устройства	
ſ		Additionalization	
	eToken	Key	
ſ	Пароль:		
	•••••		
		С Назад	🛛 Далее

### примечание

Если на eToken установлен пароль, требующий смены при первом использовании, вам будет предложено сменить его на постоянный (подробнее см. в пункте в пункте 1 <u>Приложения Б</u>).

#### Рис. 12. Ввод информации о персоне

🧍 Создание/уд	даление персоны - QIWI Защита 🛛 🛛 🔀
Ввод информации о персоне Введите информацию о персоне, которая должна быть записана в хранилище	
Псевдоним:	Персона 1
Логин:	Persona
ID терминала:	5555555
Пароль:	1234567
	Показать пароль
	🔇 Назад 💽 Далее

- 5. Введите данные персоны и нажмите кнопку Далее (Рис. 12):
  - Псевдоним введите любое имя учетной записи, которое в дальнейшем будет использоваться для авторизации в ПО *QIWI Кассир*.
  - Логин логин персоны.
  - **ІD терминала** номер терминала.
  - Пароль одноразовый пароль для сертификата.
  - Показать пароль флаг позволяет отображать значение поля Пароль.
- 6. Дождитесь сообщения «*Информация о персоне успешно сохранена на eToken*» и нажмите кнопку **Завершить** (<u>Рис. 13</u>).

Рис. 13. Успешная запись данных

🔒 Создание персоны - QIWI Защита	
Запись информации о персоне Запись созданной персоны в выбранное хранилище. Данный процесс может занять некоторое время.	
Информация о персоне успешно сохранена на eToken	
	√ Завершить

Авторизационные данные персоны сохранены на eToken.

# 7.2. Удаление персоны ПО QIWI Кассир

Для удаления авторизационных данных персоны в главном окне приложения выберите (см. Рис. 3).

С помощью мастера управления персонами выполните следующее:

- 1. Выберите Удалить.
- 2. Выберите тип хранилища:
  - eToken;

ПРИМЕЧАНИЕ

A

Вам будет предложено выбрать необходимый еТокеп и указать пароль к нему.

### Системное хранилище;

- 3. Выберите псевдоним персоны, авторизационные данные которой необходимо удалить.
- 4. Нажмите кнопку Далее.

Авторизационные данные персоны будут удалены.

# 8. НАСТРОИТЬ ЭТОТ КОМПЬЮТЕР ДЛЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

ПО *QIWI Защита* позволяет установить программное обеспечение для получения и установки сертификата ЭЦП.

При открытии ПО *QIWI Защита* автоматически выявляет наличие установленных программ *КриптоПро CSP* и *ЭЦП Browser Plug-in*. Если хотя бы одна из программ не установлена на компьютере пользователя, то ПО *QIWI Защита* предложит установку указанных программ.



На компьютере с оперативной системой *Windows 7* все действия должны производиться под учетной записью администратора ПК.

Для установки ПО КриптоПро CSP и ЭЦП Browser Plug-in сделайте следующее:

1. В главном окне приложения выберите действие **Настроить этот компьютер для электронного документооборота** (см. <u>Рис. 3</u>).

Будет открыт мастер настройки компьютера для электронного документооборота (Рис. 14).

Рис. 14. Подтверждение установки ПО



- 2. Нажмите кнопку Далее.
- Ознакомьтесь с лицензионным соглашением и подтвердите свое согласие, нажав кнопку Принять, установить (<u>Рис. 15</u>).

#### Рис. 15. Лицензионное соглашение

8	Настроить этот компьютер для электронного документооборота
	Лицензионное соглашение КриптоПро СSP Пожалуйста, ознакомътесь с лицензионным соглашением
	ВНИМАТЕЛЬНО ОЗНАКОМЬТЕСЬ С ЛИЦЕНЗИОННЫМ СОГЛАШЕНИЕМ НА ИСПОЛЬЗОВАНИЕ ИЗДЕЛИЯ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ
	1. Исключительные права на программу для ЭВМ, включая документацию в электронном виде, (далее – Изделие) принадлежат ООО «КРИПТО-ПРО», далее – Правообладатель.
	2. Настоящее соглашение является офертой ООО «КРИПТО-ПРО» к физическому или юридическому лицу, далее - Пользователь.
	3. Пользователь в соответствии с настоящим соглашением получает право использовать Изделие на территории Российской Федерации.
	4. Установка Изделия в память ЭВМ рассматривается как безусловное согласие 🔹
	🔾 Назад 💽 Принять, установить

4. В окне Регистрация ключа продукта КриптоПРО CSP выберите один из пунктов (Рис. 16):

### Рис. 16. Регистрация ключа продукта КриптоПро CSP

Настроить этот компьютер для электронного документооборота	×
Регистрация ключа продукта КриптоПро СSP Приобрести лицензию на продукт КриптоПро CSP можно на сайте КриптоПро <u>cryptopro.ru/order/</u> Q	
Оспользовать лицензионную версию КриптоПро CSP	
Введите серийный номер	
Использовать демонстрационную версию продукта	
Срок действия демонстрационной версии составляет 3 месяца. За это время Вы долж приобрести лицензию и ввести серийный номер продукта. Подробнее в Руководстве Электронно-цифровой подписи.	по
С Назад С Д	алее

 Использовать лицензионную версию продукта - при выборе данного пункта необходимо указать серийный номер продукта в полях Введите серийный номер.



- Использовать демонстрационную версию КриптоПро CSP при выборе данного пункта вводить серийный номер не надо, но возможность использовать ПО бесплатно доступна только в течение трех месяцев, после чего необходимо будет приобрести лицензию.
- 5. Нажмите кнопку Далее.
- 6. В окне Регистрация ключа продукта КриптоПро OCSP Client и в окне Регистрация продукта Криптопро TSP Client введите серийные номера продуктов КриптоПро OCSP Client и TSP Client. Если Вы еще не приобрели лицензии на них, оставьте поля пустыми (в последнем случае возможность использовать ПО бесплатно доступна только в течение трех месяцев, после чего необходимо будет приобрести лицензию). Затем нажмите кнопку Далее (Рис. 17).

#### Рис. 17. Регистрация ключа продукта КриптоПро OCSP Client и КриптоПро TSP Client

Настроить этот компьютер для электронного документооборота	🕺 Настроить этот компьютер для электронного документооборота
Регистрация ключа продукта КриптоПро OCSP Client Приобрести лицензию на продукт КриптоПро OCSP Client ножно на сайте КриптоПро <u>cryptopro.ru/order/</u>	Регистрации продукта Криптопро TSP Client Приобрести лицензию на продукт КриптоПро TSP Client можно на сайте КриптоПро <u>стуріорго.ru/order/</u>
Введите серийный номер	Веедите серийный номер
• Назад • Далее	С Назад О Далее

- 7. Дождитесь окончания установки ПО КриптоПро CSP и ЭЦП Browser Plug-in.
- 8. На последнем шаге мастера, выберите один из предложенных вариантов перезагрузки ПК:
  - Перезагрузить сейчас рекомендуется выбрать данный пункт. Компьютер перезагрузится самостоятельно, после нажатия кнопки. После перезагрузки ПО QIWI Защита запустится автоматически.
  - Перезагрузить позже пользователю придется самостоятельно провести аппаратную перезагрузку компьютера и вручную открыть ПО QIWI Защита.
- 9. Продолжите настройку для получения возможности подписывать документы в электронном виде. Для этого создайте запрос на получение сертификата ключа ЭЦП и/или установите уже полученный от Удостоверяющего Центра сертификат в хранилище (см. далее).

# 9. СЕРТИФИКАТЫ ЭЛЕКТРОННО-ЦИФРОВОЙ ПОДПИСИ

При выборе данного пункта можно оформить заявку на получение сертификата ЭЦП или произвести установку ранее полученного от удостоверяющего центра сертификата ЭЦП на компьютер (<u>Рис. 18</u>):

 Для оформления заявки на сертификат ЭЦП в главном окне программы выберите действие Сертификаты электронно-цифровой подписи → Заявка на сертификат (подробнее смотрите главу <u>9.1</u>).

🚊 QIWI Защита	
	← <u>Главное меню</u>
	Сертификаты электронно-цифровой подписи
	Заявка на сертификат Создайте заявку, если Вам необходимо получить новый сертификат ЭЦП
	Установка сертификата Установите полученный от Удостоверяющего Центра сертификат ЭЦП

Рис. 18. Меню «Сертификаты электронно-цифровой подписи»

### 9.1. Создание заявки на сертификат ЭЦП

При выборе данного шага откроется мастер создания заявки на сертификат.

1. В первом окне мастера укажите, получает ли ваша организация сертификат впервые, выбрав пункт **Да** или **Нет** (<u>Рис. 19</u>).

### внимание

Если реквизиты (в т.ч. банковские) вашей организации после получения предыдущего сертификата изменились или вы получали сертификата на ДРУГОЕ юридическое лицо, выберите пункт **Да**.

Рис. 19. Выбор повторного или первого получения сертификата

🔒 Запрос на выпуск сертификата ЭЦП	
Ваша организация получает сертификат в УЦ Инфотекс в первый раз? Укажите нужную опцию для заявки QUWI	
Да	
После нажатия кнопки "Далее" Вам необходимо будет указать реквизиты Вашей организации	
🔘 Нет	
В сертификате будут указаны реквизиты Вашей организации, взятые из запроса, который отправлялся в Удостоверяющий Центр ранее	
🔾 Далее	)

- 2. Нажмите кнопку Далее.
- В окне Реквизиты организации укажите данные организации (<u>Рис. 20</u>). Пункты: Краткое наименование, КПП, Юридический адрес и Почтовый адрес - заполняются только в том случае, если организация получает сертификат впервые. Поле КПП не требуется заполнять индивидуальным предпринимателям.

Данные реквизиты также указаны в договоре ОСМП.

COBET

### Рис. 20. Реквизиты организации

🦷 Запрос на выпуск сертификата	а ЭЦП	_ X _ )
Реквизиты организации Реквизиты указаны в догово	ope c OCMN	
Организационно-правовая форма	Выберите форму 💌	
Краткое наименование		
Полное наименование		
ИНН		
кпп		
ОГРН/ОГРНИП		
Регион		
Город		
Юридический адрес		
Почтовый адрес		
	С Назад	Далее

- 4. Нажмите кнопку Далее.
- 5. Если вы получаете сертификат впервые, то в следующем окне мастера введите банковские реквизиты и нажмите кнопку **Далее** (<u>Рис. 21</u>). Если вы уже получали сертификат ранее, то ввод банковских реквизитов будет автоматически пропущен.

_		COBET	
_	Данные реквизиты также указаны в договоре ОСМП.		

### Рис. 21. Ввод банковских реквизитов

Наименование банка БИК СССССССССССССССССССССССССССССССССССС	Банковские рекви Реквизиты указа	<b>зиты</b> аны в договоре с ОСМП	
БИК к/с р/с	Наименование банка		
κ/c	БИК		
p/c	к/c		
	p/c		

6. Укажите данные будущего владельца сертификата (<u>Рис. 22</u>). Поле **Должность** заполнять не обязательно, если организация – индивидуальный предприниматель.

Рис. 22. Ввод данных будущего владельца сертификата

	 sauje
Фамилия	
Имя	
Отчество	
СНИЛС (если можете указать)	
Должность в организации	
Подразделение	
Телефон	
Факс	
E-mail	

### внимание

Будьте внимательнее при указании e-mail. В дальнейшем на указанную почту вам будет отправлен счет на оплату сертификата.

- 7. Нажмите кнопку Далее.
- Укажите тип документа, подтверждающего полномочия будущего владельца сертификата на подписание документов от лица организации (<u>Рис. 23</u>).

Рис. 23. Указание документа, подтверждающего полномочия на подписание документов от лица организации

💦 Запрос на выпуск сертификата ЭЦП	×
Данные будущего владельца сертификата Данные сотрудника организации, для которого запрашивается выпуск сертификата	QIWI
Тип документа, подтверждающего полномочия владельца сертификата на подписание документов	2
Устав	
🔘 Свидетельство	
🔘 Доверенность	
Реквизиты доверенности	
Укажите номер доверенности и дату выдачи. Например, № 123 от 01.01.2012	
С Назад	🕽 Далее

Если в качестве документа выбран тип **Доверенность**, то в поле **Реквизиты доверенности** введите номер и дату выдачи.

- 9. Нажмите кнопку Далее.
- 10. Укажите, является ли будущий владелец сертификата руководителем организации, и нажмите кнопку **Далее** (<u>Рис. 24</u>).

Рис. 24. Указание дол	тжности будущего	владельца	сертификата
-----------------------	------------------	-----------	-------------

🕺 Запрос на выпуск сертификата ЭЦП	X
Данные будущего владельца сертификата Данные сотрудника организации, для которого запрашивается выпуск сертификата	
Является ли будущий владелец сертификата руководителем организации?	
Руководитель	
🔘 Не руководитель	
• Назад	🛛 Далее

11. Если вы указали пункт **Руководитель**, то перейдите к следующему пункту. Если вы выбрали пункт **Не руководитель**, то в следующем окне введите данные руководителя организации и нажмите кнопку **Далее** (<u>Рис. 25</u>).

Рис. 25. Ввод информации о руководителе организации

Данные о руководите Данные руководите выпуск сертификата	еле организации пя организации, для сотрудника которой запрашивается	QIWI
Укажите сведения о руко	водителе организации	astayina
ФИО		
Должность в организации		
Документ, на основании которого действует		
	🔘 Устав	
	Овидетельство	
	🔘 Доверенность	
Реквизиты доверенности		
	-	
	🔾 Назад	🗘 Далее

12. Укажите папку, в которой будут сохранены созданные файлы **CertReq.p10** и **заявка.html**, которые по окончании работы мастера нужно будет отправить в удостоверяющий центр:

Рис. 26. Задание адреса для сохранения заявки на сертификат

Запрос на выпуск сертификата ЭЦП	×
Укажите папку для сохранения заявки на сертификат	Q
	QIWI
Далее Вам следует указать папку на компьютере, в которую будут помещены созданные файлы Вашей заявки на сертификат. Запомните указанную папку. После создания заявки вам необходимо будет отправить созданные файлы в удостоверяющий центр	
• Назад	🕄 Далее



Запомните указанную папку. После создания запроса вам необходимо будет отправить созданные файлы в Удостоверяющий Центр.

13. В следующем окне внимательно ознакомьтесь с информацией и нажмите кнопку Далее (Рис. 27).

Вставьте нос	тель для сохранения секретного кл	юча подписи
		QI
Вставъте съемн секретный клю Ва нужно выбр то в поле "Встав носителя нажми	ый носитель (рекомендуется eToken), на к подписи. Нажиите кнопку Далее - появи ать из списка устройств этот носитель (п ленный носитель' должно присутствоват ленный носитель' армкно присутствоват те ОК и следуйте появляющимся на экран	оторый будет записан Ваш тся окно "КриптоПро СSP", в которо дасказка: если используется eToker , опово ETOKEN). После указания не инструкциям

Рис. 27. Информация о работе с носителем информации

 В появившемся окне КриптоПро CSP из списка устройств выберите внешний носитель, на который будут записаны ключи ЭЦП (выберите устройство, у которого в поле Вставленный носитель будет присутствовать слово ETOKEN) (Рис. 28).

КриптоПро CSP	×
Вставьте чистый кли "{e4103e2b-0e71-42d	0:09:57 очевой носитель I6-862d-94bb45a1b4d3}''.
Сведения	
Устройства:	Вставленный носитель:
AKS VR 0	Состояние:
AKS if dh 1	
0	К Отмена Сведения <<

Рис. 28. Выбор внешнего носителя

- 15. Нажмите кнопку ОК.
- Откроется окно Биологический датчик случайных чисел (<u>Рис. 29</u>). Нажимайте на клавиатуре любые клавиши или перемещайте указатель мыши до тех пор, пока зеленый индикатор выполнения не дойдет до конца.

D	20				
Рис	29	Биологический	латчик слу	/чайных	чисел
i rici	~ .		dar mix ch		- IFICCS I

КриптоПр	o CSP	×
		0:09:57
<b>\$</b> <i>w</i>	Биологический датчик случай	ных чисел
Нажима мыши над	айте клавиши или перемещайте а этим окном до тех пор, пока кл создан	указатель юч не будет
	G	
	Отмена	

17. В новом окне укажите pin-код на контейнер (если в качестве контейнера paнee была выбрана смарт-карта eToken, то укажите пароль от этой смарт-карты), в который будут помещены созданные ключи ЭЦП, и нажмите кнопку **ОК**.

	внимание	
Ріп-код необходимо обязательно запомнить и записать, так как он пона	адобится в дальнейше	em.
Pin-код должен быть известен только владельцу сертификата.		

18. В окне Запрос на сертификат создан нажмите кнопку Завершить (Рис. 30).

Рис. 30. Завершение создания запроса на сертификат

Запрос на выпуск сертификата ЭЦП	×
Запрос на сертификат создан	Q
	QIWI
Поздравляем, Ваша заявка на получение сертификата электронной подписи успешно со	оздана.
Для получения сертификата Вам необходимо отправить созданные файл с запросом (CertReq.p10) и заявку (заявка.htm) на e-mail <u>SalesIIT@infotecs.ru</u> , в теме письма ука "Заявка КИВИ-агент". После выпуска сертификата Вы получите уведомление.	ажите
Не удаляйте с этого компьютера программу QIWI Защита и программы КриптоПро.	
	Завершить

### 9.2. Установка сертификата

После того как сертификат ЭЦП получен (подробнее о том, как получить сертификат, смотрите в <u>Приложении Ж</u>) установите его, выполнив следующие действия:

- 1. В главном окне ПО *QIWI Защита* выберите пункт **Сертификаты электронно-цифровой** подписи → Установка сертификата.
- 2. В окне мастера установки сертификата нажмите кнопку **Обзор** и выберите файл полученного сертификата (<u>Рис. 31</u>).

### Рис. 31. Выбор расположения сертификата

🕺 Установка сертификата ЭЦП	×
Установка сертификата ЭЦП Для получения сертификата свяжитесь с Удостоверяющим центром, в который Вы направляли заявку, или с Вашим менеджером ОСМП	
Пожалуйста, укажите расположение полученного Вами сертификата электронной подписи (файл с расширением .cer)	
[	🗘 Далее

- 3. Нажмите кнопку Далее.
- 4. В окне Завершения установки сертификата нажмите кнопку Завершить (<u>Рис. 32</u>).

### Рис. 32. Завершение установки сертификата

🕺 Установка сертификата ЭЦП	×
Поздравляем! Сертификат ЭЦП успешно установлен на этот компьютер	Q
	QIWI
Поздравляем, все необходимое для использования электронного документооборота н компьютере установлено. Теперь Вы можете подписывать документы Вашей электрон подписью на сайте agent.qiwi.com, при условии действительности Ваших полномочий н подписания.	а этом іной на момент
✓ 3	авершить

Установка сертификата завершена.

### 10. ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

Приложение реализует следующие дополнительные возможности:

- <u>Список сертификатов</u> открывает системное хранилище сертификатов;
- <u>Сетевые настройки</u> позволяет задать сетевые настройки для доступа к Интернету;
- <u>Загрузить драйверы</u> позволяет загрузить драйверы, необходимые для работы с eToken в различных OC;
- Загрузить документацию позволяет загрузить последнюю версию руководства пользователя;
- <u>О программе</u> открывает окно с информацией о приложении.

### 10.1.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. 33</u>).



#### Рис. 33. Системные сертификаты

Сертификаты			? 🛛
Назначение: <	>		<b>₩</b>
Личные Другие пользова	тели Промежуточны	е центры сертиф	рикации Доверенны
Кому выдан	Кем выдан	Срок де	Понятное имя
and the second s	and the second		
	Varaur		
- Назначения сертификата -	Удалить		Дополнительно
пазначения сертификата			
			Просмотр
			Закоыть
			Dakperre

# 10.2. 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. 34).

Рис. 34.	Установки	прокси
----------	-----------	--------

🧍 Сетевые настройки -	QIWI Защита 🛛 🔀		
Настройка параметров сети			
Прямое подключение к Интернету			
💿 Системная конфигурация			
🔘 Настроить прокси вручн	ую:		
Хост:			
Порт:	0		
С авторизацией			
Имя пользователя:			
Пароль:			
Проверить соединение	🔚 Сохранить 🗶 Отменить		

- 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 <i>Свойствах</i> о установлен флаг <b>Автоматическое определение парамет</b>	<i>обозревателя</i> должен быть г <b>ров.</b>
Проверить флаг можно, выполнив переход Пуск-Панель у обозревателя->Подключения->Настройка сети.	управления <del>.)</del> Свойства
Настроить прокси вручную – позволяет задать сле	едующие настройки прокси:

Информацию о прокси-сервере запросите у вашего системного администратора.

- ↔ Хост адрес прокси-сервера.
- Порт порт подключения к прокси-серверу.

A

ПРИМЕЧАНИЕ

- Авторизация 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. 35).

Рис. 35. Успешное соединение с сервером

🧍 Прове	рить соединение - QIWI Защита	×
Статус:	Соединение с сервером успешно установл	ено.
	Готово	

# 10.3.Загрузка драйверов

- 1. Для загрузки драйверов для работы с eToken выберите **Загрузить драйверы** в главном окне приложения (см. <u>Рис. 3</u>).
- 2. Появится список драйверов для различных операционных систем (Рис. 36).



- eToken драйвер для OC Microsoft Windows (32-бит)
   позволяет установить драйвер для работы с eToken в следующих 32-битных OC: Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008.
- eToken драйвер для OC Microsoft Windows (64-бит) позволяет установить драйвер для работы с eToken в следующих 64-битных OC: Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008.
- **еТокеп драйвер для Ubuntu (32-бит)** позволяет установить драйвер для работы с еТокеп в операционной системе *Ubuntu 9.04*.

### 10.4.Загрузка документации

Для получения руководства пользователя к текущей версии ПО:

- Выберите пункт Загрузить 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.

# 10.5.О программе

Просмотреть информацию о приложении можно, выбрав пункт **О программе** в главном окне приложения (см. <u>Рис. 3</u>).

Будет открыто окно с информацией о приложении (Рис. 37).

Рис. 37. О программе

🖁 О программе - QIWI Защита 🛛 🔀				
	Программа <b>QIWI Защита X.X</b> представляет собой удобный инструмент для управления сертификатами, позволяющими сделать работу в системе ОСМП более безопасной Copyright © OSMP, 2008-2010 web: <u>www.osmp.ru</u> email: <u>quard@osmp.ru</u> Данный продукт включает в себя программное обеспечение, разработанное OpenSSLProject для использования в OpenSSL Toolkit web: <u>www.openssl.org</u>			
	🗙 Закрыть			

### 11. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

### Ошибка 202 при записи сертификата

Проблема: при попытке записать сертификат возникает ошибка данных запроса 202

#### Решение:

- Убедитесь в том, что вы вводите существующий логин;
- Проверьте правильность написания логина или фамилии персоны (отсутствие недопустимых символов);
- Возможно настройки сети не позволяют сформировать запрос на получение сертификата. Попробуйте отправить запрос в другом интернет канале.

#### Ошибка «Неверный пароль» при получении сертификата

Проблема: при получении сертификата возникает ошибка, с неверным паролем.

Решение: проверять, чтобы персона обладала нужными правами + привязка к терминалу, номер которого вводится в киви-защите.

#### Ошибка 49 при записи сертификата

Проблема: при попытке записать сертификат для приложения QIWI Кассир возникает ошибка 49

Данная ошибка возникает в том случае, если на ключе eToken уже присутствует сертификат для данной персоны.

Решение: удалить предыдущий сертификат.

Если удаление ненужных сертификатов не помогает, то необходимо произвести форматирование etoken

#### Потерян pin-код eToken

Проблема: pin-код неверно введен 10 раз, eToken заблокирован.

Решение:

- 1. Зайдите в свойства eToken;
- 2. Выберите пункт меню Разблокировать eToken;
- 3. Укажите пароль администратора;
- 4. Произведите разблокировку.



В том случае, если вы не знаете пароля администратора, то проблему решит только форматирование eToken с уничтожением всех данных.

#### Pin-код отформатированного eToken

Вопрос: какой pin-код у eToken после форматирования?

Ответ: 123467890 (если при инициализации не задавался иной).

#### Не определяется eToken

Проблема: eToken подключен, но система его не видит.

#### Решение:

- Проверьте правильность установки eToken в слоте;
- Вставьте eToken в другой слот;
- Перезагрузите компьютер;
- Переустановите драйверы eToken.

Перед установкой драйверов, необходимо сохранить путь к ранее установленным драйверам, и при переустановке указать этот путь.



Драйвера eToken должны быть установлены на системном диске с операционной системой.

#### Где взять eToken

Вопрос: где я могу приобрести eToken, и какая модель мне нужна?

Ответ: вам нужна модель ключа eToken pro java. По вопросам приобретения обращайтесь к курирующему менеджеру.

#### Форматирование eToken

Вопрос: как отформатировать eToken?

Ответ: откройте свойства eToken и выберите пункт меню Инициализация -> Форматирование.

#### Вместимость eToken

Вопрос: сколько сертификатов можно сохранить на одном eToken.

Ответ: по умолчанию на eToken можно сохранить 5 сертификатов. Для того чтобы увеличить объем ключа, необходимо при инициализации (форматировании) на вкладке **Дополнительно** задать нужное количество сертификатов.

### ПРИЛОЖЕНИЕ А: Рекомендации по безопасности

Для предотвращения несанкционированного проведения платежей с другого оборудования необходимо осуществить «привязку» каждого Терминала к серийному номеру оборудования. Определить серийный номер конкретного типа Терминала можно следующим образом:

- *QIWI Кассир* в окне авторизации, нажав кнопку **Инфо** (либо в меню приложения, выбрав **QIWI→Помощь→О программе**).
- *QIWI POS Nurit* в меню POS терминала, выбрав **Сервис->Серийный номер**.
- *Автомат самообслуживания* в разделе **Монитор терминалов** личного кабинета агента. Серийный номер указан в поле **Инфо** после версии ПО.

Серийный номер необходимо указать в поле **Привязан к SN** в разделе **Редактирование терминала** (в личном кабинете агента).

Для снижения ущерба и локализации источника в случае кражи учётных данных Персоны (под *Персоной* понимается учетная запись для доступа к Системе), необходимо при проведении платежей использовать учётные записи с минимальным набором прав *Продавец*. Кроме того, следует произвести привязку Персон к Терминалам, с которых эти Персоны проводят платежи.

Для защиты от кражи компьютерными вирусами авторизационных данных персон необходимо использовать антивирусные средства защиты компьютеров, с которых ведётся работа с Системой. Рекомендуется также использовать криптоключи eToken Pro. Настоятельно не рекомендуется заходить в Систему с общедоступных компьютеров (например, с компьютеров в интернет-кафе).

На компьютерах, используемых для работы с Системой, рекомендуется ограничить доступ в сеть Интернет (кроме платежных серверов Системы). Также воздержаться от открытия подозрительных писем с вложениями. При получении такого письма от имени Оператора Системы рекомендуется переслать его в адрес <u>sb@osmp.ru</u>.

### ПРИЛОЖЕНИЕ Б: Подготовка eToken к работе

Перед началом использования eToken необходимо отформатировать, а также сменить пароль администратора, установленный по умолчанию.

Приложение содержит инструкции:

- 1. <u>Смена пароля в ПО QIWI Защита</u> процесс смены пароля на постоянный в случае, если вы уже начали, например, генерировать сертификат.
- 2. <u>Форматирование eToken</u> процесс форматирования и смены пароля с помощью драйвера eToken.
- 3. Смена пароля eToken смена пароля через драйвер.

### 1. Смена пароля в ПО QIWI Защита

Мастер создания сертификата/персоны выполняет проверку пароля eToken. Если на eToken установлен пароль, требующий смены при первом использовании, вам будет предложено сменить его на постоянный (Рис. <u>38</u>).

Рис. 38. Сообщение о необходимости смены пароля на eToken

🧎 Создание сер	тификата - QIWI Защита	
Пароль более н Введите и по	недействителен дтвердите новый пароль	
Пароль Подтверждение		
	Надежность пароля 0%	
		🔇 Назад 💿 Далее

В полях Пароль и Подтверждение укажите новый пароль и нажмите кнопку Далее.

ПРИМЕЧАНИЕ	î

В случае, если в интерфейсе ПО QIWI Защита сменить пароль к еТокеп не удалось, это можно сделать с помощью драйвера еТокеп (см. пункт 3 данного Приложения).

### 2. Форматирование eToken



примечание Пароль администратора позволяет разблокировать ключ, заблокированный вследствие превышения максимального числа попыток авторизации.

Для смены пароля администратора выполните следующее:

- 1. Перейдите Пуск → Все программы → eToken → eToken Properties.
- 2. В Свойствах eToken выберите вкладку Дополнительно (Рис. 39).

Рис. 39. Свойства eToken

Свойства eToken		
eToken		
CIORCII	YOUR KEY TO eSECUTTY	
Caŭt e Token	дополнительно основить с программе	помощь
	Переименовать eToken	
eToken		
	and the second sec	

3. Выберите eToken и нажмите кнопку Инициализация eToken (<u>Рис. 40</u>).

### Рис. 40. Выбор инициализации eToken

eloken	-			
eroken	YOUR KEY TO eSECURITY			
йт eToken		Назад	Обновить	Помощь
	Инициализация eToken 🖌 🗛 🖌 yen	Импорт сертифия	ката	*
	VES			^
Token PKI Client	Категория eToken			
<ul> <li>В стокеп'ы и считывателя.</li> </ul>	Иня считывателя			
- I=I eloken	Серийный номер			
Contraction of the second seco	Общий объем памяти на самрт-карте eToken			
ПОЛЬЗОВАТЕЛЬ	Свободная память на смарт-карте eToken			
TOO DO D	Версия оборудования			
Це Цертификаты				
<ul> <li>Ц Сертификаты</li> <li>П Orphan Objects</li> </ul>	Версия встроенного ПО			
<ul> <li>В. Сертификаты</li> <li>В. Оrphan Objects</li> <li>Насторйки</li> </ul>	Версия встроенного ПО			
Сертификаты     Оrphan Objects     Настройки	Версия встроенного ПО Идентификатор снарт-карты Изент пополита			

Будет открыто диалоговое окно Инициализация eToken (<u>Рис. 41</u>).

### Рис. 41. Параметры форматирования eToken

🖻 Инициализация eToken		
Параме	тры форматирования eToken	
Имя eToken:	eToken	
<ul> <li>Назначение пароля:</li> <li>Подтверждение:</li> </ul>	Максимальное число ошибок при авторизации: 15	
Задать пароль администратора: Подтверждение: Примечание: для разблокировани	Максимальное число ошибок при авторизации: 15	
Дополнительные параметры При первой авторизации необходимо изменить пароль Лополнительно		
Текущий я	азык: EN Запуск Закрыть	

- 4. Установите флаг Задать пароль администратора и задайте пароль.
- 5. Нажмите кнопку Запуск.

Будет выполнено форматирование eToken и пароль администратора будет изменен.

### 3. Смена пароля eToken

В случае если требуется только сменить пароль, а не форматировать eToken, выполните следующее:

- 1. Нажмите правой кнопкой мыши на иконке **PKI Client** 🔤 в системном лотке.
- 2. Выберите пункт Изменить пароль eToken:

Рис. 42. Смена пароля eToken

🛃 Открыть Свойства eTol	ken
📡 Изменить пароль eToke	n Jun
📄 Устройства eToken	$\bigcirc$
🚺 О Программе	
🔁 Скрыть	

- 3. Введите данные:
  - Текущий пароль для eToken введите действующий пароль;
  - Новый пароль и Подтверждение введите новый пароль.

Рис. 43. Смена пароля

🖻 Изменить пароль: eToken - guard1	×	
Изменить пароль eToker	r	
Текущий пароль для eToken:		
Новый пароль для eToken:	0%	
Стойкий пароль должен быть не короче 8 знаков и содержать сими нижнем и верхнем регистрах, цифры и знаки препинания.	волы в	
Текущий язык: RU		
OK	Отмена	
Введите значение в поле Текущий пароль.		

# ПРИЛОЖЕНИЕ В: Авторизация на сайте

Для авторизации на агентском сайте ОСМП выполните следующее:

Перейдите по ссылке на необходимый сайт <u>agent.qiwi.com</u>, <u>portal.qiwi.com</u> или <u>prov.osmp.ru</u>.
 Будет открыто диалоговое окно **Выбор сертификата** (<u>Рис. 44</u>).

Рис. 44. Выбор сертификата при входе на сайт

Выбор ц Иденти	ифрового сертифи фикация	ката	?
⚠	Веб-узел, который вы проверку подлинности	хотите просмотреть, запро и. Выберите сертификат.	сил
	Имя	Поставщик	~
	Persona	OSMP Client CA	
	<		~
	Подробнее	Просмотр сертифика	та
		ок о	тмена

2. Выберите нужный сертификат.

	П	РИМЕЧА	НИЕ	U
Сертификаты различаются по имени владельца, которое было з агентском сайте (в полях <b>Фамилия, Имя и Отчество</b> ).	задано при	создании	персоны	на

- 3. Введите пароль для хранилища сертификата:
  - eToken (<u>Рис. 45</u>)

### Рис. 45. Ввод пароля eToken

🖻 Авторизация: eToken		×
	Авторизация eToken	eToken
Введите паро	ль eToken	
Имя eToken:	eToken	
Пароль:		
	Текущий язык: Е	
	OK	Отмена

Системное хранилище (<u>Рис. 46</u>)

								ПРИ	МЕЧАНИ	1E	Ü
Пароль	будет	запрошен,	если	при	создании	сертификата	ВЫ	выбрали	высокий	урове	ЭНЬ
безопас	ности сі	истемного хр	анили	ща.							

### Рис. 46. Ввод пароля для закрытого ключа в системном хранилище

Для подпись	івания используется ваш закрытый клю 🗙
	Приложение запрашивает доступ к защищенному элементу. Закрытый ключ CryptoA
	ОК Отмена Сведения

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



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

# ПРИЛОЖЕНИЕ Г: Сохранение в системное хранилище



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

Для сохранения в системное хранилище вам необходимо выполнить следующие шаги:

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

#### 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 персоны для QIWI Кассира:
  - Выберите пункт Создание/удаление персоны для QIWI Кассир.
  - Выберите **Создание**.
  - Выберите тип хранилища Системное.

#### Рис. 47. Ввод информации о персоне

🧍 Создание/удаление персоны - QIWI Защита 🛛 🛛 🔀				
Ввод информации о персоне Введите информацию о персоне, которая должна быть записана в хранилище				
Псевдоним:	QIWI Кассир			
Логин:	Person			
ID терминала:	5555555			
Пароль:	1234567			
	Показать пароль			
Выберите тип доступа:	<ul> <li>Для текущего пользователя</li> </ul>			
	Для всех пользователей			
	🔾 Назад 🖸 Далее			

- Введите данные персоны (<u>Рис. 47</u>):
  - **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 флаг позволяет отображать значение поля Пароль.



На данном шаге указываются данные персоны и терминала, ранее зарегистрированных на сайте https://agent.osmp.ru.

- 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. 48).
- Рис. 48. Создание нового ключа подписи RSA

Создание нового ключа подписи RSA			
	Приложение создает защищенный элемент.		
	Закрытый ключ CryptoA		
al	Установлен средний уровень безопасности		
	Уро <u>в</u> ень безопасности	]	
	ОК Отмена <u>С</u> остав	]	

2. Выберите уровень защиты и нажмите кнопку Далее (Рис. 49):

Рис. 49. Выбор уровня защиты

Создание нового клю	ча подписи RSA 🛛 🔀
	Выберите уровень защиты, соответствующий этому элементу. Высокий Запрашивать мое разрешение с паролем при использовании элемента. Средний Запрашивать мое разрешение при использовании элемента.
	< <u>Н</u> азад Далее > Отмена



Для повышения уровня защиты установите Высокий уровень.

- Высокий уровень – задайте пароль для сертификата и нажмите кнопку Готово (Рис. 50):

Рис. 50. Установка пароля сертификата

Создание нового ключа подписи RSA		
<u>a</u> Q,	Задайте пароль для защиты этого элемента.	
	Создайте новый пароль для этого элемента. Пароль для: Закрытый ключ CryptoA	
	Пароль:	
	Подтверждение:	
< Назад <u>Г</u> отово Отмена		

примечание

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

 Средний уровень – прочитайте информацию о процессе авторизации и нажмите кнопку Готово (Рис. 51):

Рис. 51. Информация об авторизации при среднем уровне безопасности системного хранилища

Создание нового ключа подписи RSA		
	Был установлен средний уровень безопасности. При попытке обратиться к этому объекту на экран будет выведено диалоговое окно, запрашивающее ваше разрешение.	
< Назад <u>Г</u> отово Отмена		

Вы будете возвращены к первому шагу *Мастера создания нового ключа подписи RSA* (см. <u>Рис. 48</u>).

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/данных персоны и нажмите кнопку **Завершить** (см. <u>Рис. 8</u>).

## ПРИЛОЖЕНИЕ Д: 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 <u>6</u>.
- 2. Выберите тип хранилища Файл.

Вы перейдете к следующему шагу (Рис. 52).

Рис. 52. Выбор файла для записи сертификата

	ования фаила	-
Выберите файл для з	аписи сертификата:	
D:/cert.p12		(
Введите пароль:	•••••	
Подтвердите пароль	••••••	
	Filizen det de la Stores 7586	

3. Выберите файл для записи сертификата.



По умолчанию сертификат предлагается сохранить на рабочий стол под именем cert.p12. Изменяемая часть имени сертификата – cert (.p12 расширение файла). Если вы решили изменить имя файла, убедитесь что расширение осталось без изменения.

4. Задайте пароль. Данный пароль необходимо будет ввести при импорте сертификата в системное хранилище.



внимание

Для сохранения сертификата в файл уровень надежности должен быть не менее 75%.

5. Нажмите кнопку Далее.

Вы будете возвращены в Мастер создания сертификатов.

6. Дождитесь, пока *Мастер создания сертификатов* отобразит информацию об окончании записи сертификата, и нажмите кнопку **Завершить** (см. <u>Рис. 8</u>).

Сертификат будет сохранен в файле.

### 2. Экспорт сертификата

Для экспорта файла сертификата в системное хранилище выполните следующее:

1. Щелкните дважды левой кнопкой мыши по файлу сертификата.

Будет запущен Мастер импорта сертификатов (Рис. 53).

Рис. 53. Мастер импорта сертификатов

Мастер импорта сертификатов	×
Втот настер поногает копировать сертификаты, списки доверия и списки отзыва сертификатов с локального диска в хранилище сертификатов. Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установления защищенных сетевых подключений. Хранилище сертификатов - это область системы, предназначенная для хранения сертификатов. Для продолжения нажните кнопку "Далее".	
< Назад Далее > Отмена	

- 2. Для перехода к первому шагу нажмите кнопку Далее.
- 3. Подтвердите или укажите расположение файла сертификата.
- 4. Нажмите кнопку Далее (Рис. 54).



### Рис. 54. Импортируемый файл

портируемый файл Укажите импортируемый файл.	
Иня файла:	
D:\cert.p12	O630p
Стандарт Cryptographic Message Хранилище сериализованных се	e Syntax - сертификаты PKCS #7 (.p7b) ертификатов (.sst)

5. Установите флаг Включить усиленную защиту ключа (<u>Рис. 55</u>).



### Рис. 55. Ввод пароля для файла сертификата

Мастер импорта сертификатов 🛛 🔀
Пароль Для обеспечения безопасности закрытый ключ защищен паролем.
Введите пароль для закрытого ключа.
Пароль:
**************
<ul> <li>Включить усиленную защиту закрытого ключа. В этом случае при каждом использовании приложением закрытого ключа будет выдаваться запрос.</li> <li>Пометить этот ключ как экспортируемый, что позволит вам сохранять архивную копию ключа и перемещать его.</li> </ul>
< Назад Далее > Отмена

- 6. Введите пароль для доступа к файлу и нажмите кнопку Далее.
- 7. Выберите **Автоматически выбрать хранилище на основе типа сертификата** и нажмите кнопку **Далее** (<u>Рис. 56</u>).

Рис. 56. Выбор размещения сертификата

нилище серти	фикатов
хранение серти	фикатов.
Выбор хранили. можно указать	ца может быть произведен Windows автоматически, или же размещение сертификата вручную.
• Автонати	чески выбрать хранилище на основе типа сертификата
ОПонестит	ь все сертификаты в следующее хранилище
Хранилии	це сертификатов:
	Обзор

Будет выполнен импорт сертификата, и *Мастер импорта сертификатов* отобразит параметры импорта (<u>Рис. 57</u>).

Рис. 57. Параметры импорта сертификата

Мастер импорта сертифика	атов	X
	Завершение работы мас импорта сертификатов Работа мастера импорта сертификатов завершена. Были указаны следующие параметры:	с <b>тера</b> услешно
	Выбранное хранилище сертификатов Содержание Имя файла	ABTOMATINHECK PFX D:\vic.p12
	< Назад Готово	Отнена

8. Нажмите кнопку Готово.

Импорт сертификата в системное хранилище будет завершен и вам будет предложено задать уровень безопасности сертификата (<u>Рис. 58</u>).

Рис. 58. Создание защищенного элемента

Импорт нового закрытого ключа обмена 🛛 🔀				
	Приложение создает защищенный элемент. Закрытый ключ CryptoA			
Ŷ	Установлен федний уровень безопасности Уровень безопасности ОК Отмена Состав			

9. Нажмите кнопку Уровень безопасности.

Будет открыто диалоговое окно с выбором уровня защиты (Рис. 59).

### Рис. 59. Выбор уровня безопасности



10. Выберите уровень безопасности и нажмите кнопку Далее>.

	В целях повышения уровня защиты установите Высокий уровень.	COBET	
_	Высокий уровень – задайте пароль для сертификата и нажмите кнопн	ху <b>Готово</b> ( <u>F</u>	<u>ис. 60</u> ).
	ПРИ	МЕЧАНИЕ	<b>0</b>

Данный пароль необходимо будет вводить при авторизации на сайте ОСМП. Подробнее об авторизации на сайте см. в <u>Приложении В</u>.

Рис. 60. Установка пароля сертификата

Создание нового кли	ча подписи RSA	×
	Задайте пароль для защиты этого элемента.	
	Создайте новый пароль для этого элемента. Пароль для: Закрытый ключ CryptoA	
	Пароль:	
	Подтверждение:	
		_
	< Назад Готово Отмена	

 Средний уровень – прочитайте информацию о процессе авторизации и нажмите кнопку Готово (<u>Рис. 61</u>).

Рис. 61. Информация об авторизации при среднем уровне безопасности системного хранилища

Создание нового ключа подписи RSA		
	Был установлен средний уровень безопасности. При попытке обратиться к этому объекту на экран будет выведено диалоговое окно, запрашивающее ваше разрешение.	
К Назад Готово Отмена		

Вы будете возвращены к первому шагу Мастера создания нового ключа подписи RSA (см. Рис. 58).

11. Нажмите кнопку ОК.

Будет открыто диалоговое окно, информирующее об успешном импорте сертификата (Рис. 62).

### Рис. 62. Успешный импорт сертификата

Мастер	импорта сертификатов	×
(į)	Импорт успешно выполнен.	
	ОК	

12. Нажмите кнопку ОК.

Настройки сертификата будут заданы.

## ПРИЛОЖЕНИЕ Е: Синхронизация времени

### Windows XP

Для синхронизации локального времени выполните следующее:

- 1. Выберите Пуск->Панель управления->Дата и время.
- 2. Выберите вкладку Время Интернета.
- 3. Нажмите кнопку Обновить сейчас.

При успешной синхронизации вы увидите сообщение «Время было успешно синхронизировано».

### Windows Vista и Windows 7

Для синхронизации локального времени выполните следующее:

- 1. Выберите Пуск->Панель управления->Дата и время.
- 2. Перейдите на вкладку Время Интернета.
- 3. Нажмите кнопку Изменить параметры.
- 4. Нажмите кнопку Обновить сейчас.

При успешной синхронизации вы увидите сообщение «Время было успешно синхронизировано».

### ПРИЛОЖЕНИЕ Ж: Получение сертификата ЭЦП

Для получения сертификата в удостоверяющем центре (далее УЦ) выполните следующее:

- Отправьте созданные в приложении файл (CertReq.p10) и заявку (заявка.htm) на e-mail SalesIIT@infotecs.ru. В теме письма укажите «Заявка КИВИ-агент». Используйте электронную почту, указанную вами ранее при создании запроса на сертификат.
- 2. Получите в ответном письме счет на оплату и оплатите его.
- Получите по электронной почте уведомление о готовности сертификата (процедура изготовления может занять до 10-ти дней с момента оплаты счета) и заберите его лично в ближайшем офисе, указанном сотрудником УЦ в письме.



При получении сертификата в УЦ (центральном офисе или региональном представительстве) при себе необходимо иметь:

- распечатанное заполненное заявление на сертификат ключа подписи (файл с заявлением вы получите от сотрудника УЦ в письме с подтверждением готовности сертификата);
- ксерокопию паспорта будущего владельца сертификата (копии всех страниц, где есть записи, заверенные подписью руководителя и печатью организации);

В случае если сертификат ключа подписи получает не владелец сертификата, а его уполномоченный представитель, ему дополнительно при себе требуется иметь:

- нотариально заверенную доверенность на получение сертификата ключа подписи, выданную ему будущим владельцем сертификата;
- копию своего паспорта.

Специалисты УЦ могут записать сертификат как на электронный носитель, предоставленный агентом, так и выдать его на своем электронном носителе.

# СПИСОК РИСУНКОВ

Рис. 1. Мастер установки	8
Рис. 2. Финальный шаг установки	9
Рис. 3. Главное окно приложения	10
Рис. 4. Мастер создания сертификатов	14
Рис. 5. Ввод авторизационных данных	15
Рис. 6. Выбор хранилища сертификата	16
Рис. 7. Выбор устройства хранения информации	16
Рис. 8. Запись сертификата	17
Рис. 9. Мастер управления персонами	18
Рис. 10. Выбор устройства хранения информации о персонах	19
Рис. 11. Выбор устройства хранения информации	20
Рис. 12. Ввод информации о персоне	21
Рис. 13. Успешная запись данных	22
Рис. 14. Подтверждение установки ПО	23
Рис. 15. Лицензионное соглашение	24
Рис. 16. Регистрация ключа продукта КриптоПро CSP	24
Рис. 17. Регистрация ключа продукта КриптоПро OCSP Client и Криптопро TSP Client	25
Рис. 18. Меню «Сертификаты электронно-цифровой подписи»	26
Рис. 19. Выбор повторного или первого получения сертификата	27
Рис. 20. Реквизиты организации	
Рис. 21. Ввол банковских реквизитов	
Рис. 22. Ввол ланных булушего влалелы а сертификата	
Рис. 23. Указание документа, полтверждающего полномочие на полписание документов от лица	<u>ر ــــــــــــــــــــــــــــــــــــ</u>
Организации	
Рис. 24. Указание должности будущего владельна сертификата	
Рис 25. Ввол информации о руковолителе организации	31
Рис 26. Залание адреса для сохранения заявки на сертификат	32
Рис 27 Информация о работе с носителем информации	33
Рис 28 Выбор внешнего носителя	33
Рис 29 Биологический датчик случайных чисел	34
Рис. 30. Завершение создания запроса на сертификат	34
Рис. 31. Выбор расположения сертификат	35
Рис. 32. Завершение установки сертификата	36
Рис. 33. Системные сертификаты	30
Рис. 34. Установки прокси	38
Рис. 35. Успешное соелинение с сервером	30
Рис. 36. Загрузка драйверов	39
Рис. 37. О программе	40
Рис. 38. Сообщение о необхолимости смены пароля на еТокер	44
Рис. 39. Свойства еТокеп	45
	46
Puc 41. Параметры форматирования еТокеп	46
	40 47
	ד/ 47
	ידי 20
	סד ∩⊿
гис. то, вод парода для законтого клина в системием уранизиисе.	۲ <del>۲</del> ۱۸
гис. то, воод нароля для закрытого ключа в системном хранилище Рис. 47. Врод информации о порсоно	79
	E1
	51

Рис.	49.	Выбор уровня защиты	52
Рис.	50.	Установка пароля сертификата	53
Рис.	51.	Информация об авторизации при среднем уровне безопасности системного хранилища	53
Рис.	52.	Выбор файла для записи сертификата	55
Рис.	53.	Мастер импорта сертификатов	56
Рис.	54.	Импортируемый файл	57
Рис.	55.	Ввод пароля для файла сертификата	58
Рис.	56.	Выбор размещения сертификата	58
Рис.	57.	Параметры импорта сертификата	59
Рис.	58.	Создание защищенного элемента	59
Рис.	59.	Выбор уровня безопасности	60
Рис.	60.	Установка пароля сертификата	61
Рис.	61.	Информация об авторизации при среднем уровне безопасности системного хранилища	61
Рис.	62.	Успешный импорт сертификата	62