



Пособие

по созданию мультиоператорных SIM-карт



Содержание

Общие положения	3
Возможности SIM-Эмулятора	4
Считывание КИ и IMSI	6
Программа для считывания IMSI и Ки	6
Настройка SIM-Эмулятора	8

Общие положения

Что такое SIM-эмулятор ?

Это удобное средство для создания мультифункциональной sim-карты, содержащей в себе одновременно несколько номеров телефонов (на данный момент до 10ти) от различных операторов (или различных номеров от одного и того же оператора). Так же с помощью SIM-эмулятора может быть увеличен объем хранимых номеров телефонной книжки и/или SMS сообщений.

Как все это работает?

После установки карты-эмулятора в мобильный телефон специальное программное обеспечение, запрограммированное в чип-карту, создает прототип sim-карты с необходимыми настройками выбранного вами номера телефона. Для каждого номера программируется свой PIN код, как только вам нужно переключиться с одного номера на другой, вам всего лишь достаточно ввести другой PIN код, соответствующий выбираемому телефонному номеру.

Какие типы чип-карт применяются ?

На данный момент все применяемые карты построены на базе микроконтроллеров PICMicro (в будущем, по заверению автора SimEmu, будет выпущена версия для Purple Card, карточке на базе Atmel микроконтроллера)

Предоставляет ли SIM-эмулятор те же функции что и sim-карта?

Да, несомненно. Для каждого телефонного номера в SIM-эмуляторе назначаются отдельный PIN, PUK коды и номер SMS центра. Также, в случае с SIM-EMU 6, имеется возможность хранения 254 номеров записной книжки и 99 SMS сообщений на карте-эмуляторе.

Возможно ли использование всех телефонных номеров одновременно ?

Нет, только один номер может быть активен. Однако вы можете использовать функцию переадресации звонков с неиспользуемых номеров на активный номер для того , чтобы не пропустить звонки с этих номеров. При первой же необходимости вы можете быстро и легко сменить активный номер посредством ввода другого PIN кода.

Как перенести текущий телефонный номер из sim-карты в карту-эмулятор?

Для этого нужно считать регистрационные ключи sim-карты и записать их в карту-эмулятор (запись производится вручную или программатором, зависит от эмулятора)

Будет ли это работать с моим сотовым оператором ?

Последние версии SIM-эмуляторов превосходно работают со всеми операторами использующими для своих sim-карт алгоритм COMP128 v1. Они были полностью протестированы с большинством европейских GSM операторов, и не должно возникать никаких проблем с любыми другими операторами.

Какие преимущества появятся при использовании SIM-эмулятора ?

Если вы постоянно используете больше одной sim-карты, то SIM-эмулятор станет наилучшим решением для вас. С SIM-эмулятором не придется постоянно носить с собой несколько sim-карт и заниматься неприятной процедурой замены одной на другую. Теперь для всех телефонных номеров будет одна общая обширная

записная книжка. На случай утери или кражи телефона, у вас всегда будет под рукой информация для восстановления sim-карты.

PS. С помощью представленных здесь программ и описанных здесь технологий считывание или программирование заблокированных sim-карт невозможно!!! Так же не пытайтесь использовать 2 sim-карты с одинаковыми KI и IMSI кодами одновременно, это приведет к блокированию вашей sim-карты оператором, вследствие чего вам придется ехать в технический отдел оператора и долго объяснять что вы ни в чем не виноваты. Мы снимаем с себя любую ответственность за все ваши действия.

Возможности SIM-Эмулятора

К основным возможностям эмулятора SIM-EMU 6 можно отнести следующее:

- Поддержка до 10 телефонных номеров от различных операторов (или различных номеров от одного и того же оператора)
- Управление вводом PIN кодов такое же как и в оригинальной SIM карте (3 попытки для ввода PIN кода+ 10 для ввода PUK кода)
- Улучшенная совместимость с большим количеством телефонов различных моделей. Автором были протестированы телефоны следующих фирм производителей
 - NOKIA
 - SIEMENS
 - ALCATEL
 - PHILIPS
 - ERICSSON
 - MOTOROLA
 - MAXON
 - PANASONIC
 - MITSUBISHI
 - NEC
 - SAMSUNG
- Возможность гибкой настройки размера записной книжки от 1 до 254 ячеек, при этом имя ячейки может иметь длину до 18 знаков.
- Возможность настройки памяти для хранения от 1 до 99 SMS сообщений
- Настройка памяти для хранения 254 номеров записной книжки и 99 SMS сообщений одновременно
 - Для каждого из 8ми телефонных номеров может быть назначен отдельный номер "SMS центра"
 - Встроенный загрузчик для возможности чтения/записи внешней EEPROM памяти
 - Поддержка команд необходимых для работы с некоторыми телефонами (SEEK), в основном для таких как Ericsson и Philips
 - Для лучшей совместимости переписана подпрограмма связи с телефоном

- Сохранение 10 последних набранных номеров (только для телефонов, поддерживающих данную функцию)
- Настройка эмулятора под 10 различных номеров непосредственно через SMS
- Настройка коэффициента емкости SMS/ТЕЛЕФОННАЯ КНИГА с помощью мобильного телефона
- Новые skript-файлы для записи/восстановления SMS сообщений и содержимого телефонной книги
- Управление SIM-эмулятором с помощью меню мобильного телефона* (*при условии что телефон поддерживает функцию SIM ATK)
- Изменение активного номера не выключая телефон* (не работает в некоторых мобильных телефонах)
- Пункт меню "сброс телефона" для повторного ввода PIN-кода* (если функция смены активного номера через меню не работает)
- Настройка эмулятора под 8 различных номеров используя меню телефона*
- Настройка емкости SMS/ТЕЛЕФОННАЯ КНИГА с помощью меню телефона*
- Присвоение каждому из 8ми номеров своего названия используя меню телефона*
- Индикация активного номера с присвоенным ему названием*
- Индикация текущих настроек (SMS/ADN и количества активных номеров)*
- Вывод информации о разработчике и о версии эмулятора.
- Выполнение команды INCREASE для управления информацией о стоимости звонков (работает с prepaid карточками)
- Совместим с программой Cardinal, позволяющей управлять записной книжкой.
- Постоянная индикация информации о активном номере на экране телефона
- Меню выбора необходимого номера из списка доступных номеров
- Каждая позиция описывающая телефонный номер может иметь длину до 16 знаков
- Возможность выбора активного номера из списка доступных номеров
- Каждой позиции может быть присвоено имя длиной в 16 символов
- Управление стоимостью разговоров для каждой позиции отдельно
- Отдельный пункт меню для смены PIN2/PUK2
- Поддержка GPRS
- Назначение одного общего PIN2/PUK2 кода для всей карточки и 10 PIN/PUK для каждой позиции отдельно.
- В версии 6.00 улучшена защита от считывания конфиденциальной информации, (отключение загрузчика eergom памяти, защита от дозаписи кода во flash память и др)

Более полную информацию можно получить на сайте разработчика <http://simemu.cjb.net>

Сокращения :

ADN - active databook numbers (номера телефонной книги)
FDN - favorite databook numbers (номера быстрого набора)
SMS - smart message system (короткие сообщения)
SIM ATK - SIM Application Toolkit

Считывание KI и IMSI

Для создания SIM-эмулятора необходимо считать с оригинальной sim-карты следующие ключи:

***KI** - индивидуальный ключ аутентификации пользователя, используемый для вычисления значения отклика и ключа шифрования*

***IMSI** - международный идентификационный номер пользователя*

С помощью KI и IMSI производится регистрация абонента у оператора сотовой связи.

Ключ Ki представляет собой очень важную и секретную информацию. Никогда не доверяйте изготовлению мультисимкарт посторонним людям. Считанный Ki храните в строгом секрете,



Чтение IMSI и Ki производится при помощи *CardReader* (устройство для чтения SIM-карт) и программного обеспечения (sim_scan или WoronScan) в следующей последовательности:

1. Подсоедините Card Reader к свободному разъему COM-порта.
2. Вставьте оригинальную карту в разъем Card Reader
3. Установите требуемый режим Card-Reader (3.57 Mhz – переключатель 1 в положении «ON», переключатель 2 в положении «OFF», 7,14 Mhz - переключатель 1 в положении «OFF», переключатель 2 в положении «ON»). Как правило большинство SIM-карт могут считываться на частоте 7.14 Mhz. Это рекомендуемый режим.
4. Запустите программу Sim_scan или WoronScan (описание программ дано ниже).

Программа для считывания IMSI и Ki Simscan

Для считывания IMSI и Ki Вам поребуется программа Sim_Scan 2.1, которую можно скачать с сайта разработчика <http://users.net.yu/~dejan> или с нашего сайта http://www.silver.h12.ru/dl/sim_scan.zip

Программа является Win32 приложением, что обеспечивает нормальную работоспособность в среде Windows. Улучшен алгоритм поиска A38 и добавлен новый "Strong Ki"

Для установки запустите из распакованного архива **install.bat** после чего будет создана папка **C:\sim_scan** в которой будут находиться все необходимые файлы.

После первого запуска программа загрузится с установками "по умолчанию". Установите соответствующий COM Port, к которому подключен Card Reader (COM1, COM2 и т.д.)

Скорость обмена данными (COM Port Speed) зависит от номинала кварцевого резонатора в схеме Card Reader. Установите скорость обмена в соответствии с частотой используемого кварца. (например при использовании кварца на 7.14 МГц скорость обмена будет 19200 bps)

Нажмите кнопку "TEST" если все настроено правильно программа покажет ATR карты (последовательность байт выдаваемых при сбросе карты).

Если программа не выдает ATR, проверьте правильность установки COM-порта (проверьте не используется ли он другими устройствами), проверьте соответствие номинала кварцевого резонатора и установленного значения скорости обмена, работоспособность Card Reader.

При правильном получении ATR жмем кнопку "Find Ki". Если на Вашей карте включен PIN то появится окно запроса. Введите PIN1 и программа приступит к выполнению алгоритма поиска Ki

Поиск Ki занимает в среднем около часа. При успешном окончании поиска появится окно с ключами вашей карты и создается файл **imsi&ki.dat** в каталоге **sim_scan**. Сохраните его.

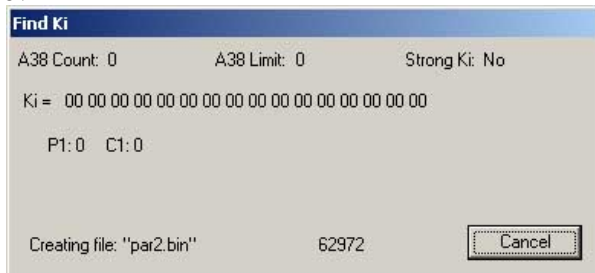


Если вы первый раз используете функцию нахождения ключей, то должно появиться сообщение указывающее на необходимость создания программой файла **par2.bin**. На компьютере P4 1,5 GHz эта процедура займет 35 минут.

После создания **par2.bin** будет начат процесс поиска KI и IMSI.

- **Режим "Strong KI"**

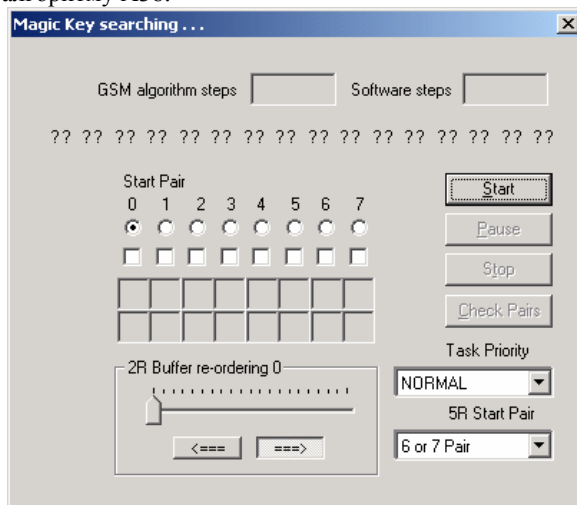
Если вы не уверены что ваша sim-карта использует данный режим, попробуйте сначала найти KI в нормальном режиме. Если после 60000 цикла подстановки криптограммы не будет найдено ни одной пары ключа, жмите "cancel" для остановки процесса поиска. Выберите режим "Strong Ki" и начните поиск заново. Если же в итоге поиск не увенчается успехом, значит алгоритм исследуемой sim-карты не COMP128v1



WoronScan

Рекомендуем воспользоваться новой программой для чтения IMSI и Ki WoronScan. Последнюю версию программы можно скачать с форума www.kievsat.com или с нашего сайта <http://www.silver.h12.ru/dl/WS1.06.zip>

Достоинством данной программы является более продуманный алгоритм считывания ключей, возможность непосредственного ввода команд APDU (Application Protocol Data Units), возможность работы с записной книжкой как оригинальной карты так и карты-эмулятора. Также существует возможность продолжить поиск ключей, зная одну или несколько пар Ki и существенно сократить число обращений к алгоритму A38.



Настройка SIM-Эмулятора Через меню Вашего телефона.

Изначально в эмуляторе запрограммированы 3 номера со следующими значениями кодов доступа:

№	Позиция	PIN	PUK	Оператор
1		1111	11111111	Amena
2		2222	22222222	Movistar
3		3333	33333333	Airtel

!!! По умолчанию PIN2 код - 1234

Установите sim-эмулятор в телефон. После включения телефона введите PIN-код 1111. Настройка эмулятора под ваши собственные номера может быть осуществлена двумя способами:

1. С помощью меню телефона*
2. С помощью программы Configurator

* Этот метод возможен при условии что ваш телефон поддерживает функцию SIM ATK (В основном все телефоны выпускающиеся с 1998 года поддерживают эту функцию)

○ Меню SIM-EMU 6.00

Ниже подробно описано меню SIM-EMU, а также процедура настройки эмулятора.

1. Sel.Phone #
2. Configure
3. Information
4. Reset

Для того, чтоб добавить новый номер в карточку-эмулятор произведите все действия описанные в пункте 2.2.

1) Sel.Phone

Выбор активного номера из списка возможных. Перед активным номером отображается знак "+", все остальные номера помечены знаком "-"



2) Configure



Выбор меню настройки эмулятора



2.1) Edit

Редактирование названия текущей позиции. Максимальная длина 16 символов



2.2) Config.Pos.

Этот пункт меню предназначен для создания новой позиции, которая будет содержать такие данные как **KI/IMSI/PUK** и **PIN**.



2.2.1) PIN2

Введите PIN2-код. (по умолчанию это 1234). Данная процедура введена в целях безопасности.



2.2.2) Position

Номер позиции, в списке телефонных номеров. Число от 0 до 8



2.2.3) IMSI

Здесь необходимо ввести полученный вами ранее ключ IMSI . Этот ключ имеет длину 16 знаков и представлен в десятичном виде (цифры 0-9), где первые две цифры всегда **08**



2.2.4) KI

В этом пункте вводим ключ KI. Длина ключа 32 знака, представлен он в шестнадцатеричном виде (цифры 0-9 и латинские буквы ABCDEF)



2.2.5) PUK

PUK-код для текущей позиции, любое число длиной в 8 символов



2.2.6) PIN

PIN код для текущей позиции, любое число от 4 до 8 символов



2.3) *Config SMS*

Позволяет настроить число SMS сообщений хранимых в памяти sim-эмулятора.



2.3.1) *PIN2*

Ведите PIN2-код. (по умолчанию это **1234**). Данная процедура введена в целях безопасности.



2.3.2) *Nr.SMS*

Для GREEN карточки число от **01** до **40**.



2.4) *Config ADN*

Позволяет установить число активных ячеек записной книжки sim-эмулятора



2.4.1) PIN2

Ведите PIN2-код. (по умолчанию это **1234**). Данная процедура введена в целях безопасности.



2.4.2) Nr.ADN

Для GREEN карточки число от **001** до **250**.



2.5) PIN2/PUK2

Позволяет изменить коды безопасности PIN2 и PUK2



2.5.1) PIN2

Для начала необходимо ввести старый PIN2-код



2.5.2) PUK2

Укажите новый PUK2-код, число в 8 знаков



2.5.3) New PIN2

Ввод нового PIN2-кода, число от 4 до 8 знаков



2.6) ErasePos.

Удаление выбранной позиции



2.6.1) PIN2

Ведите PIN2-код. (по умолчанию это **1234**). Данная процедура введена в целях безопасности.



2.6.2) Position

Номер позиции из списка, которая будет стерта.



3) Information

Информация по настройкам SIM-EMU и др.



3.1) Actual Nr.

Показывает название позиции используемой в данный момент (активный номер)



3.2) Configuration

Информация Распределение активной памяти эмулятора и номерах активизированных позиций.



3.3) Version

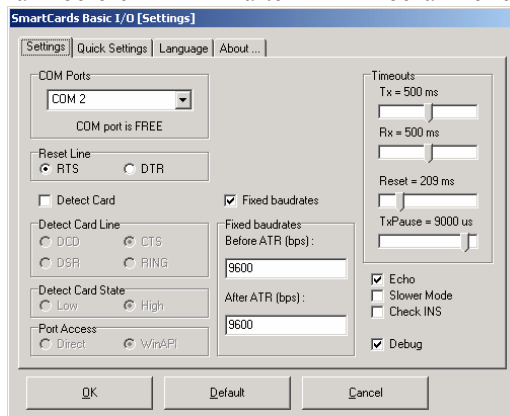
Версия прошивки эмулятора

3.4) Autor

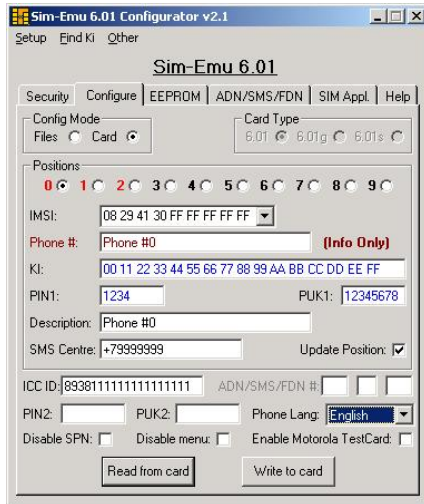
Информация об авторе SIM-EMU

При помощи программы Configurator

1. Вставьте карту, прошитую SimEmu 6.01 в CardReader. Установите выключатель 1 в положение «ON», выключатель 2 в положение «OFF» (частота 3.5 МГц)
2. Запустите программу Configurator v2.1
3. В меню «Setup» выберите «Phoenix plugin (BasicIO.dll)», затем «Setup plugin», установите требуемый COM-порт, а также отметьте «Echo», «Debug» и «Fixed baudrates», в окнах «before ATR» и «after ATR» поставьте «9600».



4. После того, как вы нажмете «OK» наверху черными буквами должна появиться надпись «Sim Emul 6.01». Если горит надпись красным «This is not SimEmu Card», проверьте правильность установок, увеличьте TxPause.
5. В закладке Security введите один из PIN-кодов по умолчанию, например 0000, нажмите «OK». В поле PIN выберите PIN2 и наберите 1234 и снова нажмите «OK».
6. Перейдите в закладку Configure, в Config Mode поставьте Card. Теперь переключая позиции от 0 до 9 вводите данные (IMSI, Ki, описание, PIN, PUK, номер SMS центра).



7. После того, как все необходимые позиции были введены правильно, нажмите кнопку «Write to card» и дождитесь появления сообщения «Configuration written OK».

Карта готова к использованию.

Примечание: в папке, где установлена программа Configurator, остается файл `sim_emu_cfg.ini`, в котором хранятся введенные вами ключи. Необходимо стереть этот файл сразу после записи ключей в карту в целях безопасности.

Некоторая информация взята с сайта www.flycont.com

На нашем сайте

<http://silver.h12.ru>

Вы можете найти интересную информацию по мультиоператорным SIM-картам, скачать необходимое программное обеспечение, узнать, где купить, а также задать интересующий Вас вопрос на форуме.

Пожелания, а так же замеченные ошибки и недостатки принимаются по адресу:

heopsadmin@mail.ru