# DVCrypt
## Conditional Access System

## Quick start guide

### 1. Introduction

**DVCrypt** is a hardware/software conditional access system for digital TV broadcasting networks (*DVB*).

Broadcasting equipment consists of one or more (up to 32) 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). The conditional access system is integrated into the modules. Modules interface with the server PC via *Ethernet* (*TCP/IP*) or *RS-485* (serial bus) 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.

**DVCrypt** software runs on a server PC and is used for modules setup and subscribers 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 (write subscriber ID and master keys to smartcards).

### 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.

- 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 stream.

## 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;
- LAN adapter and/or USB for modules interface;
- Operating System: Windows XP, or Windows server 2003/2008. 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 the 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 (smartcards) the network could have.

### 3.3 Equipment connection

If you're using modules with *RS-485* interface, connection cables are already included. Connect the *USB <–> RS-485* converter to the server PC. Connect one end of *RS-485* cable to the converter, and the other end to first module. Connect second module with the first one and so on. Insert a termination plug (300 Ohm) into remaining *RS-485* slot of the last module.

When you connect *USB <–> RS-485* converter to PC for the first time, Windows will prompt to install the necessary drivers (which are included in the installation package). After successful installation, open *Device Manager* (right-click on *My Computer* select *Management – Device manager*) and find a virtual serial port assigned for the converter (it should be listed as *USB Serial Port* in the *Ports* section).

If you're using modules with *Ethernet* interface, 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.

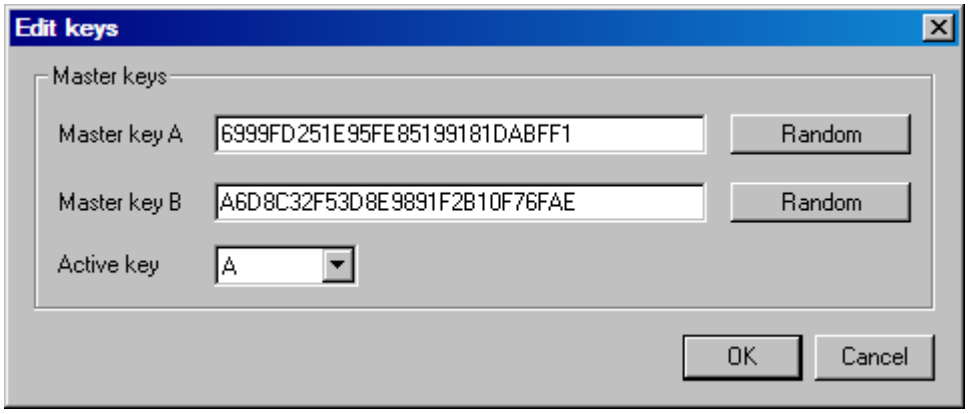
All software components have English user interface.

*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.

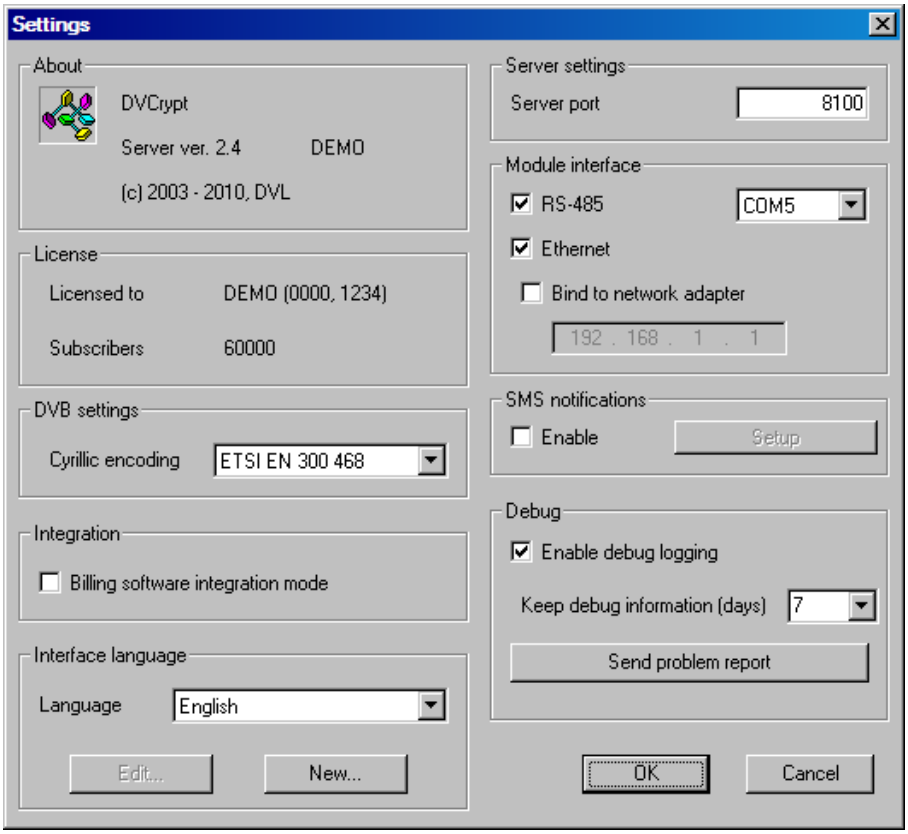
Click on the server icon in the traybar and select *Master keys* from the menu:




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:



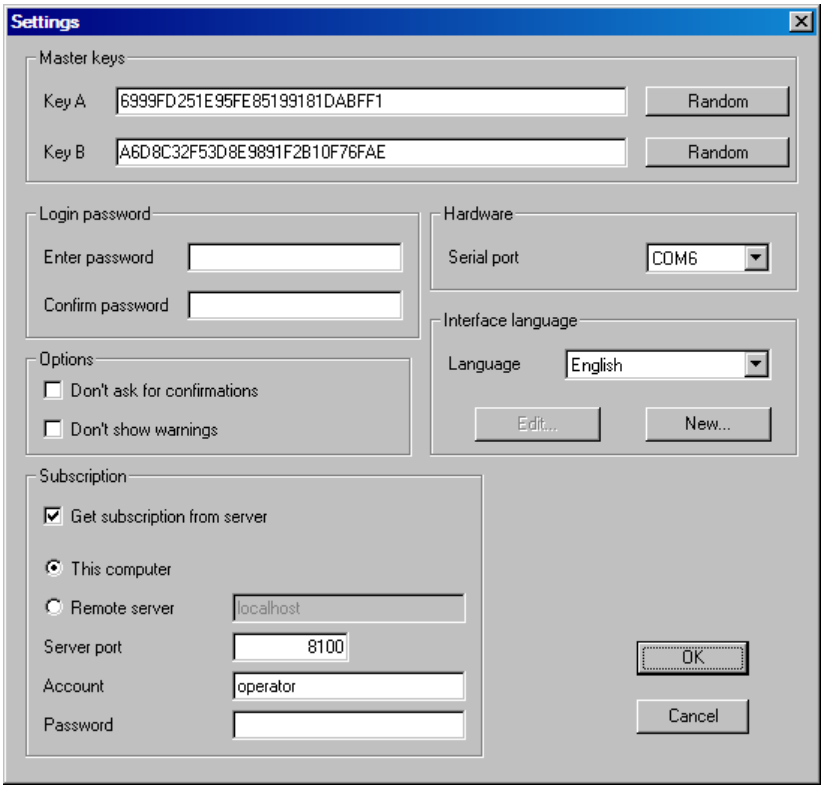

Check *RS-485* and select virtual serial port to which *USB <–> RS-485* converter is connected (refer to *3.3 Equipment connection* section above). If you're not using any modules with *RS-485* interface, uncheck *RS-485* checkbox.

Check *Ethernet* checkbox if you're using modules with *Ethernet* interface. 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*:




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

Select virtual *serial port* to which smartcard programmer hardware is connected.

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.

### 3. 7 Configuring channels and bouquets

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

Subscriptions are managed on *bouquet* basis. You can broadcast up to 8 different bouquets, each having up to 128 *programs* (TV channels). Each subscriber can view any combination of bouquets.

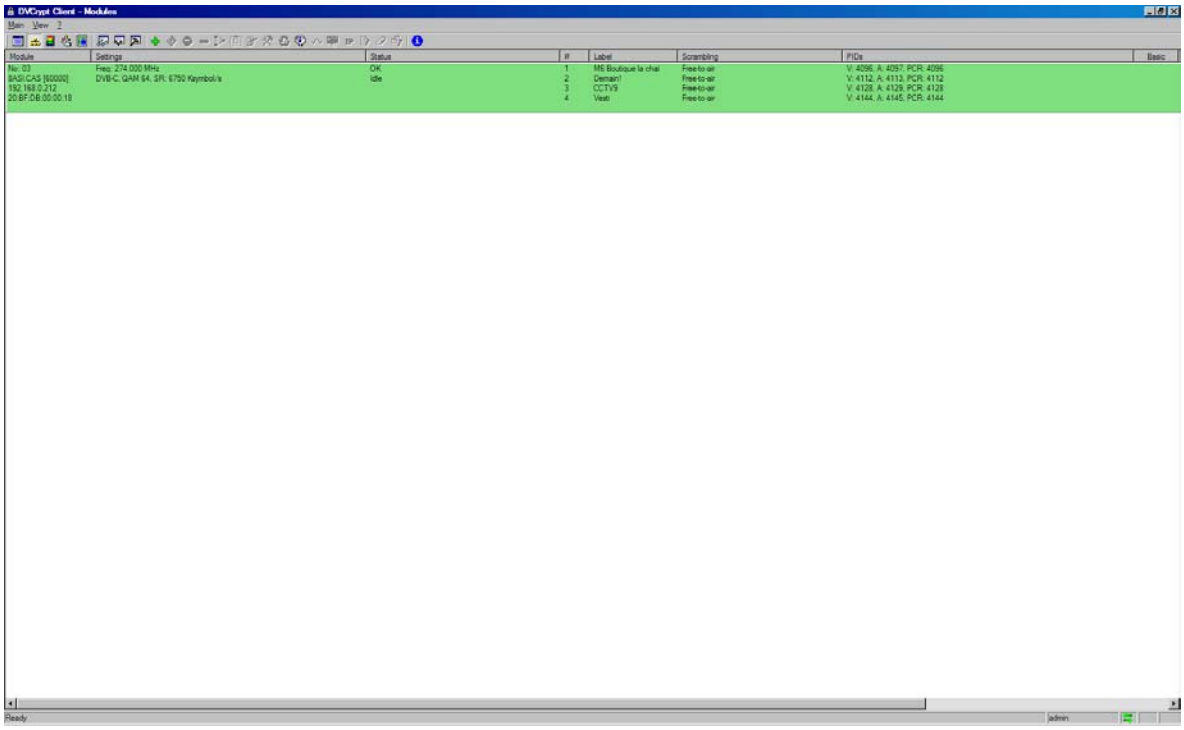
Select *View – Programs* from the menu. Enter names for all programs you intend to broadcast.

Select *View – Bouquets* from the menu. Enter names for all bouquets you intend to broadcast. Select programs included in each bouquet. Note that one program may belong to more than one bouquet.

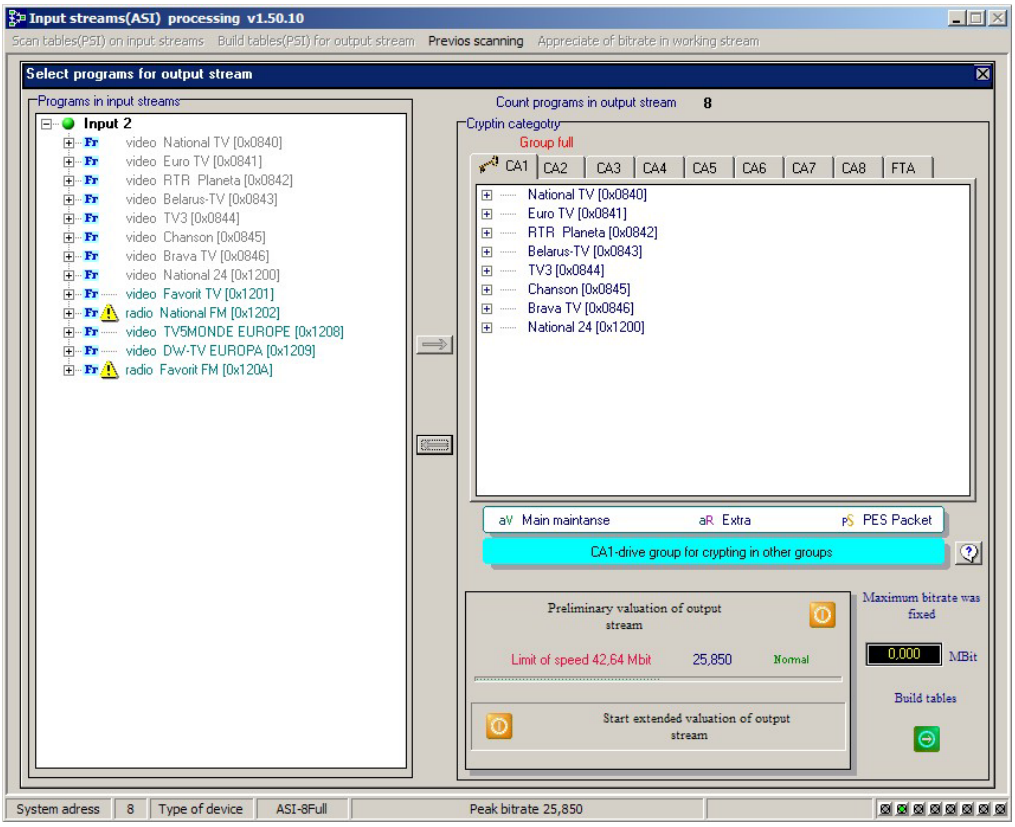
You may choose not to encrypt some of the channels. These channels are not included in the bouquets and can be viewed by any subscriber, even with no smartcard!

### 3. 8 Configuring modules

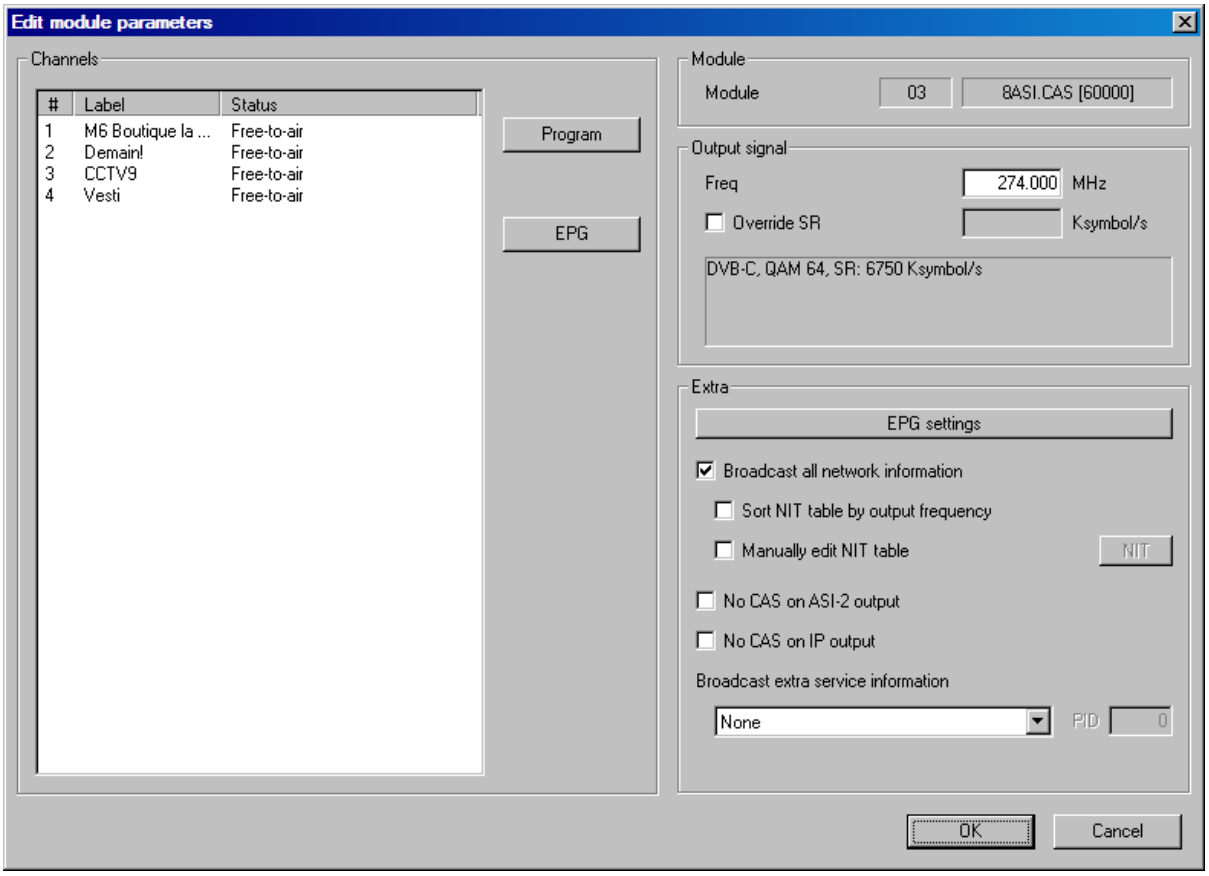
Select *View – Modules* from the menu. Click on *Add new module* icon and follow the wizard prompts. The wizard will help you connect each of the modules to the system one by one:



For modules with *ASI* digital 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 TV channels to include in the output stream:



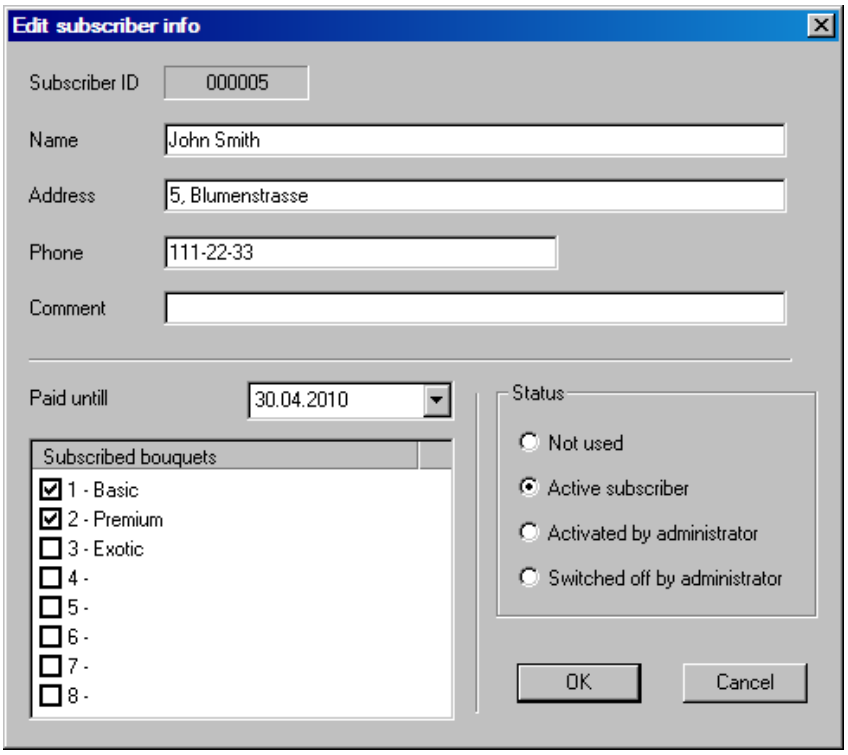
After all modules are added, double-click on each of them to change the *settings*:




Enter output signal *frequency*. Click on each *program*, correct the *label* (channel name) if needed, and select *conditional access mode* for the program. If you choose to encrypt the channel (*scrambled*), select the logical program number for this channel.

### 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):




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:

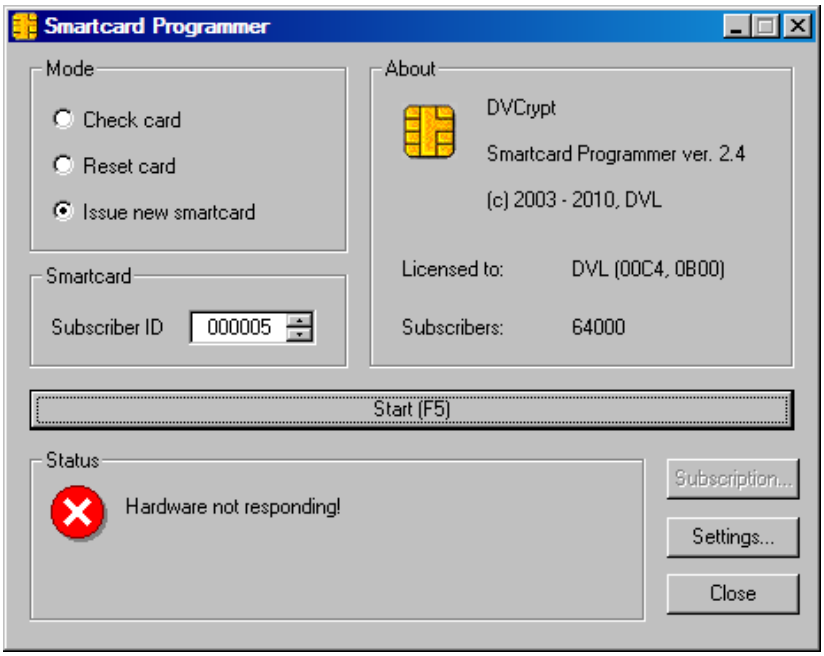
- *Active* – subscriber can watch enabled *bouquet(s)* as long as the *paid until date* is extended. If the *paid date* is reached, subscription is closed and would reopen only if a future *date* is entered. Subscription is automatically checked on each midnight as long as the server is running. This 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 smartcard reaction to any subscription changes is not immediate! Subscriber might have to wait 3-5 minutes before the command reaches the card.***

### 3. 10 Issuing smartcard

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.

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




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.