DVCrypt
Conditional Access System

Quick start guide

1. Introduction

DVCrypt is a conditional access system for digital TV broadcasting networks (*DVB*). It consists of hardware modules and client/server configuration software.

Broadcasting equipment may consist of one or more hardware modules. Each module can multiplex analogue or digital TV channels from several sources into a single digital stream (according to *DVB-C/S/T* standard). Modules may have ASI, HDMI, SDI/HD-SDI or CVBS inputs.

The conditional access system is integrated into the modules. Modules interface with the server PC via *Ethernet* (*TCP/IP*) link.

To watch TV channels, each subscriber must have a compatible *STB* (*Set-Top-Box*) capable of receiving and decoding the signal, and a smartcard. Alternatively subscriber may have *CAM (Conditional Access Module)* installed in their TV set *CI (Common Interface)* slot. Usually CAM modules require smartcard as well but cardless CAMs are also provided.

DVCrypt software runs on a server PC and is used for configuring modules and subscribers rights management. If the PC is off or server application is not running, the system is still fully operational. All broadcasting is carried as usual; you only lose ability to control subscriber's access to channels.

Network provider uses **DVCrypt** smartcard programmer to issue smartcards and CA modules (write subscriber ID and master keys).

2. Security considerations

DVCrypt has several layers of security based on the following assumptions:

- **DVCrypt** is based on *CSA* (*Common Scrambling Algorithm*), which is developed by *ETSI* and recommended by *DVB* consortium for digital TV networks as an industry standard.

- **DVCrypt** will not work with smartcards from other network, even if that other network is another DVCrypt installation.

- Master keys, that are stored in smartcards, are chosen by network provider. It's not possible (even for **DVCrypt** developers!) to read back keys from the smartcard and decode the TV channels.

3. Setup

Before setting up the system, please check that following requirements are met:

3.1 Server PC requirements:

- CPU: 1 GHz or faster;
- RAM: 1 GB or more;
- HDD: at least 1 GB of free space;
- Ethernet LAN adapter;
- Operating System: Windows XP or later. We strongly recommend using dedicated computer for **DVCrypt**!

3.2 License key

License key is provided with your copy of the **DVCrypt** software package. *License key* encodes following information:

- ***Provider ID*** – unique identifier that allows distinguishing two or more providers in the same TV network. Smartcard with a different provider ID will not work in your network.
- ***Provider name*** – text label that describes the network. *STB* typically show provider name along with all channel names.
- ***Max. allowed subscribers*** – limits number of subscribers (unique smartcards) the network could have.

3.3 Equipment connection

Connect the modules and server PC to the regular *Ethernet* switch. Use straight *UTP-5* cables.

3.4 Software installation

Simply run the included *DVCrypt_Install.exe* installation file and follow the prompts. Choose from the following options:

- *Full installation* – install all software components. Choose this option if in doubt.
- *Server only* – install only **DVCrypt** server. Choose this option if you plan to use other computer(s) in the LAN to work with **DVCrypt**. Use next option (Client only) for installations on the LAN computer(s).
- *Client only* – install only **DVCrypt** client.
- *SmartCard programmer only* – Choose this option to install programmer software on a computer that is connected to smartcard programmer.

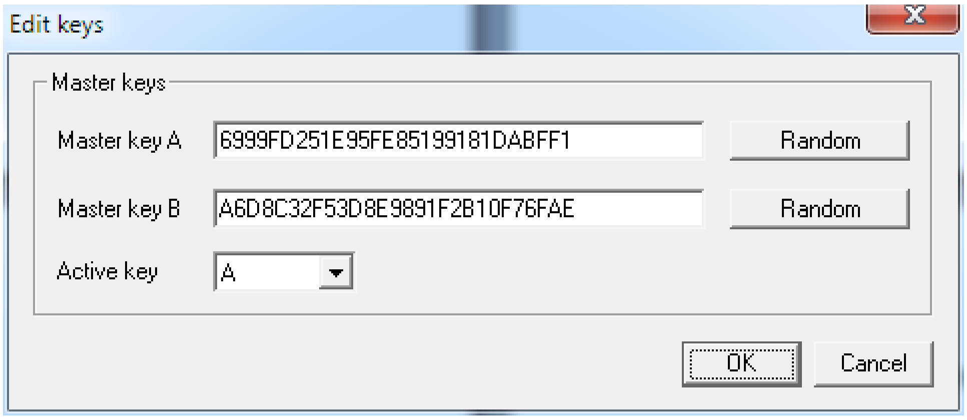
All software components have English user interface.

SetLicense program is automatically run during installation. Use it to enter your *license key*; otherwise **DVCrypt** software will not work. You can always run *SetLicense* program later.

3.5 Configuring server

Select *Start – Programs – DVCrypt* and run *DVCrypt Server* shortcut to start server application. Installation script places a link to **DVCrypt** Server in *Startup* folder to automatically run server each time the user logs on.

Click on the server icon in the traybar and select *Master keys* from the menu:



Edit keys

Master keys

Master key A 6999FD251E95FE85199181DABFF1

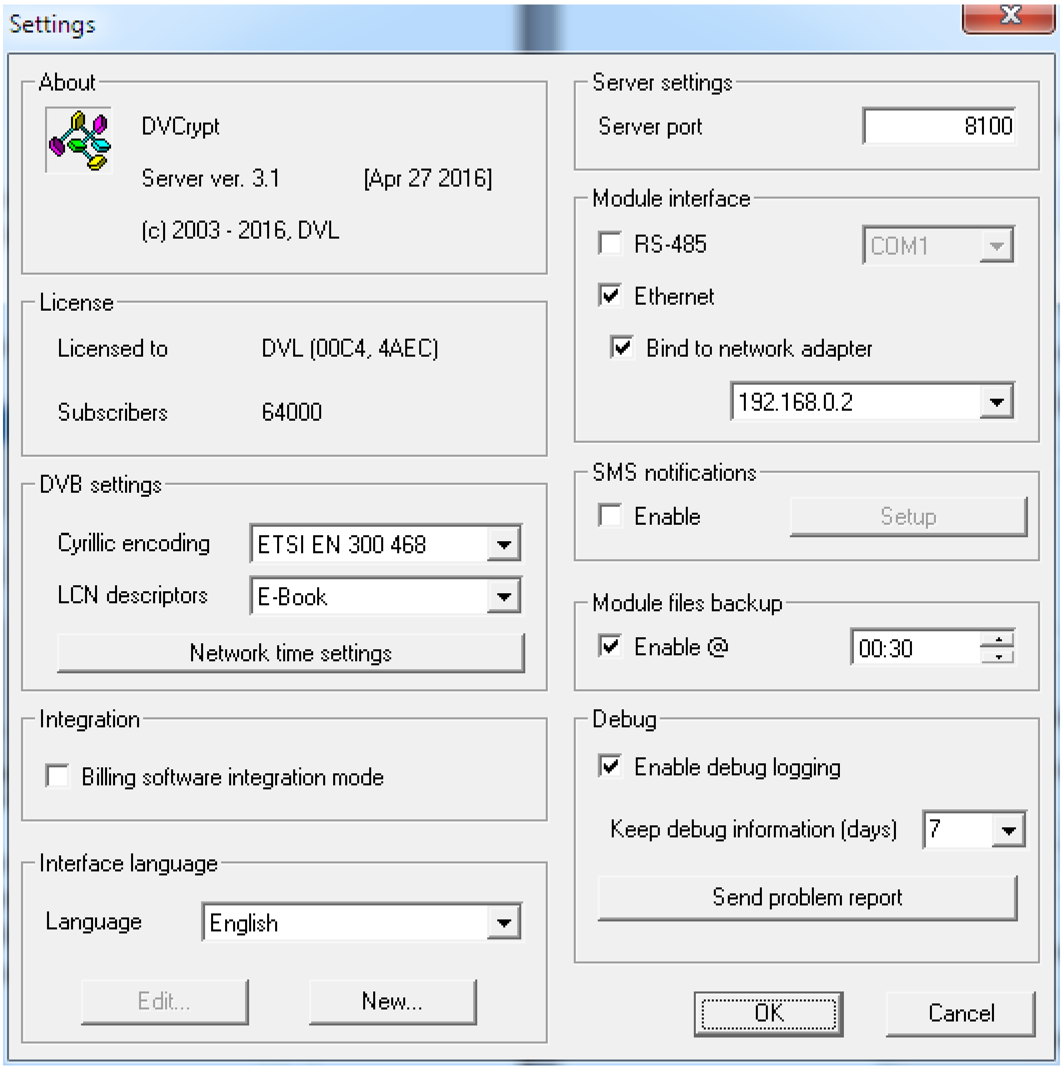
Master key B A6D8C32F53D8E9891F2B10F76FAE

Active key A

Choose two 112-bit *encryption keys* to use with your network. The quickest way is to generate random keys using built-in function. Note that there are two master keys, but only one of them (usually key *A*) is used at any given time. The second key is a backup. If you find that current key is somehow compromised, you can switch to the backup key and gradually replace the compromised key on smartcards.

Write down the keys and store them in a secure place! In case of emergency you could always restore the software and keys and continue normal operation. Otherwise you'd have to reissue smartcards for all subscribers!

Click on the server icon in the traybar and select *Settings* from the menu:



Settings

About

DVCrypt

Server ver. 3.1 [Apr 27 2016]

(c) 2003 - 2016, DVL

License

Licensed to DVL (00C4, 4AEC)

Subscribers 64000

DVB settings

Cyrillic encoding: ETSI EN 300 468

LCN descriptors: E-Book

Integration

□ Billing software integration mode

Interface language

Language: English

Server settings

Server port: 8100

Module interface

□ RS-485 COM1

☑ Ethernet

☑ Bind to network adapter

192.168.0.2

SMS notifications

□ Enable

Module files backup

☑ Enable @ 00:30

Debug

☑ Enable debug logging

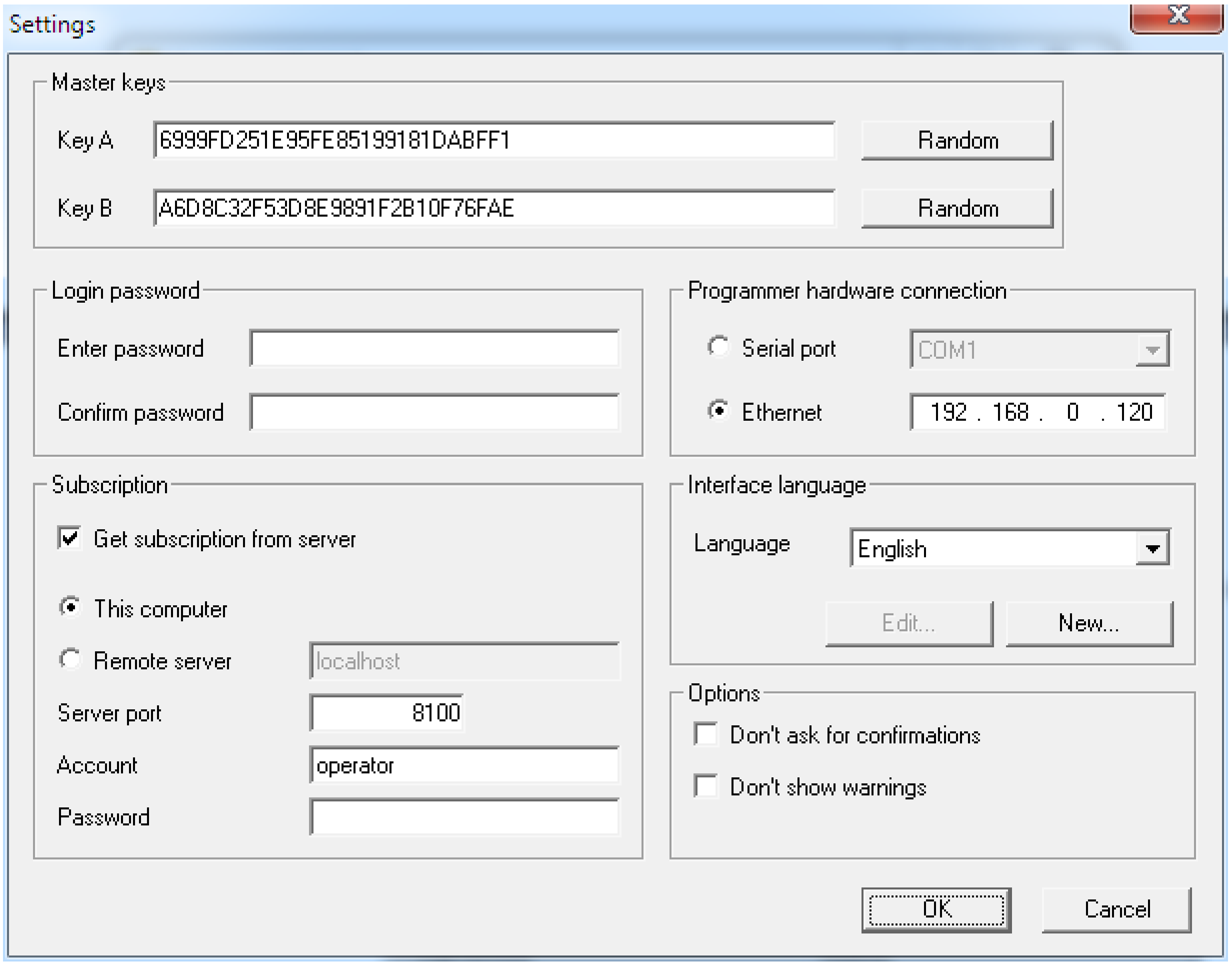
Keep debug information (days): 7

Make sure to check *Ethernet* checkbox. If server PC has more than one *LAN* adapter, also check *Bind to network adapter* and enter *IP address* of the adapter that is connected to modules.

3.6 Configuring smartcard programmer

Select *Start – Programs – DVCrypt* and run *Smartcard Programmer* shortcut. The default **password** is empty.

Click *Settings*:



Settings

Master keys

Key A: 6999FD251E95FE85199181DABFF1

Key B: A6D8C32F53D8E9891F2B10F76FAE

Login password

Enter password:

Confirm password:

Programmer hardware connection

○ Serial port: COM1

● Ethernet: 192 . 168 . 0 . 120

Subscription

☑ Get subscription from server

● This computer

○ Remote server: localhost

Server port: 8100

Account: operator

Password:

Interface language

Language: English

Options

□ Don't ask for confirmations

□ Don't show warnings

Enter two 112-bit *encryption keys* to use with your network. ***Make sure that you correctly copy keys from the server!*** Otherwise the smartcards won’t decode the channels.

Depending on the model of your programmer hardware select either:

- *Serial* and choose virtual *serial port* to which smartcard programmer hardware is connected.
- *Ethernet* and enter IP address of the programmer.

If smartcard programmer is on the same PC as server, or in the same *LAN*, check *Get subscription from server* checkbox and enter *server PC name* if needed.

Note that smartcard programmer may require permanent Internet connection. If no connection is available you could work only with limited number of smartcards or CA Modules.

3.7 Configuring bouquets

Select *Start – Programs – DVCrypt* and run *DVCrypt Client* shortcut to start client application. Enter *server PC name* if server is running on another computer. The default **passwords** for all user accounts are empty.

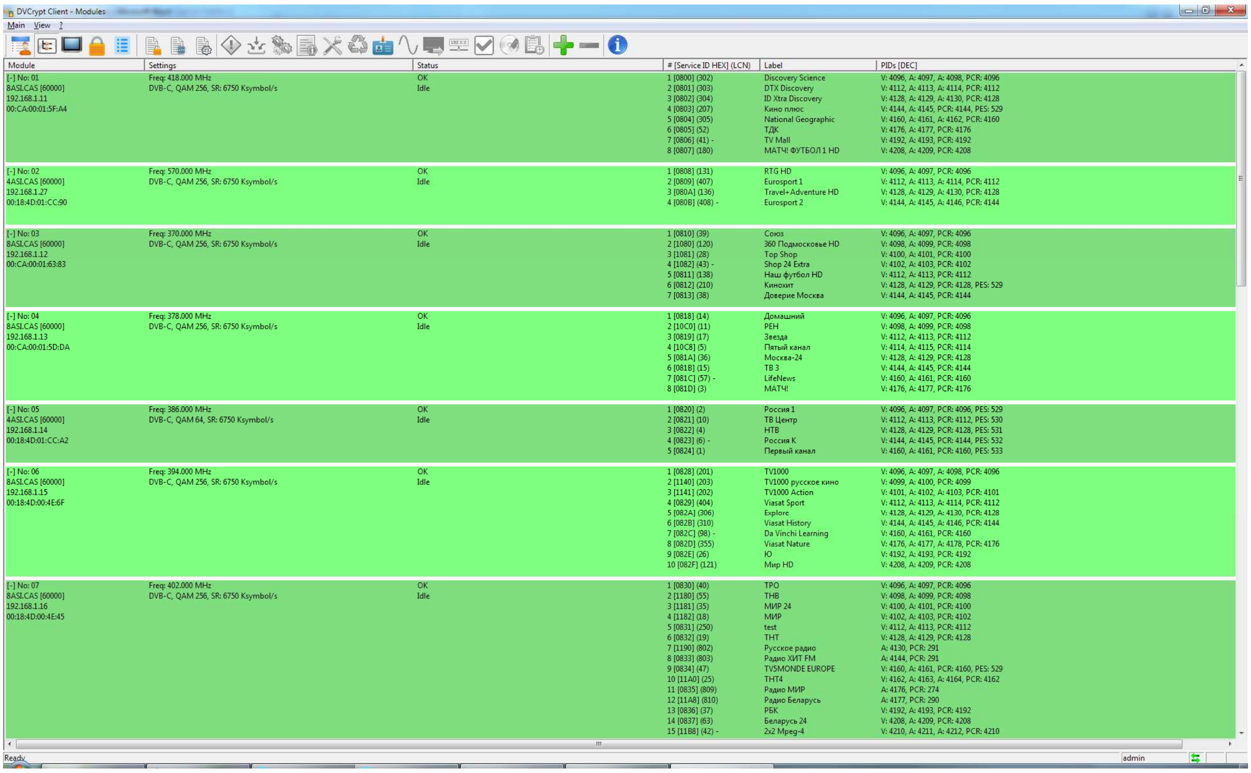
Subscriptions are managed on *bouquet* basis. You can broadcast up to 128 different bouquets. Each subscriber can view any combination of bouquets depending on access rights.

Select *View – Bouquets* from the menu. Enter names for all bouquets you intend to broadcast.

You may choose not to encrypt some of the channels. These channels are not included in the bouquets and can be viewed by any subscriber, even with no smartcard!

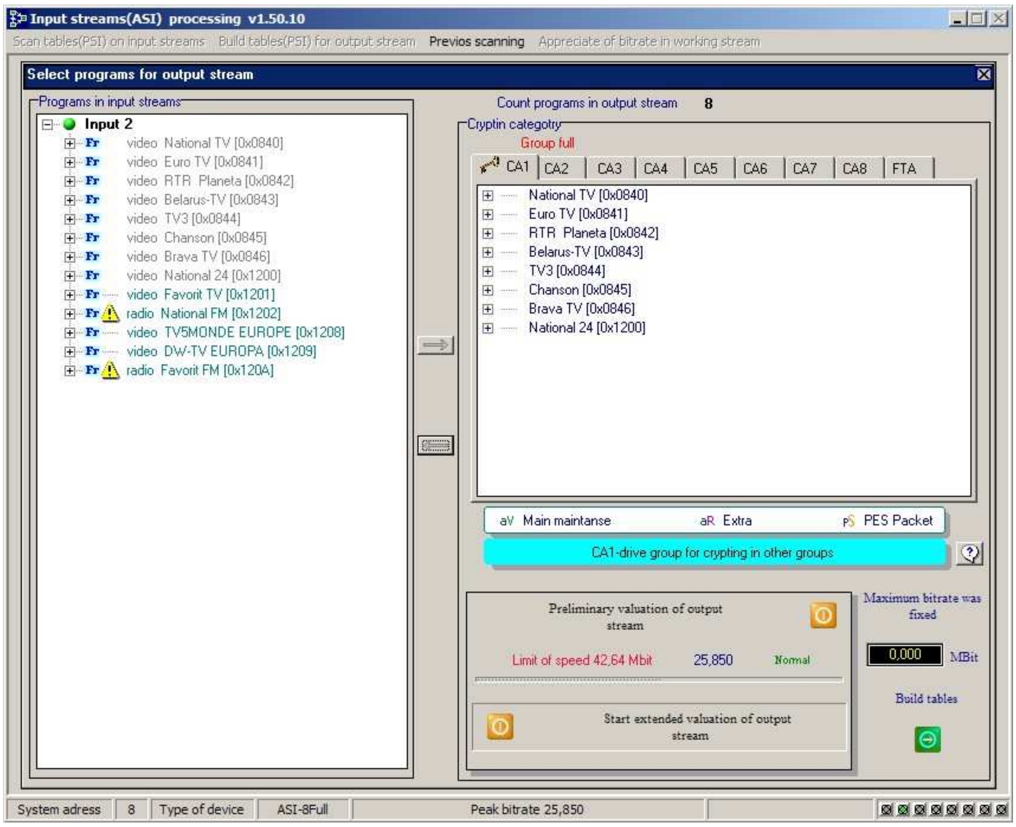
3. 8 Configuring modules

Select *View – Modules* from the menu. Click on *Add new module* icon and follow the wizard prompts. The wizard will help you connect each of the modules to the system one by one.



Module	Settings	Status	# [Service ID HEX] (LCN)	Label	PIDs [DEC]
[-] No: 01 8ASI.CAS [60000] 192.168.1.11 00:CA:00:01:5F:A4	Freq: 418.000 MHz DVB-C, QAM 256, SR: 6750 Ksymbol/s	OK Idle	1 [0800] (302) 2 [0801] (303) 3 [0802] (304) 4 [0803] (207) 5 [0804] (305) 6 [0805] (52) 7 [0806] (41) - 8 [0807] (180)	Discovery Science DTX Discovery ID Xtra Discovery Кино плюс National Geographic ТДК TV Mall МАТЧ! ФУТБОЛ 1 HD	V: 4096, A: 4097, A: 4098, PCR: 4096 V: 4112, A: 4113, A: 4114, PCR: 4112 V: 4128, A: 4129, A: 4130, PCR: 4128 V: 4144, A: 4145, PCR: 4144, PES: 529 V: 4160, A: 4161, A: 4162, PCR: 4160 V: 4176, A: 4177, PCR: 4176 V: 4192, A: 4193, PCR: 4192 V: 4208, A: 4209, PCR: 4208
[-] No: 02 4ASI.CAS [60000] 192.168.1.27 00:18:4D:01:CC:90	Freq: 570.000 MHz DVB-C, QAM 256, SR: 6750 Ksymbol/s	OK Idle	1 [0808] (131) 2 [0809] (407) 3 [080A] (136) 4 [080B] (408) -	RTG HD Eurosport 1 Travel+Adventure HD Eurosport 2	V: 4096, A: 4097, PCR: 4096 V: 4112, A: 4113, A: 4114, PCR: 4112 V: 4128, A: 4129, A: 4130, PCR: 4128 V: 4144, A: 4145, A: 4146, PCR: 4144
[-] No: 03 8ASI.CAS [60000] 192.168.1.12 00:CA:00:01:63:83	Freq: 370.000 MHz DVB-C, QAM 256, SR: 6750 Ksymbol/s	OK Idle	1 [0810] (39) 2 [1080] (120) 3 [1081] (28) 4 [1082] (43) - 5 [0811] (138) 6 [0812] (210) 7 [0813] (38)	Союз 360 Подмосковье HD Top Shop Shop 24 Extra Наш футбол HD Кинохит Доверие Москва	V: 4096, A: 4097, PCR: 4096 V: 4098, A: 4099, PCR: 4098 V: 4100, A: 4101, PCR: 4100 V: 4102, A: 4103, PCR: 4102 V: 4112, A: 4113, PCR: 4112 V: 4128, A: 4129, PCR: 4128, PES: 529 V: 4144, A: 4145, PCR: 4144
[-] No: 04 8ASI.CAS [60000] 192.168.1.13 00:CA:00:01:5D:DA	Freq: 378.000 MHz DVB-C, QAM 256, SR: 6750 Ksymbol/s	OK Idle	1 [0818] (14) 2 [10C0] (11) 3 [0819] (17) 4 [10C8] (5) 5 [081A] (36) 6 [081B] (15) 7 [081C] (57) - 8 [081D] (3)	Домашний РЕН Звезда Пятый канал Москва-24 ТВ 3 LifeNews МАТЧ!	V: 4096, A: 4097, PCR: 4096 V: 4098, A: 4099, PCR: 4098 V: 4112, A: 4113, PCR: 4112 V: 4114, A: 4115, PCR: 4114 V: 4128, A: 4129, PCR: 4128 V: 4144, A: 4145, PCR: 4144 V: 4160, A: 4161, PCR: 4160 V: 4176, A: 4177, PCR: 4176
[-] No: 05 4ASI.CAS [60000] 192.168.1.14 00:18:4D:01:CC:A2	Freq: 386.000 MHz DVB-C, QAM 64, SR: 6750 Ksymbol/s	OK Idle	1 [0820] (2) 2 [0821] (10) 3 [0822] (4) 4 [0823] (6) - 5 [0824] (1)	Россия 1 ТВ Центр НТВ Россия К Первый канал	V: 4096, A: 4097, PCR: 4096, PES: 529 V: 4112, A: 4113, PCR: 4112, PES: 530 V: 4128, A: 4129, PCR: 4128, PES: 531 V: 4144, A: 4145, PCR: 4144, PES: 532 V: 4160, A: 4161, PCR: 4160, PES: 533
[-] No: 06 8ASI.CAS [60000] 192.168.1.15 00:18:4D:00:4E:6F	Freq: 394.000 MHz DVB-C, QAM 256, SR: 6750 Ksymbol/s	OK Idle	1 [0828] (201) 2 [1140] (203) 3 [1141] (202) 4 [0829] (404) 5 [082A] (306) 6 [082B] (310) 7 [082C] (98) - 8 [082D] (355) 9 [082E] (26) 10 [082F] (121)	TV1000 TV1000 русское кино TV1000 Action Viasat Sport Explore Viasat History Da Vinchi Learning Viasat Nature Ю Мир HD	V: 4096, A: 4097, A: 4098, PCR: 4096 V: 4099, A: 4100, PCR: 4099 V: 4101, A: 4102, A: 4103, PCR: 4101 V: 4112, A: 4113, A: 4114, PCR: 4112 V: 4128, A: 4129, A: 4130, PCR: 4128 V: 4144, A: 4145, A: 4146, PCR: 4144 V: 4160, A: 4161, PCR: 4160 V: 4176, A: 4177, A: 4178, PCR: 4176 V: 4192, A: 4193, PCR: 4192 V: 4208, A: 4209, PCR: 4208
[-] No: 07 8ASI.CAS [60000] 192.168.1.16 00:18:4D:00:4E:45	Freq: 402.000 MHz DVB-C, QAM 256, SR: 6750 Ksymbol/s	OK Idle	1 [0830] (40) 2 [1180] (55) 3 [1181] (35) 4 [1182] (18) 5 [0831] (250) 6 [0832] (19) 7 [1190] (802) 8 [0833] (803) 9 [0834] (47) 10 [11A0] (25) 11 [0835] (809) 12 [11A8] (810) 13 [0836] (37) 14 [0837] (63) 15 [11B8] (42) -	ТРО ТНВ МИР 24 МИР test ТНТ Русское радио Радио ХИТ FM TV5MONDE EUROPE ТНТ4 Радио МИР Радио Беларусь РБК Беларусь 24 2x2 Mpeg-4	V: 4096, A: 4097, PCR: 4096 V: 4098, A: 4099, PCR: 4098 V: 4100, A: 4101, PCR: 4100 V: 4102, A: 4103, PCR: 4102 V: 4112, A: 4113, PCR: 4112 V: 4128, A: 4129, PCR: 4128 A: 4130, PCR: 291 A: 4144, PCR: 291 V: 4160, A: 4161, PCR: 4160, PES: 529 V: 4162, A: 4163, A: 4164, PCR: 4162 A: 4176, PCR: 274 A: 4177, PCR: 290 V: 4192, A: 4193, PCR: 4192 V: 4208, A: 4209, PCR: 4208 V: 4210, A: 4211, A: 4212, PCR: 4210

For modules with *ASI* inputs, click on the module and run *input stream selection utility* (select icon from toolbar). Follow the utility prompts to scan input streams and select which channels to include in the output stream:



Input streams(ASI) processing v1.50.10

Scan tables(PSI) on input streams
Build tables(PSI) for output stream
Previos scanning
Appreciate of bitrate in working stream

Select programs for output stream

Programs in input streams

Input 2
- Fr video National TV [0x0840]
- Fr video Euro TV [0x0841]
- Fr video RTR Planeta [0x0842]
- Fr video Belarus-TV [0x0843]
- Fr video TV3 [0x0844]
- Fr video Chanson [0x0845]
- Fr video Brava TV [0x0846]
- Fr video National 24 [0x1200]
- Fr video Favorit TV [0x1201]
- Fr radio National FM [0x1202]
- Fr video TV5MONDE EUROPE [0x1208]
- Fr video DW-TV EUROPA [0x1209]
- Fr radio Favorit FM [0x120A]

Count programs in output stream 8

Cryptin categotry

Group full

- National TV [0x0840]
- Euro TV [0x0841]
- RTR Planeta [0x0842]
- Belarus-TV [0x0843]
- TV3 [0x0844]
- Chanson [0x0845]
- Brava TV [0x0846]
- National 24 [0x1200]

CA1-drive group for crypting in other groups

Preliminary valuation of output stream

Limit of speed 42,64 Mbit 25,850 Normal

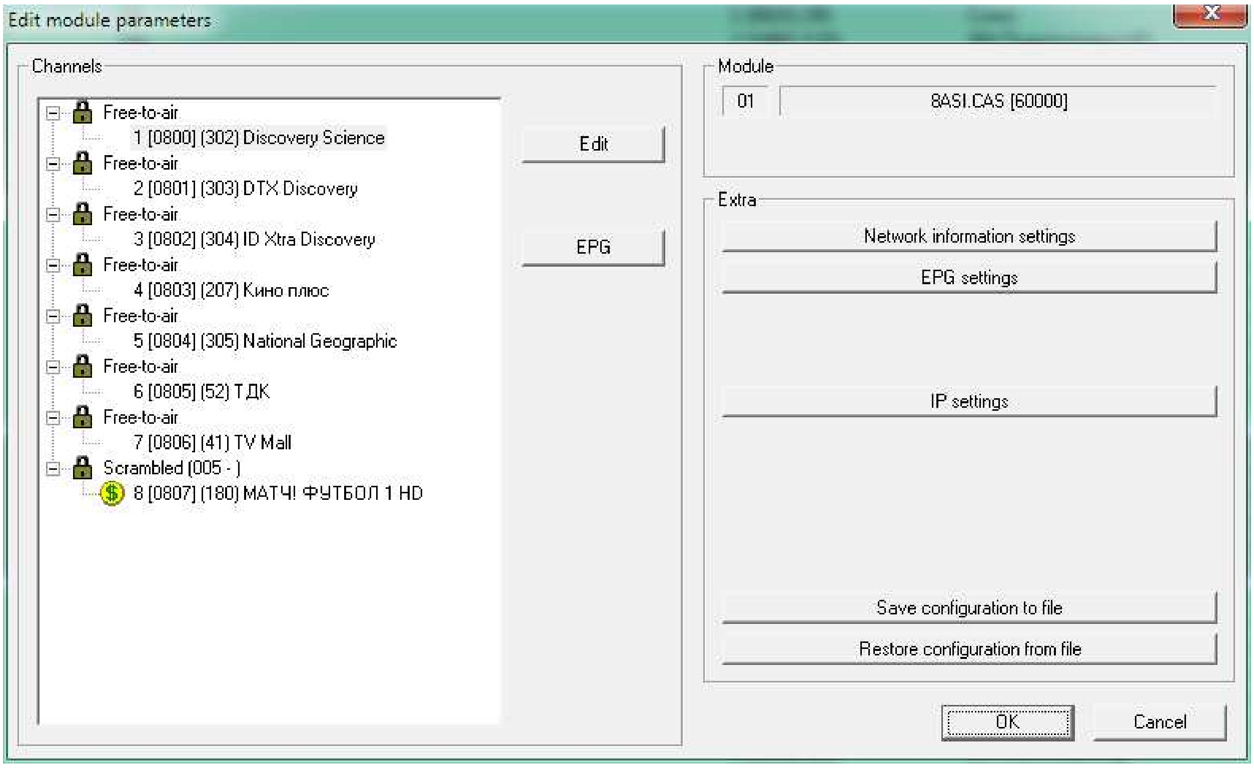
Start extended valuation of output stream

Maximum bitrate was fixed

0,000 MBit

System adress 8 Type of device ASI-8Full Peak bitrate 25,850

After all modules are added and configured, double-click on each of them to change *settings*:



Edit module parameters

Channels

Free-to-air
1 [0800] [302] Discovery Science
Free-to-air
2 [0801] [303] DTX Discovery
Free-to-air
3 [0802] [304] ID Xtra Discovery
Free-to-air
4 [0803] [207] Кино плюс
Free-to-air
5 [0804] [305] National Geographic
Free-to-air
6 [0805] [52] ТДК
Free-to-air
7 [0806] [41] TV Mall
Scrambled [005 -]
8 [0807] [180] МАТЧ! ФУТБОЛ 1 HD

Module
01
8ASI.CAS [60000]

Edit
EPG
Extra
Network information settings
EPG settings
IP settings
Save configuration to file
Restore configuration from file
OK
Cancel

Click on each *channel*, correct the *label* (channel name) if needed. You may also assign *LCN (Logical Channel Number)* to the channel here.

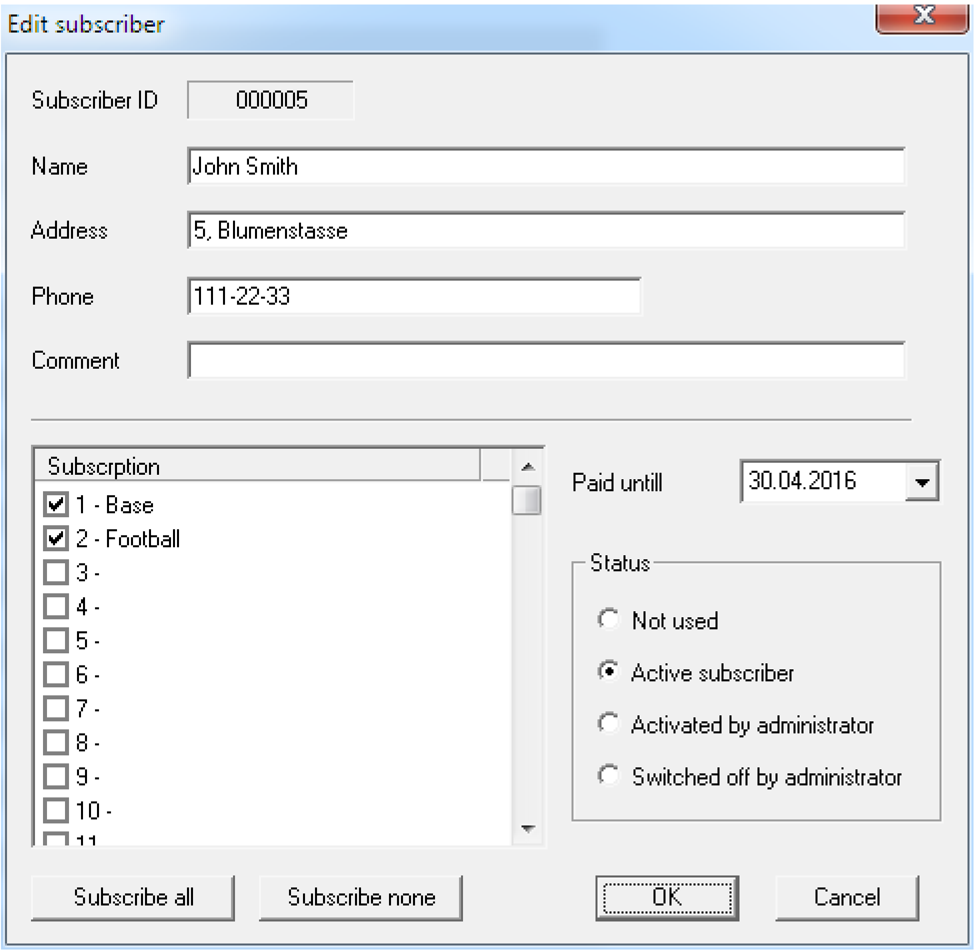
Select *conditional access mode* for the scrambling group.

If you choose to encrypt the channel (*scrambled*), select which bouquet number to use.

You can also change settings for EPG (Electronic Program Guide) and DVB network search in this window.

3.9 Managing subscribers

Select *View – Subscribers* from the menu. Note that all subscribers are initially disabled. To *add* a subscriber, simply double-click on the *subscriber ID* (number):



Subscriber ID: 000005

Name: John Smith

Address: 5, Blumenstasse

Phone: 111-22-33

Comment:

Subscrption

- ☑ 1 - Base
- ☑ 2 - Football
- □ 3 -
- □ 4 -
- □ 5 -
- □ 6 -
- □ 7 -
- □ 8 -
- □ 9 -
- □ 10 -
- □ 11

Paid untill: 30.04.2016

Status

- ○ Not used
- ● Active subscriber
- ○ Activated by administrator
- ○ Switched off by administrator

Enter subscriber information (*Name*, *Address*, *Phone number(s)* and optional *Comments*).

Select which *bouquets* are enabled for this subscriber to watch.

Choose the *control mode* from following options:

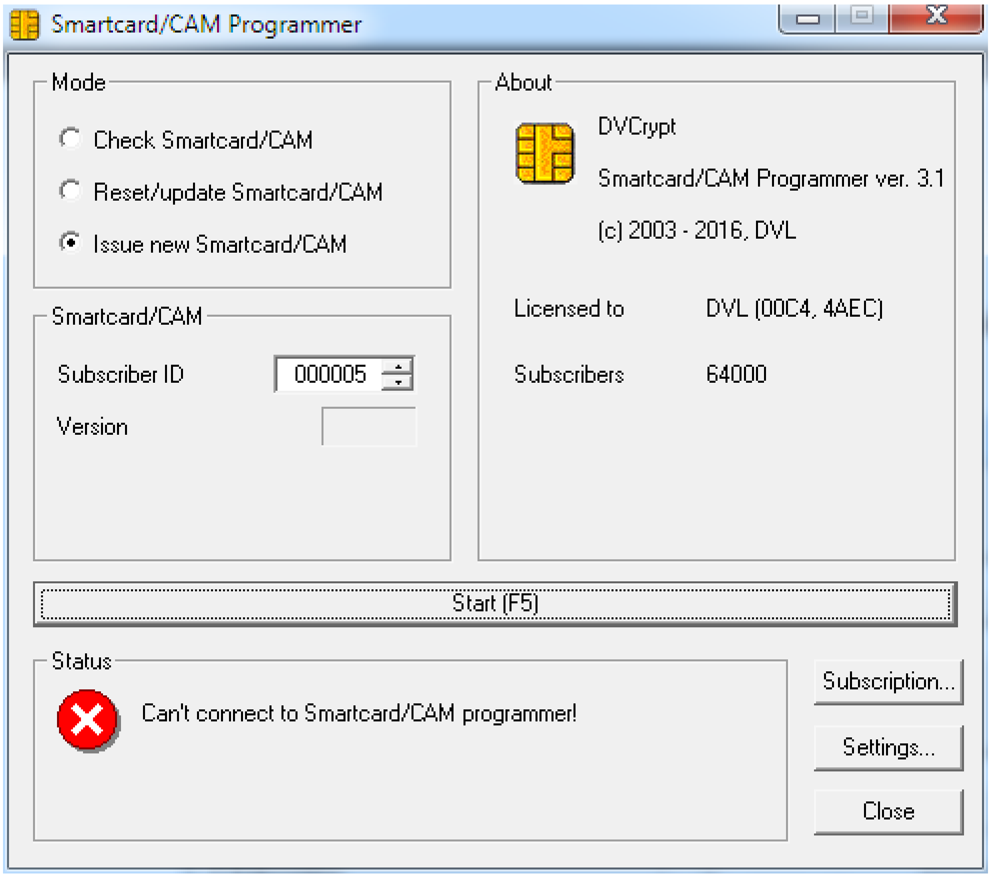
- *Active* – subscriber can watch enabled *bouquet(s)* as long as the *paid until date* is extended. If the *paid date* is reached, subscription is closed and would reopen only if a future *date* is entered. Subscription is automatically checked on each midnight as long as the server is running. This is a default mode of operation.
- *Activated by administrator* – subscriber can watch enabled *bouquet(s)* regardless of the paid until date. Typically used for technicians and service staff smartcards.
- *Switched off by administrator* – subscriber cannot watch any scrambled channel. Use this option to quickly switch off subscription of a particular smartcard.
- *Not used* – select this option to delete the subscriber.

Note that STB/TV reaction to any subscription change is not immediate! Subscriber might have to wait 3-5 minutes before scrambled channel can be viewed.

3. 10 Issuing smartcards and CAMs

Smartcards come preloaded with the firmware that already contains all necessary components of **DVCrypt**. Network provider only needs to assign a *subscriber id* (number) and *master keys* to each smartcard before giving it out to a client. The same applies to cardless Conditional Access Modules.

Select *Start – Programs – DVCrypt* and run *Smartcard Programmer* shortcut:



Smartcard/CAM Programmer

Mode

○ Check Smartcard/CAM

○ Reset/update Smartcard/CAM

● Issue new Smartcard/CAM

Smartcard/CAM

Subscriber ID: 000005

Version:

About

DVCrypt

Smartcard/CAM Programmer ver. 3.1

(c) 2003 - 2016, DVL

Licensed to: DVL (00C4, 4AEC)

Subscribers: 64000

Status

Can't connect to Smartcard/CAM programmer!

Insert an empty smartcard into the card slot.

Select *Mode – Check card*. Click *Start* to make sure that the card is empty.

Select *Mode - Issue new smartcard* and choose a *subscriber ID*. Click *Start* and wait for card programming to complete. Smartcard is now ready for customer. Note that *subscriber ID* is automatically incremented each time you issue a new smartcard.

The procedure for issuing cardless CA Modules is the same, you just have to use different slot for CAMs.