

**AnyRAM, «ARD Trade»
Production**

«ARD Trade», 1, 2-Priberezhnaya St, Vitebsk, Belarus

Tel: +375-29-5968565

Fax: +375-21-2586250

Website: <http://www.anyram.net>

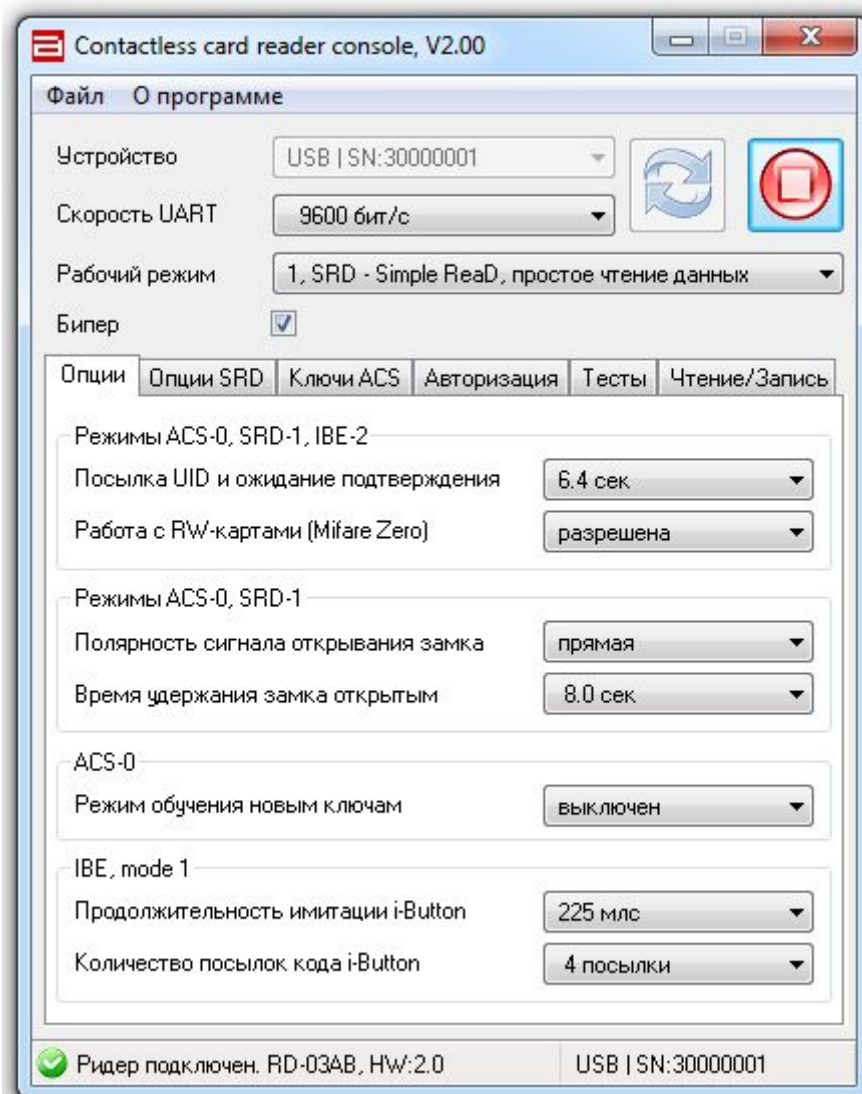
E-Mail: client@anyram.net



**Краткое описание
демонстрационного ПО под
ОС Windows и ОС Linux для
ридера бесконтактных карт
RD-03AB**

CCR (только для Windows)

CCR - основная утилита для конфигурирования ридера. Позволяет подключаться к выбранному ридеру через USB и последовательный интерфейс. Настройки сгруппированы по функционалу. Помимо настроек, утилита **ccr** позволяет управлять внутренней базой ключей ACS, а также базой ключей авторизации АК. Утилита также позволяет проверить подачу звукового сигнала и протестировать управление замком, и считать или записать данные на бесконтактную карту (также как и программа **scc**, см. далее).



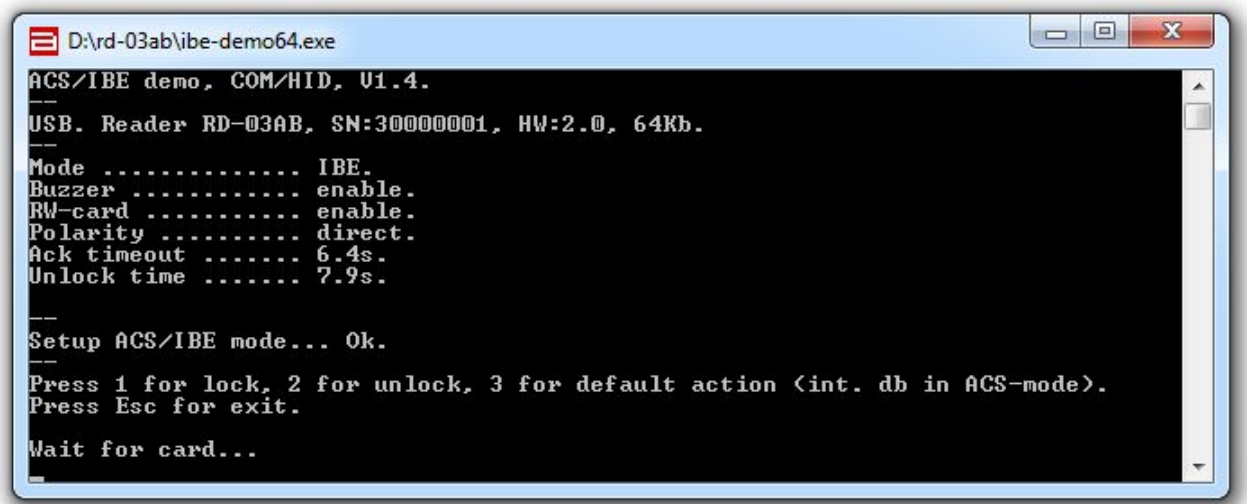
Каталог *acs-ibe*

В этом каталоге находятся исходные тексты для получения двух исполняемых файлов: *ibe-demo* и *acs-demo*. Оба исполняемых файла показывают принципы функционирования ридера в соответствующих режимах *с внешним решателем*. Для того чтобы в режиме ACS карты проходили “по усмотрению” ридера, их надо предварительно прописать в ридер с помощью утилиты *scr.exe*. Запуск файлов без параметров вызывает поиск доступного USB-подключения к ридеру. Запуск файлов с параметрами *COM10 9600* вызывает подключение к ридеру на COM-порте 10 со скоростью 9600 бод/с.

Чтобы получить *ibe-demo*, программу, демонстрирующую работу ридера в **IBE** режиме, следует в текстовом редакторе открыть файл *acs-ibe.cpp* и установить переменную **_DEMO_MODE_** в **0** (2я строка).

```
#define _DEMO_MODE_      0
```

После этого следует откомпилировать программу командой *build* в среде [WinDDK](#) в соответствии с требованиями к процессору. Параметры компилирования программы для WinDDK задаются в файле *sources*. Полученный исполняемый файл следует переименовать из *acs-ibe.exe* в *ibe-demo.exe*.



```
D:\rd-03ab\ibe-demo64.exe
ACS/IBE demo, COM/HID, U1.4.
USB. Reader RD-03AB, SN:30000001, HW:2.0, 64Kb.
Mode ..... IBE.
Buzzer ..... enable.
RW-card ..... enable.
Polarity ..... direct.
Ack timeout ..... 6.4s.
Unlock time ..... 7.9s.
Setup ACS/IBE mode... Ok.
Press 1 for lock, 2 for unlock, 3 for default action (int. db in ACS-mode).
Press Esc for exit.
Wait for card...
```

Программа при запуске переводит ридер в требуемый режим, дополнительных настроек не требуется. Изменить параметры программы можно, изменив заголовок (14я строка *acs-ibe.cpp*):

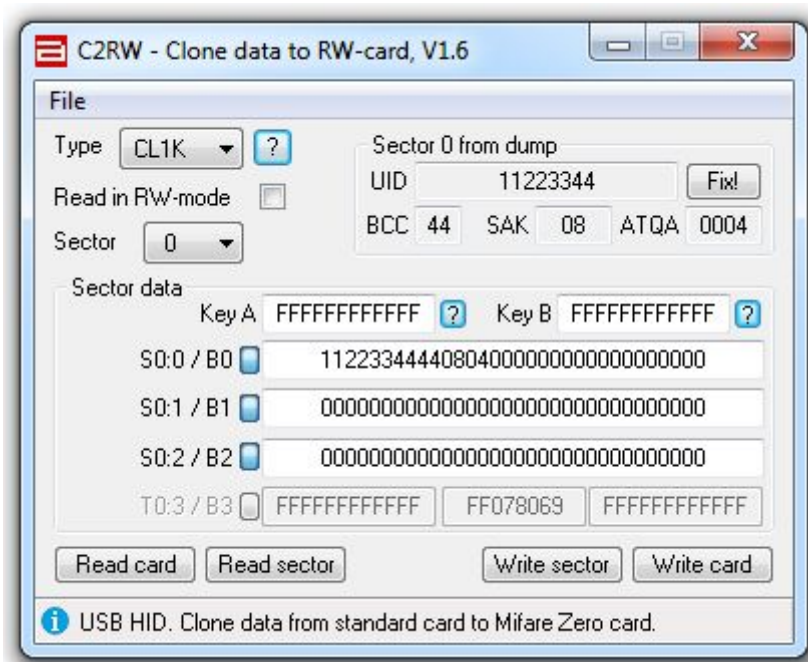
```
#pragma message("*** IBE demo compiling ***")
#define PRG_NAME          TEXT("ibe-demo.exe") // program name
#define DEVM_CN           (2 + 8)             // ACS(0) or IBE(2) mode + buzz_en(+8)
#define OPTS_CN           (4)                 // rwc_en(+4)+sto_en(+2)+polar(+1)
#define TMRS_CN           ((15 << 4) + 9)     // lnk_tout (0..15 << 4) + on_tout(0..15)
```

Сборка исполняемого файла *acs-demo* производится аналогично *ibe-demo*, но переменную, управляющую условной компиляцией **_DEMO_MODE_**, следует установить в **1**.

Каталог c2rw (только для Windows)

В этом каталоге находятся исходные тексты для получения исполняемого файла *c2rw32.exe* (*c2rw64.exe*). Программа *c2rw* позволяет **клонировать** карты Mifare (байт в байт, включая UID) на карты Mifare Zero, или **копировать** данные на обычные карты Mifare. Запуск файла с параметрами *COM10 9600* вызывает подключение к ридеру на COM-порте 10 со скоростью 9600 бод/с.

Сборка программы производится командой *build* в среде [WinDDK](#) в соответствии с требованиями к процессору.

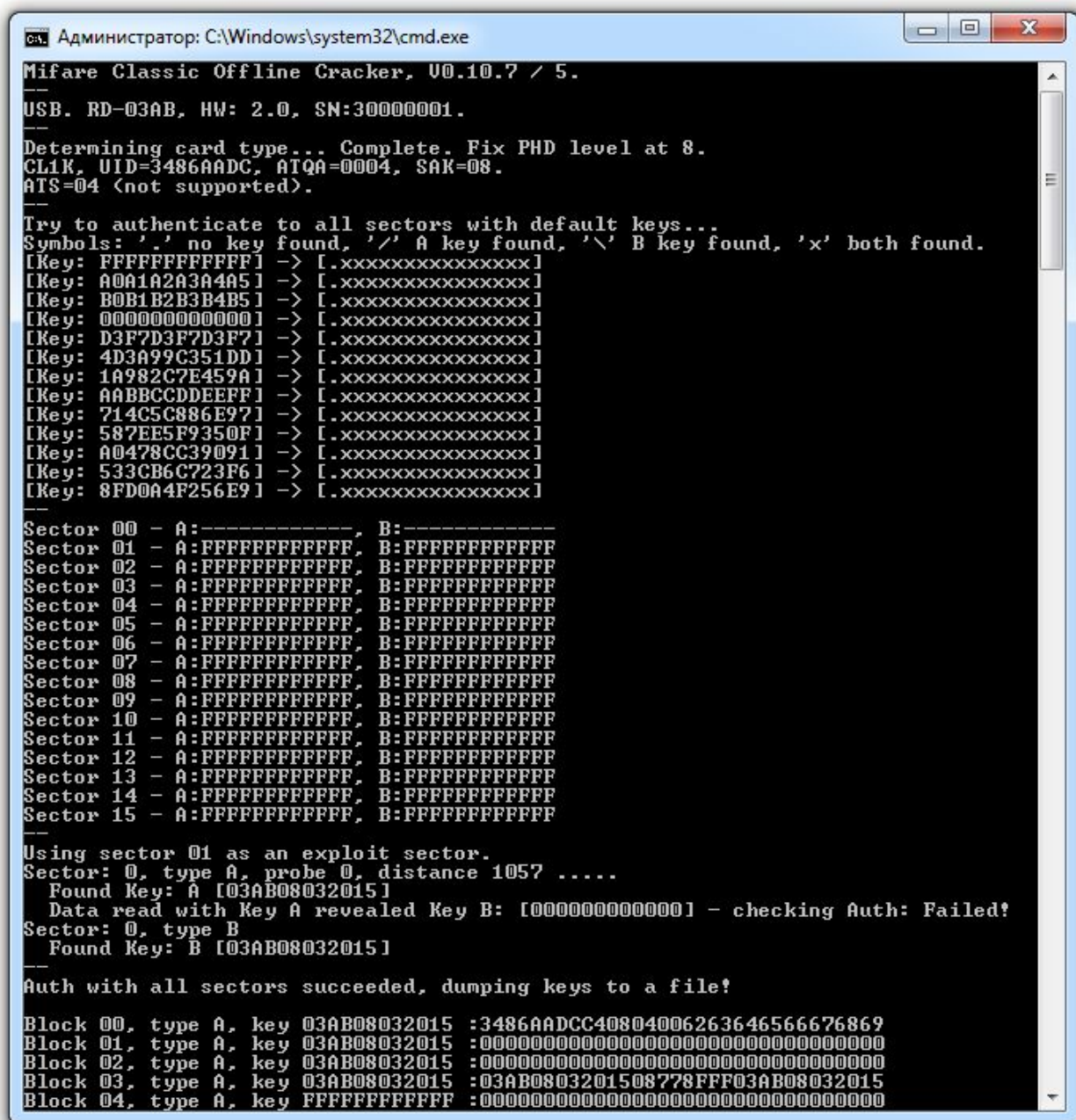


Программа позволяет определить тип карты, UID, исправить UID в случае повреждения, подобрать ключ авторизации Crypto1 из встроенного списка ключей, считать/записать целиком сектор данных (для карт Mifare Classic или Mifare Plus), или страницы данных (для карт Mifare Ultralight).

Программа также сохраняет и загружает дампы карт в различных форматах.

Каталог mfoc0.10.7.6

В этом каталоге находятся исходные тексты для получения исполняемого файла *mfoc*. Программа *mfoc* позволяет узнать значение ключей авторизации Срупто1 на карте, если известен ключ доступа хотя бы к одному сектору. Новые типы бесконтактных карт не имеют уязвимости, используемой *mfoc*. Подробности можно прочитать на сайте проекта <https://github.com/nfc-tools/mfoc>. Запуск файла без параметров вызывает поиск доступного USB-подключения к ридеру. Запуск файла с параметрами *-COM10 9600* вызывает подключение к ридеру на COM-порте 10 со скоростью 9600 бод/с.



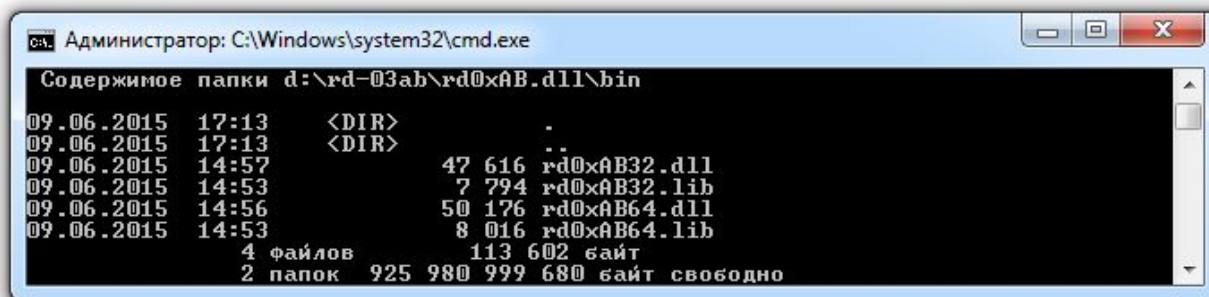
```
Администратор: C:\Windows\system32\cmd.exe
Mifare Classic Offline Cracker, V0.10.7 / 5.
---
USB. RD=03AB, HW: 2.0, SN:300000001.
---
Determining card type... Complete. Fix PHD level at 8.
CLK, UID=3486AADCC, ATQA=0004, SAK=08.
ATS=04 (not supported).
---
Try to authenticate to all sectors with default keys...
Symbols: '.' no key found, '/' A key found, '\' B key found, 'x' both found.
[Key: FFFFFFFFFF] -> [.xxxxxxxxxxxxxxxx]
[Key: A0A1A2A3A4A5] -> [.xxxxxxxxxxxxxxxx]
[Key: B0B1B2B3B4B5] -> [.xxxxxxxxxxxxxxxx]
[Key: 000000000000] -> [.xxxxxxxxxxxxxxxx]
[Key: D3F7D3F7D3F7] -> [.xxxxxxxxxxxxxxxx]
[Key: 4D3A99C351DD] -> [.xxxxxxxxxxxxxxxx]
[Key: 1A982C7E459A] -> [.xxxxxxxxxxxxxxxx]
[Key: AABBCDDDEEFF] -> [.xxxxxxxxxxxxxxxx]
[Key: 714C5C886E97] -> [.xxxxxxxxxxxxxxxx]
[Key: 587EE5F9350F] -> [.xxxxxxxxxxxxxxxx]
[Key: A0478CC39091] -> [.xxxxxxxxxxxxxxxx]
[Key: 533CB6C723F6] -> [.xxxxxxxxxxxxxxxx]
[Key: 8FD0A4F256E9] -> [.xxxxxxxxxxxxxxxx]
---
Sector 00 - A:-----, B:-----
Sector 01 - A:FFFFFFFF, B:FFFFFFFF
Sector 02 - A:FFFFFFFF, B:FFFFFFFF
Sector 03 - A:FFFFFFFF, B:FFFFFFFF
Sector 04 - A:FFFFFFFF, B:FFFFFFFF
Sector 05 - A:FFFFFFFF, B:FFFFFFFF
Sector 06 - A:FFFFFFFF, B:FFFFFFFF
Sector 07 - A:FFFFFFFF, B:FFFFFFFF
Sector 08 - A:FFFFFFFF, B:FFFFFFFF
Sector 09 - A:FFFFFFFF, B:FFFFFFFF
Sector 10 - A:FFFFFFFF, B:FFFFFFFF
Sector 11 - A:FFFFFFFF, B:FFFFFFFF
Sector 12 - A:FFFFFFFF, B:FFFFFFFF
Sector 13 - A:FFFFFFFF, B:FFFFFFFF
Sector 14 - A:FFFFFFFF, B:FFFFFFFF
Sector 15 - A:FFFFFFFF, B:FFFFFFFF
---
Using sector 01 as an exploit sector.
Sector: 0, type A, probe 0, distance 1057 ....
Found Key: A [03AB08032015]
Data read with Key A revealed Key B: [000000000000] - checking Auth: Failed!
Sector: 0, type B
Found Key: B [03AB08032015]
---
Auth with all sectors succeeded, dumping keys to a file!
Block 00, type A, key 03AB08032015 :3486AADCC40804006263646566676869
Block 01, type A, key 03AB08032015 :00000000000000000000000000000000
Block 02, type A, key 03AB08032015 :00000000000000000000000000000000
Block 03, type A, key 03AB08032015 :03AB0803201508778FFF03AB08032015
Block 04, type A, key FFFFFFFFFF :00000000000000000000000000000000
```

Сборка программы производится командой *build* в среде [WinDDK](#) в соответствии с требованиями к процессору.

Простой запуск программы производится командой: *mfoc.exe -O dump.bin*, где *dump.bin* – файл, в который будет скопировано содержимое бесконтактной карты.

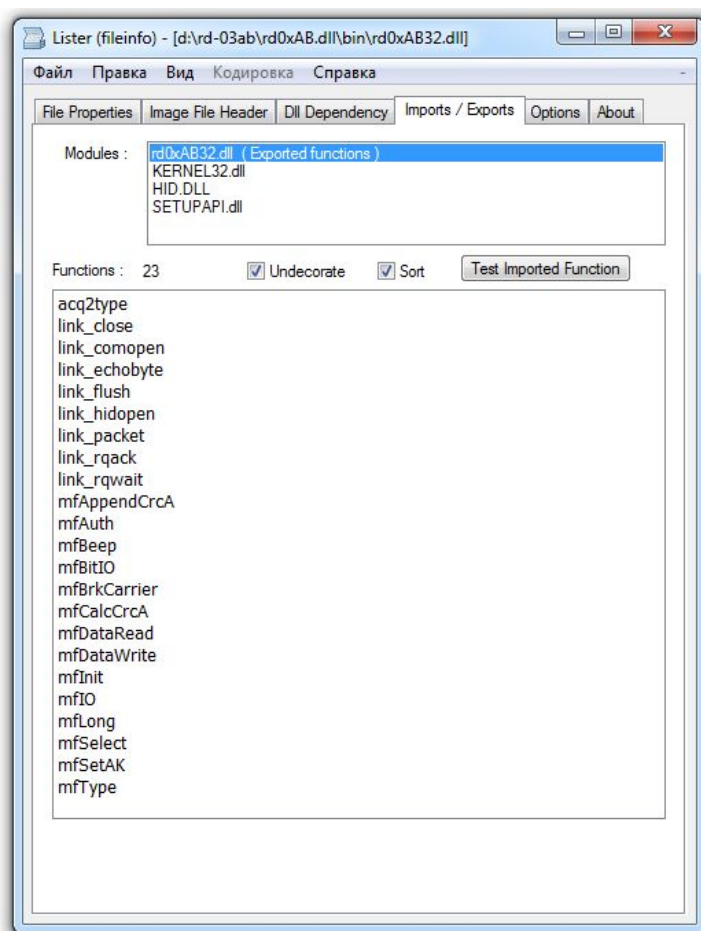
Каталог *rd0xAB.dll*

В этом каталоге находятся исходные тексты *rd0xAB.cpp* и *mf0xAB.cpp*, и предназначен он только для сборки динамической библиотеки *rd0xAB.dll*. Динамическая библиотека может использоваться в тех случаях, когда использование исходных текстов *rd0xAB.cpp* и *mf0xAB.cpp* затруднено или невозможно, например, при построении проекта на *Delphi*, *Java* и др..



```
Администратор: C:\Windows\system32\cmd.exe
Содержимое папки d:\rd-03ab\rd0xAB.dll\bin
09.06.2015 17:13 <DIR> .
09.06.2015 17:13 <DIR> ..
09.06.2015 14:57          47 616 rd0xAB32.dll
09.06.2015 14:53          7 794 rd0xAB32.lib
09.06.2015 14:56          50 176 rd0xAB64.dll
09.06.2015 14:53           8 016 rd0xAB64.lib
          4 файлов          113 602 байт
          2 папок          925 980 999 680 байт свободно
```

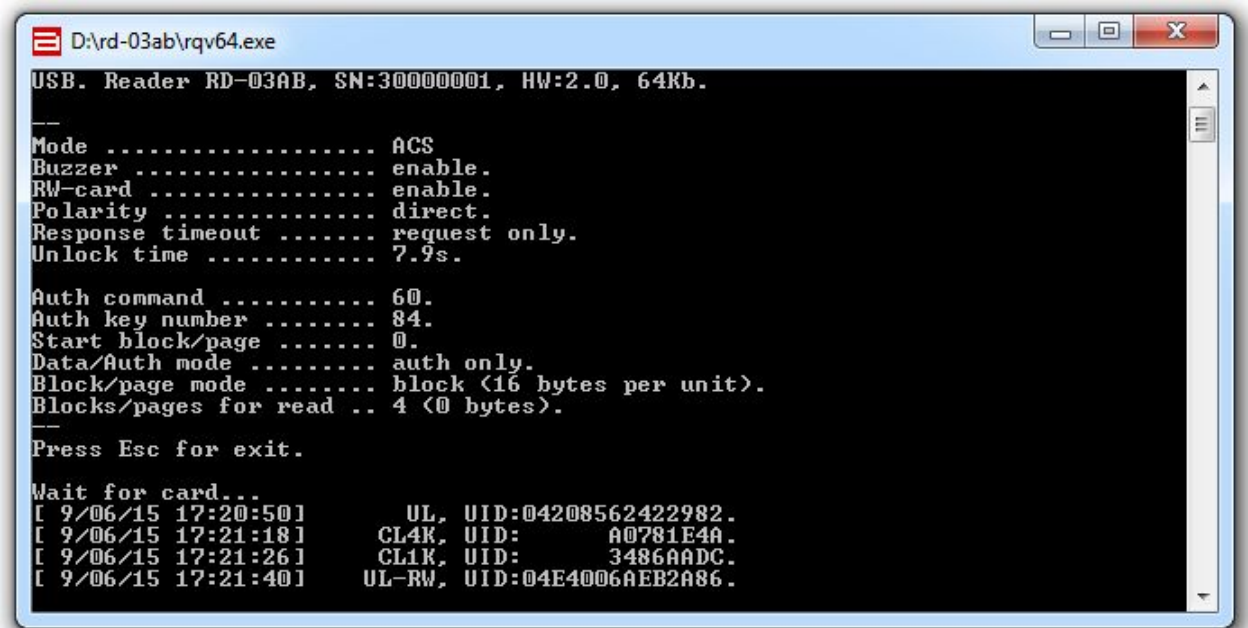
Сборка программы производится командой *build* в среде [WinDDK](#) в соответствии с требованиями к процессору.



Результатом работы компилятора являются два файла: динамическая библиотека *rd0xAB.dll* и библиотека импорта dll *rd0xAB.lib* для подключения к проекту.

Каталог *rqv*

В этом каталоге находятся исходные тексты для получения исполняемого файла *rqv.exe*. Программа *rqv* демонстрирует принципы работы программы логгера, фиксируя на экране *CD*-запрос (*CD* – *Card Descriptor*) и время его прихода. Запуск файла без параметров вызывает поиск доступного USB-подключения к ридеру. Запуск файла с параметрами *COM10 9600* вызывает подключение к ридеру на COM-порте 10 со скоростью 9600 бод/с.



```
D:\rd-03ab\rqv64.exe
USB. Reader RD-03AB, SN:300000001, HW:2.0, 64Kb.
---
Mode ..... ACS
Buzzer ..... enable.
RW-card ..... enable.
Polarity ..... direct.
Response timeout ..... request only.
Unlock time ..... 7.9s.
---
Auth command ..... 60.
Auth key number ..... 84.
Start block/page ..... 0.
Data/Auth mode ..... auth only.
Block/page mode ..... block (16 bytes per unit).
Blocks/pages for read .. 4 (0 bytes).
---
Press Esc for exit.
Wait for card...
[ 9/06/15 17:20:50]      UL,  UID:04208562422982.
[ 9/06/15 17:21:18]      CL4K,  UID:      A0781E4A.
[ 9/06/15 17:21:26]      CL1K,  UID:      3486AADC.
[ 9/06/15 17:21:40]      UL-RW,  UID:04E4006AEB2A86.
```

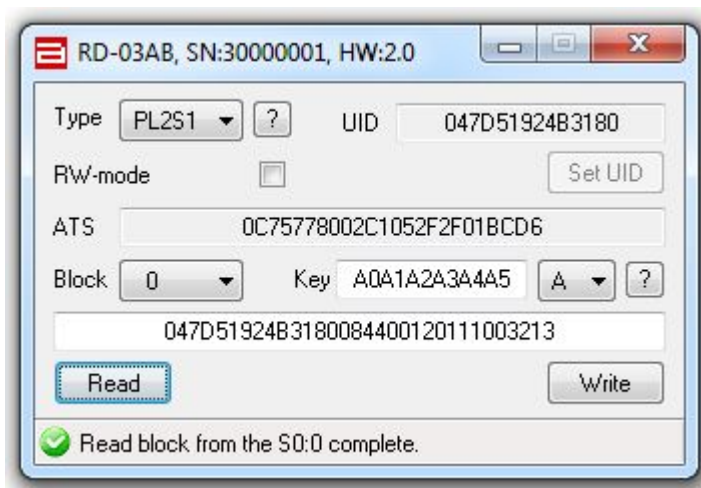
Сборка программы производится командой *build* в среде [WinDDK](#) в соответствии с требованиями к процессору.

Настройка ридера для генерации *CD*-запросов производится утилитой *ccr.exe*.

Каталог scc (только для Windows)

В этом каталоге находятся исходные тексты для получения исполняемого файла *scc.exe*. Программа *scc* демонстрирует принципы работы с картами Mifare и другими совместимыми картами. Запуск файла без параметров вызывает поиск доступного USB-подключения к ридеру. Запуск файла с параметрами *COM10 9600* вызывает подключение к ридеру на COM-порте 10 со скоростью 9600 бод/с.

Сборка программы производится командой *build* в среде [WinDDK](#) в соответствии с требованиями к процессору.

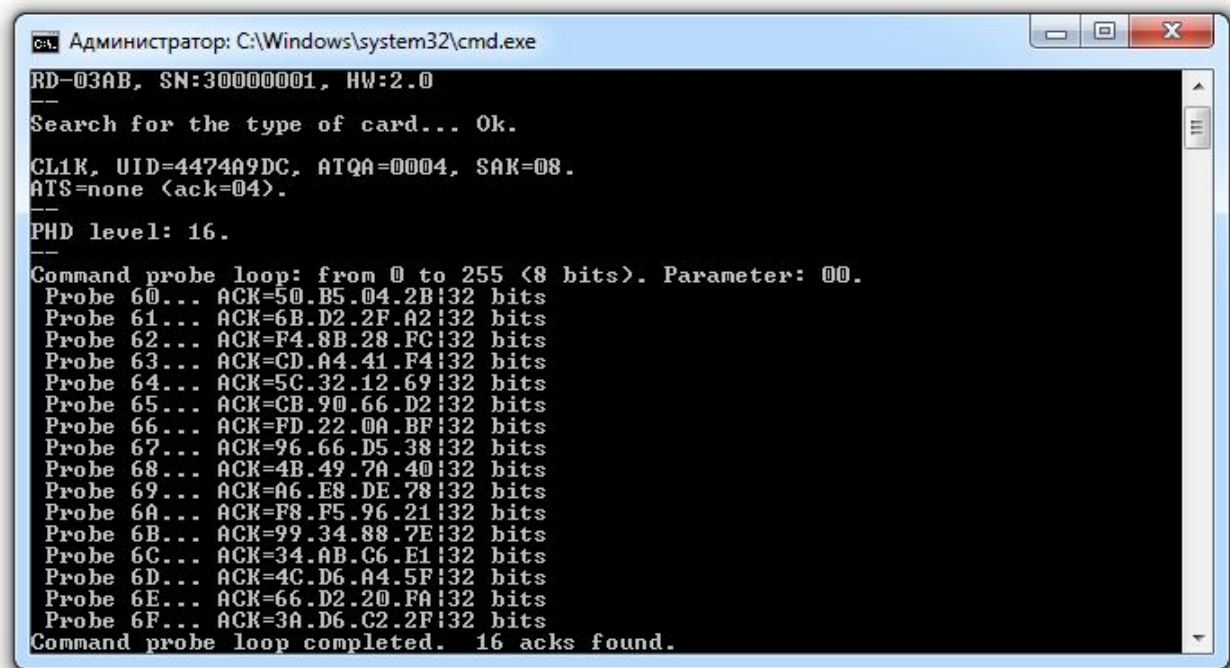


Программа позволяет определить тип карты, UID, считать значение ATS, если карта поддерживает ATS, подобрать ключ авторизации Crypto1 из встроенного списка ключей, считать или записать блок данных (для карт типа Ultralight записывается и читается сразу 4 страницы, чтобы длина данных была 16 байт), поменять UID в картах Mifare Zero.

Каталог *scprobe*

В этом каталоге находятся исходные тексты для получения исполняемого файла *scprobe.exe*. Программа *scprobe* позволяет провести простой анализ команд активации и коротких команд после фазы SELECT. Программа работает с ридером, подключенным по USB интерфейсу.

Сборка программы производится командой *build* в среде [WinDDK](#) в соответствии с требованиями к процессору.



```
Администратор: C:\Windows\system32\cmd.exe
RD=03AB, SN:300000001, HW:2.0
--
Search for the type of card... Ok.
CL1K, UID=4474A9DC, ATQA=0004, SAK=08.
ATS=none (ack=04).
--
PHD level: 16.
--
Command probe loop: from 0 to 255 (8 hits). Parameter: 00.
Probe 60... ACK=50.B5.04.2B:32 bits
Probe 61... ACK=6B.D2.2F.A2:32 bits
Probe 62... ACK=F4.8B.28.FC:32 bits
Probe 63... ACK=CD.A4.41.F4:32 bits
Probe 64... ACK=5C.32.12.69:32 bits
Probe 65... ACK=CB.90.66.D2:32 bits
Probe 66... ACK=FD.22.0A.BF:32 bits
Probe 67... ACK=96.66.D5.38:32 bits
Probe 68... ACK=4B.49.7A.40:32 bits
Probe 69... ACK=A6.E8.DE.78:32 bits
Probe 6A... ACK=F8.F5.96.21:32 bits
Probe 6B... ACK=99.34.88.7E:32 bits
Probe 6C... ACK=34.AB.C6.E1:32 bits
Probe 6D... ACK=4C.D6.A4.5F:32 bits
Probe 6E... ACK=66.D2.20.FA:32 bits
Probe 6F... ACK=3A.D6.C2.2F:32 bits
Command probe loop completed. 16 acks found.
```

Запуск *scprobe* без параметров вызывает поиск коротких команд с параметром равным 0x00 после SELECT. Если требуется поиск доступных коротких команд с параметром отличным от 0x00, *scprobe* следует вызывать с командной строкой, указывая значение параметра, например, *scprobe.exe -COMM 30*, где 30 одно из возможных hex-значений параметра (0...FF). Например, при поиске коротких команд, в китайских картах Classic 1K будет найдено не 2 команды авторизации, а 16.

Запуск *scprobe* с командной строкой *-WUPA* вызовет поиск команд активации карты (7бит). Например, при поиске команд активации, в картах Mifare Zero будет найдена дополнительная команда активации 0x40.

Запуск *scprobe* с командной строкой *-C2PL A0 0C* вызывает поиск длины данных для двухфазной команды 0xA0 с параметром 0x0C после SELECT. Во время первой фазы передаётся короткая команда A0 0C, во время второй фазы передаётся инкрементальная последовательность 0, 1, 2, ..., 15; длина последовательности при поиске изменяется от 1 до 16. Например, в картах Ultralight для команды A0 будет найдена длина последовательности 16 байт.

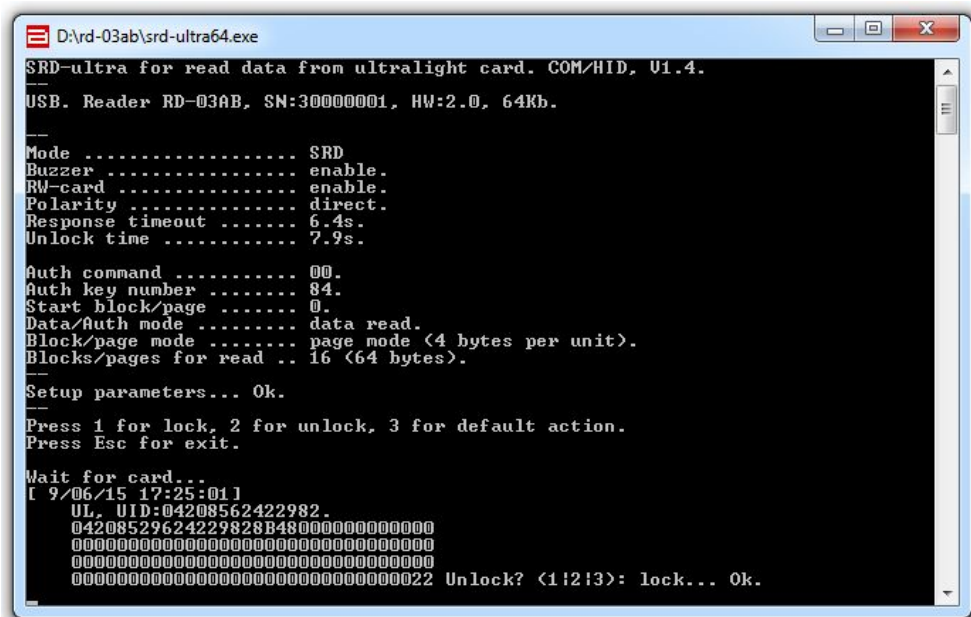
Каталог *srd*

В этом каталоге находятся исходные тексты для получения трёх исполняемых файлов: *srd-auth*, *srd-read* и *srd-ultra*. Все исполняемые файлы показывают принципы функционирования ридера в различных вариациях **SRD**-режима *с внешним решателем*. Запуск файлов без параметров вызывает поиск доступного USB-подключения к ридеру. Запуск файлов с параметрами *COM10 9600* вызывает подключение к ридеру на COM-порте 10 со скоростью 9600 бод/с.

Чтобы получить *srd-ultra*, программу, демонстрирующую чтение данных в SRD-режиме без авторизации (с картами Ultralight), следует в текстовом редакторе открыть файл *srd.cpp* и установить переменную `_DEMO_MODE_` в **0** (2я строка).

```
#define _DEMO_MODE_ 0
```

После этого следует откомпилировать программу командой *build* в среде [WinDDK](#) в соответствии с требованиями к процессору. Параметры компилирования программы для WinDDK задаются в файле *sources*. Полученный исполняемый файл следует переименовать в *srd-ultra.exe*.



Программа при запуске переводит ридер в требуемый режим, дополнительных настроек не требуется. Изменить параметры программы можно, изменив заголовок (14я строка *srd.cpp*):

```
#pragma message("*** SRD-ULTRA demo compiling ***")
#define PRG_NAME TEXT("srd-ultra.exe") // program name
#define START_MSG TEXT("SRD-ultra for read data from ultralight card.")
#define DEVN_CN (1 + 8) // SRD(+1) mode + buzz_en(+8)
#define OPTS_CN (4) // rwc_en(+4) + sto_en(+2) + polar(+1)
#define TMRS_CN ((15 << 4) + 9) // link_tout (0..15 << 4) + unlock_tout(0..15)
#define SRD_A_CN 0x00 // AKSD: A - authorization command, 0x00 - none
#define SRD_K_CN 84 // AKSD: K - AK number, dummy value
#define SRD_S_CN 0 // AKSD: S - start block/page for read
#define SRD_D_CN 0xF1 // AKSD: D - Data descriptor
```

Сборка исполняемых файлов *srd-auth* и *srd-read* производится аналогично *srd-ultra*, но переменную, управляющую условной компиляцией `_DEMO_MODE_`, следует установить в **1** для *srd-auth* и в **2** для *srd-read*.