

**Операционная система модуля идентификации абонентов (SIM-карт)
«ElvisSIM.OS»**

Руководство по установке и эксплуатации
программного обеспечения

Листов 6

СОДЕРЖАНИЕ

АННОТАЦИЯ.....	3
1. НАЗНАЧЕНИЕ ПО	3
2. АДМИНИСТРИРОВАНИЕ ОС.....	3
3. УСТАНОВКА ОС	3
4. ПРАВИЛА ПОЛЬЗОВАНИЯ	5
5. ВЗАИМОДЕЙСТВИЕ С ОПЕРАТОРОМ СОТОВОЙ СВЯЗИ.....	5
СПИСОК ЛИТЕРАТУРЫ.....	6

АННОТАЦИЯ

Настоящий документ является руководством по установке и эксплуатации программного обеспечения «Операционная система модуля идентификации абонентов (SIM-карт)» (далее по тексту ОС).

В руководстве приведена информация об установке и эксплуатации программного обеспечения при серийном производстве SIM-карт, а также инструкция по установке ПО для проверки единичных и опытных образцов SIM-карт.

1. НАЗНАЧЕНИЕ ПО

ОС «ElvisSIM.OS» предназначена для работы в качестве встроенного программного обеспечения (прошивки) модулей идентификации абонентов (SIM-карт) мобильных терминалов, соответствующих стандартам ETSI и 3GPP GSM связи.

2. АДМИНИСТРИРОВАНИЕ ОС

- 2.1. Административное управление и настройка ОС после прошивки SIM-карты не требуется и не предусмотрено.
- 2.2. Ввод в эксплуатацию ОС осуществляется одновременно с вводом в эксплуатацию SIM-карты.
- 2.3. Специальные действия по выводу из эксплуатации ОС не требуются, вывод из эксплуатации осуществляется одновременно с выводом из эксплуатации SIM-карты.

3. УСТАНОВКА ОС

Штатная установка ОС при серийном производстве SIM-карт должна производиться путем прошивки образа ПО совместно с профилем оператора сотовой связи в микроконтроллер согласно соответствующей технологической карте предприятия производителя SIM-карт.

Переустановка ОС на SIM-карту не предусмотрена и невозможна.

Настройка ОС после прошивки SIM-карты не требуется.

Приведенная ниже инструкция по установке может использоваться исключительно для проверки единичных и опытных образцов SIM-карт с использованием приложения CellSimScripter и считывателя SMART-карт.

3.1. Подготовка данных

Проверить наличие всех необходимых данных (файл с кодом операционной системы (ОС), ключ лицензии ОС на прошивку и ключи оператора).

Примечание. Если поступили обновления каких-либо скриптов, то при работе с CellSimScripter рекомендуется закрыть все открытые файлы и заново открыть их из папки `sim_os/scripts` (чтобы исключить вероятность использования открытых старых файлов).

3.2. Перевод SIM-карты в режим бутлоадера

SIM-карта может находиться в двух состояниях: в режиме бутлоадера и в режиме ОС.

Определить текущий режим можно следующим образом:

- Подключить считыватель карт к компьютеру.
- Вставить SIM-карту в считыватель карт.
- Запустить CellSimScripter.
- Нажать «Connect».
- Выполнить скрипт `sim_os/scripts/read_atr.sz`.
- Проверить значение ATR, которое вернула SIM-карта.

Если полученный ATR короткий и заканчивается на EA (например, 3F90978010EA), то SIM-карта уже в режиме бутлоадера и ничего делать не нужно.

Если был возвращен длинный ATR (например, 3B9F96803FC7008031E073FE2113670000008800000171), то SIM-карта в режиме ОС и ее необходимо перевести в режим бутлоадера. Для этого требуется выполнить скрипт `sim_os/scripts/km_bootloader.sz`.

3.3. Загрузка кода ОС

Рекомендуется указанные ниже действия производить на ноутбуке или компьютере с бесперебойным источником питания.

Для загрузки кода ОС необходимо выполнить следующие действия::

- Выполнить скрипт `sim_os/scripts/elvis_kmxsce512_3G_CAT_LTE.sz`.
- Выполнить скрипт `sim_os/scripts/read_atr.sz`.

Примечание. Полученный ATR уже должен быть длинным.

3.4. Загрузка профилей 2G/3G

Для загрузки профилей 2G/3G необходимо выполнить следующие действия:

- Выполнить скрипт `sim_os/scripts/1.Profile_2G3G_ini.sz`
- Выполнить скрипт `sim_os/scripts/2.Profile_2G3G_perso_amended`. В списке выбирать открытый набор ключей `test_output_20190905_cut.out`.

Примечание. Поле «Use record number» задает номер строки с параметрами ключей (условно - номер карты).

3.5. Установка апплета крипто-библиотеки

3.5.1. Перед прошивкой первой карты необходимо убедиться, что хэш крипто-библиотеки, прописанный в апплете, и фактический хэш крипто-библиотеки в ОС совпадают.

Запросить хэш в ОС можно выполнив скрипт `sim_os/scripts/os_readCIHash.sz`. В ответ будет получена конкатенация хеша с успешным кодом возврата 9000. Успешный код возврата не является значением хэша.

Хэш в апплете прописывается последней командой в скрипте. Открыть последнюю команду скрипта `sim_os/scripts/3.applet_ini_20191127.sz` и проверить в конце этой команды значение хэша, отделенное пробелами (примерный формат: `XXXXXXXXXX HASH 00`).

Если хэш в ОС не совпадает с хэшем в скрипте загрузки апплета, то в последнем необходимо задать корректное значение (пробелы удалять не нужно).

3.5.2. Выполнить скрипт `sim_os/scripts/3.applet_ini_20191127.sz`.

3.6. Прописывание ключей оператора

Выполнить скрипт `sim_os/scripts/4.putkey.sz`. В списке выбрать открытый набор ключей `test_output_20190905_cut.out`.

Примечание. Поле «Use record number» должно совпадать с тем, что было задано в п.3.4.

3.7. Инициализация крипто-библиотеки

Выполнить скрипт `sim_os/scripts/cl_init.sz`.

4. ПРАВИЛА ПОЛЬЗОВАНИЯ

4.1. Роль пользователя и пользовательское управление ОС не предусмотрены. Владелец SIM-карты должен руководствоваться правилами пользования SIM-карты соответствующего оператора сотовой связи.

5. ВЗАИМОДЕЙСТВИЕ С ОПЕРАТОРОМ СОТОВОЙ СВЯЗИ

Взаимодействие ОС с инфраструктурой оператора сотовой связи осуществляется в соответствии с международными стандартами:

- UICC (ETSI 102 221 Rel. 8);
- SIM/USIM (3GPP 31.102 Rel. 8);
- CAT/STK (ETSI 102 223 Rel. 8, 3GPP 31.111 Rel. 8);

- 2G, 3G и LTE.

СПИСОК ЛИТЕРАТУРЫ

- /JCAPI/ *JavaCard Platform. Application Programming Interface. Version 2.2.1*
Published by SUN Microsystems, 2003
- /STK/ *3GPP TS 31.111: USIM Application Toolkit (USAT) Version 6.15.0 (Release 6).*
Published by 3GPP, 2012
- /USIM/ *3GPP TS 31.102: Characteristics of the USIM application. Version 6.23.0 (Release 6).*
Published by 3GPP, 2012
- /ISIM/ *3GPP TS 31.103: Characteristics of the IP Multimedia Services Identity Module (ISIM) application. Version 8.6.0 (Release 8).*
Published by 3GPP, 2014
- /RAM/ *ETSI TS 102 226: Remote APDU Structure for UICC Based Applications. Version 6.18.0 (Release 6).*
Published by ETSI, 2009
- /MLNG/ *3GPP TS 35.205: Specification of the MILENAGE Algorithm Set. An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General. Version 6.0.0*
Published by 3GPP, 2004
- /MLNG2/ *3GPP TS 35.206: Specification of the MILENAGE Algorithm Set. An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm Specification. Version 6.0.0*
Published by 3GPP, 2004
- /SECAR/ *3GPP TS 33.102: Security architecture. Version 6.5.0*
Published by 3GPP, 2005
- /JCAPI/ *JavaCard Platform. Application Programming Interface. Version 2.2.1*
Published by SUN Microsystems, 2003