ООО «ЦЗИ «ГРИФ»

**Программное обеспечение**

 **«Крипторегистратор»**

руководство пользователя

г. Рыбинск,

2024 г.

Оглавление

[1. Введение 3](#_Toc156494949)

[1.1. Перечень сокращений 3](#_Toc156494950)

[1.2. О программе 3](#_Toc156494951)

[2. Установка и настройка системы 4](#_Toc156494952)

[2.1. Технические требования 4](#_Toc156494953)

[2.2. Программные требования 4](#_Toc156494954)

[2.3. Процедура установки системы 4](#_Toc156494955)-5

[3. Работа с системой 6](#_Toc156494956)

[3.1. Автоматическая установка сертификата 6](#_Toc156494957)

[3.2. Работа с установленными сертификатами 6](#_Toc156494958)-7

[4. Решение проблем 8](#_Toc156494959)

[5. Удаление 9](#_Toc156494960)

# Введение

## Перечень сокращений:

* uPKCM – User Public Key Certificate Manager;
* CRL – список отозванных сертификатов;
* CSP – Cryptography Service Provider;
* ЭЦП – Электронная цифровая подпись;
* ЛВС – локальная вычислительная сеть;
* GUI – Graphical User Interface – графический интерфейс пользователя;
* ОС – операционная система;
* ПО – программное обеспечение.

## О программе

Система управления пользовательскими сертификатами открытого ключа – User Public Key Certificate Manager (uPKCM - крипторегистратор). Данная система предназначена для автоматического определения подключенного носителя с сертификатом пользователя и подготовки сертификата к работе (подписание, шифрование). Так же система выполняет функцию сопроводителя установленных сертификатов, осуществляя закачку и установку списков отзыва по определенному расписанию.

Данная система предназначена для использования совместно с любыми системами, использующими ЭЦП в качестве сервис-менеджера личных сертификатов пользователей.

Система предназначена для автоматического управления пользовательскими сертификатами. Задача системы – автоматизация процесса подготовки пользовательского сертификата к использованию и сопровождение пользовательских сертификатов путем обновления CRL. Так же система должна обеспечить удаление сертификата из системы после истечения срока его действия.

Система состоит из модуля обслуживания сертификатов и модуля взаимодействия с пользователем (GUI).

Требования к численности и квалификации персонала системы

Пользователи системы должны иметь опыт работы с персональным компьютером на базе операционных систем Microsoft Windows на уровне квалифицированного пользователя и свободно осуществлять базовые операции в стандартных Windows.

Рекомендуемая численность персонала для эксплуатации системы: - Администратор – 1 штатная единица; - Пользователь – число штатных единиц определяется структурой организации, в которой используется система.

# Установка и настройка системы

## Технические требования

Минимальные требования к техническим характеристикам ПК пользователя:

* + Процессор – не менее 2 ГГц;
	+ Количество ядер – не менее 2;
	+ Объем оперативной памяти – 2 Гб;
	+ Дисковая подсистема – 120 Гб;
	+ Один свободный порт USB;
	+ Подключение к сети Интернет (не менее 10 Кбит/с).

## Программные требования

Система работает в ОС Microsoft Windows 7/8/10/11

Для работы системе требуется установленный крипто провайдер Crypto Pro CSP версии 4.0, 5.0 (<http://crypto-pro.ru/>) и Microsoft .Net Framework версии 4.8.

## Процедура установки системы

Система поставляется в виде дистрибутива. Установка запускается файлом. Система может поставляться на флэш-накопителе, или же доступна для скачивания с какого либо сетевого ресурса (интернет сайт, общая папка в ЛВС).

Для установки необходимо запустить файл setup.exe на выполнение. Вы увидите мастера по установке. В окне мастера нажимайте «Установить» (Рисунок 2‑1).



Рисунок 2‑1

После завершения процесса установки и закрытия мастера установки будет запущено GUI приложение. Иконка приложения отображается в системном лотке панели задач рядом с часами.

Внимание! Если вы не видите иконку, возможно, она скрыта под спойлером (он имеет вид стрелочки).

После процесса установки система сконфигурирована таким образом, что сервис обслуживания представляет собой обычное exe приложение.

Управление системой производится с помощью основного меню (Рисунок 2‑2).



Рисунок 2‑2

Вызов меню осуществляется нажатием правой кнопки мыши на иконке программы в системном лотке.

# Работа с системой

Система работает в автоматическом режиме при установке ключевых контейнеров. Но пользователю все равно требуется взаимодействие с системой, например, для настройки установленных сертификатов. Для этого нужно использовать основное меню системы, которое появляется при щелчке правой кнопкой мыши по иконке приложения в системном лотке.

## Автоматическая установка сертификата

После установки и настройки система готова к работе. Для активации системы достаточно установить носитель информации, содержащий контейнеры ключей. После обнаружения такого носителя (необходимо, чтобы в ОС был установлен драйвер носителя) система автоматически установит сертификаты, содержащиеся на этом носителе, скачает корневые сертификаты и списки отзыва для всех установленных сертификатов (если данные опции включены в системе) и свяжет сертификат с контейнером закрытого ключа.

Внимание! Если вы используете электронные идентификаторы Rutoken, EToken или смарт-карты, то Вам необходимо установить драйверы этих устройств, доступных на сайте производителя.

При обнаружении устройства, содержащего контейнер ОС, система немедленно начнет установку сертификатов, о чем свидетельствует активность в системном лотке в виде сообщений. Система не установит сертификат, срок действия которого уже истек или еще не наступил. При этом будет выдано соответствующее сообщение.

Поиск доступных ключевых контейнеров и установку сертификатов можно инициировать при помощи пункта основного меню системы «Найти новые сертификаты».

## Работа с установленными сертификатами

Для работы с сертификатами пользователя необходимо выбрать пункт основного меню системы «Сертификаты пользователя». После щелчка по этому пункту откроется окно «Список личных сертификатов» (Рисунок 3‑1), в котором доступна информация об уже установленных личных сертификатах.



Рисунок 3‑1

Внимание! Отображаются только сертификаты учетной записи, выполнившей вход в систему (от имени которой открыто GUI-приложение).

В данном окне доступно меню (Рисунок 3‑2), вызываемое правой кнопкой мыши, состоящее из следующих пунктов:

* Показать
* Удалить
* Обновить



Рисунок 3‑2

«Показать» - при выборе данного пункта выводится стандартное окно ОС с данными сертификата, на котором установлен курсор.

«Удалить» - при выборе данного пункта для сертификата, на котором установлен курсор, сертификат будет удален из реестра текущего пользователя.

Пункт меню «Обновить» обновляет список сертификатов в таблице.

# Решение проблем

Во время работы с системой у пользователя могут возникать различные проблемы. В данном разделе даются указания по решению некоторых из них. Для примера приведены ниже предложения системы по решению проблем.

|  |  |  |
| --- | --- | --- |
| **Проблема** | **Причина** | **Решение** |
| При установке контейнера ничего не происходит. | Не установлены драйвера ключевого контейнера | Установите драйвера ключевого контейнера |

# Удаление

Для удаления системы запустите деинсталляцию системы «Крипторегистратор» через элемент «Установка и удаление программ» панели управления Windows.