ООО Фирма «ИнфоКрипт»

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «Токен++»

МОДУЛЬ АДМИНИСТРИРОВАНИЯ

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

11485466.72.21.12.097-02 91 01

2022

Содержание

1 Введение

Модуль администрирования tpp_admin предназначен для выполнения сервисных операций с устройствами «Токен++» с установленным программным обеспечением из состава СКЗИ «Токен++» и устройствами «Токен++ Lite».

Программно-аппаратный комплекс (ПАК) «Токен++» предназначен для создания и защищенного хранения ключевой информации, защиты информационного обмена с прикладным ПО, выработки ключей обмена VKO и реализации функций электронной подписи.

2 Режимы работы и состояния устройства

Устройство «Токен++» может работать в двух режимах: технологическом режиме и режиме приложения.

В технологическом режиме доступны только сервисные команды. Штатным режимом работы является режим приложения. Если устройство находится в технологическом режиме, для работы по прямому назначению его следует переключить в режим приложения (см. раздел 4.2).

Определить, в каком режиме находится устройство, можно либо по световой индикации (см. раздел 5), либо при помощи команды "i" (см. раздел 4.1), либо по имени устройства в операционной системе (режим приложения – «Token++», технологический режим – «Token++ LOADER»).

В режиме приложения устройство может находиться в одном из четырёх состояний:

- Не готово к работе,
- Готово к работе, пароль по умолчанию,
- Готово к работе, пароль сменён,
- Внутреннее ПО повреждено.

Устройство «Токен++» попадает к пользователю в состоянии «Не готово к работе». При подключении к компьютеру информация о состоянии устройства сообщается пользователю с помощью световой индикации (см. раздел 5). В состоянии «Не готово к работе» устройство «Токен++» не может функционировать как ключевой носитель и не доступно криптопровайдеру «КриптоПро CSP».

После того как подготовка к работе выполнена (см. раздел 4.5), а также в случае принудительной установки пароля по умолчанию (см. раздел 4.6), устройство переходит в состояние «Готово к работе, пароль по умолчанию». В этом состоянии функциональность устройства «Токен++» ограничена: его невозможно использовать для выполнения криптографических операций и записи информации. На устройстве установлен пароль по умолчанию, который может использоваться только для смены пароля доступа к устройству с помощью «КриптоПро CSP» (для «Токен++ Lite» см. раздел 4.9).

После смены пароля с помощью «КриптоПро CSP» устройство переходит в состояние «Готово к работе, пароль сменён». В этом состоянии устройство «Токен++» доступно криптопровайдеру «КриптоПро CSP» для полноценной работы, в том числе для выполнения криптографических операций и записи информации.

Состояние «Внутреннее ПО повреждено» является временным – примерно через минуту или при следующем подключении устройство перейдет в технологический режим. О нахождении устройства в состоянии «Внутреннее ПО повреждено» сообщается с помощью соответствующей световой индикации (см. раздел 5). Устройство в этом состоянии отсутствует в списке устройств в операционной системе.

3 Получение справки

В случае запуска модуля администрирования tpp_admin без параметров, без устройства или с ошибочными параметрами на экран выдается краткая информация о командах, доступных в зависимости от режима работы устройства.

```
tpp_admin 1.0.0 (c) ИнфоКрипт, 2017

tpp_admin.exe <action> [<old_pswd new_pswd>] [option value]

action
Технологический режим (только Токен++)
        -c - Проверить целостность внутреннего ПО.
        -f - Инициализировать защищенное хранилище. ВСЕ ПОЛЬЗОВАТЕЛЬСКИЕ ДАННЫЕ БУДУТ ПОТЕРЯНЫ.
        -r - Переключить устройство в режим приложения.
        -i - Показать сведения об устройстве.
Режим приложения
        -a - Переключить устройство в технологический режим (только Токен++).
        -p - Выполнить подготовку устройства к работе.
        -d - Установить пароль по умолчанию. ВСЕ ПОЛЬЗОВАТЕЛЬСКИЕ ДАННЫЕ БУДУТ ПОТЕРЯНЫ.
        -s - Установить новое значение инициализирующей последовательности ДСЧ (только Токен++).
        -i - Показать сведения об устройстве.
        -w - Изменить пароль (только Токен++ lite). Старый и новый пароли должны быть указаны.

old_pswd  - Старый (текущий) пароль (для команды 'w').
new_pswd  - Новый пароль (для команды 'w').

option
        -k - Позволяет указать разновидность датчика случайных чисел для команд 'p' и 's'.
value
       rng_cp - Использовать датчик случайных чисел криптопровайдера КриптоПро CSP (для опции 'k').
```

4 Команды

4.1 Команда получения сведений об устройстве

Для получения сведений об устройстве используется команда "i" (**tpp_admin -i**). В зависимости от состояния устройства выводимые сведения могут отличаться. Единственное поле, которое присутствует всегда, – это «Результат самотестирования».

Устройство в режиме приложения, состояние «Не готово к работе»

```
tpp_admin 1.0.0 (c) ИнфоКрипт, 2017

Устройство «Токен++», режим приложения

Информация об устройстве

  Результат самотестирования: Обнаружены ошибки (0x4):
                               - Файловая система повреждена или не создана.

     Конфигурация устройства: ICr_T32S0000L_C1_VT1FK1

               Серийный номер: TST000000160

     Контрольное значение ПО: E922176968E4351D8F14963C10D2F121FAAC63373E2984D524813E5832ACBB39

                   Версия ПО: 1.0.6 RC 5689M
```

Если в результате самотестирования ошибок не обнаружено (Результат самотестирования: OK), и устройство работает в режиме приложения, то оно готово к работе по прямому назначению.

Если в результате самотестирования обнаружены ошибки, следует поступить в соответствии с рекомендациями, изложенными в разделе 6.

Устройство после выполнения команды инициализации

```
tpp_admin 1.0.0 (c) ИнфоКрипт, 2017

Устройство «Токен++», режим приложения

Информация об устройстве

  Результат самотестирования: OK

     Конфигурация устройства: ICr_T32S0000L_C1_VT1FK1

               Серийный номер: TST000000160

     Контрольное значение ПО: E922176968E4351D8F14963C10D2F121FAAC63373E2984D524813E5832ACBB39

                   Версия ПО: 1.0.6 RC 5689M
```

4.2 Команда переключения в режим приложения

Для переключения в режим приложения используется команда "r" (**tpp_admin -r**).

```
tpp_admin 1.0.0 (c) ИнфоКрипт, 2017

Устройство «Токен++», технологический режим

Переключение в режим приложения выполнено.
```

4.3 Команда проверки целостности внутреннего ПО

Проверка целостности внутреннего ПО в режиме приложения выполняется автоматически во время самотестирования. Если целостность внутреннего ПО нарушена, устройство не может использоваться по своему прямому назначению. При этом устройство «Токен++» не переключается в режим приложения и на нем горит красный светодиод.

Для проверки целостности внутреннего ПО в технологическом режиме используется команда "c" (**tpp_admin -c**).

```
tpp_admin 1.0.0 (c) ИнфоКрипт, 2017

Устройство «Токен++», технологический режим

Контрольная сумма внутреннего ПО верна.
```

4.4 Команда инициализации защищенного хранилища

Для инициализации защищенного хранилища используется команда "f" (**tpp_admin -f**). Команда доступна только в технологическом режиме. Инициализация защищенного хранилища приводит к гарантированному удалению всех пользовательских данных с устройства.

После ввода этой команды появляется предупреждение о том, что все пользовательские данные будут безвозвратно утеряны.

```
tpp_admin 1.0.0 (c) ИнфоКрипт, 2017

Устройство Токен++, технологический режим

ВНИМАНИЕ

Вы собираетесь инициализировать защищенное хранилище. При этом ВСЕ ПОЛЬЗОВАТЕЛЬСКИЕ ДАННЫЕ БУДУТ
ПОТЕРЯНЫ

Для подтверждения этой операции необходимо нажать клавишу "y" (или "Y")...

Переключение в режим приложения выполнено.
```

Для подтверждения инициализации защищенного хранилища необходимо ввести букву «y» (или «Y») и нажать клавишу Enter. Для отказа от инициализации защищенного хранилища следует ввести любой другой символ и нажать клавишу Enter. После ввода буквы «y» (или «Y»), защищенное хранилище будет инициализировано.

```
tpp_admin 1.0.0 (c) ИнфоКрипт, 2017

Устройство «Токен++», технологический режим

Защищенное хранилище инициализировано.
```

После выполнения данной команды необходимо выполнить команду подготовки устройства к работе (см. раздел 4.5) для перевода устройства в режим приложения.

4.5 Команда подготовки устройства к работе

Команда подготовки к работе доступна только в режиме приложения. Она необходима, когда устройство «Токен++» находится в состоянии «Не готово к работе» (попеременное мигание зеленого и красного светодиодов).

Команда может быть задана в двух формах: **tpp_admin -p** (случайные данные берутся с биологического датчика случайных чисел (биоДСЧ), встроенного в «Модуль администрирования») и **tpp_admin -p -k rng_cp** (случайные данные берутся с ДСЧ криптопровайдера «КриптоПро CSP»).

В случае использования встроенного биоДСЧ в открывшемся окне (см. **Рисунок 1**) следует перемещать указатель мыши, многократно меняя направление движения по горизонтальной оси до исчезновения окна.

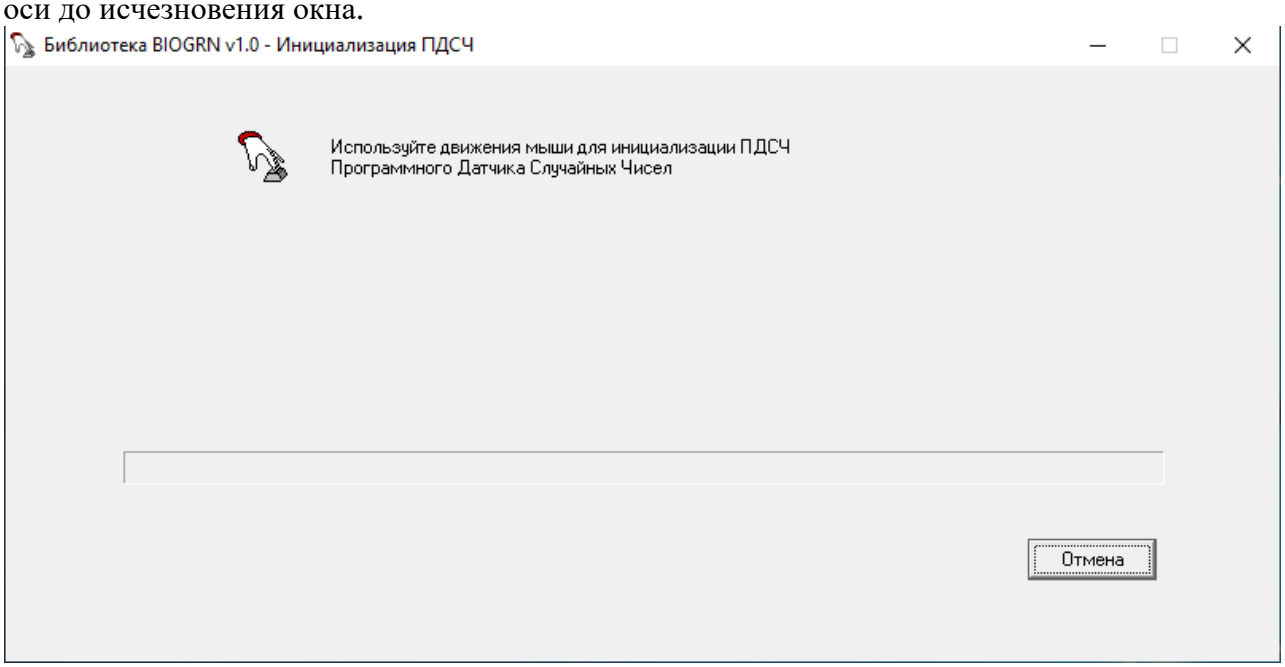

Рисунок 1 – Инициализация встроенного ДСЧ

В случае использования ДСЧ криптопровайдера «КриптоПро CSP» следует обратиться к документации на «КриптоПро CSP».

При выполнении этой команды на устройстве будет гореть зеленый светодиод, до окончания его свечения не следует извлекать устройство из разъема.

```
tpp_admin 1.0.0 (c) ИнфоКрипт, 2017

Устройство «Токен++», режим приложения

Для подготовки устройства к работе необходимо задать значение инициализирующей последовательности ДСЧ.

Подготовка к работе выполнена.
```

После выполнения команды подготовки устройства к работе на устройстве будет установлен так называемый пароль по умолчанию. Для полноценной работы с устройством пароль необходимо поменять. До смены пароля выполнение функций, которые требуют записи на устройство или используют секретный ключ, будет невозможно.

Если устройство «Токен++» находится в состоянии «Готово к работе, пароль по умолчанию» или «Готово к работе, пароль сменён», при выполнении команды подготовки устройства к работе выдается сообщение

```
tpp_admin 1.0.0 (c) ИнфоКрипт, 2017

Устройство «Токен++», режим приложения

Подготовка к работе уже выполнена.
```

4.6 Команда установки пароля по умолчанию

Для установки пароля по умолчанию используется команда "d" (**tpp_admin -d**).

Поскольку при выполнении этой команды все данные пользователя будут безвозвратно утеряны, это действие должно быть подтверждено пользователем: после появления на экране сообщения «Ожидание подтверждения…» необходимо извлечь устройство из USB разъема в течение трёх секунд, пока на устройстве мигают оба светодиода одновременно. Для продолжения работы необходимо снова вставить устройство в разъем. После повторного подключения устройство будет недоступно в течение небольшого периода времени (менее 15 секунд). В течение всего этого времени на устройстве будет гореть зеленый светодиод, до окончания его свечения не следует извлекать устройство из разъема.

```
tpp_admin 1.0.0 (c) ИнфоКрипт, 2017

Устройство «Токен++», режим приложения

ВНИМАНИЕ

Вы собираетесь установить на устройстве пароль по умолчанию. При этом ВСЕ ПОЛЬЗОВАТЕЛЬСКИЕ ДАННЫЕ БУДУТ ПОТЕРЯНЫ.

Для подтверждения этой операции необходимо ИЗВЛЕЧЬ устройство из USB разъема, пока в нем мигают диоды.
Для отказа от установки пароля по умолчанию НЕ ИЗВЛЕКАЙТЕ устройство и дождитесь, когда мигание прекратится.

Для продолжения работы программы нажмите любую клавишу...

Ожидание подтверждения...

Подтверждение установки пароля по умолчанию получено.

Установка пароля по умолчанию произойдет при следующем подключении устройства.
```

Для отказа от установки пароля по умолчанию следует, не извлекая устройство из USB разъема, дождаться, когда прекратится мигание светодиодов.

После установки пароля по умолчанию для полноценной работы с устройством пароль необходимо поменять.

4.7 Команда установки значения инициализирующей последовательности ДСЧ

Для установки нового значения инициализирующей последовательности ДСЧ устройства «Токен++» используется команда "s". Данная команда доступна независимо от результатов самотестирования. Команда может быть задана в двух формах: **tpp_admin -s** (случайные данные берутся с ДСЧ, встроенного в «Модуль администрирования») и **tpp_admin -s -k rng_cp** (случайные данные берутся с ДСЧ криптопровайдера «КриптоПро CSP»).

В случае использования встроенного биоДСЧ в открывшемся окне (см. **Рисунок 1**) следует перемещать указатель мыши, многократно меняя направление движения по горизонтальной оси до исчезновения окна.

В случае использования ДСЧ криптопровайдера «КриптоПро CSP» следует обратиться к документации на «КриптоПро CSP».

При выполнении этой команды на устройстве обновляется значение инициализирующей последовательности ПДСЧ.

```
tpp_admin 1.0.0 (c) ИнфоКрипт, 2017

Устройство «Токен++», режим приложения

Новое значение инициализирующей последовательности установлено.
```

4.8 Команда переключения в технологический режим

Для переключения в технологический режим используется команда "a" (**tpp_admin -a**).

Поскольку технологический режим не является штатным режимом работы устройства, это действие должно быть физически подтверждено пользователем: после появления на экране сообщения «Ожидание подтверждения…» необходимо извлечь устройство из USB разъема в течение трёх секунд, пока на устройстве мигают оба светодиода одновременно. Для продолжения работы необходимо снова вставить устройство в разъем.

```
tpp_admin 1.0.0 (c) ИнфоКрипт, 2017

Устройство «Токен++», режим приложения

ВНИМАНИЕ

Вы собираетесь переключить устройство в технологический режим.

Для подтверждения этой операции необходимо ИЗВЛЕЧЬ устройство из USB разъема, пока в нем мигают диоды.
Для отказа от переключения в технологический режим НЕ ИЗВЛЕКАЙТЕ устройство и дождитесь, когда мигание
прекратится.

Для продолжения работы программы нажмите любую клавишу...

Ожидание подтверждения...

Переключение в технологический режим выполнено.
```

4.9 Команда изменения пароля

Данная команда доступна только для устройства «Токен++ Lite». Более подробно см. «11485466.72.21.12.097 91 02 Модуль администрирования. Руководство пользователя».

5 Световая индикация

Световая индикация при вставке устройства в USB разъем	**Режим и состояние устройства**
– загораются зеленый и красный светодиоды; – красный светодиод мигает несколько раз при горящем зеленом; – зеленый светодиод гаснет, красный остается гореть	Технологический режим
– загораются зеленый и красный светодиоды; – светодиоды горят в течение небольшого периода времени (менее 3 секунд); – оба светодиода гаснут	Режим приложения Состояние «Готово к работе, пароль по умолчанию» или «Готово к работе, пароль сменён»
– загораются зеленый и красный светодиоды; – светодиоды горят в течение небольшого периода времени (менее 3 секунд); – светодиоды начинают попеременно мигать (красный, зеленый, красный, зеленый и т.д.)	Режим приложения Состояние «Не готово к работе»
– загораются зеленый и красный светодиоды; – мигают одновременно красный и зеленый светодиоды	Режим приложения Состояние «Внутреннее ПО повреждено» (Устройство в этом случае отсутствует в списке устройств в операционной системе. Примерно через минуту мигания или при следующем подключении устройство перейдет в технологический режим)

6 Разбор возможных ошибочных ситуаций

Для проверки работоспособности устройства следует выполнить команду **tpp_admin –i** (см. раздел 4.1).

При выполнении этой команды производится самотестирование, в результате которого могут быть получены следующие сообщения об ошибках:

Ошибка	Рекомендуемые действия
Инициализирующая последовательность повреждена	Критическая ошибка. Необходимо вернуть устройство производителю
Контрольная сумма ПО токена отличается от эталонной	
Ключевая информация повреждена или отсутствует	
Ошибка инициализации криптоядра	Следует извлечь устройство и снова вставить его в USB разъем. Если устранить проблему не удалось, необходимо вернуть устройство производителю
Прочие ошибки (код ошибки)	
Файловая система повреждена или не создана	Необходимо воспользоваться командой подготовки устройства к работе **tpp_admin -p** (см. раздел 4.5)
Ошибка инициализации ДСЧ	Необходимо воспользоваться командой установки нового значения инициализирующей последовательности ДСЧ **tpp_admin -s** (см. раздел 4.7), затем извлечь устройство и снова вставить его в USB разъем
Защищенное хранилище повреждено или не создано	Необходимо воспользоваться командой инициализации защищенного хранилища **tpp_admin -f** (см. раздел 4.4)
Была выполнена аварийная перезагрузка устройства	Необходимо воспользоваться командой переключения в режим приложения **tpp_admin -r** (см. раздел 4.2)
Устройство ожидает физического подтверждения выбранного действия.	На устройстве попеременно мигают красный и зеленый светодиоды. Необходимо дождаться, когда это мигание прекратится.

Если в результате самотестирования получено несколько сообщений об ошибках, их следует устранять последовательно. После устранения очередной ошибки следует извлечь устройство из USB разъема, затем снова вставить его в разъем и заново выполнить команду **tpp_admin –i**.

Если в результате самотестирования ошибок не обнаружено (сообщение «OK»), но устройство не может переключиться в режим приложения и остается в технологическом режиме (постоянно горит красный светодиод, в системе в списке устройств присутствует устройство «Токен++ LOADER»), необходимо выполнить следующие действия:

- Проверить целостность внутреннего ПО при помощи команды **tpp_admin -c**.
- Если внутреннее ПО повреждено, устройство необходимо вернуть производителю.
- Выполнить команду **tpp_admin -r**. В случае успешного выполнения этой команды устройство должно переключиться в режим приложения.

Если выполнение этих действий не привело к переключению устройства в режим приложения, необходимо вернуть устройство производителю.