MULTICLET®

www.multiclet.com

USER MANUAL

Key_P1 MultiClet

Digital guardian

Abstract

The present document is a user manual for operating the Key_P1 MultiClet Digital guardian information system. The general information about the Key_P1 device, its functions, features of its installation and operation are specified in the document. Before installation and operation of the Key_P1 device it is necessary to study the present guide attentively. The Key_P1 device must be operated following the general safety precautions and physical security of the PC. Device available to order on telephone or in the web-site. Cryptographic functions can not modified by user. The device Key_P1 MultiClet is patented by MultiClet corp. User install application "Key_P1 Manager" independently, next support is software update.

Note: Key_P1 inititalization, random, corporate key generation must execute on secure PC.

Contents

Abbrevation list

PC — personal computer;

CS — computer-based system;

SW — software;

FW — firmware;

RAM — random-access memory;

DET — data encryption tool;

PIN — password to access the device;

OS — operating system;

IS — information system;

Key_P1 — digital guardian «Key_P1 MultiClet».

1 General information

1.1 Description and purpose

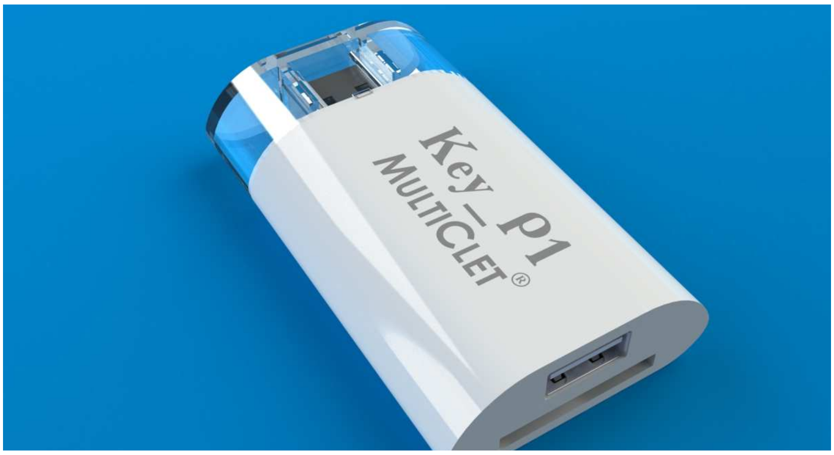


Figure 1: Digital guardian Key_P1 MultiClet

Key_P1 MultiClet digital guardian (fig. 1) is a multifunctional information system cryptographically protected and containing software and hardware encryption according to GOST 28147-89.

Key_P1 was developed on the basis of Russian multicellular processor with a universal non-von Neumann architecture. This multifunctional device will secure the data against loss, theft and unauthorized access. Key_P1 has a full set of necessary hardware functions and algorithms of data protection as well as a set of drivers and libraries to use the cryptographic functions. Key_P1 works on PC with Windows XP, Windows 7, Windows 8, Linux 2.6.x, Linux 3.x. (MacOS in terms of SW development).

The basic functionality of Key_P1:

- hierarchical access management to data. There is a possibility to control the users' access rights to the encrypted information (for example between the enterprise departments or according to the types of work (projects);

- synchronized keys management for remote enrypted data exchange in the open channel of data transfer;

- files encryption on the hard disk of the PC or portable data media (USB flash disks, MicroSD, MiniSD, MMC and SD cards);

- divide memory on public and private partition on the mass storage devices (USB flash disks, MicroSD, MiniSD, MMC and SD cards);

- storage of users' passwords and logins in the protected memory of the device. Access to this information is given only after typing the authentication password (PIN). This function makes it possible to protect the password data for access to the open mail resources like mail.ru from unauthorized access;

- prevention of information leak from the corporate computers to portable data media;

- log of the main actions made by the user (the journal describes the events directly connected with the device functionality).

Additional description of Key_P1 features:

Hierarchical access to information	The security service of the company will be able to create different rights of the departments to access to the company information. The head will have access to all files. Employees can encode files to their colleagues using Key_P1 Manager with the appropriate level of access.
Supervise	Information security service of the company can block of recording information from corporate computers on removable drives. Key_P1 will block any unauthorized entry of confidential data, viruses or other programs on the drive at the hardware level. It will be set the mode "read only". Information cannot be written to the drive in this mode, but the user can obtain permission from the Information security service to write to the drives.
Protection against spyware flash drives (problem badUSB)	Key_P1 allows connection only conventional data storage devices. Work of the "spy device" (presented at the same time keyboard and storage) will be blocked.
The ban on "off " mode	Key_P1 remains in the "event log " main events performed by the user. Viewing the "event log" can be closed for user. Unlock of the viewing is possible by administrator PIN-code. The worker is not able to quietly withdraw the device Key_P1 for load corporative data on the flash drive. Any attempt to disconnect of Key_P1 will be fixed by the security service.
An employee on a business trip	Users can create the equal keys to exchange encrypted messages with each other or with the head office of the company in case of communication during business trips using the open e-mail and other Internet resources.
Strong encryption	Encryption of information is possible on the external drives and internal HD of the computer. Encryption is performed by algorithm GOST 28147-89 with width of the key 256-bit. This algorithm encrypt information on the drive using protected method - by sectors (decryption will require thousands of years of computer time).
Data invulnerability	The user has the ability to create backups of encrypted information. In case of loss or damage Key_P1 and/or storage, the user will be able to recover your information. The device useless for the attacker in case of its loss. If the device is lost, it cannot be used for any purpose related with encryption and decryption, as well as to retrieve information about the principles of operation of similar devices.
Support at multiple drives	The device supports drives of the type SD, micro SD, and USB. You can use an USB extension cable, if the size of the landing USB port on the computer is insufficient.
The using of different operating systems	The device is supported in the operating systems Windows XP, Windows 7, Windows 8, Linux x, Linux 3.x and after development and renewal of the software MacOS also.
Safe Password	The device allows you to save user passwords and logins on the internal protected memory device Key_P1. The user can copy username to clipboard of the operating system and paste in the appropriate field for login. For password, you can do a similar operation. This ensures convenient use and storage of your passwords, as well as protection against key loggers on your PC.

1.2 Rules for information protection

To apply the Key_P1 device effectively and to maintain the desired level of protection of the PC and information resources of CS it is necessary to provide the following:

- Key_P1 device safety;

- keeping in secret the device access code (PIN code);

Apart from these measures it is necessary to make a regular routine backup of the encrypted data and encryption keys to have a possibility to recover this information on the new Key_P1 device. For more details of the procedure of the backup and recovery read chapter 2.4 «Device initialization».

DO NOT:

- leave without control the PC which run Key_P1 after inputting PIN code;

- make any changes in the Key_P1 software;

- copy the confidential information without any authorization of the security manager;

- disclose the content of the key data media or give the media to the persons not authorized to use them, present the key data on the screen, print them or present them by any other means of data presentation;

- use the device in the modes not provided for the Key_P1 functionality;

- record the extraneous data on the storages init by Key_P1;

- open the device case.

1.3 System requirements

Before starting to install and adjust the Key_P1 device it is necessary to make sure that your workstation satisfies the minimum system requirements. The requirements are given in table 1.

Table 1. System requirements.

Key_P1 device can be used on any PC equipped with the following requirements:	• WindowsXP (SP3); • Windows 7; • Windows 8; • Linux 2.6.x; • Linux 3.x.
Necessary hardware conditions	USB port

1.4 Device mark

Key_P1 device marking applied on the back side of the case.

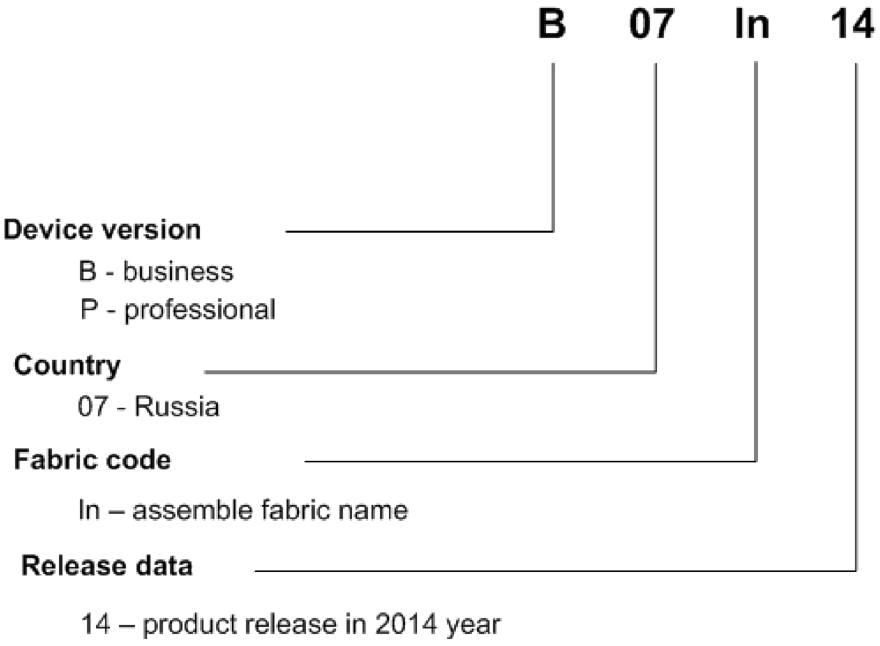


Figure 2: Device mark

1.5 Technical parameters

Table 2. Technical parameters.

Function	device purpose is encrypting middle size of data
Speed	with public partition under 3,2 Mbit/sec, with private partition and other ecnrypting - under 1,2 Mbit/sec
Support USB types	1.1, 2.0, 3.0
Support storages types	USB, SD, microSD, miniSD, MMC
Random key max count	1024
Synchro key max count	104
Corporate key max count	512
Corporate key group max count	512
Login and pass list max count	200
Login and pass group max count	32
Event log list max count	1024
Time log list max count	1024
The length of the encryption key	for Key_P1 devices which are on sale in the Russian Federation - 256 bit, for Key_P1 devices exported outside of Russian Federation - 56 bit

2 Installation and adjustment of the Key_P1

2.1 Brief decription of the installation procedure

As a first step plug Key_P1 Multiclet device to PC USB port, and find at the device connection list (in Windows OS at "My computer") Key_P1 and open it (with double mouse left key click). Open "readme" file. Then click link "Download Software" appropriate to installed OS on PC. Before start Key_P1 Multiclet needed install downloaded application Key_P1 Manager. And accordingly to this user manual necessary with Key_P1 Manager complete following steps:

1) Install internal device firmware

2) Initialize device

3) Initialize storages

Internal firmware installation descibe in "Update internal firmware" chapter.

Device initialization contain following steps:

1)Setting 1024 keys

2)Setting administrator PIN code

3)Setting user PIN code

4)Setting alarm PIN code

5)Setting device label

Storages initialization USB and SD types contain following steps:

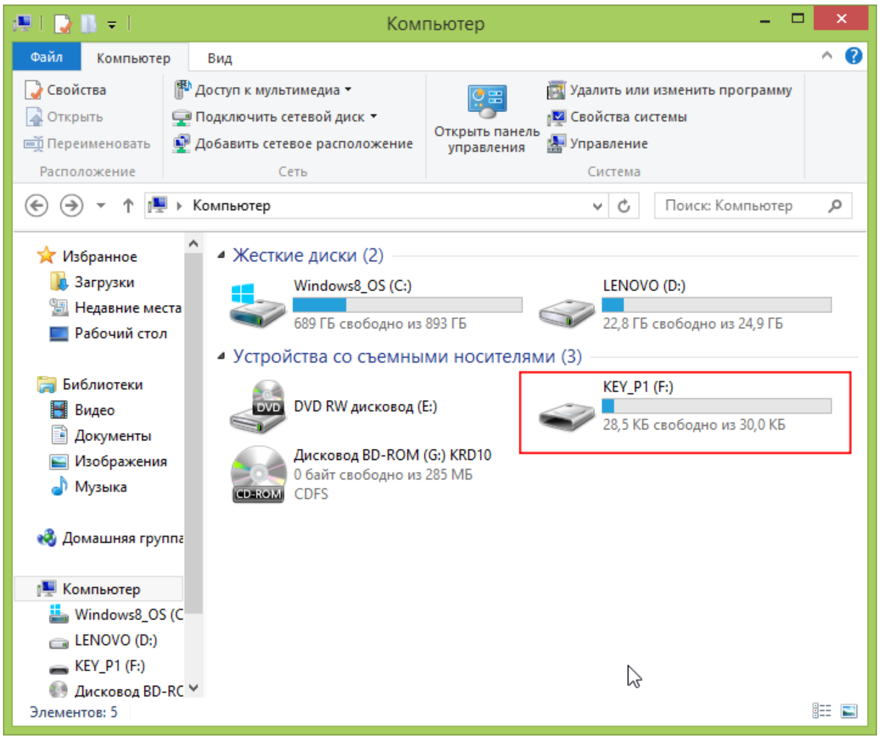
1)Divided on two partition (public and private)

2)Setting partition labels

Note that number of storages, which can work with Key_P1 device not limited. Key_P1 Manager application not required installation on PC, it means that after device initialization procedure application may be install on removable storage device(enough make copy Key_P1 Software directory). If needed work in OS Windows and OS Linux, that necessary make copy two application versions.

2.2 Software installation

Connect Key_P1 device to USB port of PC. Then device display at the system as removable storage(see example for OS Windows 8 at the picture 3). In the next step open(for example with double mouse click) removable storage Key_P1 and find readme file with html extension. View of the readme file shown at the picture 4



Жесткие диски (2)

Windows8_OS (C:)
689 ГБ свободно из 893 ГБ

LENOVO (D:)
22,8 ГБ свободно из 24,9 ГБ

Устройства со съемными носителями (3)

DVD RW дисковод (E:)

KEY_P1 (F:)
28,5 КБ свободно из 30,0 КБ

Дисковод BD-ROM (G:) KRD10
0 байт свободно из 285 МБ
CDFS

Figure 3: First connection of the Key_P1 MultiClet

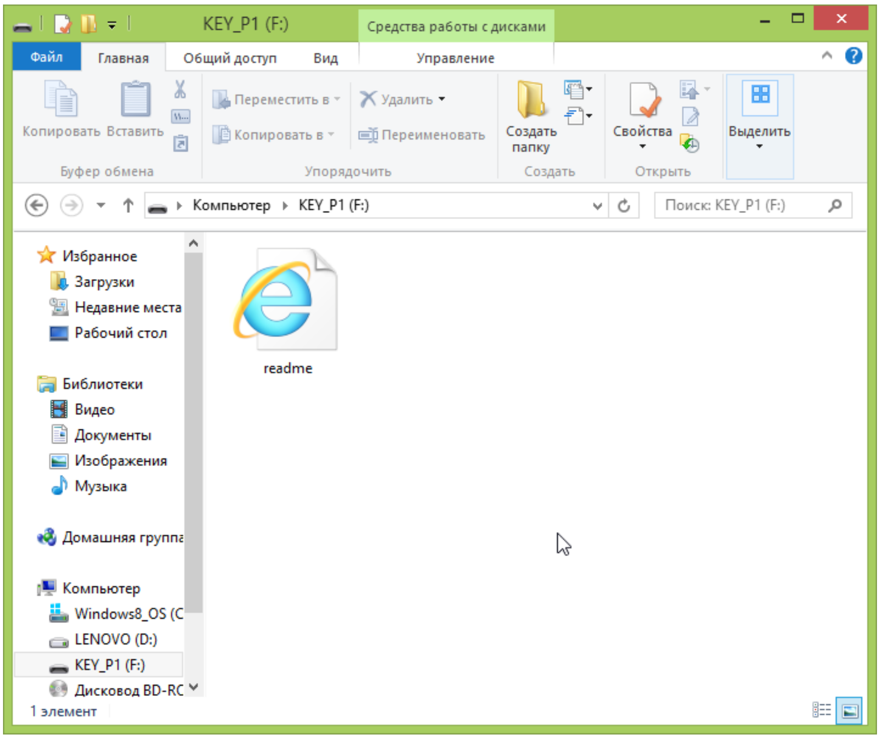
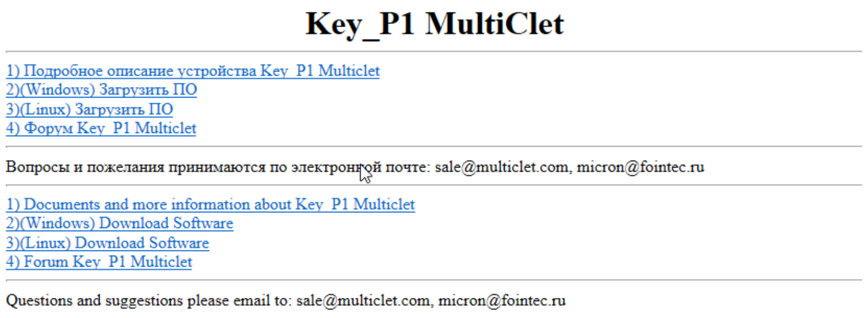


Figure 4: Help readme file on Key_P1 MultiClet

In order to get useful information about software download and available documentation about Key_P1 MultiClet device open(for example with double mouse click) readme file. If you can not open this file with default internet browser, attempt to launch readme file with other installed browser. Readme file content shown at the picture 5



Key_P1 MultiClet

1) Подробное описание устройства Key_P1 Multiclet
2)(Windows) Загрузить ПО
3)(Linux) Загрузить ПО
4) Форум Key_P1 Multiclet

Вопросы и пожелания принимаются по электронной почте: sale@multiclet.com, micron@fointec.ru

1) Documents and more information about Key_P1 Multiclet
2)(Windows) Download Software
3)(Linux) Download Software
4) Forum Key_P1 Multiclet

Questions and suggestions please email to: sale@multiclet.com, micron@fointec.ru

Figure 5: Readme file content of the Key_P1 MultiClet

Choose link for your OS. For OS Windows click link "(Windows) Download software". If downloading not start click link below:

1)If the PC has an installed OS of Windows family choose the link :

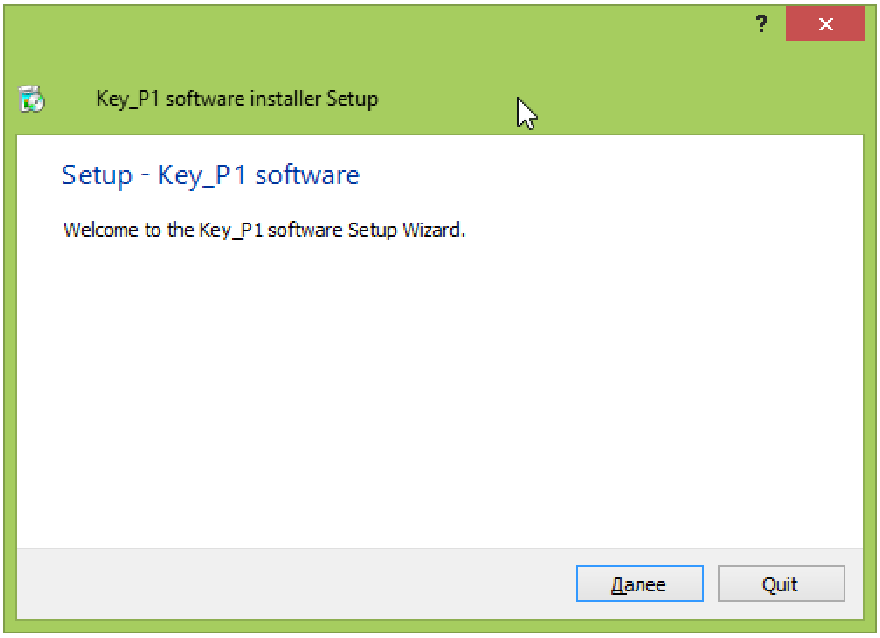
http://multiclet.com/docs/PO/Key_P1/Key_P1_Software_Installer.exe.

2)If the PC has an installed OS of Linux family choose the link :

http://multiclet.com/docs/PO/Key_P1/Key_P1_Software_Installer.tar.gz.

To install the software on the PC start the setup file **Key_P1_Software_Installer.exe** (OS Windows) or **Key_P1_Software_Installer.tar.gz** (OS Linux).

The installation wizard will start. Then follow the instructions of the installation wizard. After finishing all the actions the application will be installed on the PC.



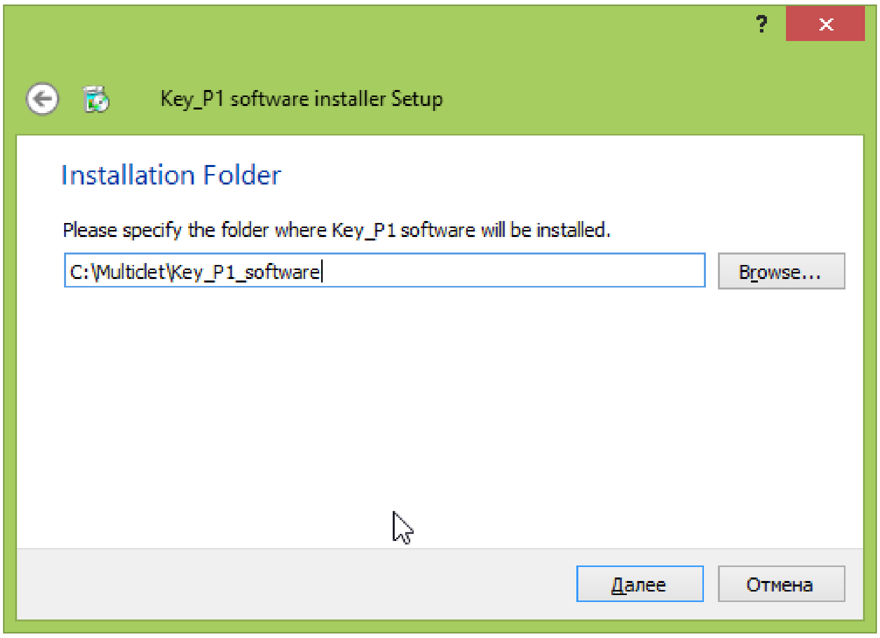
Key_P1 software installer Setup

Setup - Key_P1 software

Welcome to the Key_P1 software Setup Wizard.

Figure 6: Installation wizard

Installation wizard request installation path. Default path: "C:/Multiclet/Key_P1_software". Window with path request show at picture 7 Click Next button to continue.



Key_P1 software installer Setup

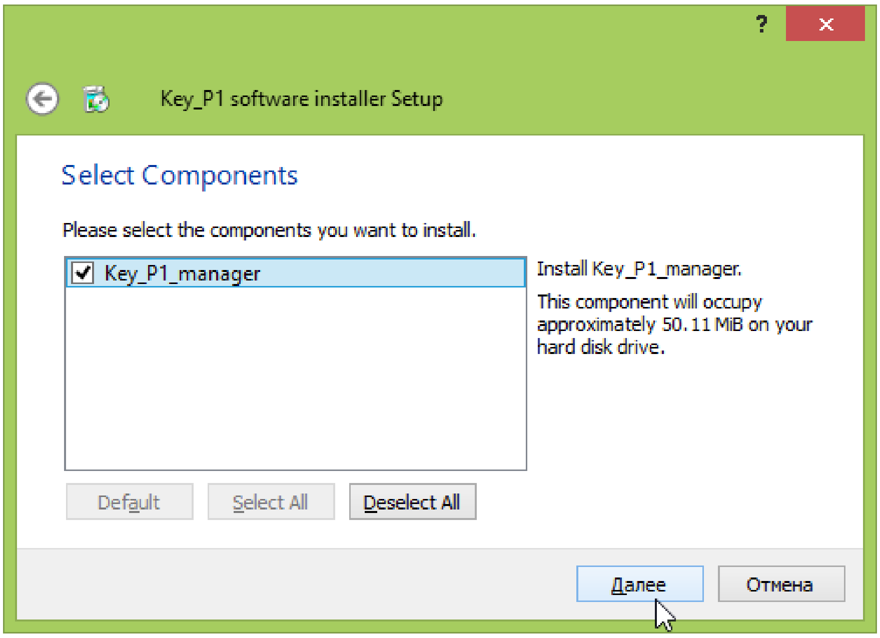
Installation Folder

Please specify the folder where Key_P1 software will be installed.

C:\Multiclet\Key_P1_software

Figure 7: Path request window

Then component choose window will be display. At this moment ready only one option. Click button "Next" to continue. Components choosing window show at the picture 8



Key_P1 software installer Setup

Select Components

Please select the components you want to install.

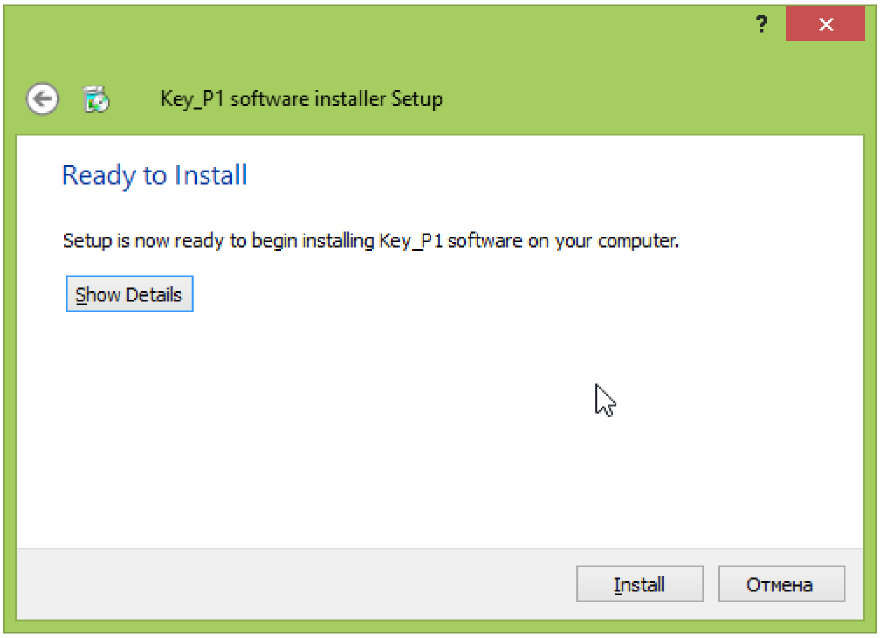
☑ Key_P1_manager

Install Key_P1_manager.

This component will occupy approximately 50.11 MiB on your hard disk drive.

Figure 8: Components choosing window

In the appeared window click "Install" button to continue installation. Window with installation option shown at the picture 9

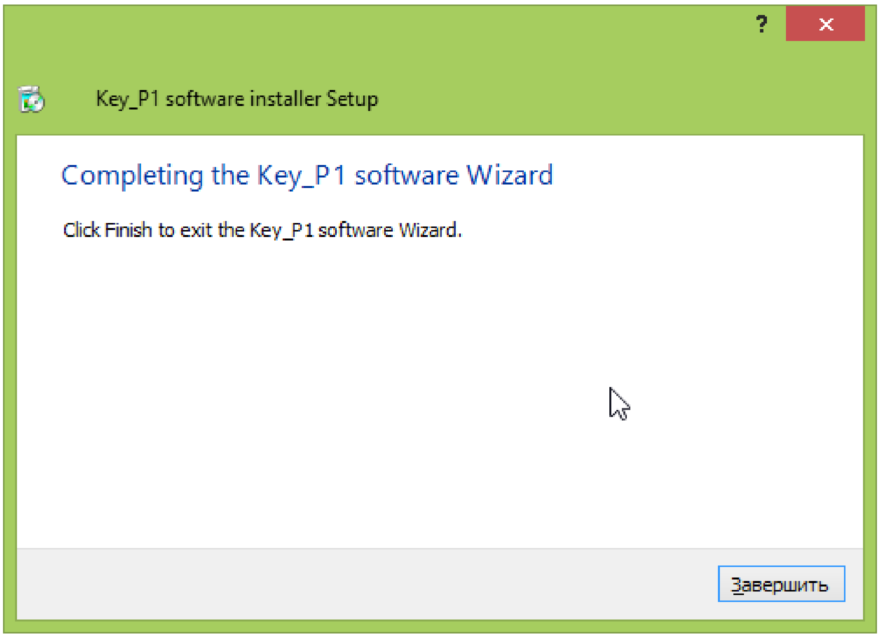


Ready to Install

Setup is now ready to begin installing Key_P1 software on your computer.

Figure 9: Window with installation parameters

After installation finish click Complete button. Finish window shown at the picture 10



Key_P1 software installer Setup

Completing the Key_P1 software Wizard

Click Finish to exit the Key_P1 software Wizard.

Figure 10: Installation finish

2.3 Key_P1 Manager application start

After installing software package on the PC it is necessary to start **Key_P1 Manager** application . To do this start the shortcut **Key_P1_Manager.lnk** located on your PC desktop or start the application in the following way **Start-> All programs-> Key_P1->Key_P1 Manager**.

After starting the application a shortcut Key_P1 Manager (put in a red rectangle) will appear in the right bottom corner of the desktop (in the system tray on the task bar). The icon display in the task bar, as see in fig.11).

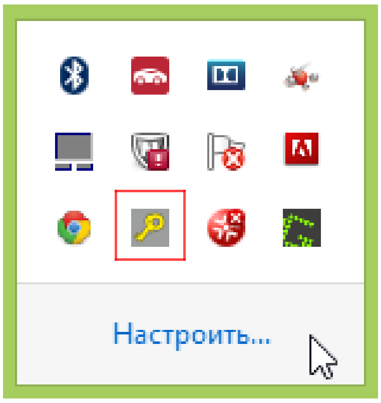
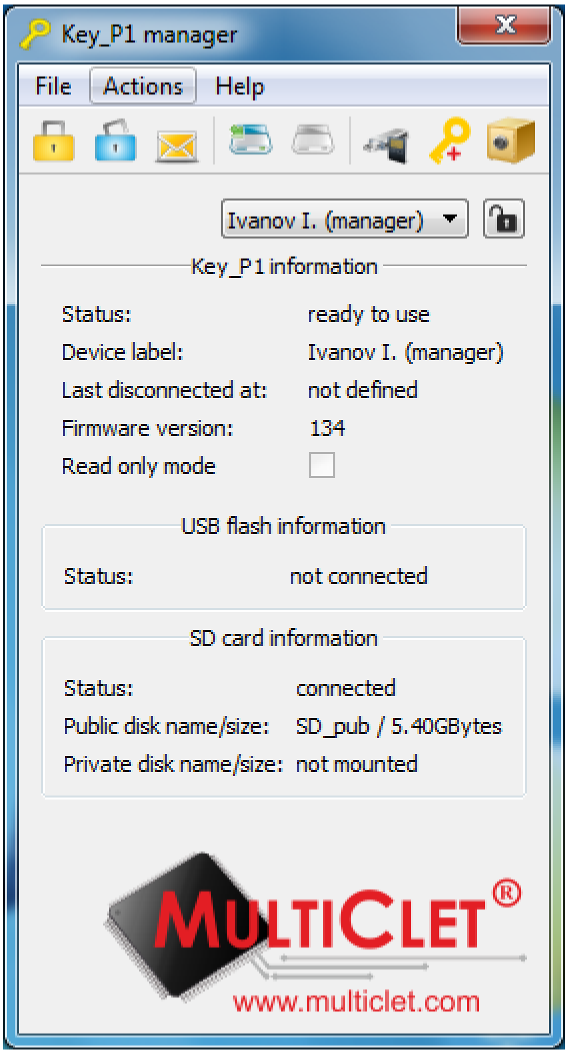


Figure 11: Icon in the system tray

User must have **root** level access for working with Key_P1 device on PC with OS Linux.

2.4 Description of the Key_P1 Manager application interface

The main menu of the Key_P1 Manager application looks like as shown in the fig. 12.



Ivanov I. (manager)

Key_P1 information

Status: ready to use
Device label: Ivanov I. (manager)
Last disconnected at: not defined
Firmware version: 134
Read only mode □

USB flash information

Status: not connected

SD card information

Status: connected
Public disk name/size: SD_pub / 5.40GBytes
Private disk name/size: not mounted

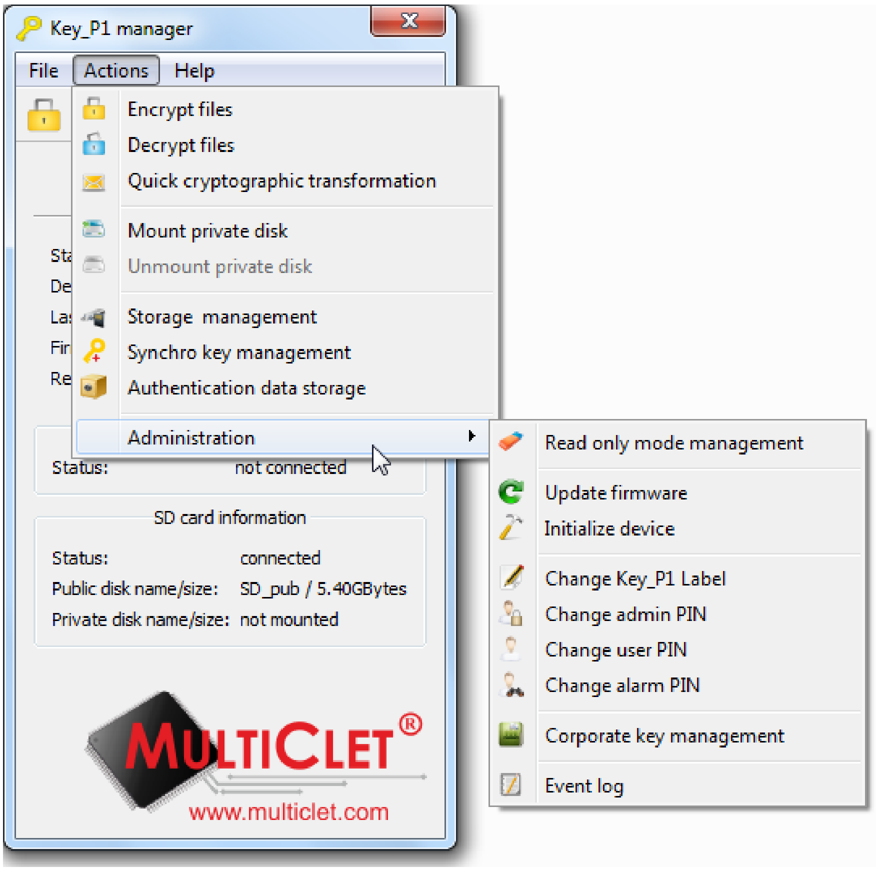
Figure 12: Main menu of the Key_P1 Manager

Menu consists of the following elements::

1) Top bar with tabs **File, Actions** и **Help**. The tab **File** consists of command **Close** and **Exit**. Starting the command **Close** will lead to folding of the application to the tray (the application will stay in the task bar). Starting the command **Exit** will lead to closing of the application.

The tab **Actions** includes the following commands: **Ecnrypt files, Decrypt files, Quick crypt transformation, Mount private partiton, Unmount private partition, Storage management, Synchro key management, Authentication data storage**

The tab **Actions** contain submenu **Administration**, which consists of the following: **Read only management, Update firmware, Initialize device, Change Key_P1 label, Change administrator PIN, Change user PIN, Change alarm PIN, Corporate key management, Log event**. Full description you can find in the next chapters. Content of the tab **Actions** shown in the fig. 13.



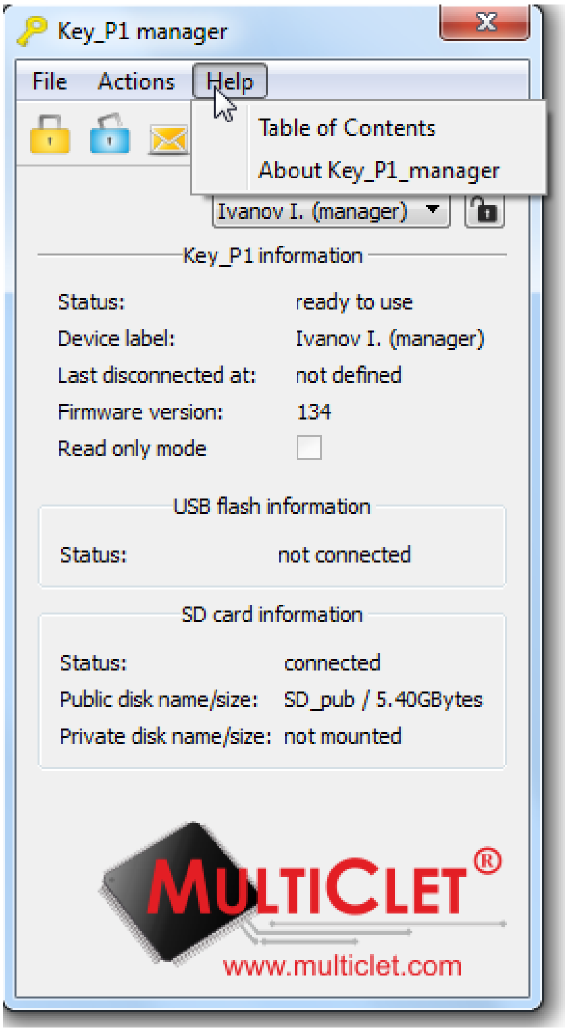
Status: not connected

SD card information

Status: connected
Public disk name/size: SD_pub / 5.40GBytes
Private disk name/size: not mounted

Figure 13: Tab Actions of the Key_P1 Manager

The tab **Help** contain usefull information about working with Key_P1. Content of the tab **Help** shown in the fig. 14.



Key_P1 information

Status: ready to use

Device label: Ivanov I. (manager)

Last disconnected at: not defined

Firmware version: 134

Read only mode □

USB flash information

Status: not connected

SD card information

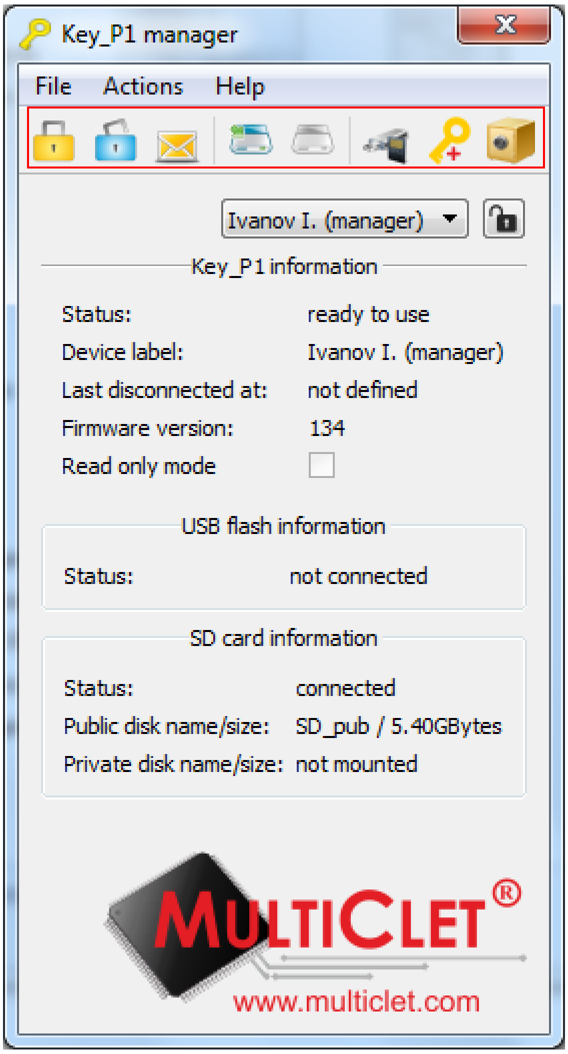
Status: connected

Public disk name/size: SD_pub / 5.40GBytes

Private disk name/size: not mounted

Figure 14: Tab Help of the Key_P1 Manager

2) Toolbar. Fully duplicates all the commands from the tab **Actions** except submenu **Administration**. Toolbar shown in the fig. 15 and highlighted in red line.



Key_P1 information

Status: ready to use
Device label: Ivanov I. (manager)
Last disconnected at: not defined
Firmware version: 134
Read only mode □

USB flash information

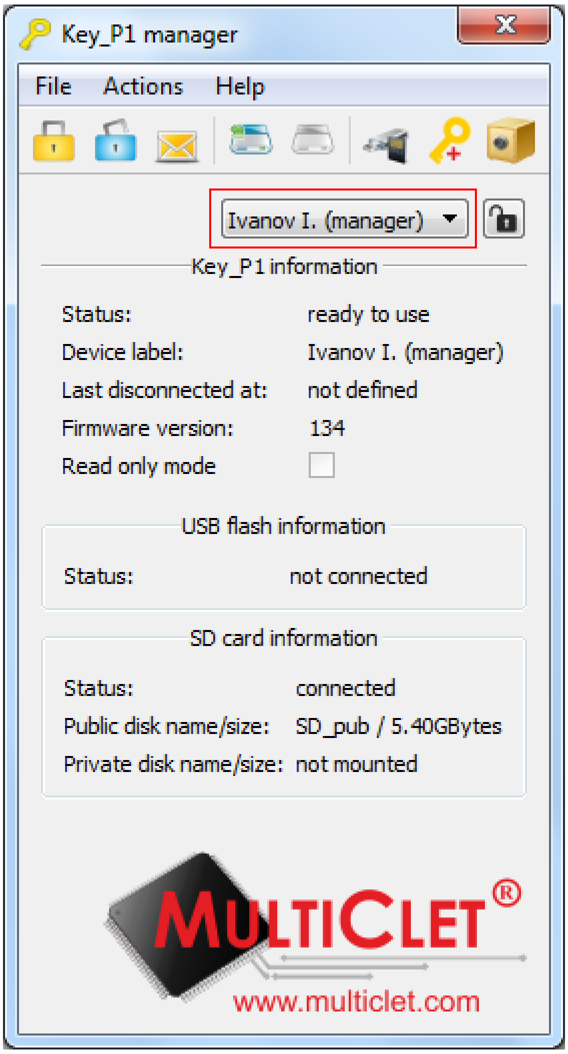
Status: not connected

SD card information

Status: connected
Public disk name/size: SD_pub / 5.40GBytes
Private disk name/size: not mounted

Figure 15: Toolbar of the Key_P1 Manager

3) Drop-down list of the attached devices of Key_P1. All the attached devices with the label display in this list. In the fig. 16 this list highlighted in red line.



Key_P1 information

Status: ready to use
Device label: Ivanov I. (manager)
Last disconnected at: not defined
Firmware version: 134
Read only mode □

USB flash information

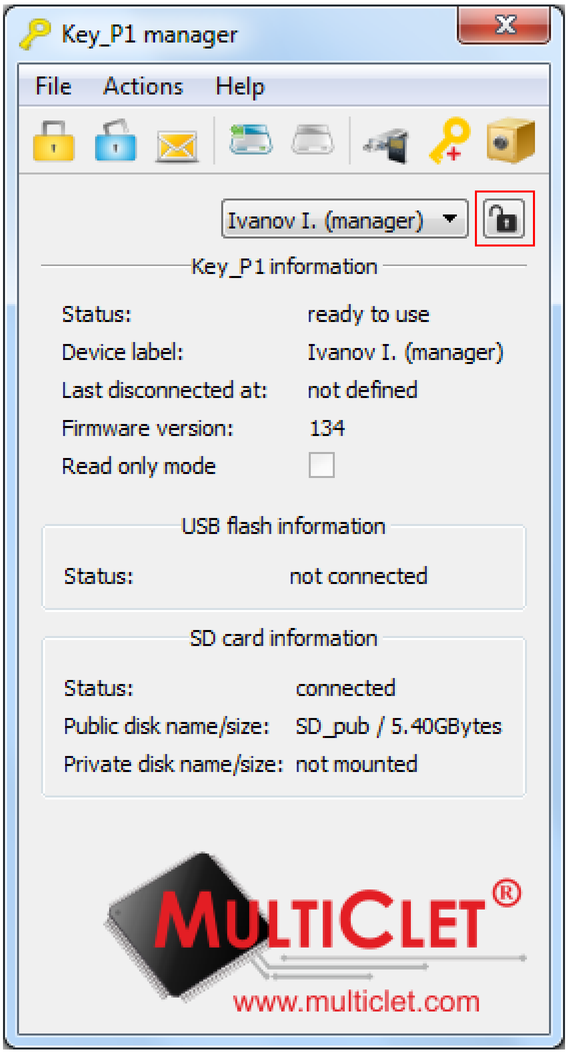
Status: not connected

SD card information

Status: connected
Public disk name/size: SD_pub / 5.40GBytes
Private disk name/size: not mounted

Figure 16: List of attached devices Key_P1

4) Button **Unlock user PIN code** shown in the fig. 17 and highlighted in red line.



Status: ready to use
Device label: Ivanov I. (manager)
Last disconnected at: not defined
Firmware version: 134
Read only mode □

Status: not connected

Status: connected
Public disk name/size: SD_pub / 5.40GBytes
Private disk name/size: not mounted

Figure 17: Button unlock user PIN code

5) Area **Information about Key_P1**. This area contain **Device status, Device label (name), Last disconnection time, Firmware version, Read only mode**.

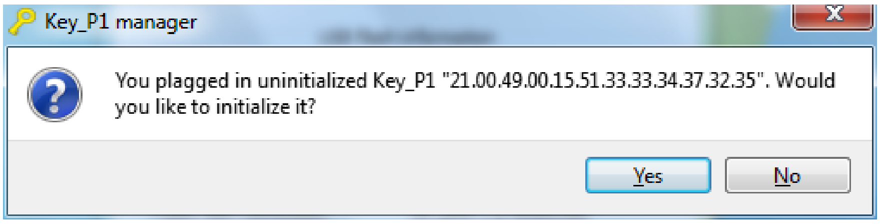
6) Area **Information about USB storage**. This area contain **Device status, Label/size public partition, Label/size private partition**

7) Area **Information about SD card**. This area contain **Device status, Label/size public partition, Label/size private partition**

2.5 Device firmware update

Update firmware (update FM) necessary make regulary, bacause ever new FM version improve Key_P1 Manager application and make work with it more stable and functionality.

Start application Key_P1 Manager. Connect Key_P1 Multiclet device at the first time to PC and pop up message with request to install firmware as shown at the fig. 18. And press button "Yes" to continue. Update firmware and install firmware are identical procedures.

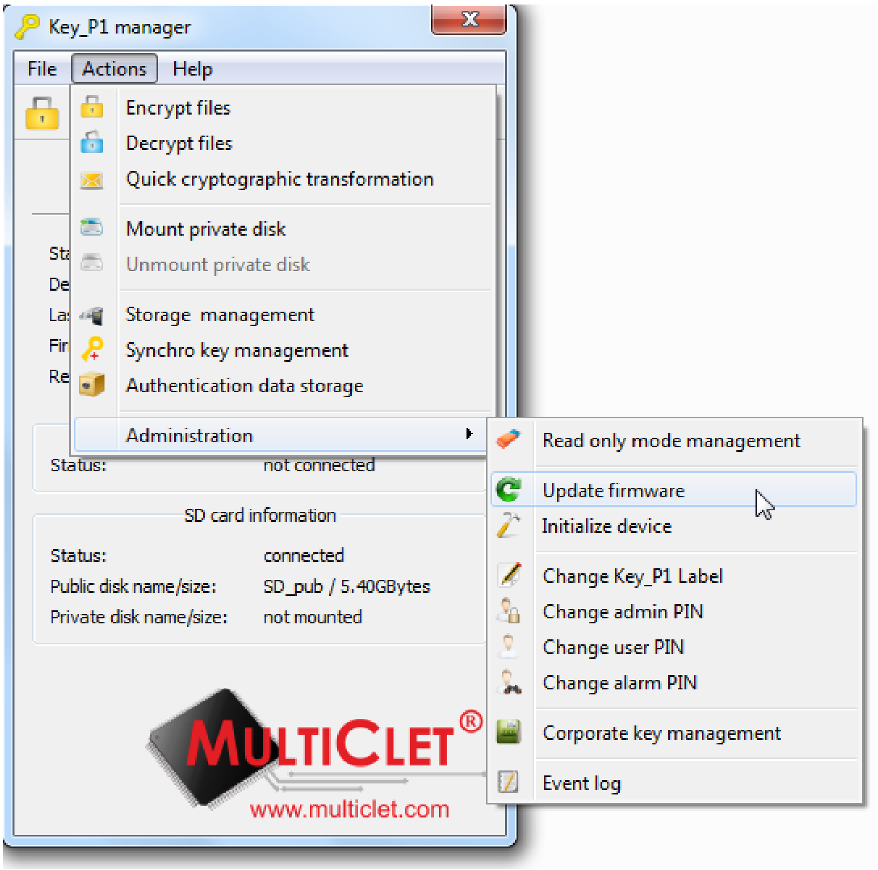


Key_P1 manager

You plagged in uninitialized Key_P1 "21.00.49.00.15.51.33.33.34.37.32.35". Would you like to initialize it?

Figure 18: Firmware install

In order to make update FM manually necessary at the main application menu choose tab **Actions** go to submenu **Administration** and select **Update firmware** item (fig. 19).



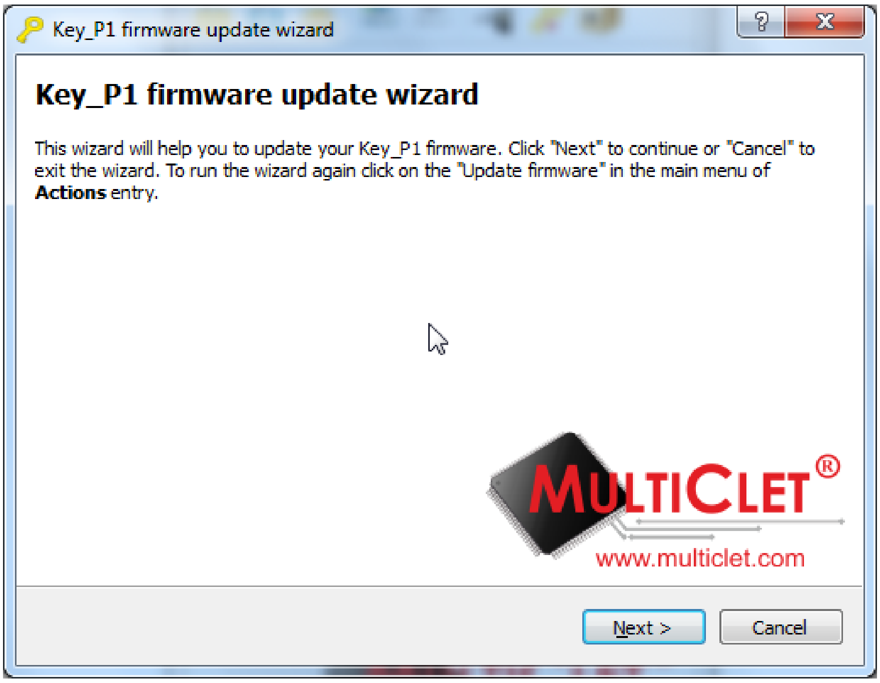
Status: not connected

SD card information

Status: connected
Public disk name/size: SD_pub / 5.40GBytes
Private disk name/size: not mounted

Figure 19: Firmware update

The window **Key_P1 update wizard** will be display (fig. 20). Press button «Next» to continue. Press button «Cancel» to abort update procedure.



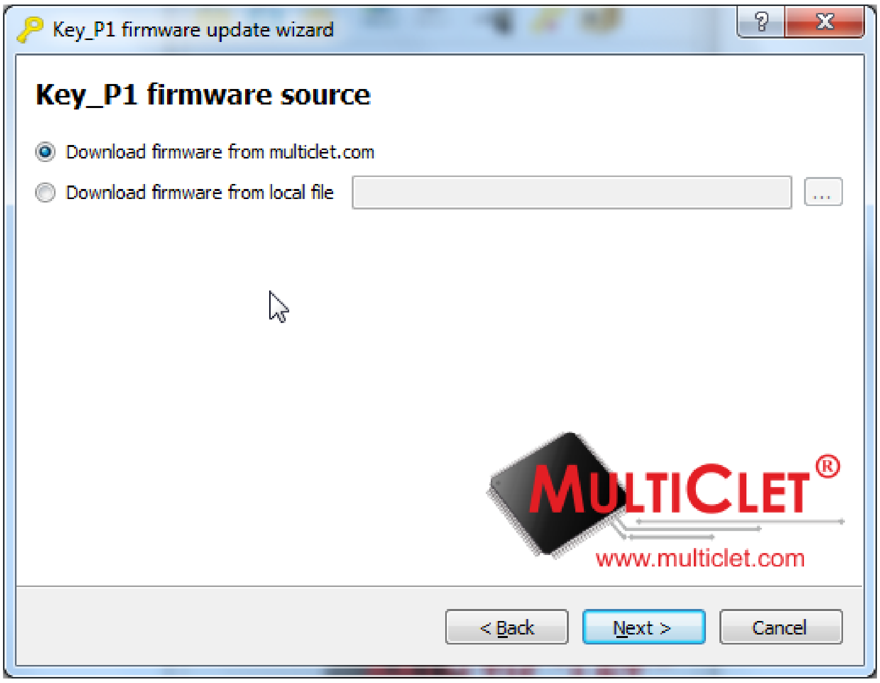
Key_P1 firmware update wizard

Key_P1 firmware update wizard

This wizard will help you to update your Key_P1 firmware. Click "Next" to continue or "Cancel" to exit the wizard. To run the wizard again click on the "Update firmware" in the main menu of **Actions** entry.

Figure 20: Firmware update wizard Key_P1

Next window - choice firmware update source. There are two options: from web-site http://multiclet.com or from file (fig. 21).



Key_P1 firmware update wizard

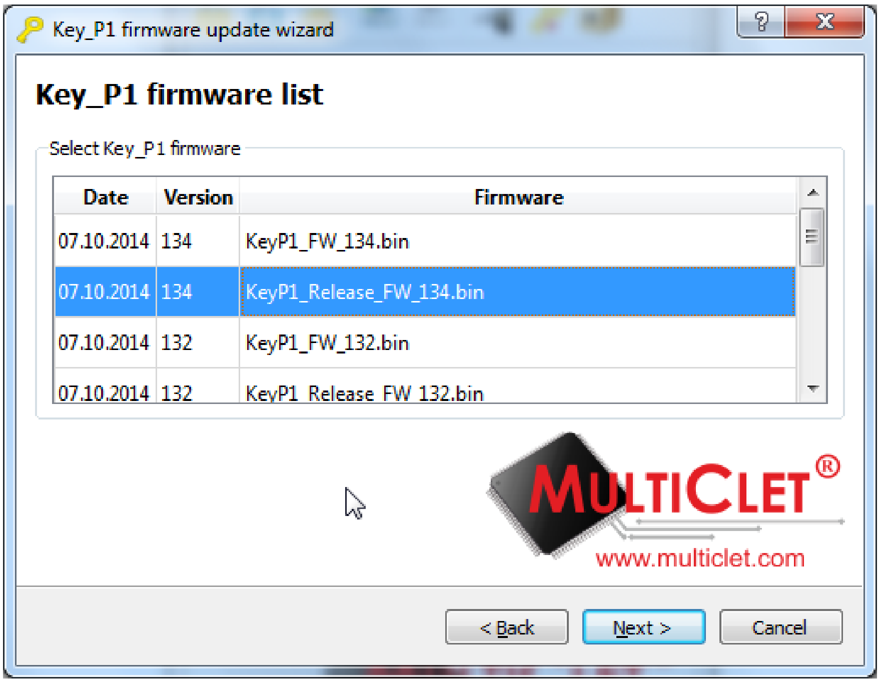
Key_P1 firmware source

● Download firmware from multiclet.com

○ Download firmware from local file

Figure 21: FM update source

As a default update from web-site http://multiclet.com and for it's way PC must be connect to Internet. Application connect to web-site and display **Firmware list** (fig. 22) with all firmware versions available to install. Choose appropriate firmware version and press button «Next».



Key_P1 firmware update wizard

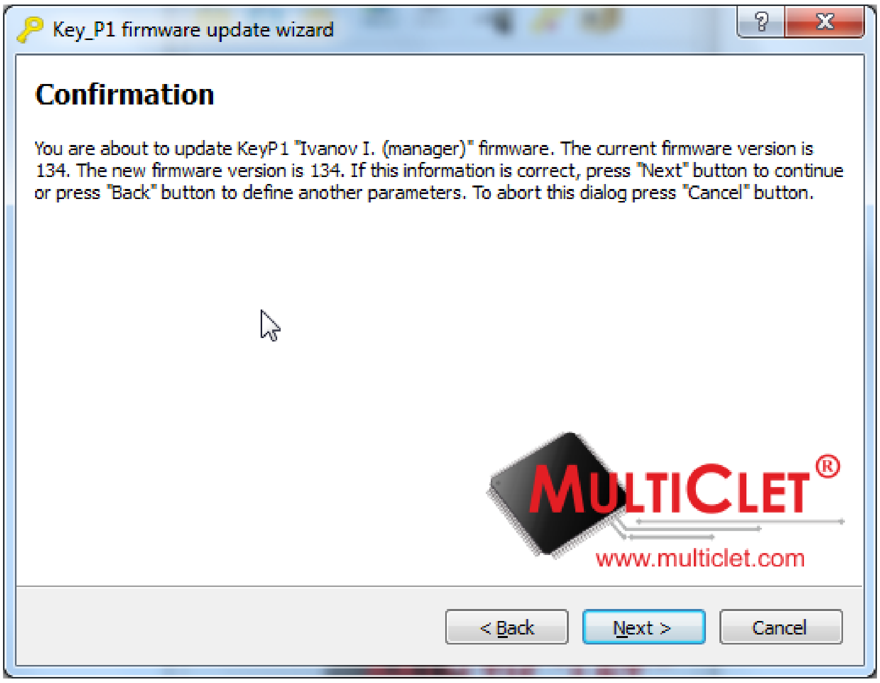
Key_P1 firmware list

Select Key_P1 firmware

Date	Version	Firmware
07.10.2014	134	KeyP1_FW_134.bin
07.10.2014	134	KeyP1_Release_FW_134.bin
07.10.2014	132	KeyP1_FW_132.bin
07.10.2014	132	KeyP1_Release_FW_132.bin

Figure 22: Key_P1 firmware list

If needed update FM from local file that necessary choose **Download firmware from local file** (fig. 23).



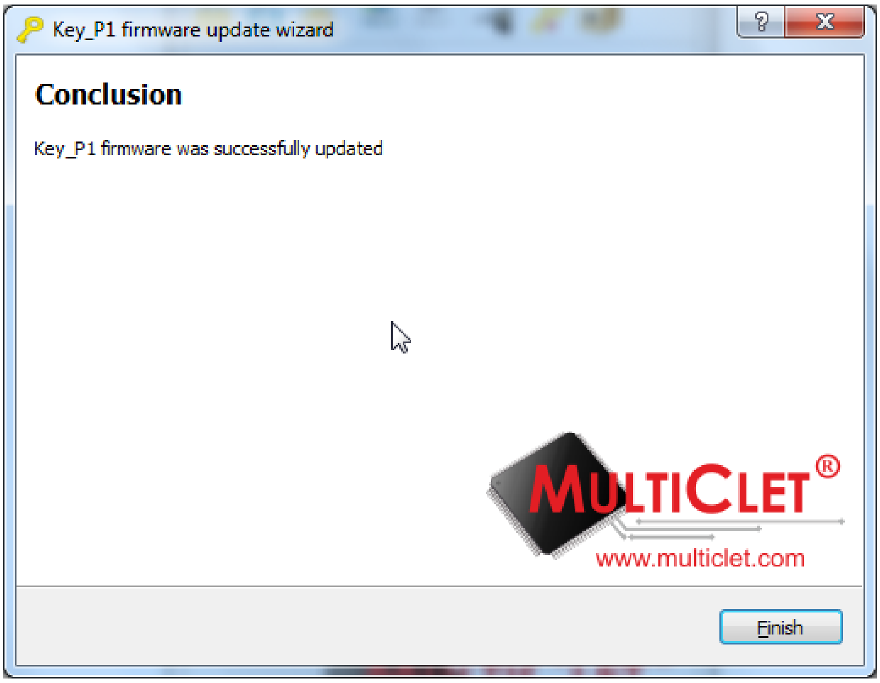
Key_P1 firmware update wizard

Confirmation

You are about to update KeyP1 "Ivanov I. (manager)" firmware. The current firmware version is 134. The new firmware version is 134. If this information is correct, press "Next" button to continue or press "Back" button to define another parameters. To abort this dialog press "Cancel" button.

Figure 23: Downloading firmware from local file

Then necessary set file path (fig. 24).



Key_P1 firmware update wizard

Conclusion

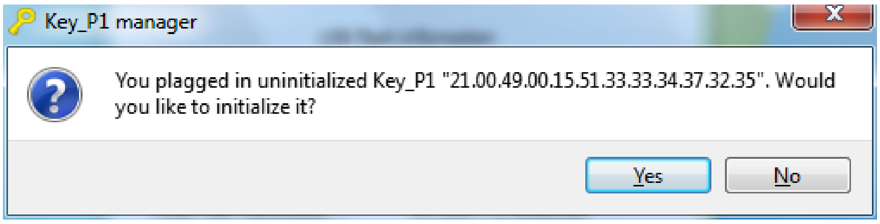
Key_P1 firmware was successfully updated

Figure 24: Updating firmware from local file

Enter administrator PIN and press button «OK» to continue update procedure. Update process will start after it.

2.6 Device initialization

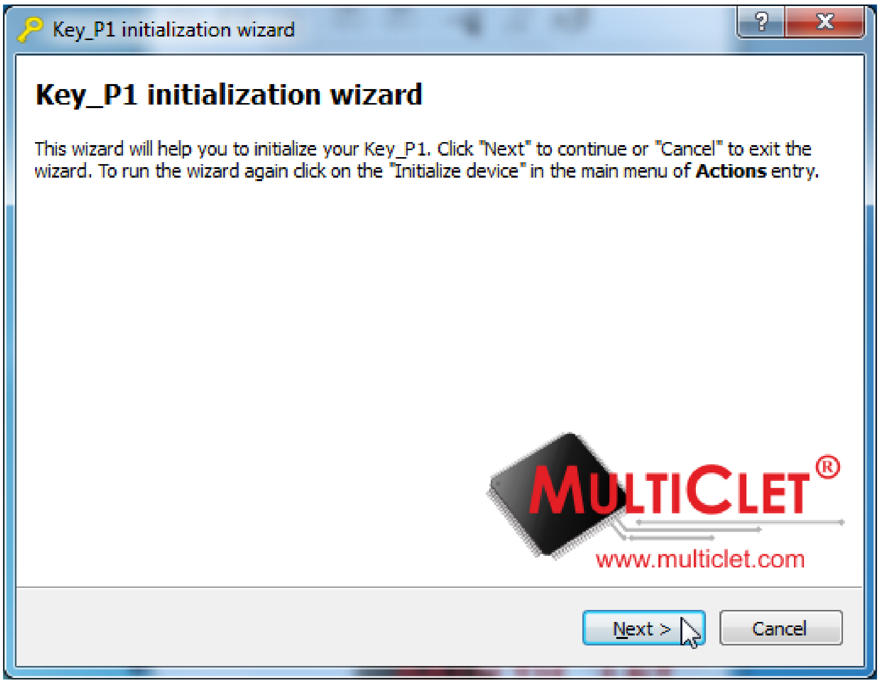
The following stage is to make device initialization. After start application Key_P1 Manager necessary connect Key_P1 Multiclet device to PC. Message about device initialization will be pop up(if device not initialized), see fig.25. Press "Yes" button to continue.



You plagged in uninitialized Key_P1 "21.00.49.00.15.51.33.33.34.37.32.35". Would you like to initialize it?

Figure 25: Start initialization Key_P1 device

Initialization wizard will be start, as see in fig.26. Also initialization wizard can be start manually, to do this in the main menu necessary select tab **Actions**, choose submenu **Administration** and select **Initialize device** item.

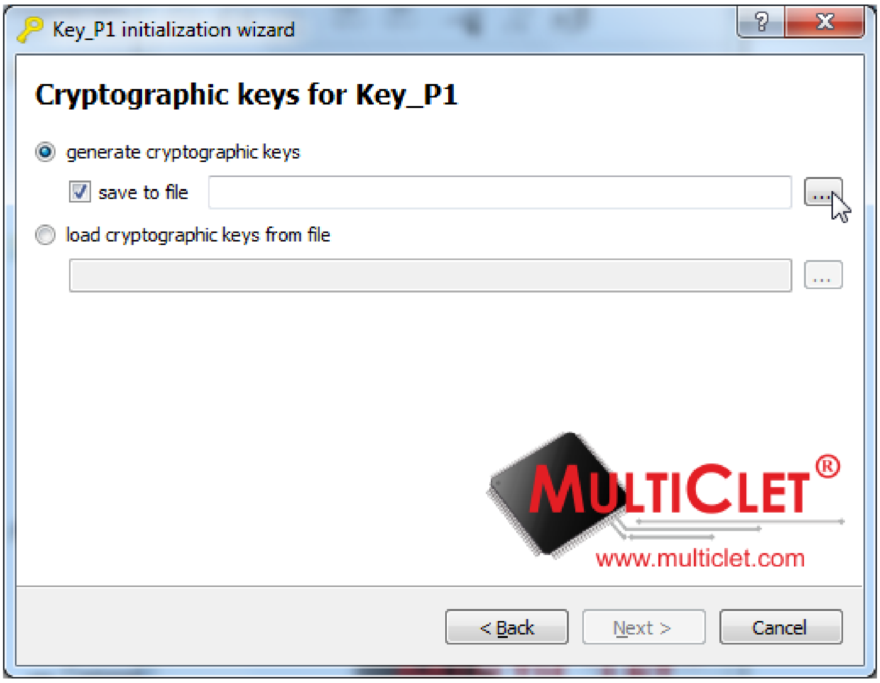


Key_P1 initialization wizard

This wizard will help you to initialize your Key_P1. Click "Next" to continue or "Cancel" to exit the wizard. To run the wizard again click on the "Initialize device" in the main menu of **Actions** entry.

Figure 26: Initialization wizard of the Key_P1

Press "Next" button to continue procedure. Press "Cancel" to abort procedure.



Key_P1 initialization wizard

Cryptographic keys for Key_P1

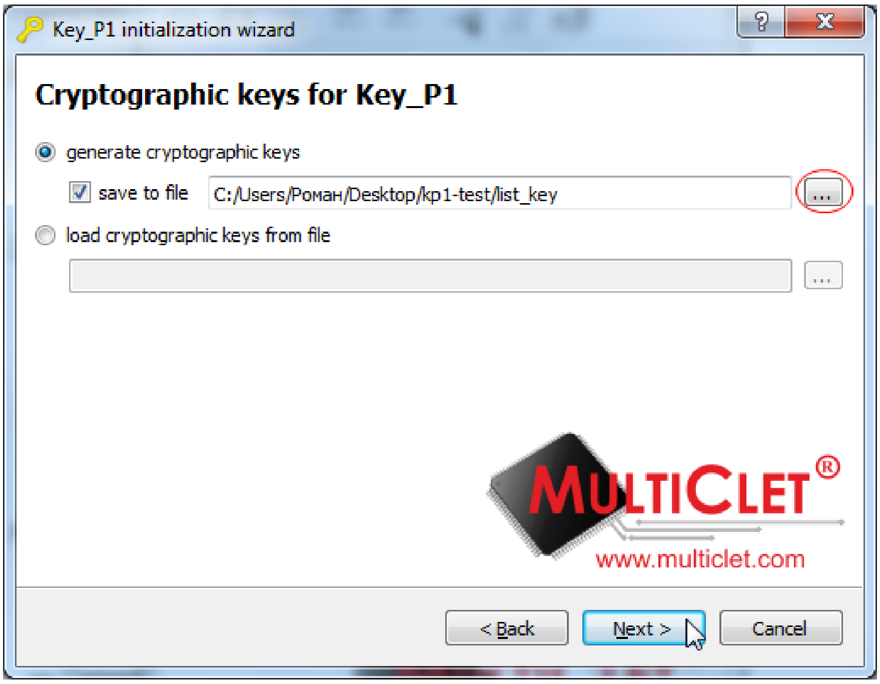
● generate cryptographic keys

☑ save to file

○ load cryptographic keys from file

Figure 27: Key_P1 initialiation options

At the first stage of the device initialization necessary set initialization options (fig. 27).



Key_P1 initialization wizard

Cryptographic keys for Key_P1

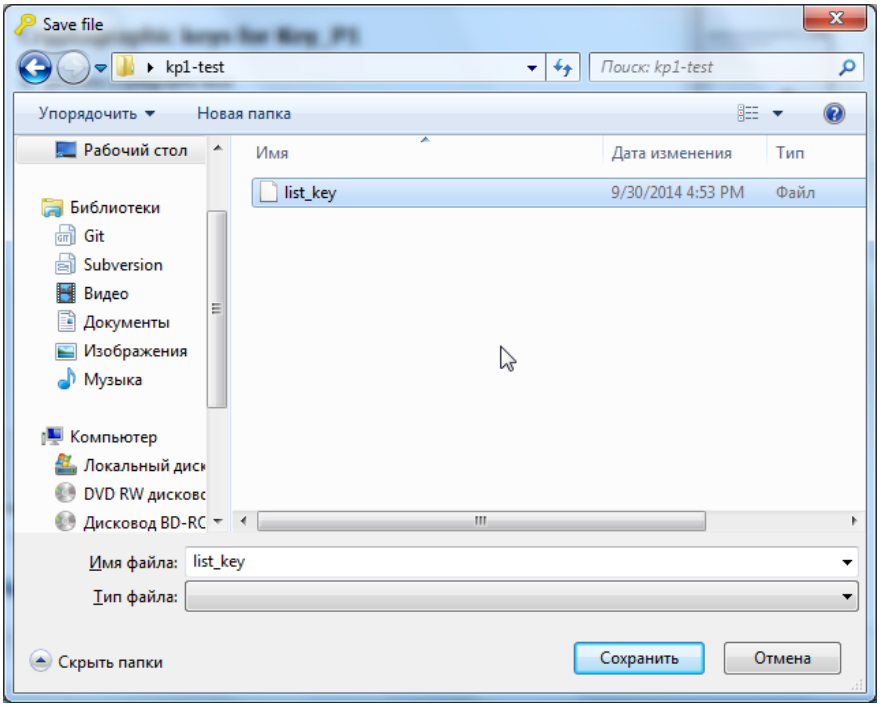
● generate cryptographic keys

☑ save to file C:/Users/Роман/Desktop/kp1-test/list_key

○ load cryptographic keys from file

Figure 28: Key_P1 set initialization options

Initially necessary to set checkbox at the string **generate cryptographic keys**. As a default all keys will be save in the internal memory of the Key_P1 device, but there is a way to make keys backup. In case Key_P1 device loss will be a way to recover cryptographic keys and transfer keys on a new device Key_P1. To do this set checkbox **Save in file** and choose file path(button highlighted in red in fig. 28). After choosing path for saving file press button "Save"(fig. 29).



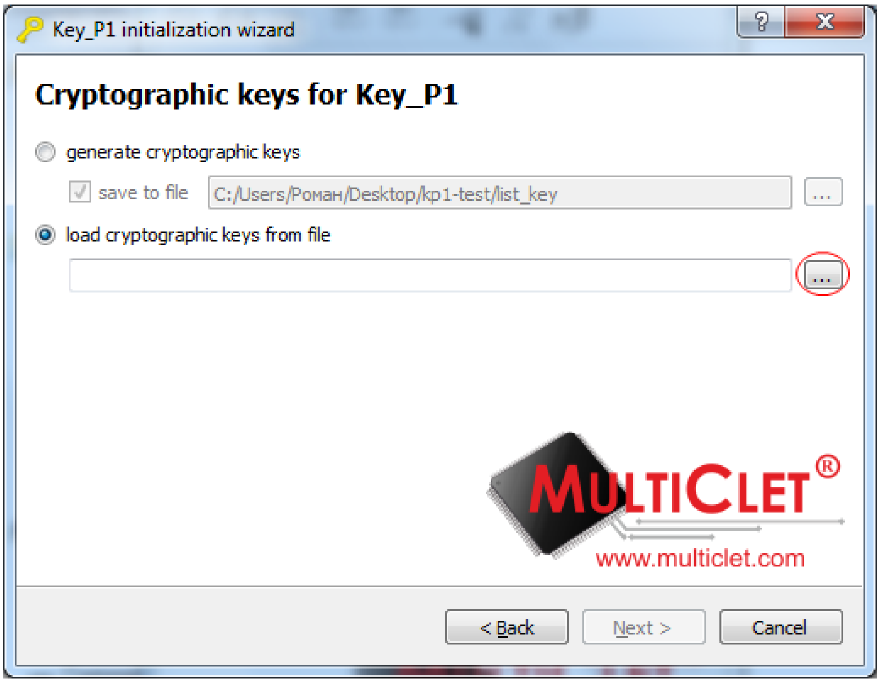
Имя	Дата изменения	Тип
list_key	9/30/2014 4:53 PM	Файл

Имя файла: list_key

Тип файла:

Figure 29: File path for keys backup

If necessary use previously saved key list, that set checkbox at the field **download cryptographic keys from file**, to do this press button, which highlighted in red (fig. 30) and choose previously saved file.



Key_P1 initialization wizard

Cryptographic keys for Key_P1

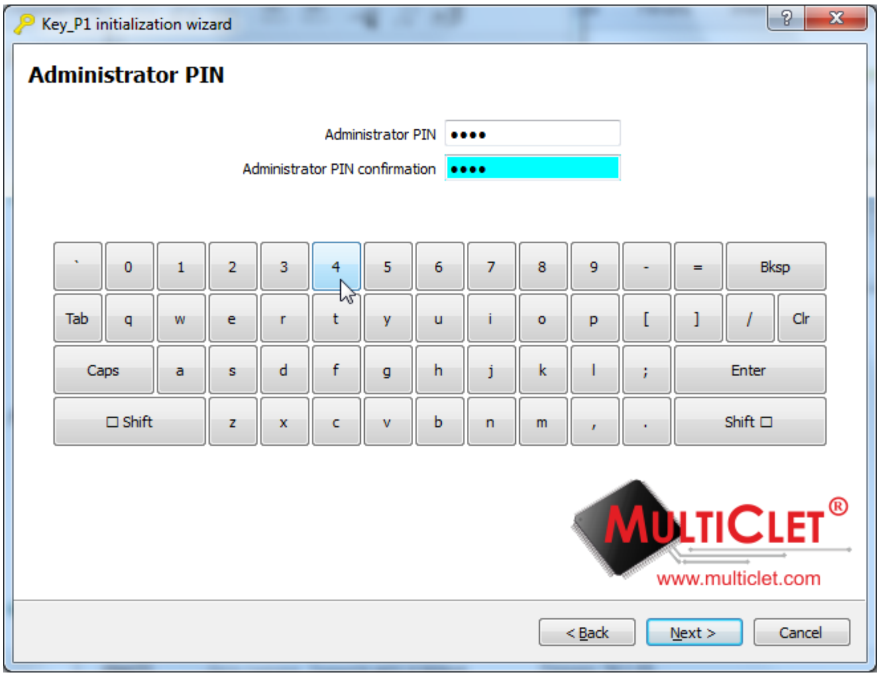
○ generate cryptographic keys

☑ save to file C:/Users/Роман/Desktop/kp1-test/list_key

● load cryptographic keys from file

Figure 30: Setting file path to previously saved key list

Press button "Next" to continue procedure and press "Cancel" to abort procedure. At the window **administrator PIN** that appeared (fig. 31) necessary set administrator PIN (when devices using in the company the setting of the administrator PIN, alarm PIN and initially user PIN is a prerogative of security service manager) and press «Next». Minimal characters count - 4, Maximal characters count - 16, uppercase and lowercase character differ.



Key_P1 initialization wizard

Administrator PIN

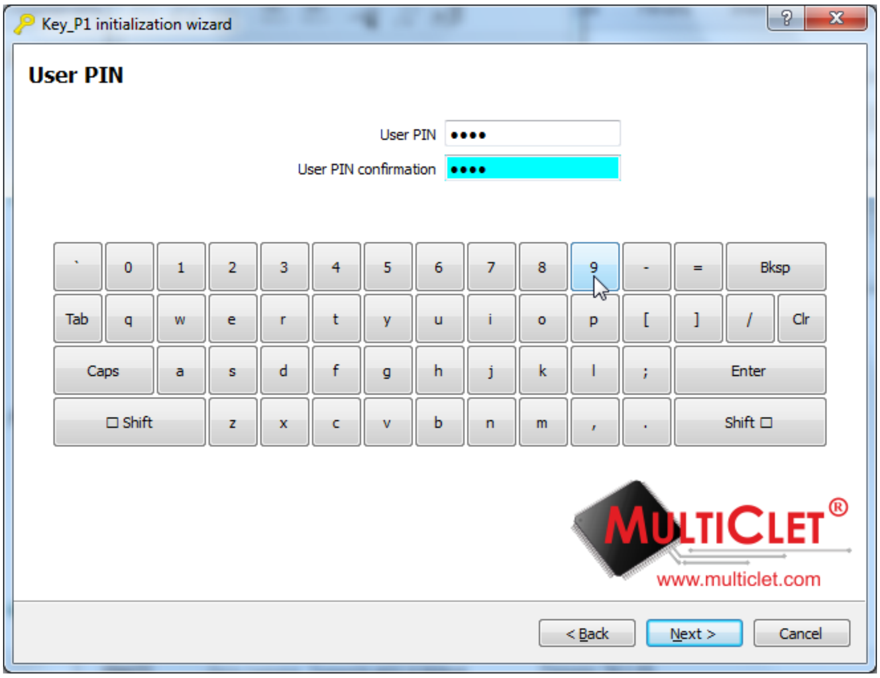
Administrator PIN ••••

Administrator PIN confirmation ••••

` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □
MULTICLET®
www.multiclet.com
< Back
Next >
Cancel

Figure 31: Setting administrator PIN

At the window **user PIN** that appeared (fig. 32) necessary set user PIN and press «Next». Minimal characters count - 4, Maximal characters count - 16, uppercase and lowercase character differ.



Key_P1 initialization wizard

User PIN

User PIN ••••

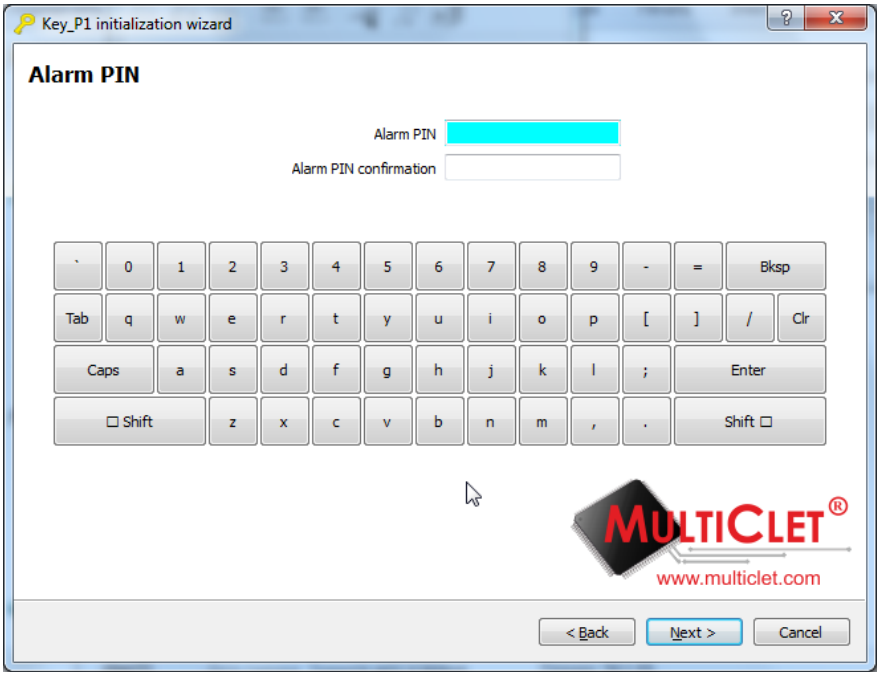
User PIN confirmation ••••

` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □
MULTICLET®
www.multiclet.com
< Back
Next >
Cancel

Figure 32: Setting user PIN

At the window **alarm PIN** (fig. 33) necessary set alarm PIN and press «Next». Using alarm PIN necessary to immediate clear all keys and data from Key_P1 device. Alarm PIN doesn't match with user PIN. In case matching alarm PIN not trigger. Minimal characters count - 4, Maximal characters count - 16, uppercase and lowercase character differ.

Note: during initialization device procedure there is a way to skip setting alarm PIN code. To do this necessary leave the fields empty and press button "Next". Thus alarm PIN will be not set.



Key_P1 initialization wizard

Alarm PIN

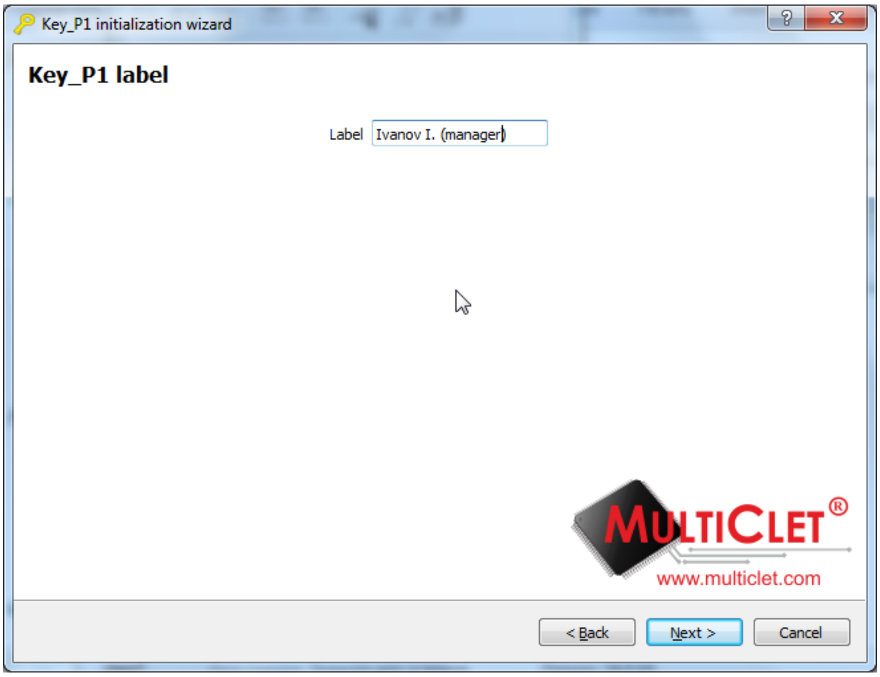
Alarm PIN

Alarm PIN confirmation

` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □
MULTICLET®
www.multiclet.com
< Back
Next >
Cancel

Figure 33: Setting alarm PIN

Next step is setting device label (fig. 34). Maximal characters count - 128. As device label might use First name or Last user name or any combination with department. For example «Ivanov Ivan» or «Ivanov I.(manager)»

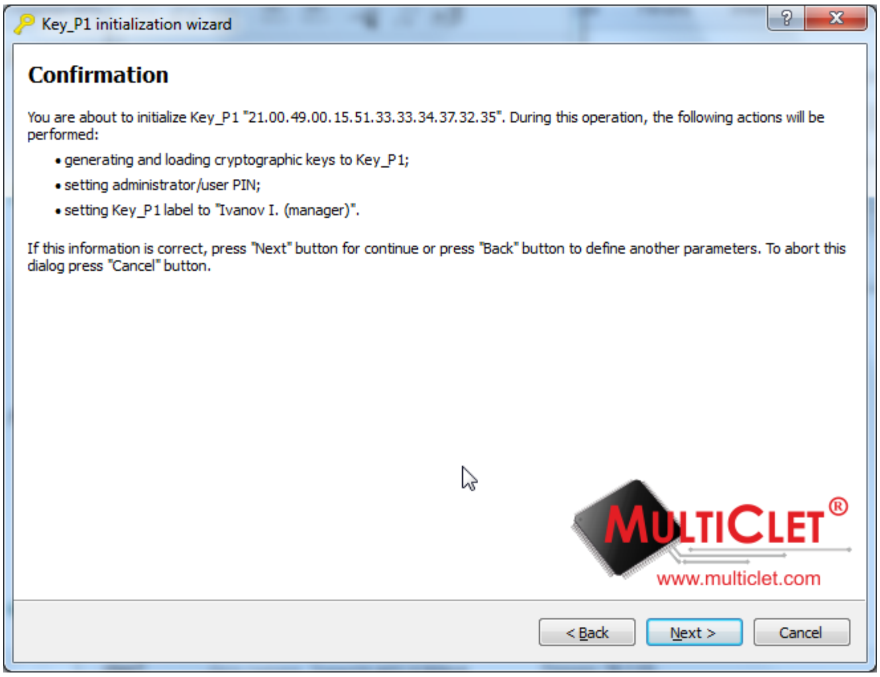


Key_P1 label

Label Ivanov I. (manager)

Figure 34: Setting device label

Necessary to check initialize options (fig. 35) and press button «Next».



Confirmation

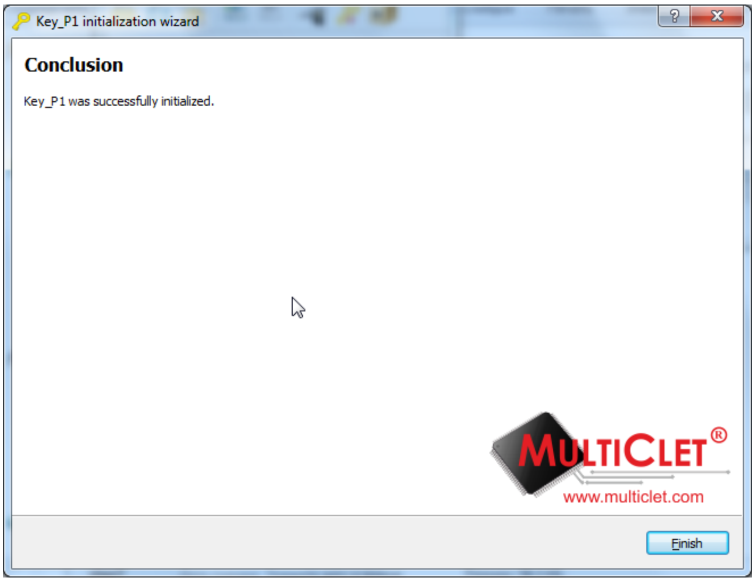
You are about to initialize Key_P1 "21.00.49.00.15.51.33.33.34.37.32.35". During this operation, the following actions will be performed:

- generating and loading cryptographic keys to Key_P1;
- setting administrator/user PIN;
- setting Key_P1 label to "Ivanov I. (manager)".

If this information is correct, press "Next" button for continue or press "Back" button to define another parameters. To abort this dialog press "Cancel" button.

Figure 35: Initialization options

Initialization process will be start and after it's complete necessary press button «Finish» (fig. 36).



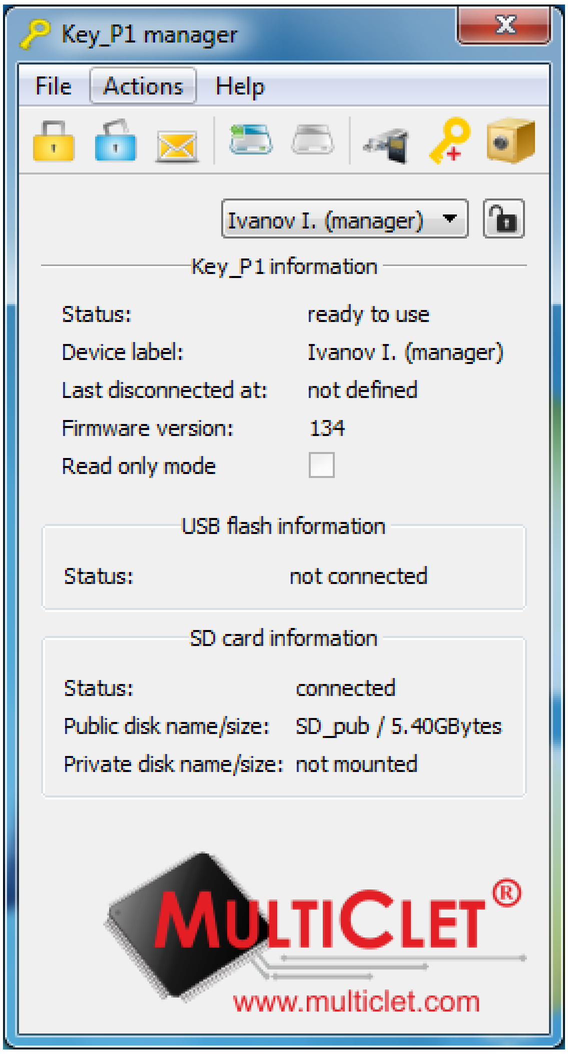
Key_P1 initialization wizard

Conclusion

Key_P1 was successfully initialized.

Figure 36: Initialization complete

Key_P1 device initialization is complete. In the main menu device will be display with their label (name): «Ivanov I.» (fig. 37).



Ivanov I. (manager)

Key_P1 information

Status:	ready to use
Device label:	Ivanov I. (manager)
Last disconnected at:	not defined
Firmware version:	134
Read only mode	□

USB flash information

Status:	not connected

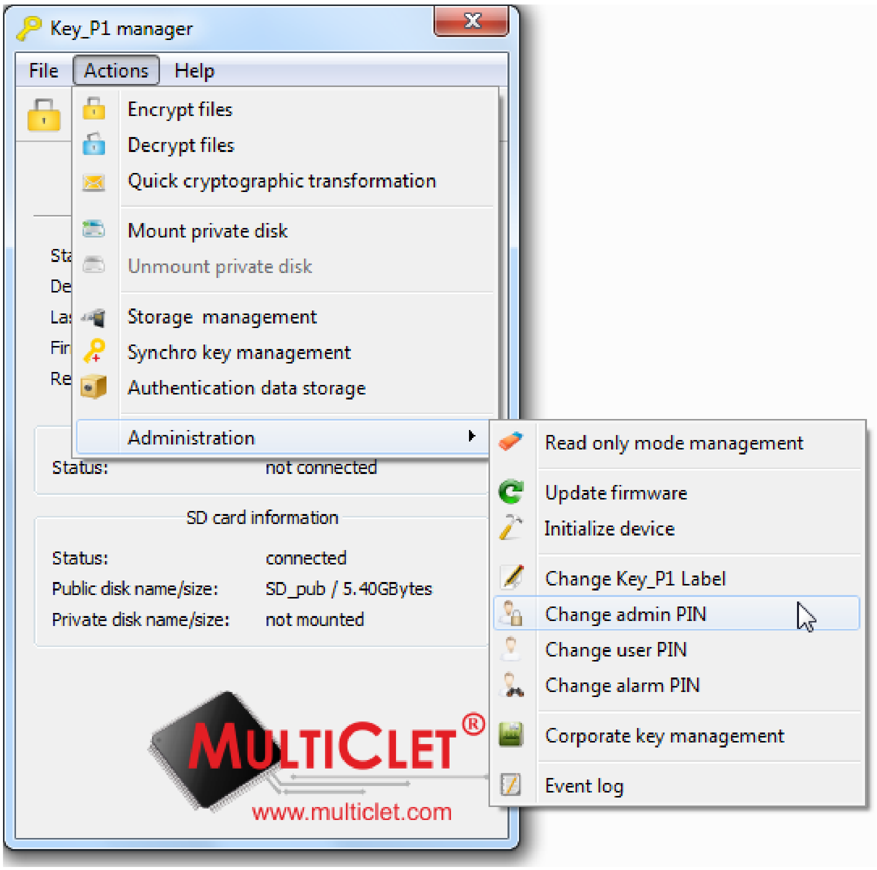
SD card information

Status:	connected
Public disk name/size:	SD_pub / 5.40GBytes
Private disk name/size:	not mounted

Figure 37: Application main menu after initialization process

2.7 Changing administrator PIN

To do this changing administrator PIN code operation should be choose tab **Actions** go to submenu **Administration** and choose **Change administrator PIN** submenu item (fig. 38)



Status: not connected

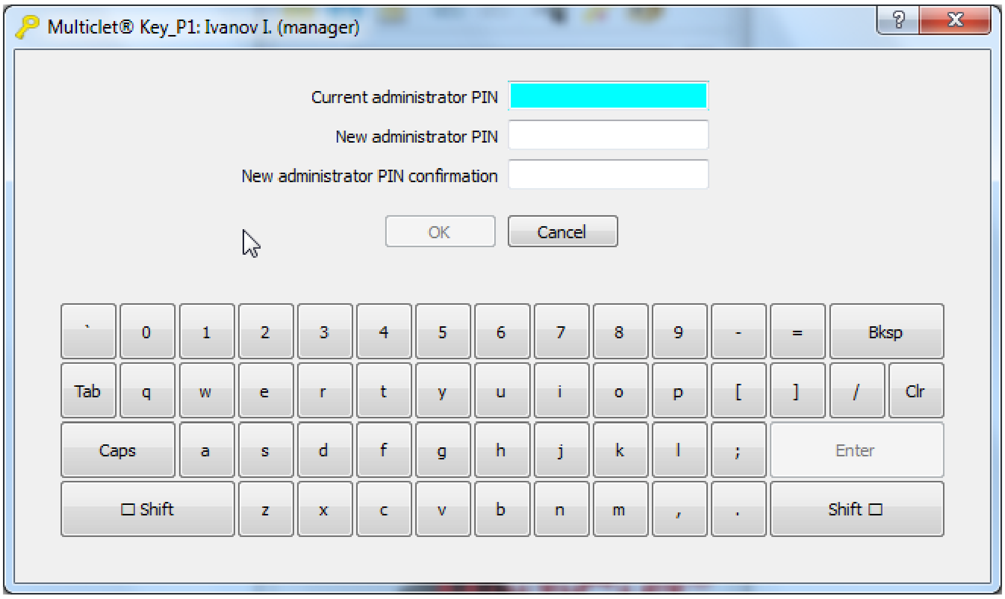
Status: connected

Public disk name/size: SD_pub / 5.40GBytes

Private disk name/size: not mounted

Figure 38: Change administrator PIN item

At the window appeared (fig. 39) necessary type administrator PIN into **Current administrator PIN** field and type new administrator PIN into **New administrator PIN** field and **Confirmation new administrator PIN** field. After these actions press button «OK» to save changes. Maximal attempt count PIN - 10, in case 10 not success attempts, administrator PIN will be locked. In administrator lock case necessary erase all data with special utility and make new device initialization procedure (Initialization procedure described in chapter 2.4).



Multiclet® Key_P1: Ivanov I. (manager)

Current administrator PIN

New administrator PIN

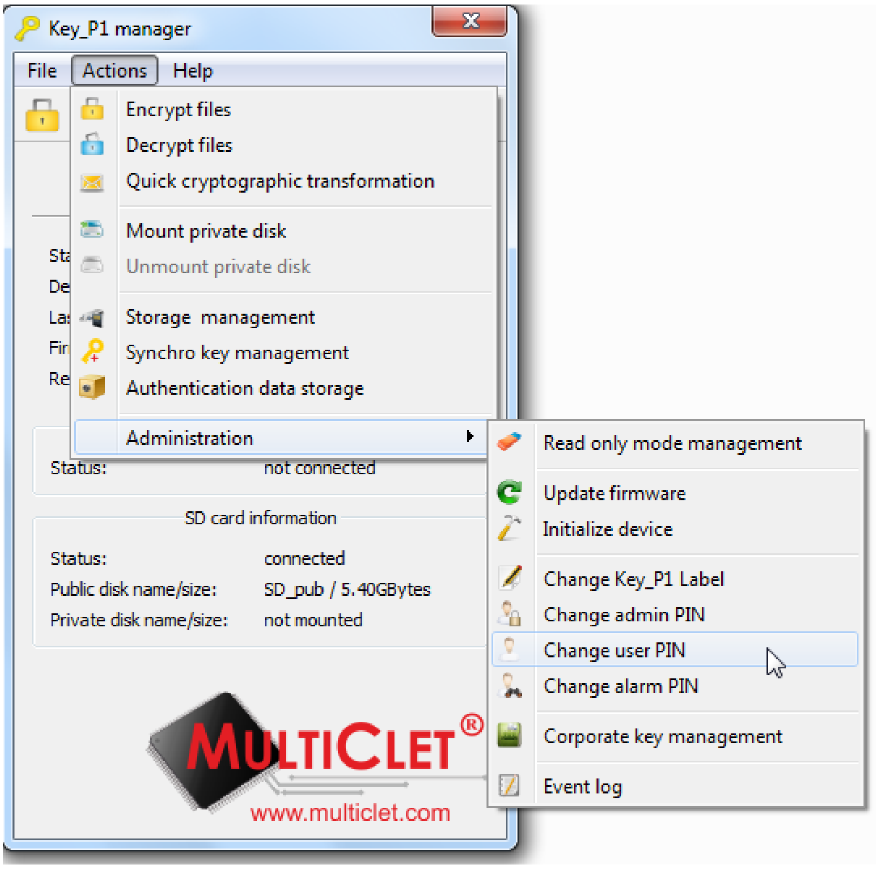
New administrator PIN confirmation

OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 39: Changing administrator PIN

2.8 Changing user PIN

To do this changing user PIN code operation should be choose tab **Actions** go to submenu **Administration** and choose **Change user PIN** submenu item (fig. 40)



Status: not connected

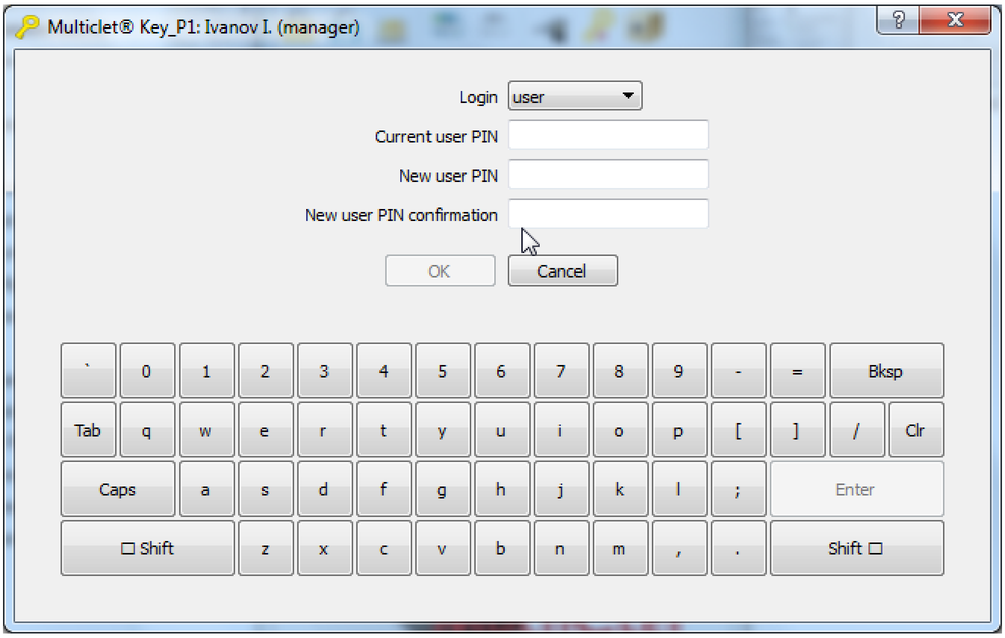
SD card information

Status: connected
Public disk name/size: SD_pub / 5.40GBytes
Private disk name/size: not mounted

Figure 40: Change user PIN item

At the window appeared into **Choose login** field necessary select PIN code with which will be change user PIN. This action can be make with user PIN or with administrator PIN.

1) Using user PIN (fig. 41). Necessary choose "user" into **Login** field. Type current user PIN into **Current user PIN** field and type new user PIN into **New user PIN** field and **Confirmation new user PIN** field. And press button «OK» to save changes. Maximal attempt count user PIN - 10, in case 10 not success attempts, user PIN will be locked. In order to unlock use administrator PIN code.



Multiclet® Key_P1: Ivanov I. (manager)

Login: user

Current user PIN

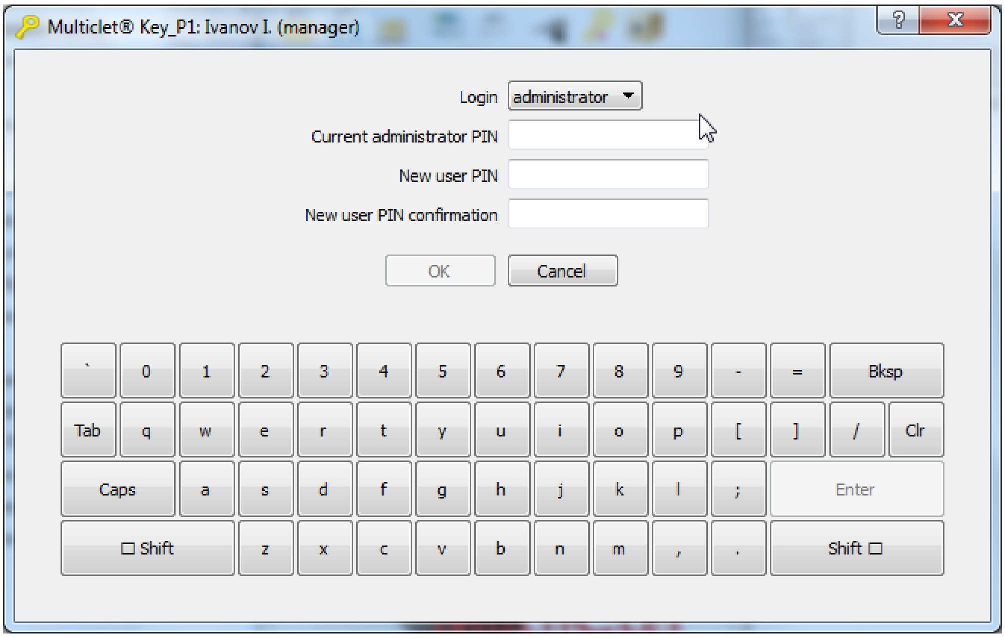
New user PIN

New user PIN confirmation

?
X
OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 41: Changing user PIN by user

2) Using administrator PIN (fig. 42). Necessary choose "administrator" into **Login** field. Type current administrator PIN into **Current administrator PIN** field, and type new user PIN into **New user PIN** field and **Confirmation new user PIN** field. And press button «OK» to save changes. Maximal attempt count user PIN - 10, in case 10 not success attempts, user PIN will be locked.



Multiclet® Key_P1: Ivanov I. (manager)

Login: administrator

Current administrator PIN

New user PIN

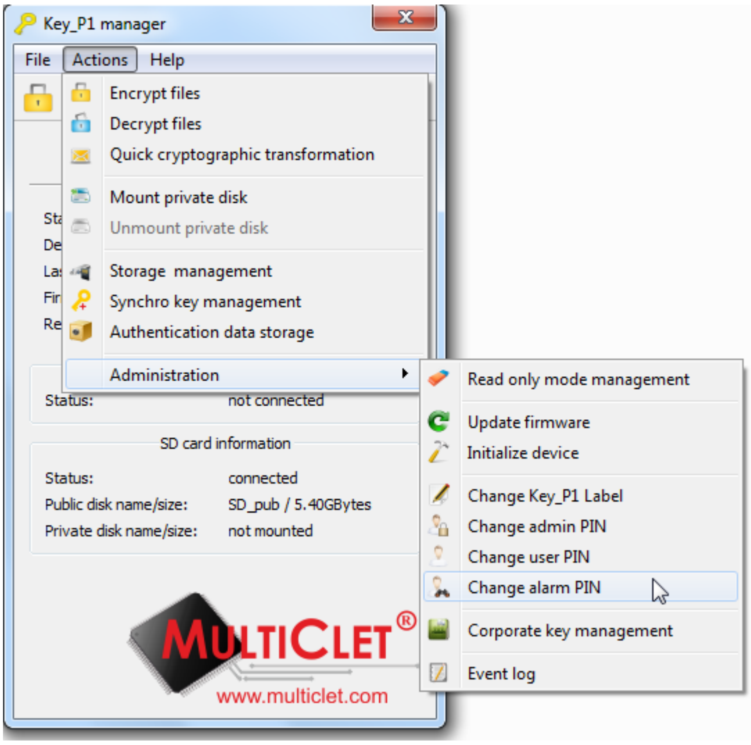
New user PIN confirmation

?
X
OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 42: Changing user PIN by administrator

2.9 Changing alarm PIN

In order to change alarm PIN necessary choose tab **Avtions** go to submenu **Administration** and select **Change alarm PIN** item (fig. 43)



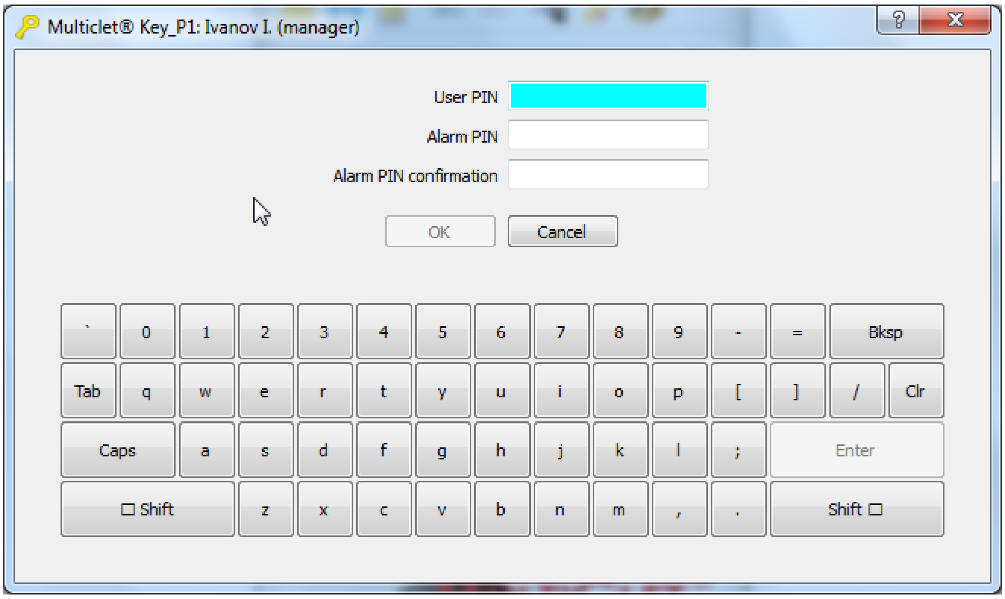
Status: not connected

SD card information

Status: connected
Public disk name/size: SD_pub / 5.40GBytes
Private disk name/size: not mounted

Figure 43: Changing alarm PIN

At the window appeared (fig. pinalarm2) necessary type current user PIN into **user PIN** and type new alarm PIN into **Alarm PIN** and **Confirmation alarm PIN**. And press button «OK» to save changes.



Multiclet® Key_P1: Ivanov I. (manager)

User PIN

Alarm PIN

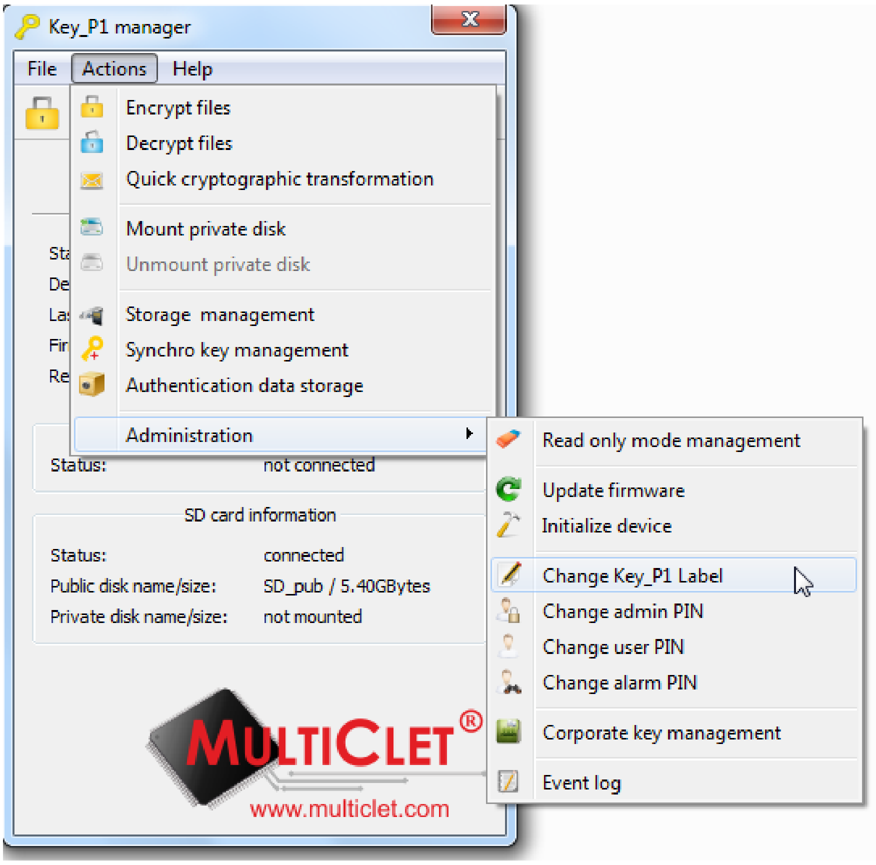
Alarm PIN confirmation

OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 44: Changing alarm PIN

2.10 Changing device label

In order to change device label (name) necessary choose tab **Actions** go to submenu **Administration** and choose **Change Key_P1 label** item (fig. 45). This operation can be performed only with administrator PIN.



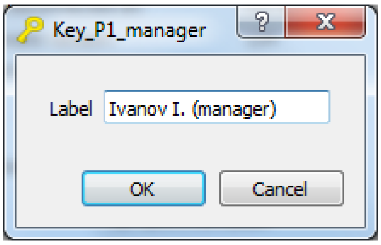
Status: not connected

SD card information

Status: connected
Public disk name/size: SD_pub / 5.40GBytes
Private disk name/size: not mounted

Figure 45: Changing device label

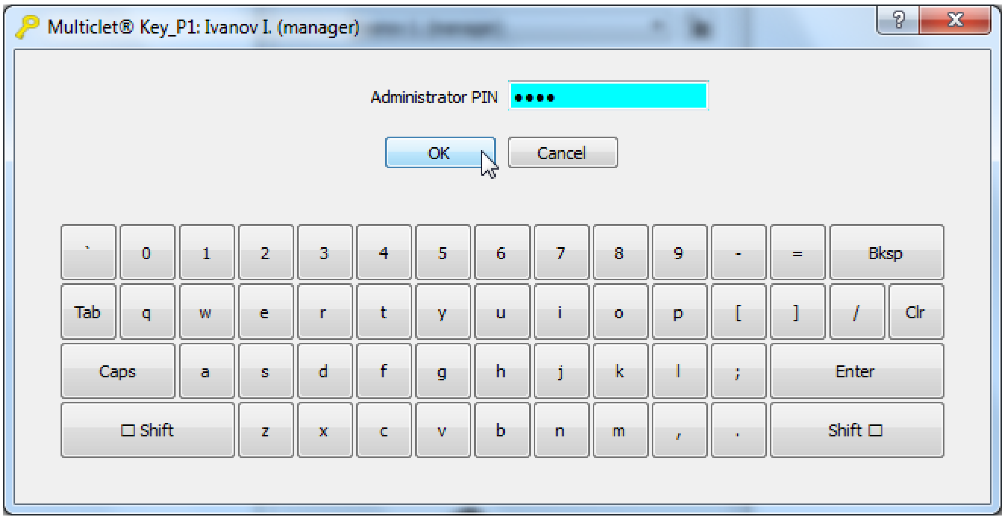
At the window appeared into **Device label** field (fig. 46) necessary type new device label (name) and press button «OK».



Label: Ivanov I. (manager)

Figure 46: Changing device label

Type current administrator PIN into **administrator PIN** field (fig. 47) and press button «OK».



Multiclet® Key_P1: Ivanov I. (manager)
Administrator PIN ••••
OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 47: Type administrator PIN

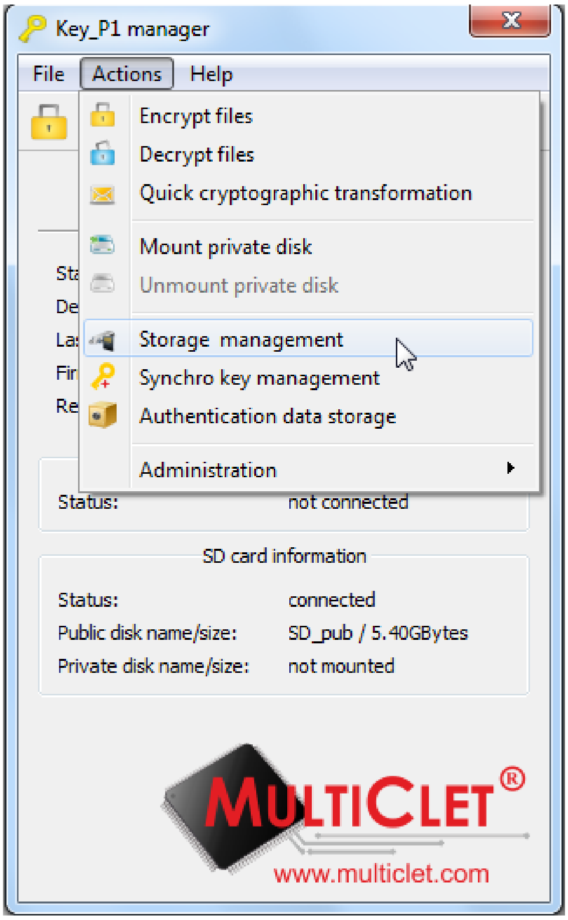
If all actions completed success that in main application menu into **Device label** field will be display new device label.

3 Using Key_P1 device

3.1 Storage management

3.1.1 Create a private partition on the USB storage

In order to make a private partition (protected and crypt) on the USB storage necessary choose tab **Actions** and choose **Storage management** item (fig. 48).



Status: not connected

SD card information

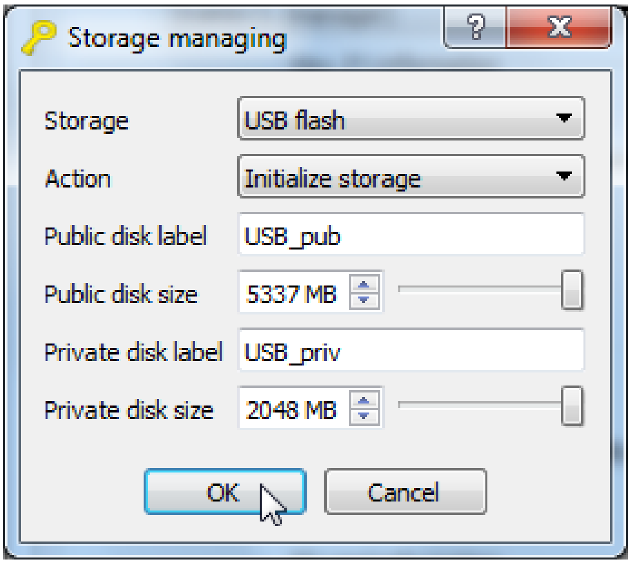
Status: connected

Public disk name/size: SD_pub / 5.40GBytes

Private disk name/size: not mounted

Figure 48: Storage management

At the window **Storage management** (fig. 49) necessary choose «USB storage» into **Storage** field , at the line **Actions** choose «Initialize storage», at the field **Public partition label** type name for public partition, at the field **Public partition size** set size of a public partition, at the field **Private partition label** type name for private partition, at the field **Private partition size** set size of a private partition. And press button «OK» to continue(fig. 49).



Storage: USB flash

Action: Initialize storage

Public disk label: USB_pub

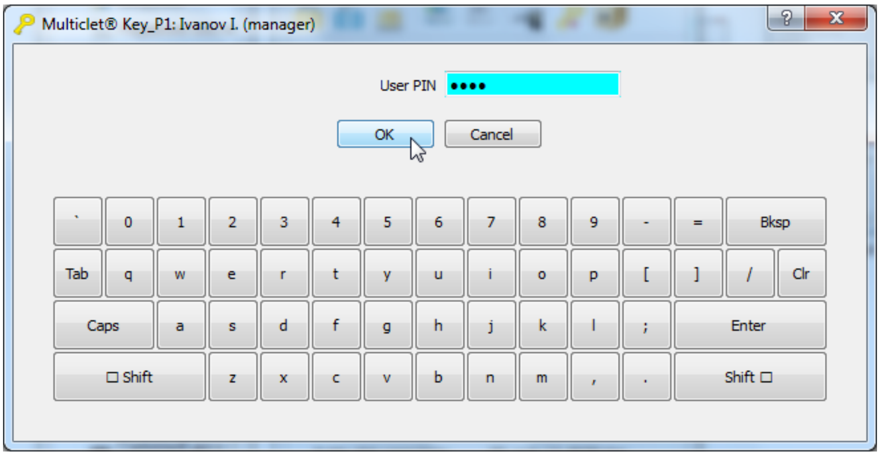
Public disk size: 5337 MB

Private disk label: USB_priv

Private disk size: 2048 MB

Figure 49: Storage initialization

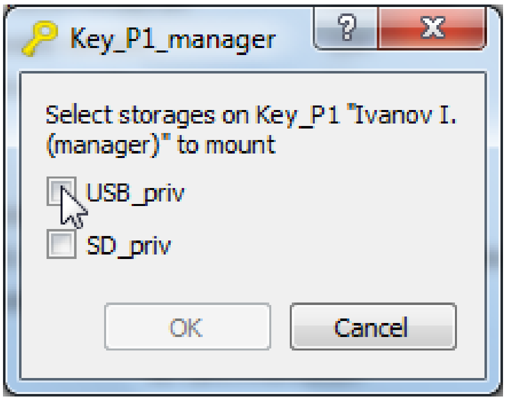
Window for entering user PIN will display. After entering user PIN code press button «OK» (fig. 50).


Multiclet® Key_P1: Ivanov I. (manager)
OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

User PIN: ••••

Figure 50: Entering user PIN

Window appeared with request mount private partition (fig. 51). Set checkbox appropriate private partition, which necessary mount and press button «OK».



Key_P1_manager

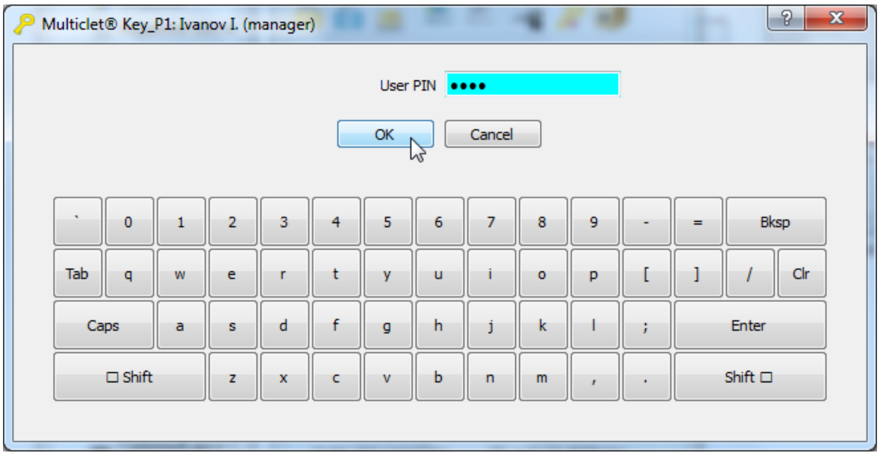
Select storages on Key_P1 "Ivanov I. (manager)" to mount

□ USB_priv

□ SD_priv

Figure 51: Mounting private partition

Window for entering user PIN will display. After entering user PIN code press button «OK» (fig. 52).



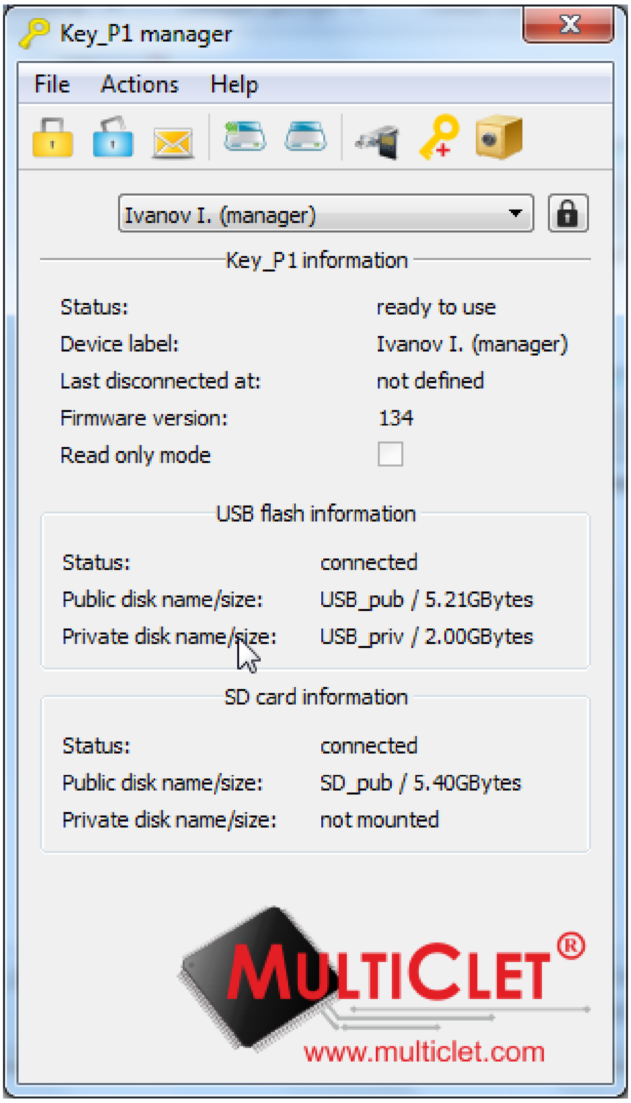
Multiclet® Key_P1: Ivanov I. (manager)

User PIN ●●●●

OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 52: Entering user PIN

After these actions completed in the field **Information about USB storage** will be display information about mount partitions. In the OS private partition display at the list of removable drive53.



Ivanov I. (manager)

Key_P1 information

Status:	ready to use
Device label:	Ivanov I. (manager)
Last disconnected at:	not defined
Firmware version:	134
Read only mode	□

USB flash information

Status:	connected
Public disk name/size:	USB_pub / 5.21GBytes
Private disk name/size:	USB_priv / 2.00GBytes

SD card information

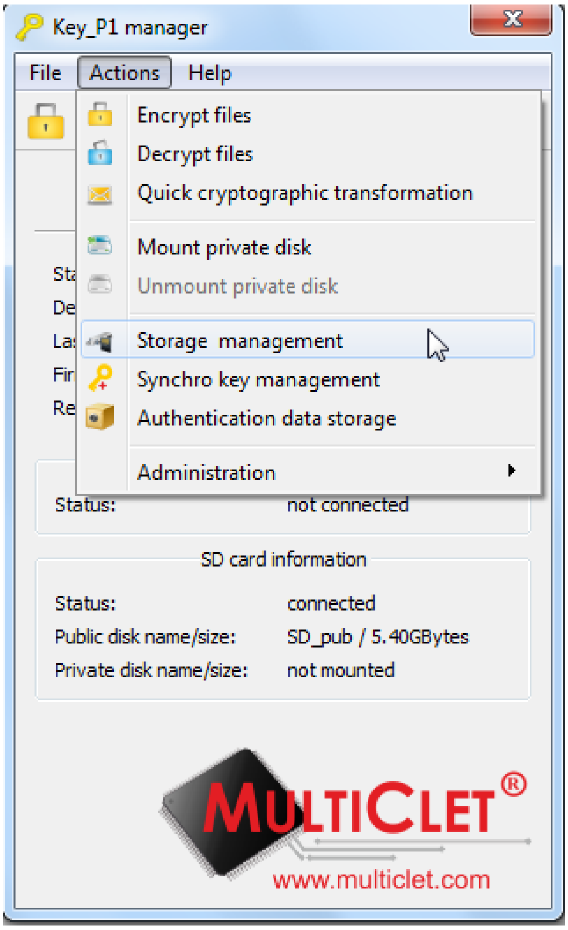
Status:	connected
Public disk name/size:	SD_pub / 5.40GBytes
Private disk name/size:	not mounted

Figure 53: Application main menu

In order to make partition label changing or format private partition necessary consequentially choose tab **Actions** go to submenu **Administration** and choose **Storage management** item. In the window **Storage management** choose «USB storage» in the **Storage** field, at the string **Actions** choose appropriate action with storage. Then make all necessary changes.

3.1.2 Create a private partition on SD card

In order to make a private partition (protected and crypt) on the USB storage necessary choose tab **Actions** and choose **Storage management** item (fig. 54).



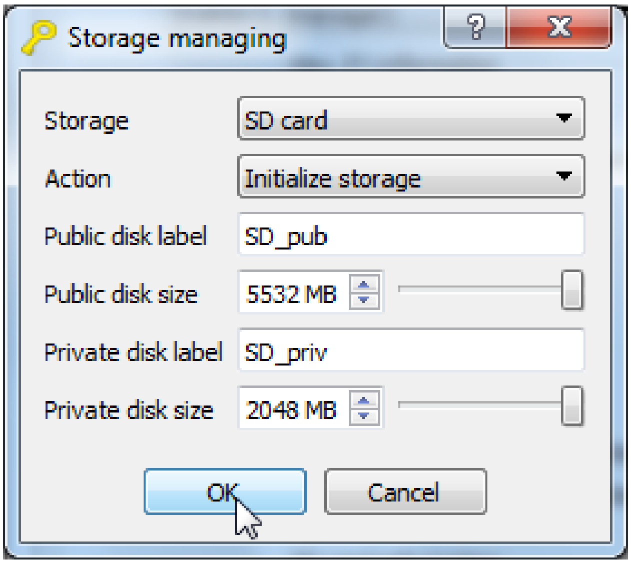
Status: not connected

SD card information

Status: connected
Public disk name/size: SD_pub / 5.40GBytes
Private disk name/size: not mounted

Figure 54: Storage management

At the window **Storage management** (fig. 55) necessary choose «SD storage» into **Storage** field, in the field **Actions** choose «Initialize storage», in the field **Public partition label** type name of public partition, in the field **Size of public partition** set size of public partition, in the field **Private partition label** type name of private partition, in the field **Size of private partition** set size of private partition. After all actions completed press button «OK».



Storage managing

Storage: SD card

Action: Initialize storage

Public disk label: SD_pub

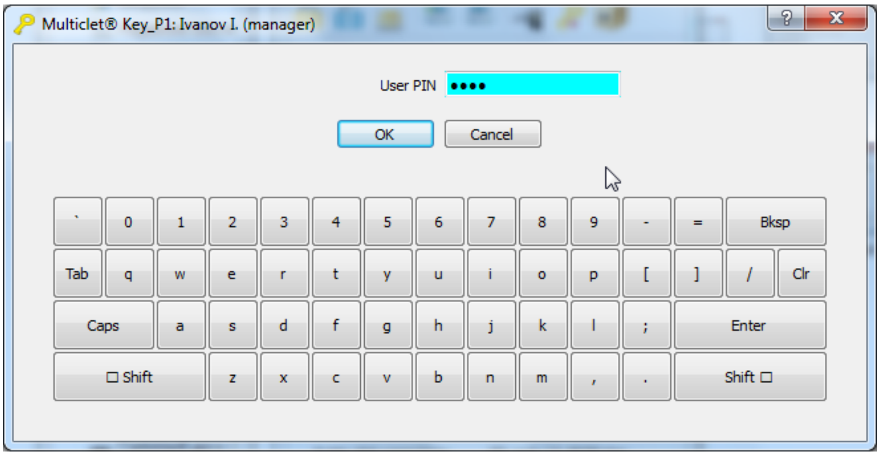
Public disk size: 5532 MB

Private disk label: SD_priv

Private disk size: 2048 MB

Figure 55: Storage initialization

Window contain entering user PIN code appeared. Press button «OK» to continue (fig. 56).



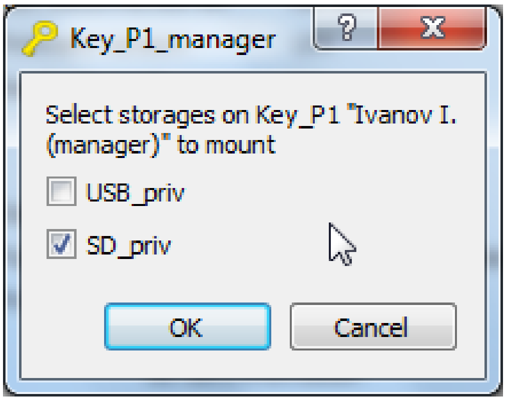
Multiclet® Key_P1: Ivanov I. (manager)

User PIN: ••••

OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 56: Entering user PIN

Window appeared with request mount private partition (fig. 57). Set checkbox appropriate private partition, which necessary mount and press button «OK».



Key_P1_manager

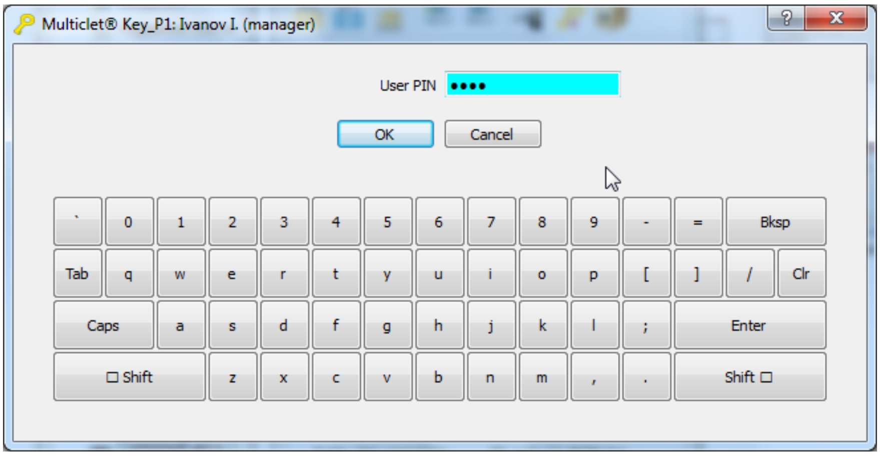
Select storages on Key_P1 "Ivanov I. (manager)" to mount

□ USB_priv

☑ SD_priv

Figure 57: Mounting private partition

Window for entering user PIN will display. After entering user PIN code press button «OK» (fig. 58).



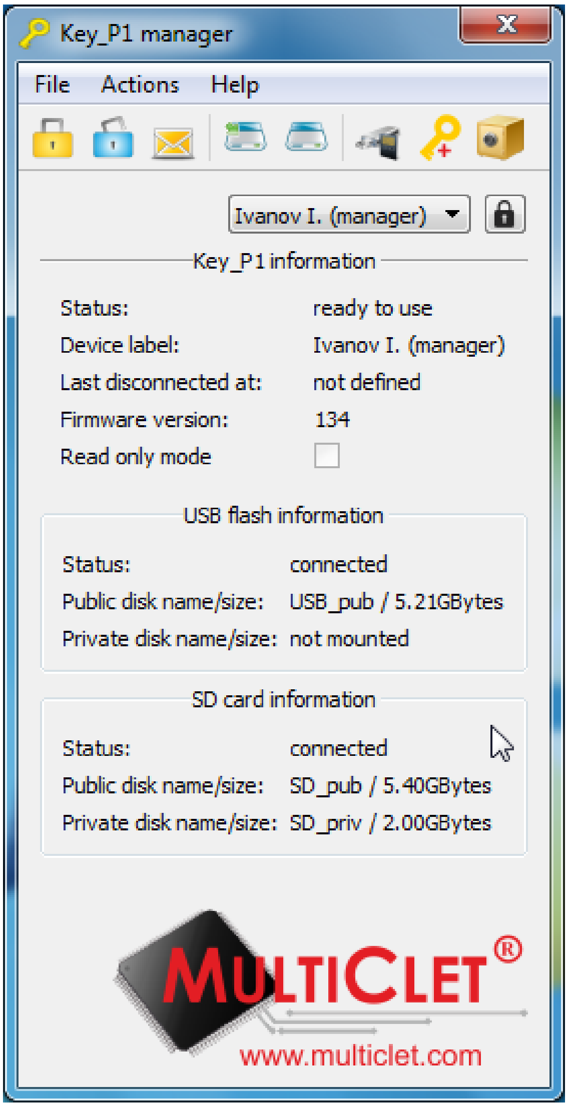
Multiclet® Key_P1: Ivanov I. (manager)

User PIN ••••

OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 58: Entering user PIN

After these actions completed in the field **Information about SD card** will be display information about mount partitions. In the OS private partition display at the list of removable drive(fig. 59).



Key_P1 information

Status: ready to use
Device label: Ivanov I. (manager)
Last disconnected at: not defined
Firmware version: 134
Read only mode □

USB flash information

Status: connected
Public disk name/size: USB_pub / 5.21GBytes
Private disk name/size: not mounted

SD card information

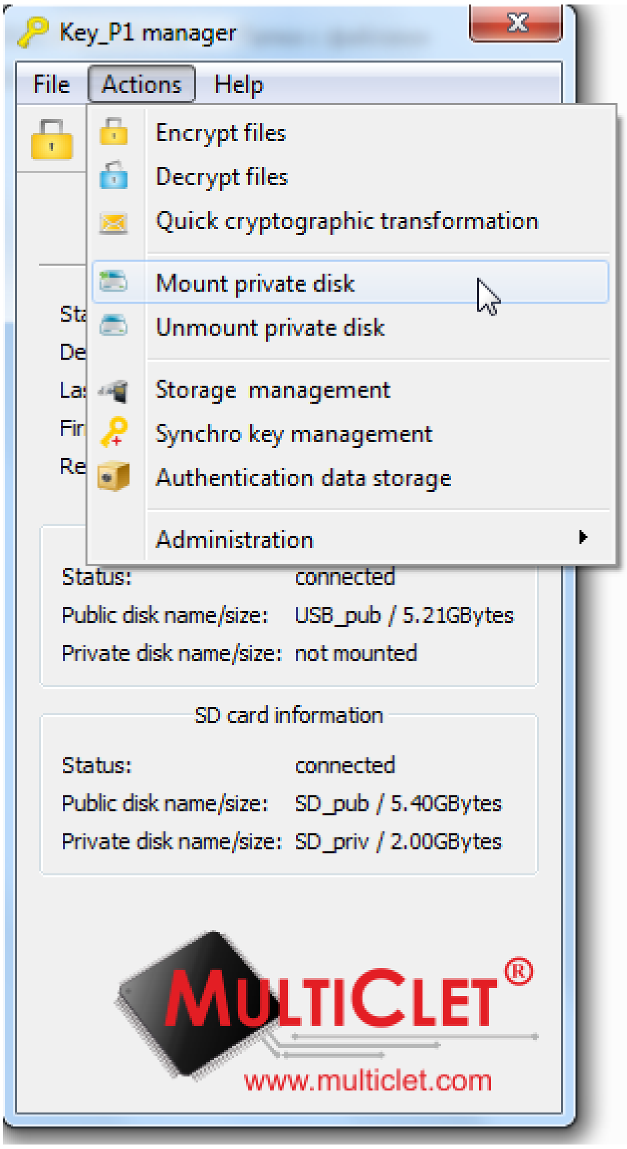
Status: connected
Public disk name/size: SD_pub / 5.40GBytes
Private disk name/size: SD_priv / 2.00GBytes

Figure 59: Application main menu

In order to make partition label changing or format private partition necessary consequentially choose tab **Actions** go to submenu **Administration** and choose **Storage management** item. In the window **Storage management** choose «SD card» in the **Storage** field, at the string **Actions** choose appropriate action with storage. Then make all necessary changes.

3.1.3 Mounting private partition on the USB storage

In order to make mounting procedure of previously created private partition on the USB storage necessary consequentially choose tab **Actions** and command **Mount private partition** (fig. 60).



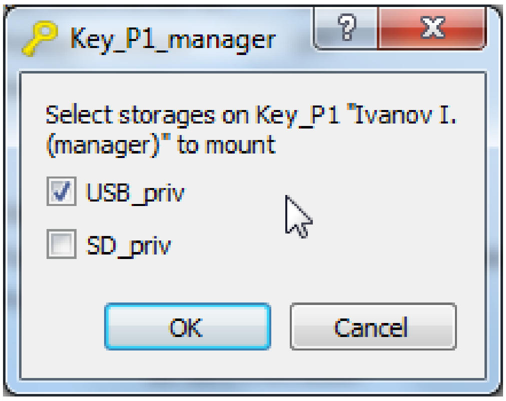
Status: connected
Public disk name/size: USB_pub / 5.21GBytes
Private disk name/size: not mounted

SD card information

Status: connected
Public disk name/size: SD_pub / 5.40GBytes
Private disk name/size: SD_priv / 2.00GBytes

Figure 60: Mounting private partition

Set checkbox appropriate private partition, which necessary mount and press button «OK». (fig. 61).



Key_P1_manager

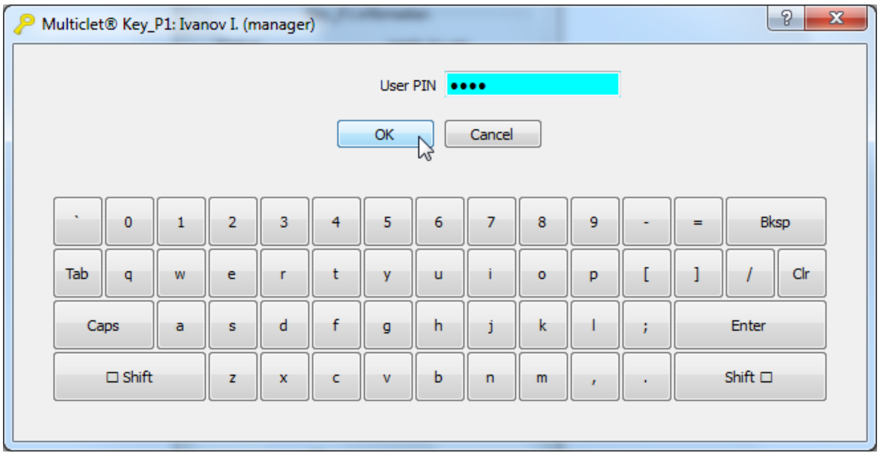
Select storages on Key_P1 "Ivanov I. (manager)" to mount

☑ USB_priv

□ SD_priv

Figure 61: Storage choice

Window for entering user PIN will display. After entering user PIN code press button «OK» (fig. 62).



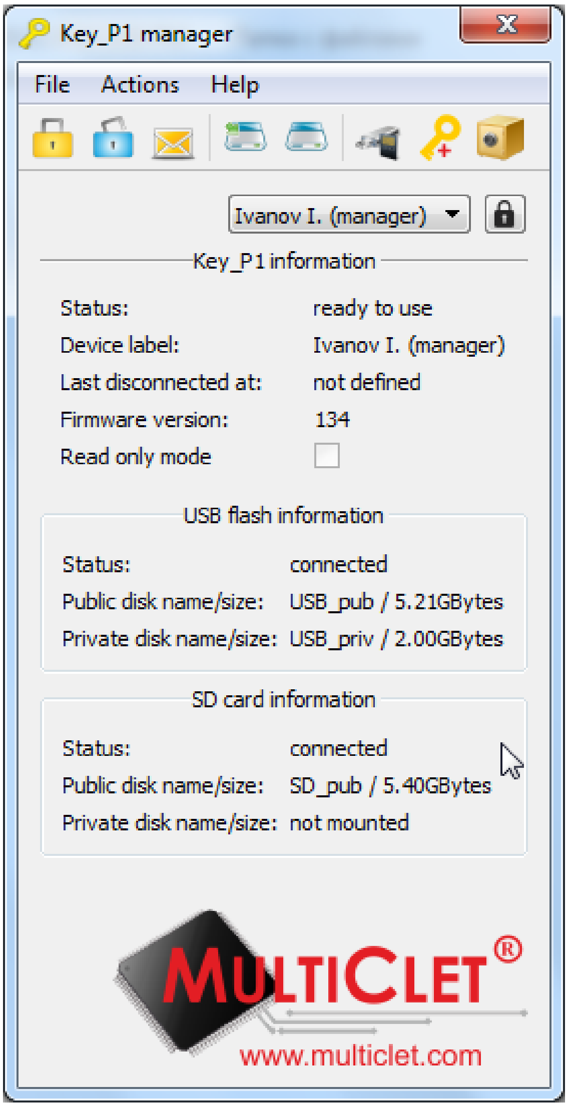
Multiclet® Key_P1: Ivanov I. (manager)

User PIN ●●●●

OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 62: Entering user PIN

Application main menu will be look like as shown at fig. 63



Ivanov I. (manager)

Key_P1 information

Status: ready to use
Device label: Ivanov I. (manager)
Last disconnected at: not defined
Firmware version: 134
Read only mode □

USB flash information

Status: connected
Public disk name/size: USB_pub / 5.21GBytes
Private disk name/size: USB_priv / 2.00GBytes

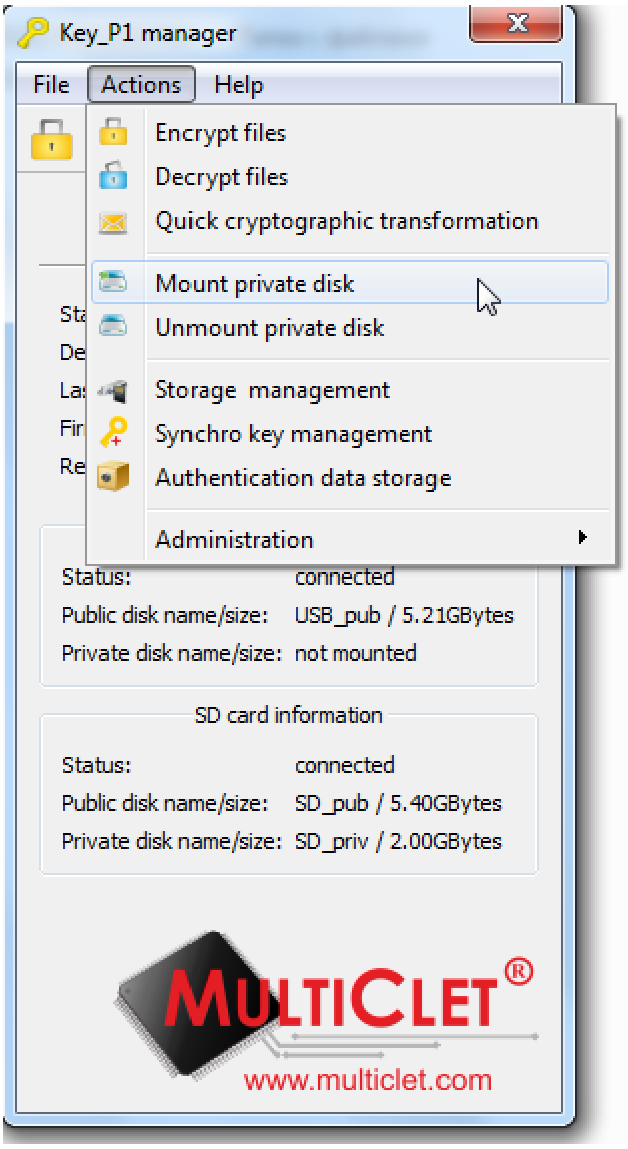
SD card information

Status: connected
Public disk name/size: SD_pub / 5.40GBytes
Private disk name/size: not mounted

Figure 63: Application main menu

3.1.4 Mounting private partition on the SD card

In order to make mounting procedure of previously created private partition on the SD card necessary consequentially choose tab **Actions** and command **Mount private partition** (fig. 64).



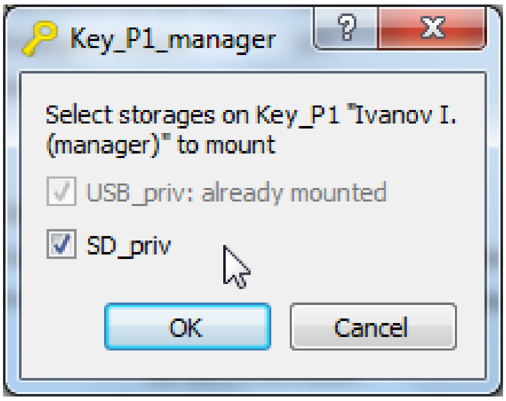
Status: connected
Public disk name/size: USB_pub / 5.21GBytes
Private disk name/size: not mounted

SD card information

Status: connected
Public disk name/size: SD_pub / 5.40GBytes
Private disk name/size: SD_priv / 2.00GBytes

Figure 64: Mounting private partition

Set checkbox appropriate private partition, which necessary mount and press button «OK» (fig. 65).



Key_P1_manager

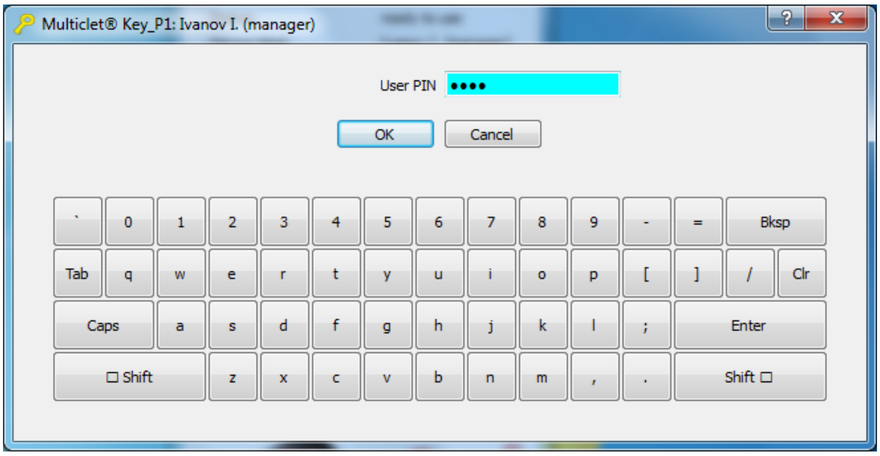
Select storages on Key_P1 "Ivanov I. (manager)" to mount

☑ USB_priv: already mounted

☑ SD_priv

Figure 65: Storage choice

Set checkbox appropriate private partition, which necessary mount and press button «OK» (fig. 66).



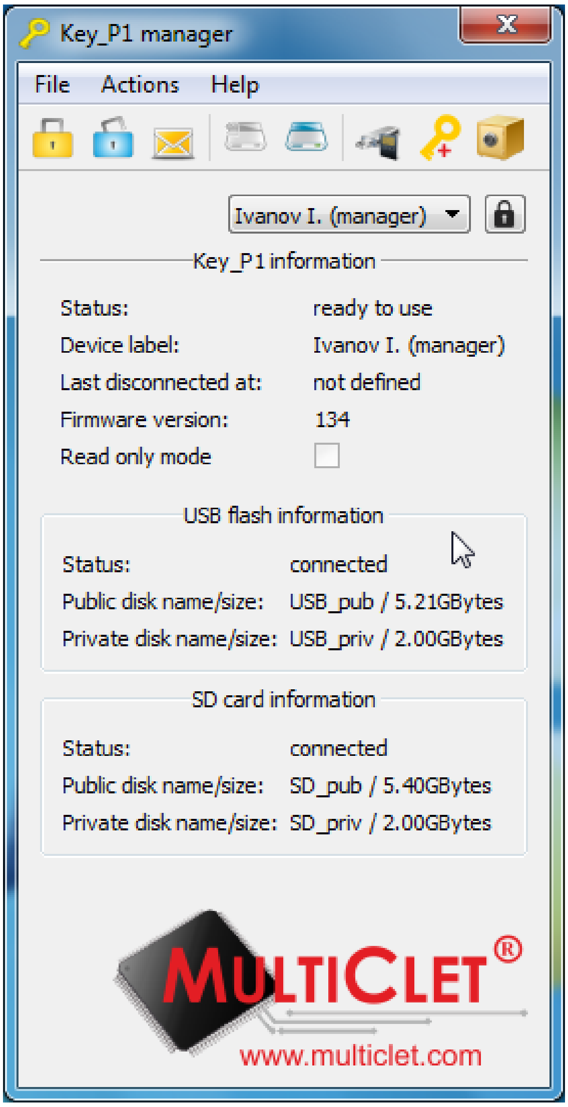
Multiclet® Key_P1: Ivanov I. (manager)

User PIN ••••

OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 66: Entering user PIN

Application main menu will be look likes as shown at fig. 67



Key_P1 information

Status:	ready to use
Device label:	Ivanov I. (manager)
Last disconnected at:	not defined
Firmware version:	134
Read only mode	□

USB flash information

Status:	connected
Public disk name/size:	USB_pub / 5.21GBytes
Private disk name/size:	USB_priv / 2.00GBytes

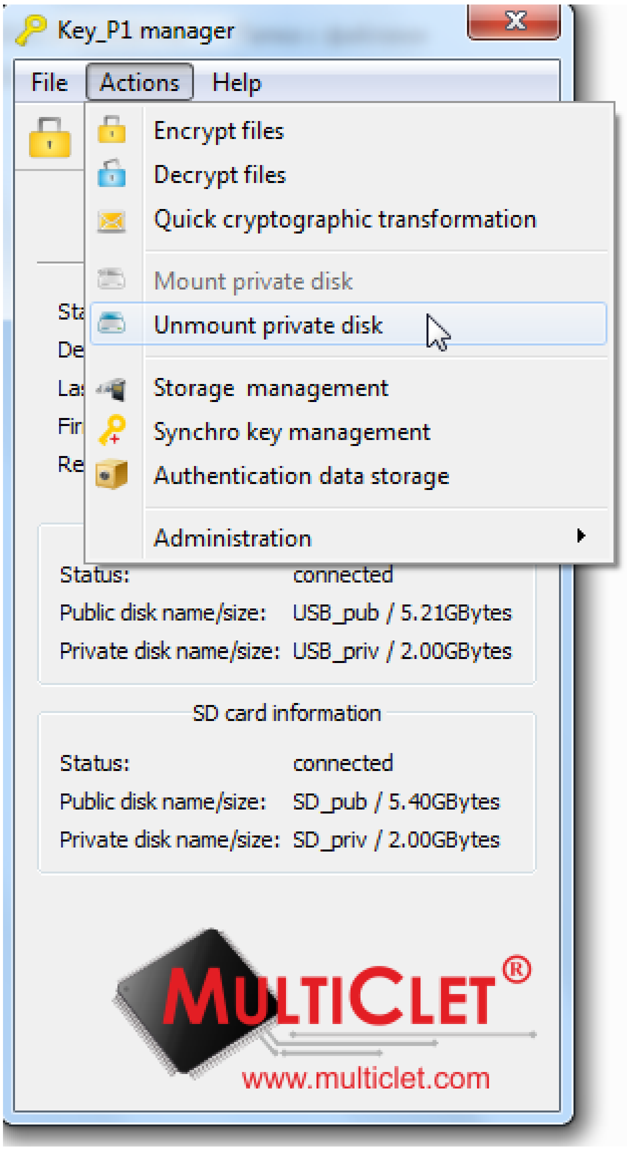
SD card information

Status:	connected
Public disk name/size:	SD_pub / 5.40GBytes
Private disk name/size:	SD_priv / 2.00GBytes

Figure 67: Application main menu

3.1.5 Unmounting private partition

In order to make unmounting procedure of previously created private partition necessary consequentially choose tab **Actions** and command **Unmount private partition** (fig. 68).



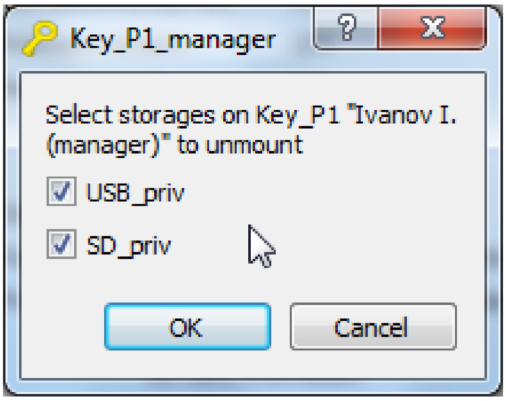
Status: connected
Public disk name/size: USB_pub / 5.21GBytes
Private disk name/size: USB_priv / 2.00GBytes

SD card information

Status: connected
Public disk name/size: SD_pub / 5.40GBytes
Private disk name/size: SD_priv / 2.00GBytes

Figure 68: Unmounting private partition

Set checkbox appropriate private partition, which necessary mount and press button «OK» (fig. 69).



Key_P1_manager

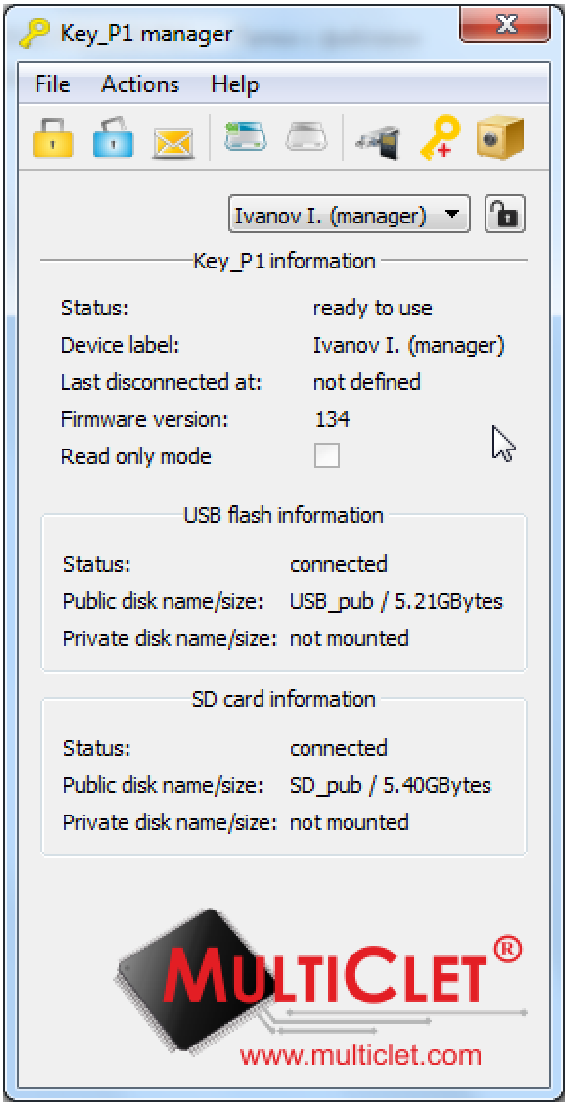
Select storages on Key_P1 "Ivanov I. (manager)" to unmount

☑ USB_priv

☑ SD_priv

Figure 69: Storage choice

Application main menu will be look likes as shown at fig. 70



Key_P1 manager

Key_P1 information

Status: ready to use

Device label: Ivanov I. (manager)

Last disconnected at: not defined

Firmware version: 134

Read only mode □

USB flash information

Status: connected

Public disk name/size: USB_pub / 5.21GBytes

Private disk name/size: not mounted

SD card information

Status: connected

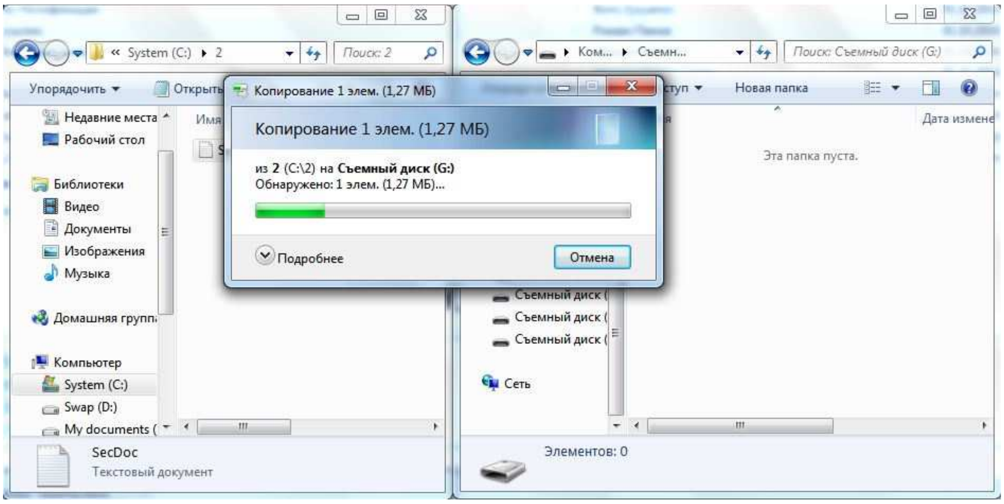
Public disk name/size: SD_pub / 5.40GBytes

Private disk name/size: not mounted

Figure 70: Application main menu

3.1.6 Using private partition

Private partition is intended to store information in an encrypted form. In order to encrypt information necessary make usual operation "copy" to private partition. This operation can be performed with command «Copy» on OS or with drag and drop system (fig. 51).



Копирование 1 элем. (1,27 МБ)

из 2 (C:\2) на Съемный диск (G:)
Обнаружено: 1 элем. (1,27 МБ)...

Figure 71: Copying information on private partition

This procedure identical for private partition, created on the USB storage, and for private partition, created on the SD card.

In order to decrypt files from private partition enough copy file from private partition to any available memory of file system.

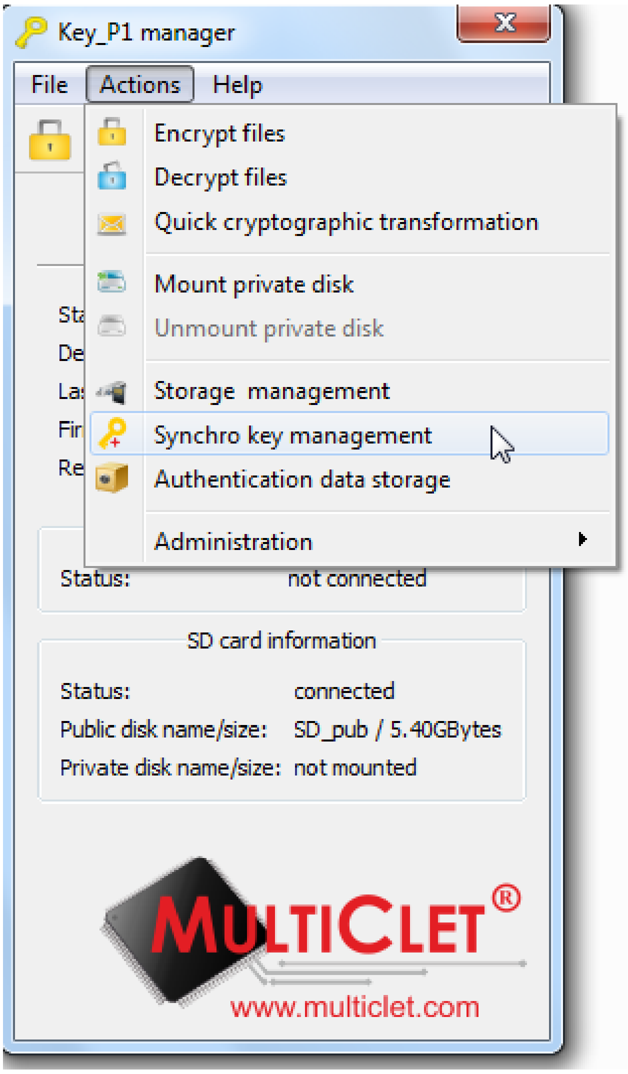
3.2 Synchro key management

Synchro key is intended that users can create identical keys to exchange encrypted messages between users and main company office in case exchange confidential data during business trip by email and other internet sources.

3.2.1 Synchro key adding

Before start creating synchro keys, users, who plan transfer encrypted information, necessary to make exchange between themselves following parameters in order to create synchro key: alghorithm number (the first, the second or the third) and key sentence (initial value or phrase) that generate identical keys for ever user.

In order to perform synchro key creating procedure necessary consequentially choose tab **Actions** and submenu item **Synchro key management** (fig. 72).



Status: not connected

SD card information

Status: connected
Public disk name/size: SD_pub / 5.40GBytes
Private disk name/size: not mounted

Figure 72: Synchro key management

Window for entering user PIN will be display. After enter user PIN press button «OK» (fig. 73).

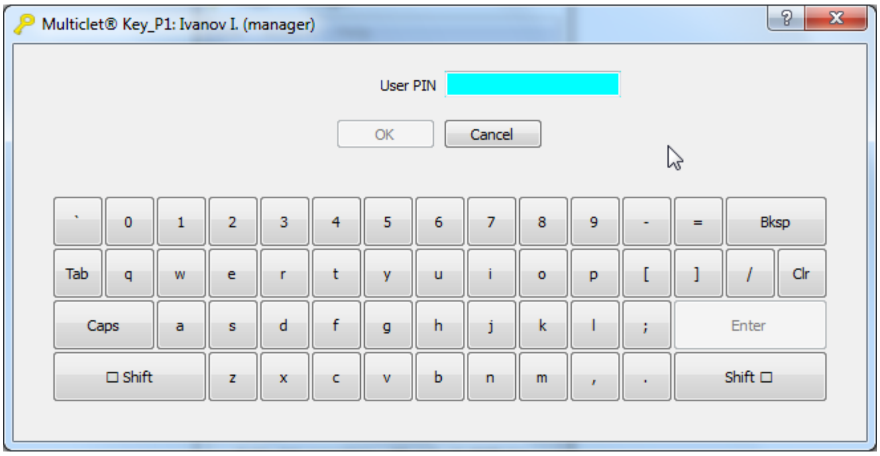

Multiclet® Key_P1: Ivanov I. (manager)
User PIN
OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 73: Entering user PIN

At the window **Synchro key management** (fig. 74) necessary press button «Add».

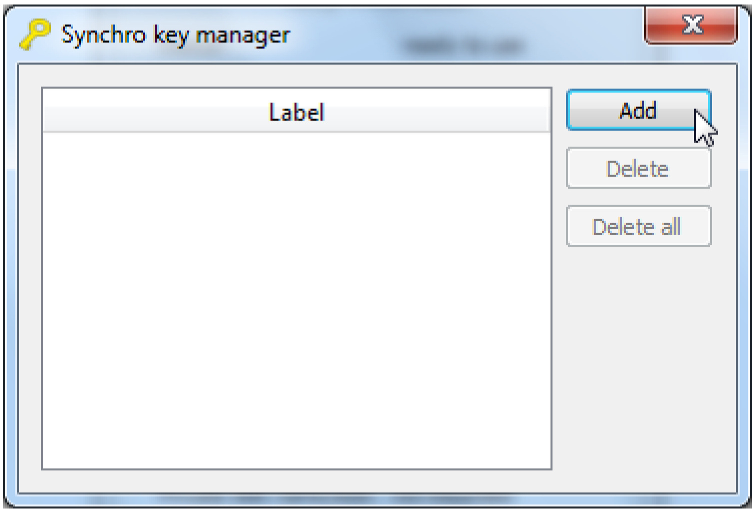
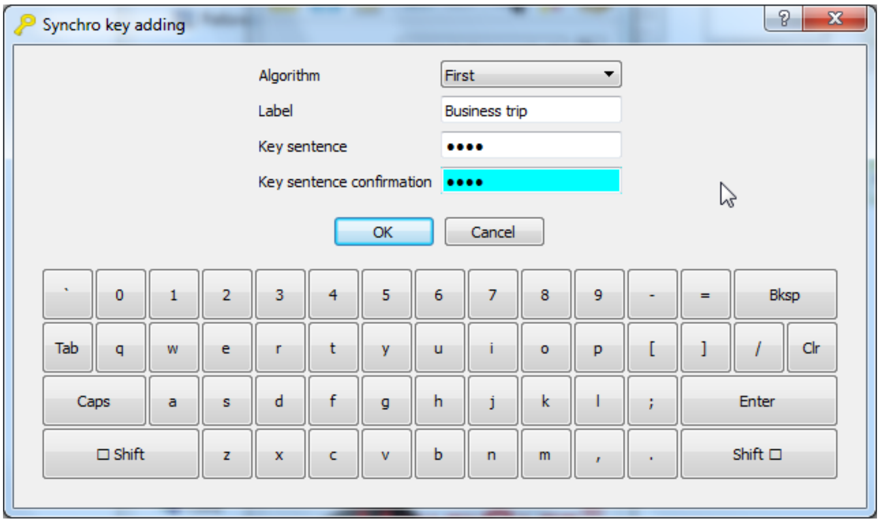


Figure 74: Synchro key management

At the window **Synchro key adding** (fig. 75) necessary set **Algorithm**, at the **Label** field type description of the key, at the **Key sentence** and **Confirmation key sentence** fields necessary type word or phrase for creating key. After all actions press button «OK».



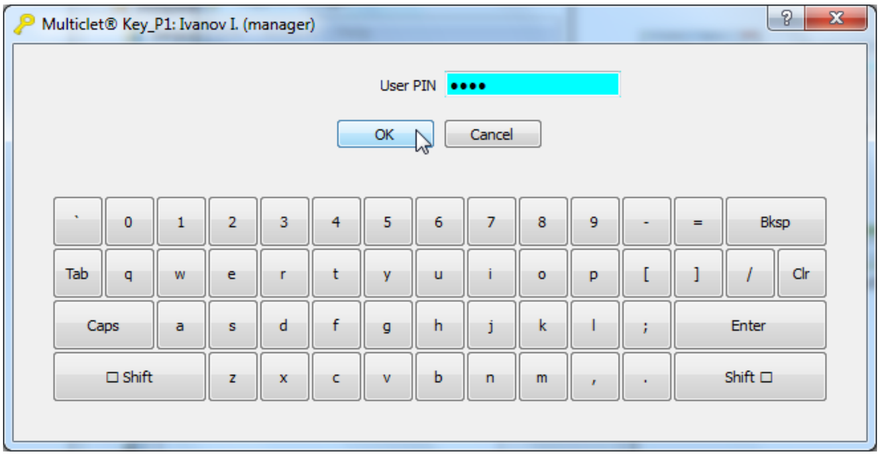
Synchro key adding

Algorithm: First
Label: Business trip
Key sentence: ••••
Key sentence confirmation: ••••

OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 75: Synchro key adding

Window for entering user PIN will be display. After enter user PIN press button «OK» (fig. 76).



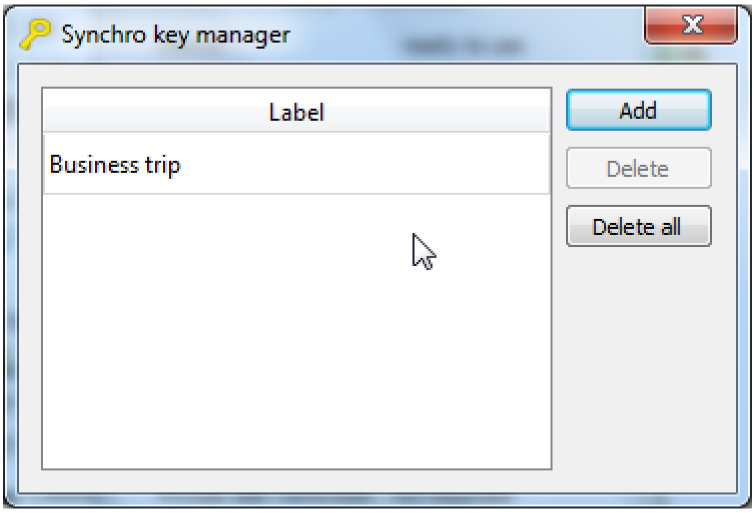
Multiclet® Key_P1: Ivanov I. (manager)

User PIN: ••••

OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 76: Entering user PIN

After all actions performed, at the window **Synchro key management** (fig. 77) will be display information about synchro key.

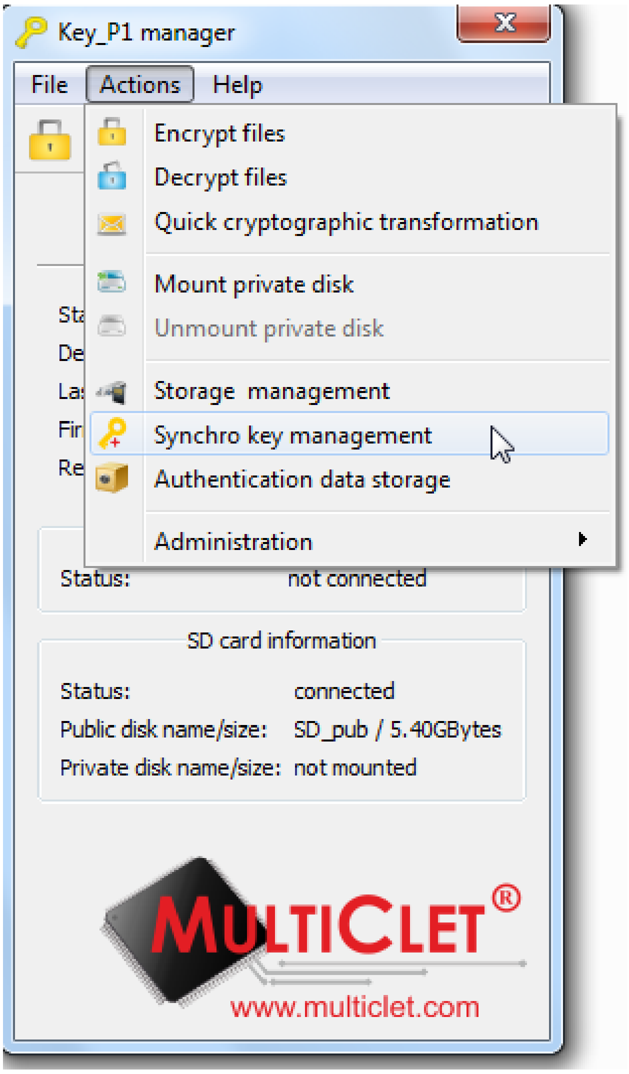


Business trip

Figure 77: Synchro key management

3.2.2 Synchro key deleting

In order to perform synchro key deleting procedure necessary consequentially choose tab **Actions** and choose **Synchro key management** item (fig. 78).



Status: not connected

Status: connected

Public disk name/size: SD_pub / 5.40GBytes

Private disk name/size: not mounted

Figure 78: Synchro key management

Window for entering user PIN will be display. After enter user PIN press button «OK» (fig. 79).

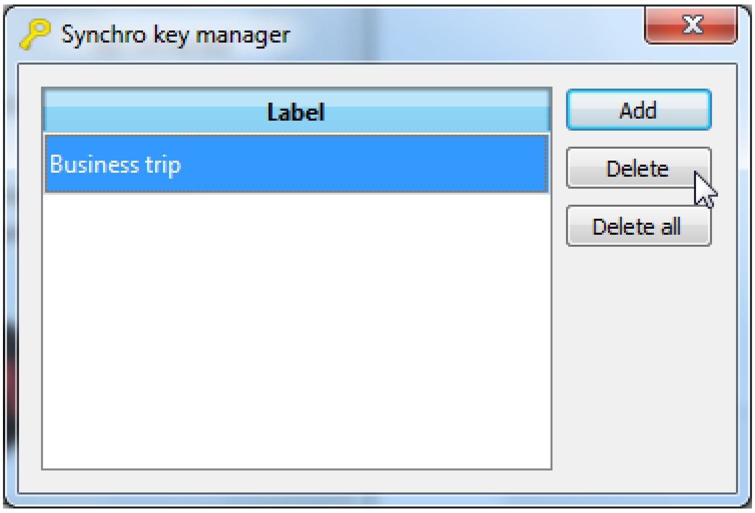


Figure 79: Entering user PIN

At the window **Synchro key management** (fig. 80) necessary select key list, which user want to remove and press button «Delete». If require remove all key list that press button «Delete all».

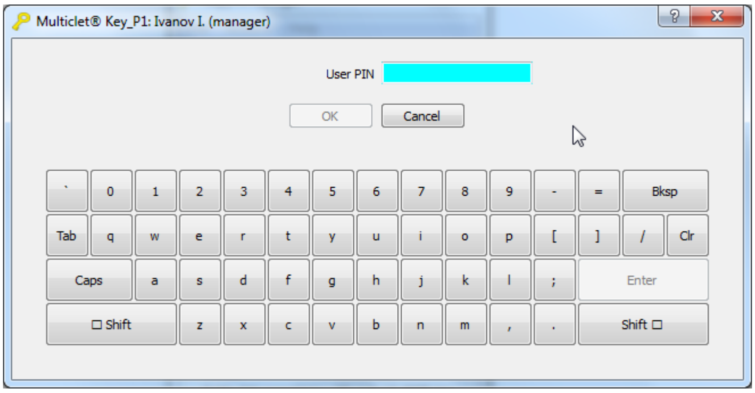
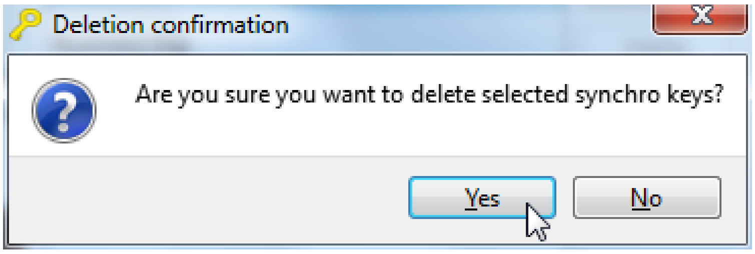

Multiclet® Key_P1: Ivanov I. (manager)
User PIN
OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 80: Synchro key deleting

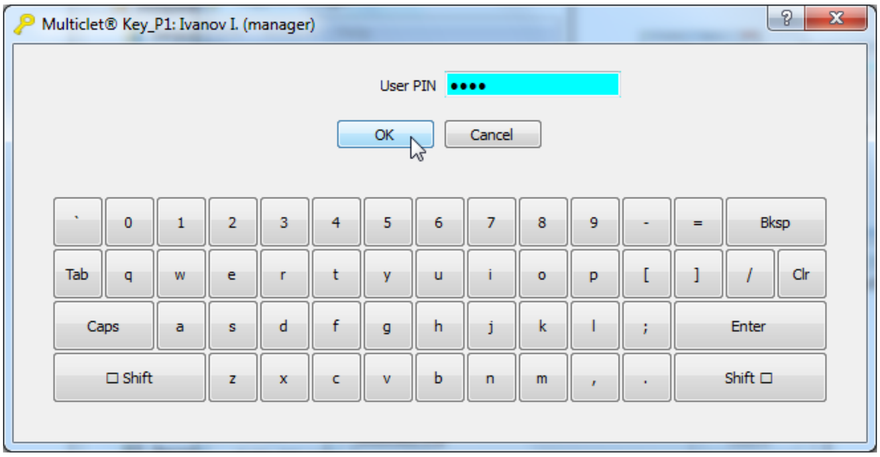
Window with request on confirmation about deleting will be display. Press button «Yes» to complete operation (fig. 81).



Are you sure you want to delete selected synchro keys?

Figure 81: Key deleting

Window for entering user PIN will be display. After enter user PIN press button «OK» (fig. 82).



Multiclet® Key_P1: Ivanov I. (manager)

User PIN ••••

OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 82: Entering user PIN

3.3 Files encryption

Files encryption on the Key_P1 device performed following ways:

1) **automatically when copying files to private partition** of the initialized storage: in this case files at the storage will be encrypted by sector group with some keys from 1024 created in during device initialization procedure.

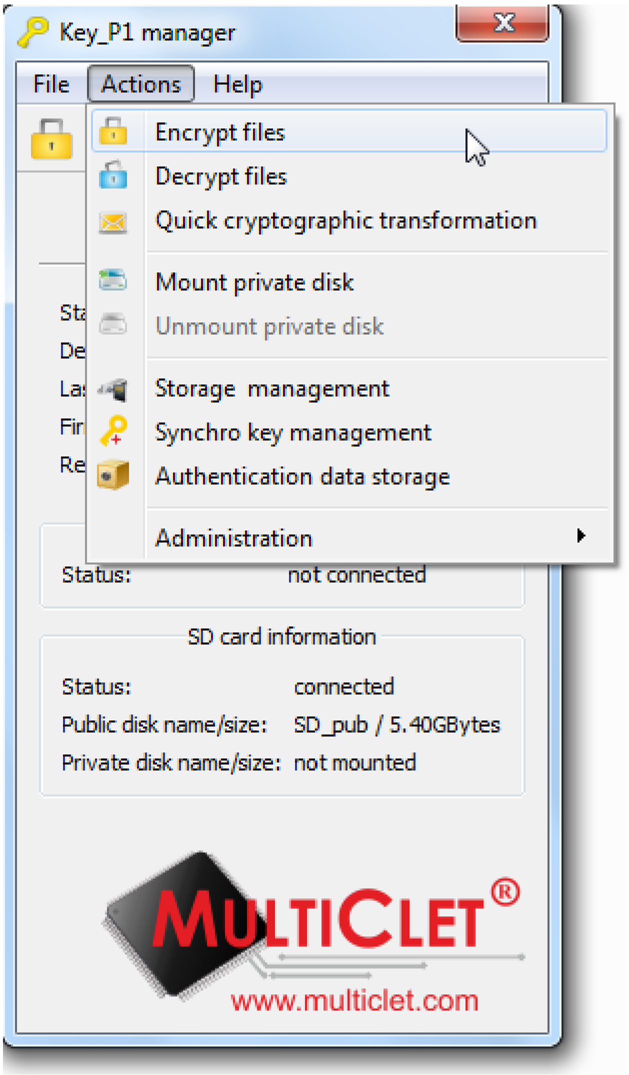
2) One of cryptographical method from field "Files encrypting": in this case files encrypting may be perform one of three methods:

- **random key** (some keys from 1024 keys, install on initialization procedure, one's file parts can be encrypted 1024 keys)

- **synchro key** (with one synchro key)

- **corporate key** (one key from some amount keys intended for corporate group)

In order to perform files encrypted procedure necessary consequentially choose tab **Actions** and **Files encrypt**(fig. 83).



Status: not connected

SD card information

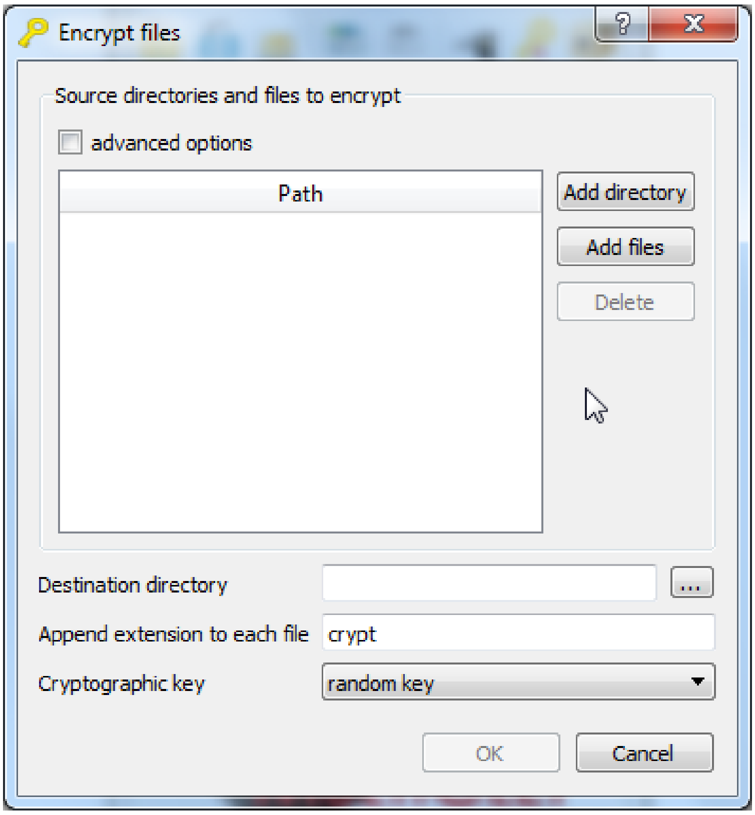
Status: connected

Public disk name/size: SD_pub / 5.40GBytes

Private disk name/size: not mounted

Figure 83: Files encryption

Window **Encrypt files** will be display (fig. 84). At the field **Source directory and files to encrypt** necessary with button **Add files** and **Add directory** add files or directory to encrypt (all files from directory will be encrypt).



Encrypt files

Source directories and files to encrypt

□ advanced options

Path

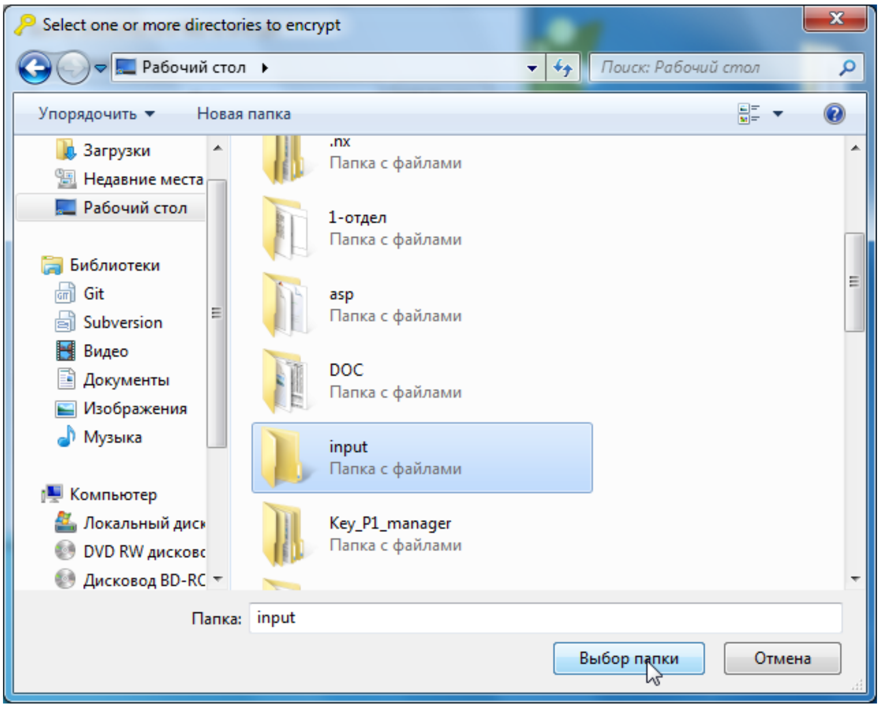
Destination directory

Append extension to each file: crypt

Cryptographic key: random key

Figure 84: Files encryption

For example press button **Add directory** and choose folder **input**. Thus all files in selected directory will be encrypt. Directory choice shown at the fig. 85

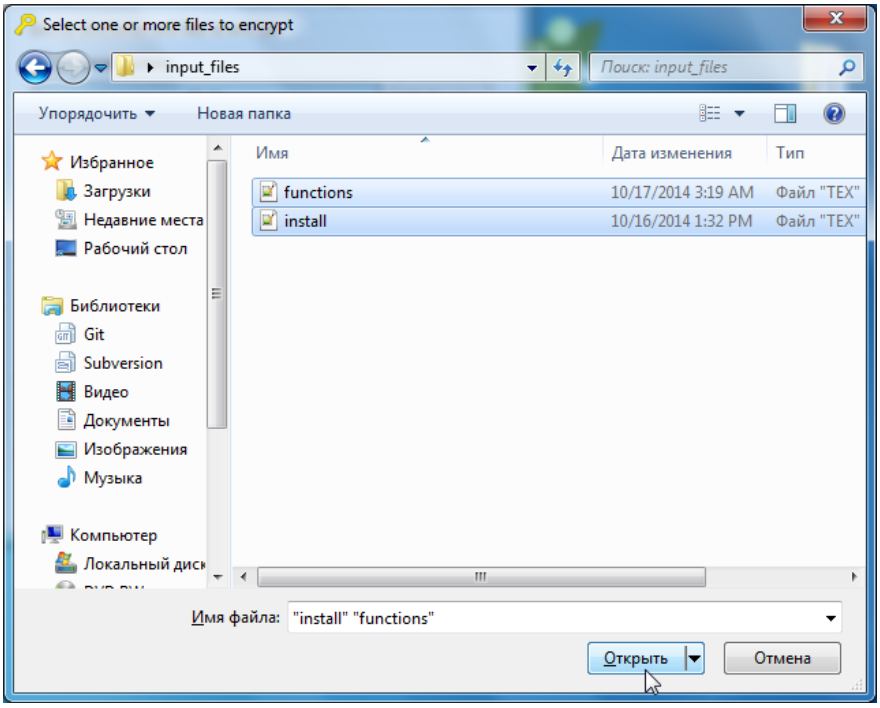


Select one or more directories to encrypt

Папка: input

Figure 85: Directory choice

In the next step press button **Add files** and choose two files, which plan to encrypt.



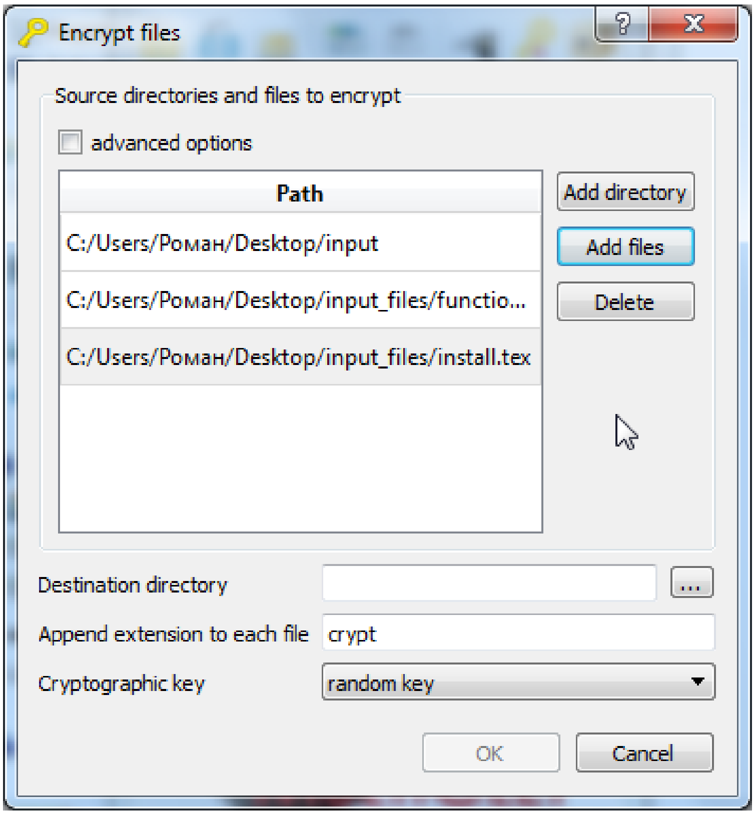
Select one or more files to encrypt

Имя	Дата изменения	Тип
functions	10/17/2014 3:19 AM	Файл "TEX"
install	10/16/2014 1:32 PM	Файл "TEX"

Имя файла: "install" "functions"

Figure 86: Files select

In the main window for encryption necessary set output directory (path to save encrypted files) and encrypted method. Current window to encrypt files shown at the fig. 87.



Source directories and files to encrypt

□ advanced options

Path
C:/Users/Роман/Desktop/input
C:/Users/Роман/Desktop/input_files/functio...
C:/Users/Роман/Desktop/input_files/install.tex

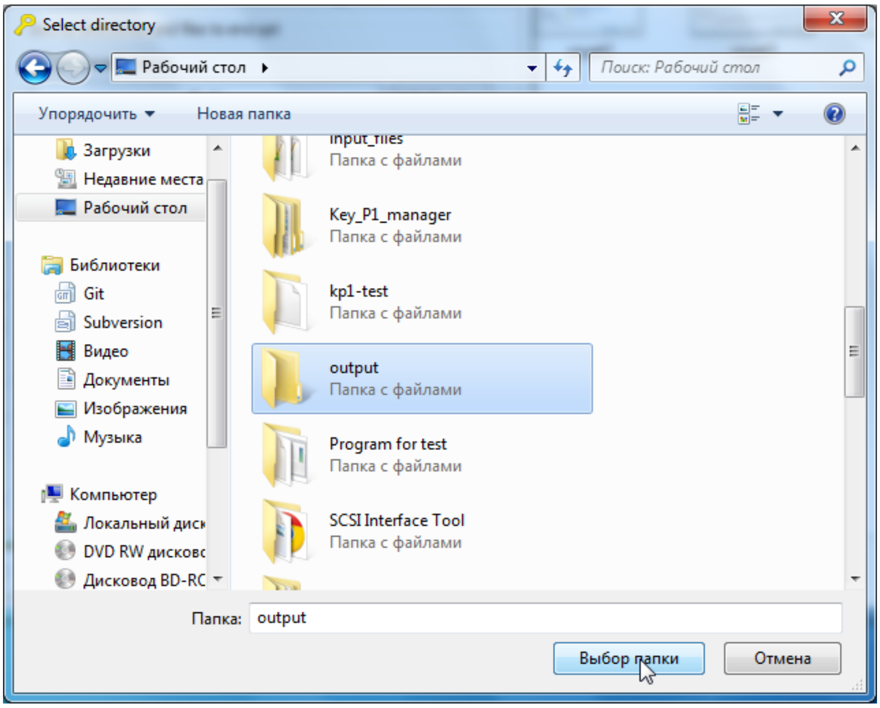
Destination directory

Append extension to each file: crypt

Cryptographic key: random key

Figure 87: Window for encryption

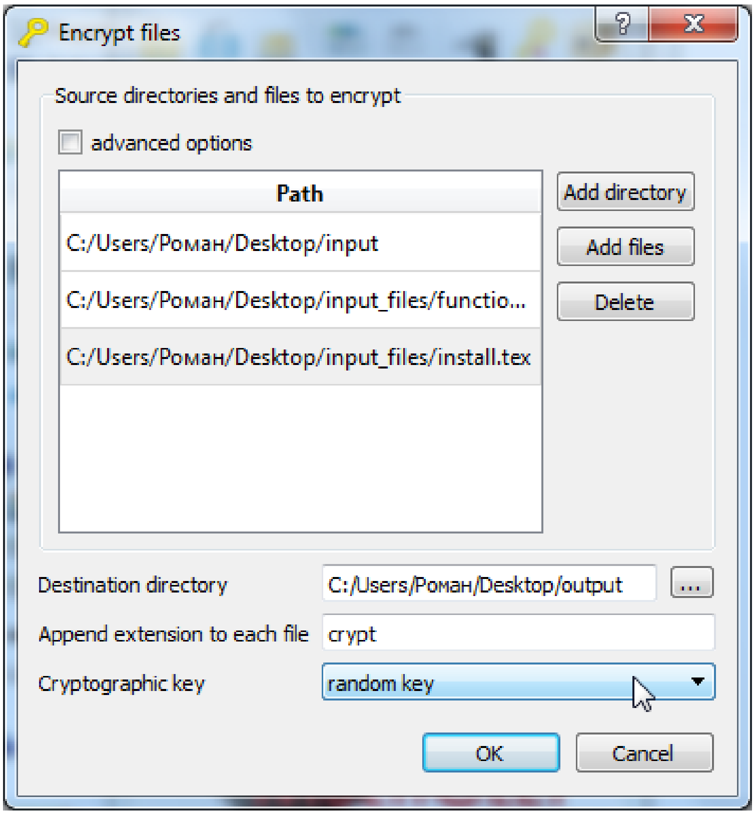
Choose directory for encrypted files as shown at the fig. 88.



Папка: output

Figure 88:

At the window for encryption choose cryptographical method (in our example its "random"). Window for encryption will be as shown at the fig. 89. Press button "OK" to start files encrypt.



Encrypt files

Source directories and files to encrypt

□ advanced options

Path
C:/Users/Роман/Desktop/input
C:/Users/Роман/Desktop/input_files/functio...
C:/Users/Роман/Desktop/input_files/install.tex

Destination directory C:/Users/Роман/Desktop/output

Append extension to each file crypt

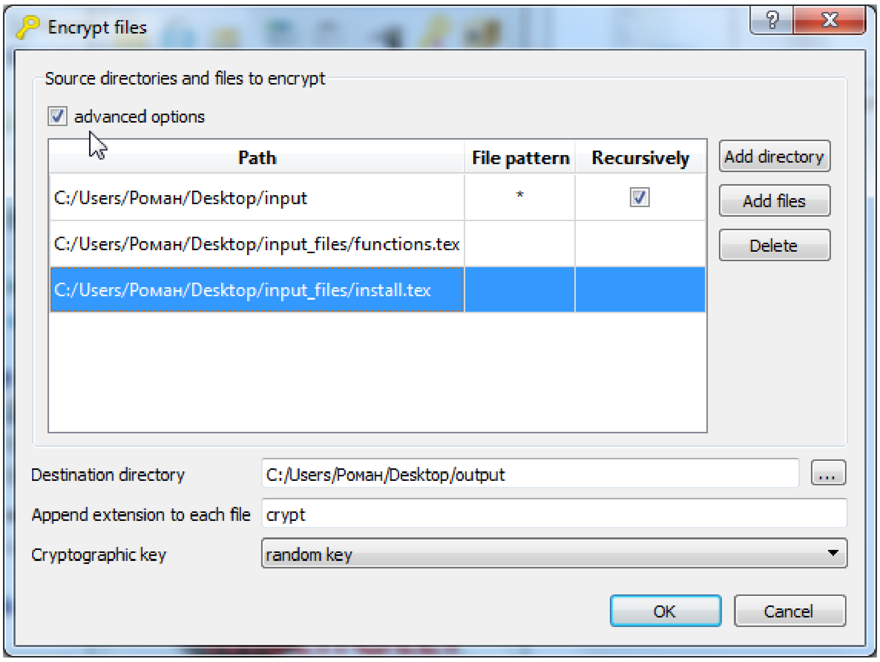
Cryptographic key random key

Figure 89: Select destination path

If at the field **Source directory and files to encrypt** was added directory that after set checkbox at the field additional options will be display following options (fig. 90):

1)File pattern. Define pattern to encrypt files. All files in the directory appropriate pattern will be encrypt.

2)Recursively. If set checkbox at this field all files at the directory and subdirectories will be encrypt. If checkbox not set that files from chose directory.



Encrypt files

Source directories and files to encrypt

☑ advanced options

Path	File pattern	Recursively
C:/Users/Роман/Desktop/input	*	☑
C:/Users/Роман/Desktop/input_files/functions.tex		
C:/Users/Роман/Desktop/input_files/install.tex		

Destination directory: C:/Users/Роман/Desktop/output

Append extension to each file: crypt

Cryptographic key: random key

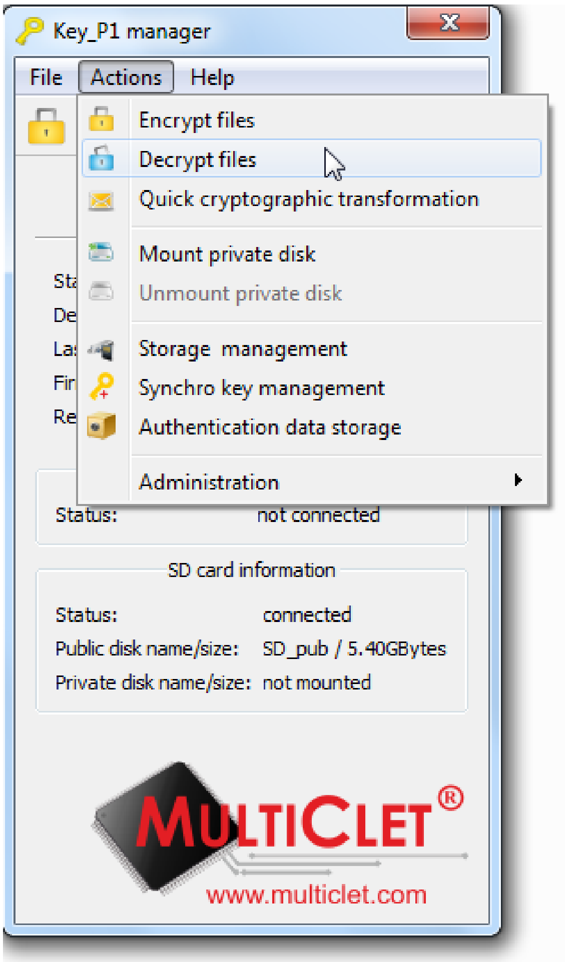
Figure 90: Encrypting files with additional options

In order to remove files or directory from list **Source directory and files to encrypt** necessary highlight files or directory and press button «Delete».

At the field **Add extension to encrypt files** there is a way to set extension, which file will be have. As a default files after enrypt procedure have extension «crypt». At the field **Cryptographical key** necessary choose encryption method, which will be use in encryption procedure. Available three methods: random key, synchro key and corporate key. After completed all actions press button «OK» to start encryption procedure.

3.4 Files decryption

In order to make files decryption procedure necessary consequentially choose tab **Actions** and **Decrypt files** item (fig. 91).



Status: not connected

SD card information

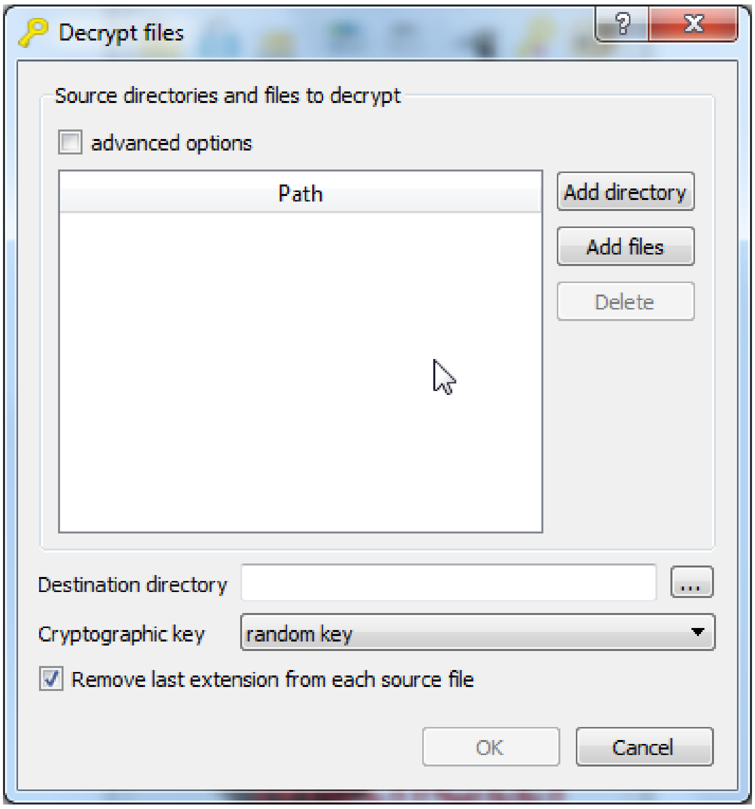
Status: connected

Public disk name/size: SD_pub / 5.40GBytes

Private disk name/size: not mounted

Figure 91: Files decryption

Window **Decrypt files** will be display(fig. 92). At the field **Source directory and files to decrypt** necessary with button **Add files** and **Add directory** add files or directory to decrypt (all files from diectory will be decrypt).



Decrypt files

Source directories and files to decrypt

□ advanced options

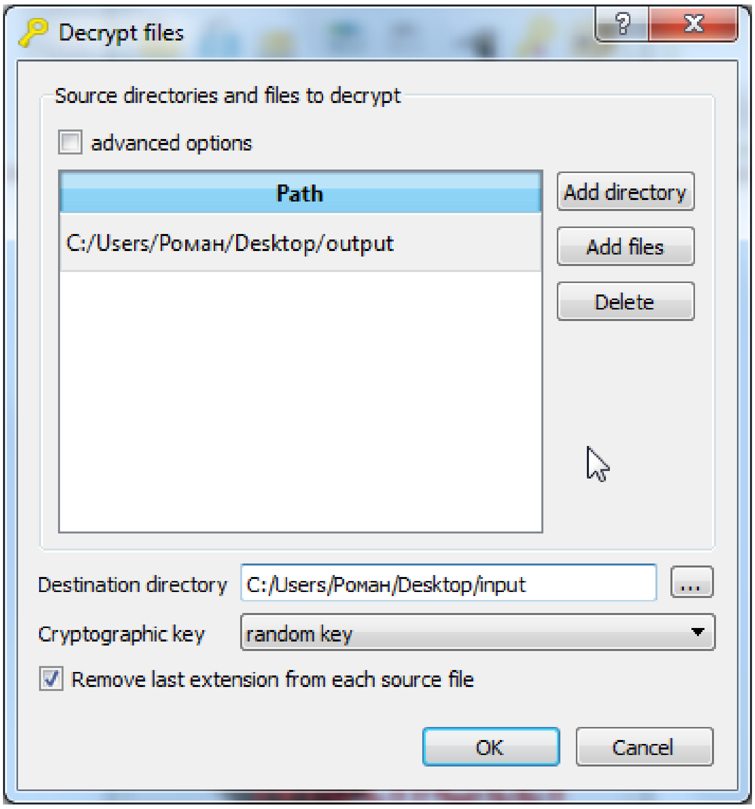
Destination directory

Cryptographic key: random key

☑ Remove last extension from each source file

Figure 92: Files decryption

For example add directory with files, which plan to decrypt. And add destination directory for decrypted files. At the fig. 93 shown example with choosing directory path.



Decrypt files

Source directories and files to decrypt

☐ advanced options

Path
C:/Users/Роман/Desktop/output

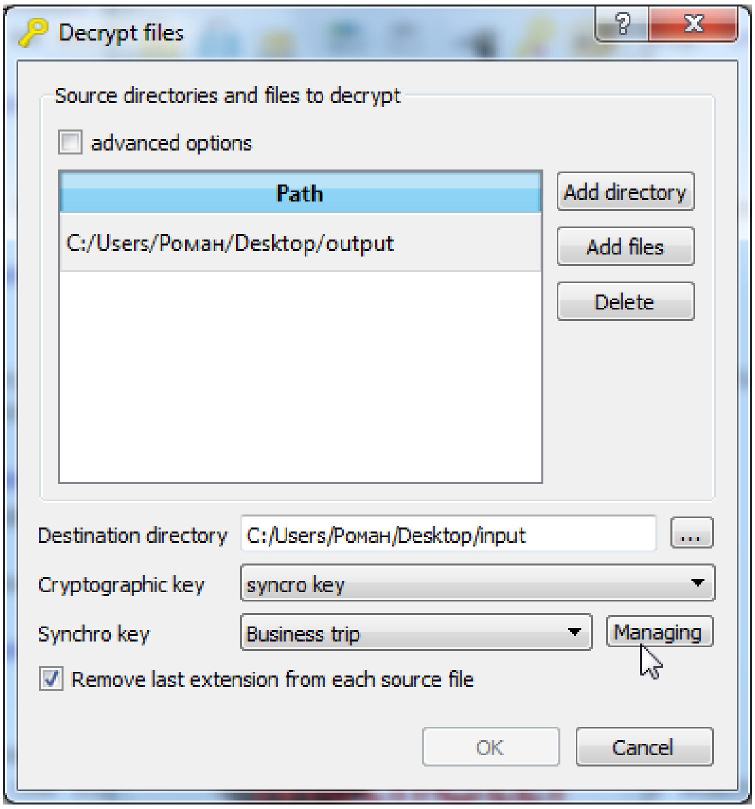
Destination directory: C:/Users/Роман/Desktop/input

Cryptographic key: random key

☑ Remove last extension from each source file

Figure 93: Directory select

Choose cryptographical key (method) - synchro key and select key with label "Business trip". There is button "Management" for quick management with synchro keys. Window illustrate it shown at the fig. 94.



Decrypt files

Source directories and files to decrypt

□ advanced options

Path
C:/Users/Роман/Desktop/output

Destination directory: C:/Users/Роман/Desktop/input

Cryptographic key: syncro key

Synchro key: Business trip

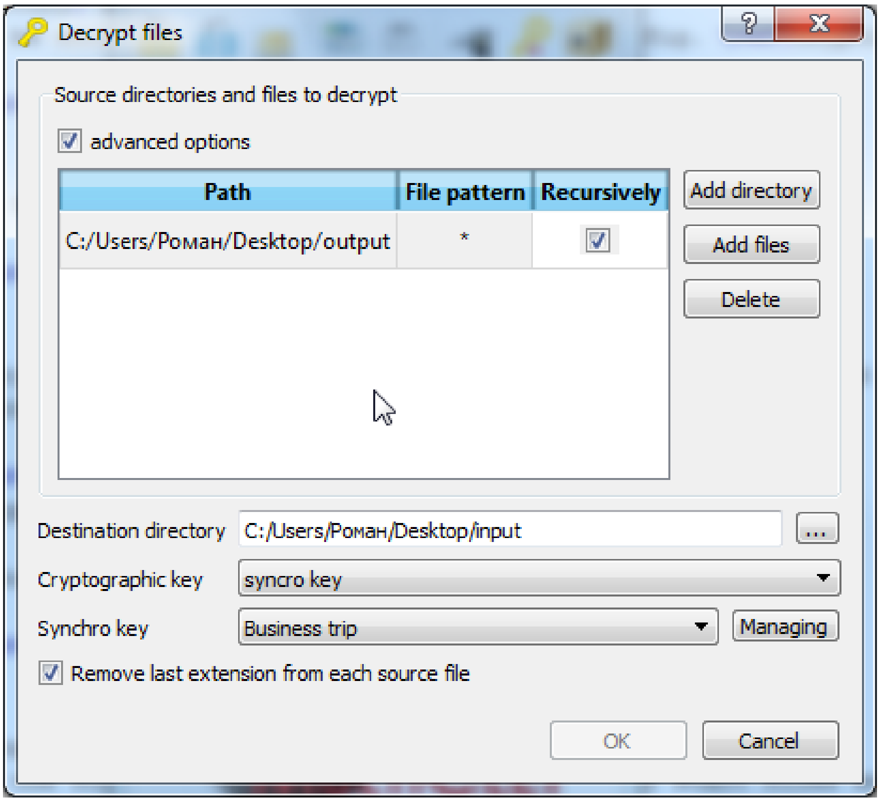
☑ Remove last extension from each source file

Figure 94: Directory select

If at the field **Source directory and files to decrypt** was added directory that after set checkbox at the field additional options will be display following options (fig. 95):

1)File pattern. Define pattern to decrypt files. All files in the directory appropriate pattern will be decrypt.

2)Recursively. If set checkbox at this field all files at the directory and subdirectories will be decrypt. If checkbox not set that files from chose directory.



Decrypt files

Source directories and files to decrypt

☑ advanced options

Path	File pattern	Recursively
C:/Users/Роман/Desktop/output	*	☑

Destination directory: C:/Users/Роман/Desktop/input

Cryptographic key: syncro key

Synchro key: Business trip

☑ Remove last extension from each source file

Figure 95: Files decryption

In order to remove files or directory from list **Source directory and files to encrypt** necessary highlight files or directory and press button «Delete».

At the field **Remove last extension from each source files** there is a way to remove extension, which file has before decryption. As a default files after decrypt procedure will be clear from extension «crypt». At the field **Cryptographical key** necessary choose encryption method, which will be use in encryption procedure. Available three methods: random key, synchro key and corporate key. After completed all actions press button «OK» to start decryption procedure.

3.5 Quick cryptographic transformation

Quick cryptographic transformation necessary for quick text messages encrypt or decrypt. In order to start work quick cryptographic transformation necessary sequentially choose tab **Actions** and choose **Quick cryptographic transformation** item (fig. 96).

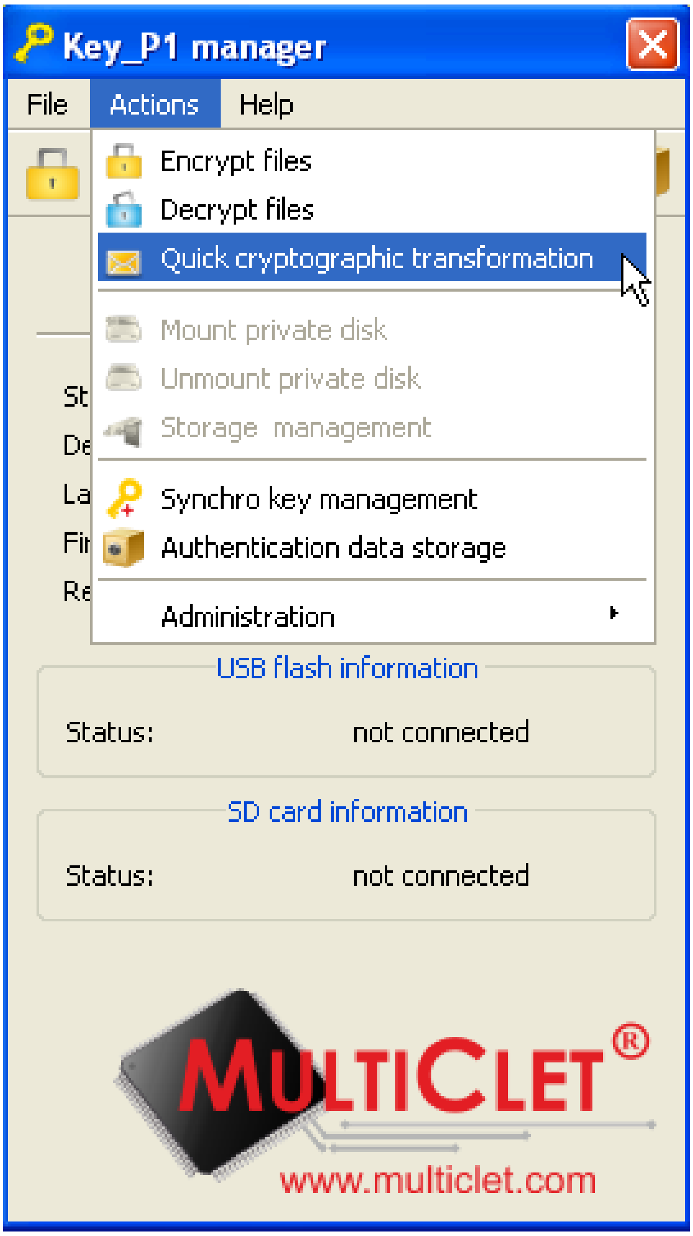
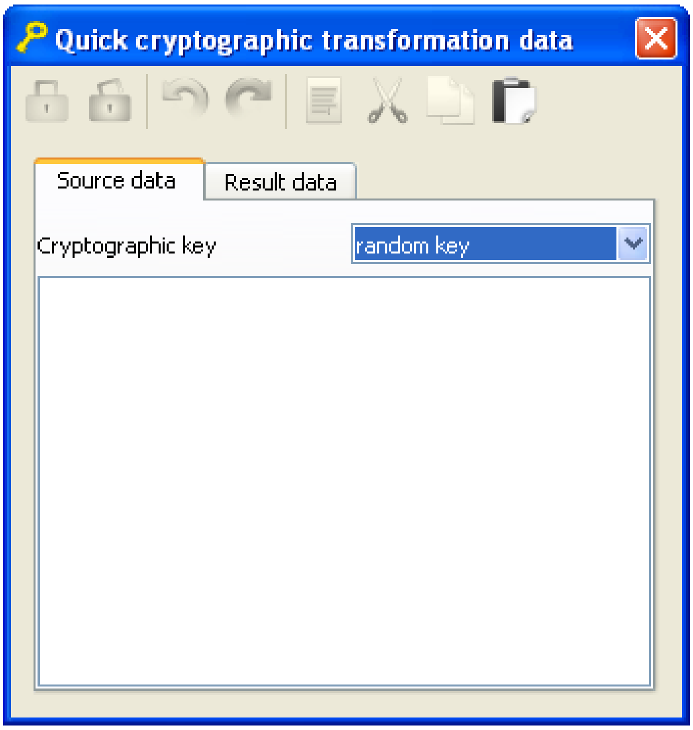


Figure 96: Choosing item

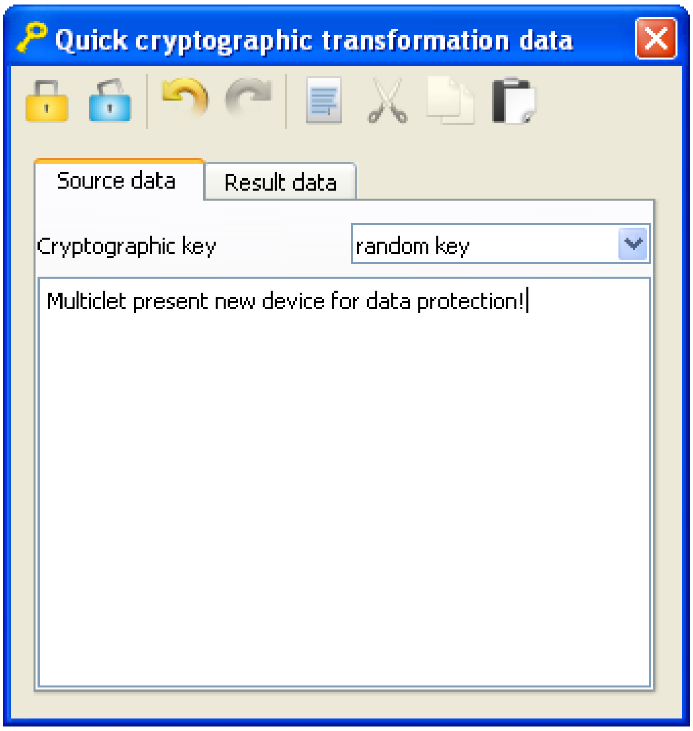
Window for text message encryption and decryption will be display (fig. 97).



Cryptographic key: random key

Figure 97: Quick cryptographic transformation

For example at the field **Source data** type text message for encryption, as shown at the fig. 98

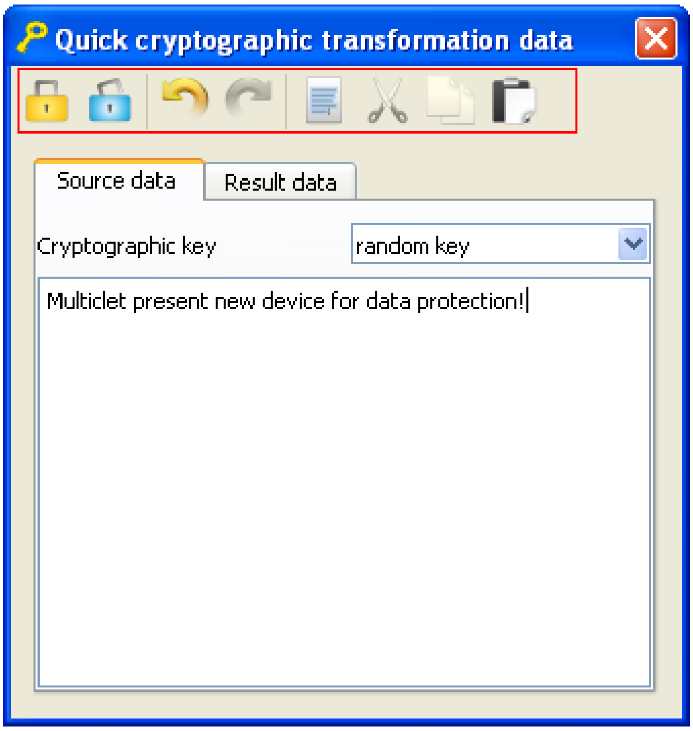


Cryptographic key: random key

Multiclet present new device for data protection!

Figure 98: Message for encryption

After typing text message toolbar will be active (put in red at the fig. 99)



Cryptographic key: random key

Multiclet present new device for data protection!

Figure 99: Toolbar

Toolbar items:

1) **Message encrypt**

2) **Message decrypt**

3) **Cancel**

4) **Return**

5) **Select**

6) **Cut**

7) **Copy**

8) **Paste**

At the field **Cryptographic key** can choose following options: random, synchro or corporate. After press button **Message encryption** and choice cryptographic key will be display window for entering user PIN, as see at the fig. 100.

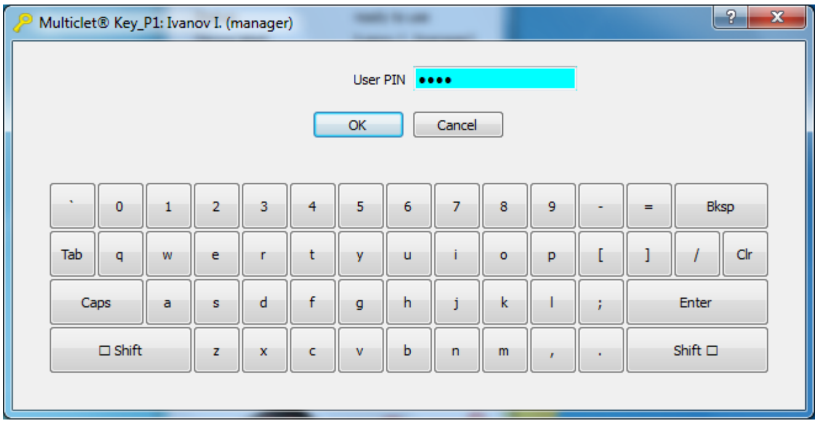
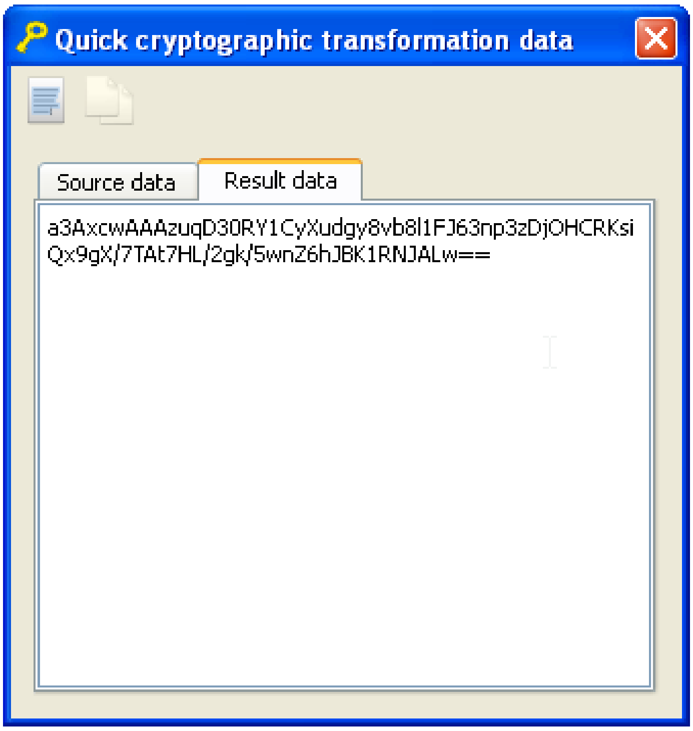

Multiclet® Key_P1: Ivanov I. (manager)
User PIN ●●●●
OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 100: Entering user PIN

In case successful entering user PIN will be display tab **Result data**, as shown at the fig. 101. Encrypted message can select with OS service or press button **Select all** at the toolbar. Then you may open messager, social net, mail client or other and paste "Result data".



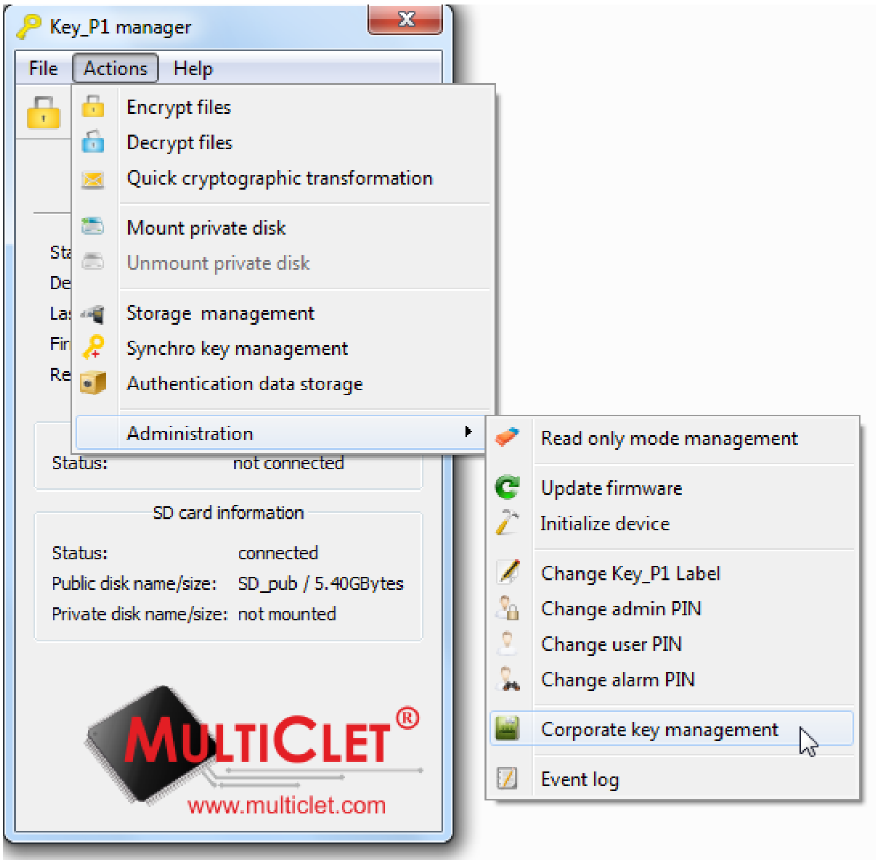
a3AxcwAAAzuqD30RY1CyXudgy8vb8l1FJ63np3zDjOHCRKsi
Qx9gX/7TAt7HL/2gk/5wnZ6hJBK1RNJALw==

Figure 101: Result data

Message decryption perform similar method.

3.6 Corporate key management

In order to start work with corporate keys necessary consequentially choose tab **Actions** go to submenu **Administration** and choose **Corporate key management**(fig. 102).



Status: not connected

SD card information

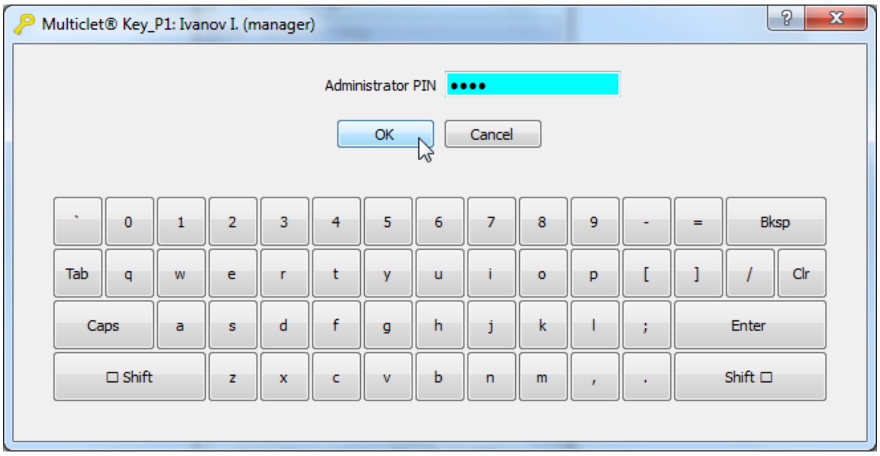
Status: connected

Public disk name/size: SD_pub / 5.40GBytes

Private disk name/size: not mounted

Figure 102: Corporate key management

Window with entering administrator PIN field will be display. Press button «OK» after entering administrator PIN (fig. 103).



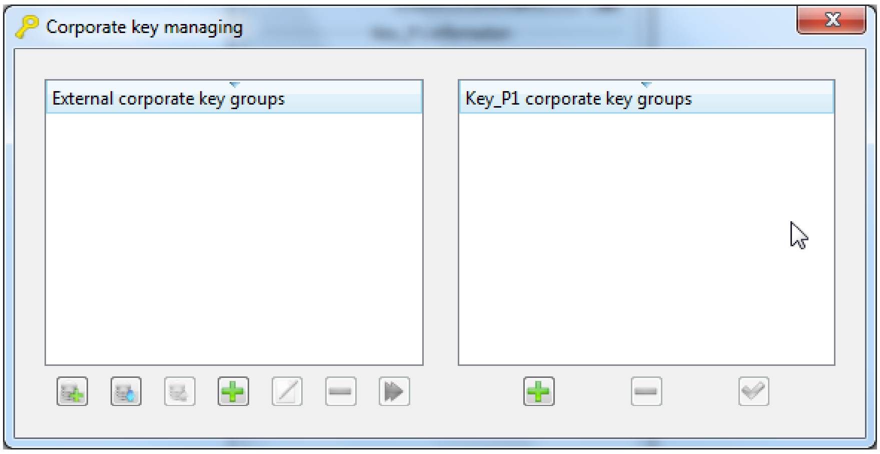
Multiclet® Key_P1: Ivanov I. (manager)

Administrator PIN ●●●●

OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 103: Entering administrator PIN

Window **Corporate key management** will be appear (fig. 104).



Corporate key managing

External corporate key groups

Key_P1 corporate key groups

Figure 104: orporate key management

This window is divide on: **Eternal corporate key base** and **Key_P1 corporate key base**. External corporate key management perform with following toolbar (fig. 105)(highlight in red):

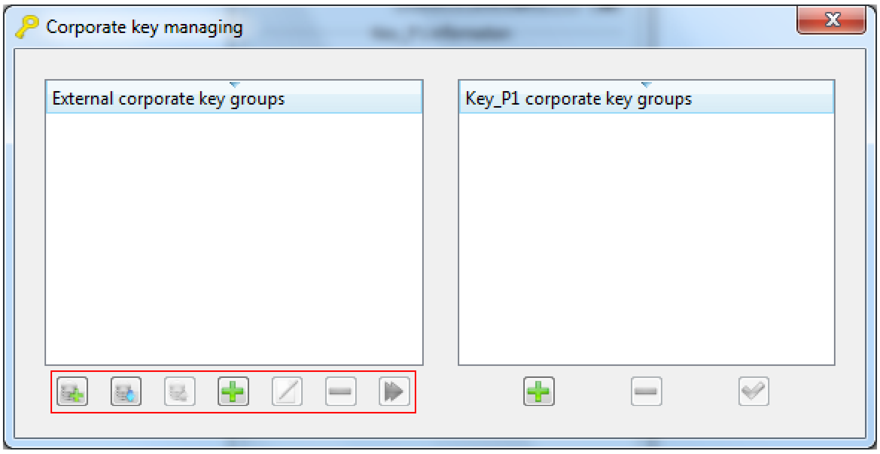


Figure 105: Corporate key management

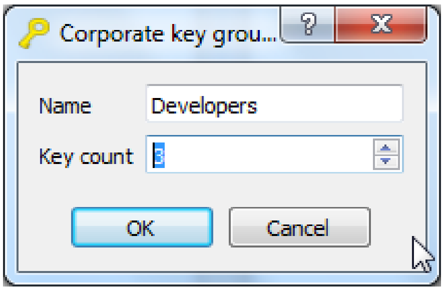
Observe items are intended to manage external base:

1) **Create new corporate key base** - creating new base;

2) **Open corporate key base** - open corporate key base;

3) **Save corporate key base** - save current base to file;

4) **Add corporate key group to base** - adding corporate key group. To do this action necessary set group label and keys count (fig. 106);



Name: Developers

Key count: 3

Figure 106: Adding corporate key group

For example add group "Developers" and for its group will be generate 3 keys. After press button "OK" will be display window shown at the fig. 107.

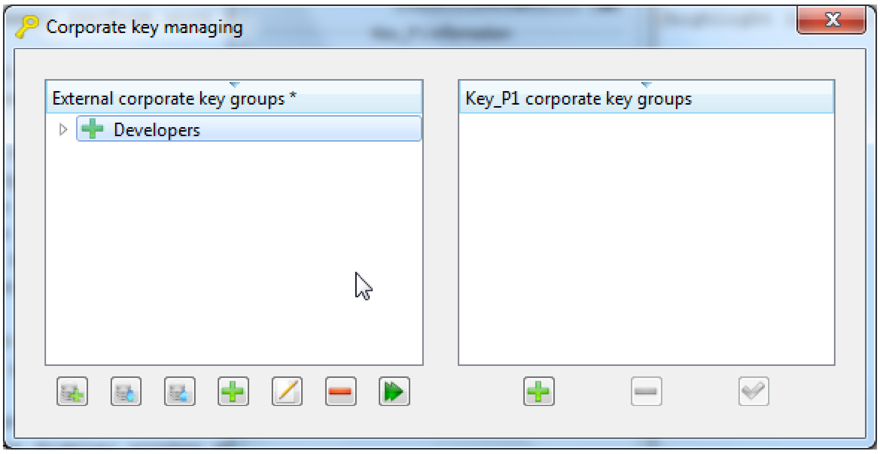
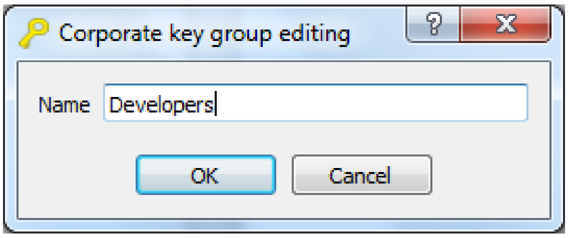


Figure 107: Adding corporate key group

5) **Edit corporate group in base** - this command allow to change corporate key group label; Window for changing corporate key group label shown at the fig. 108



Name: Developers

Figure 108: Changing corporate key label

6) **Deleting corporate key group from base** - delete corporate key group from base.

Management Key_P1 corporate key base perform with the following commands as icons from left to the right (fig. 109)(highlight in red):

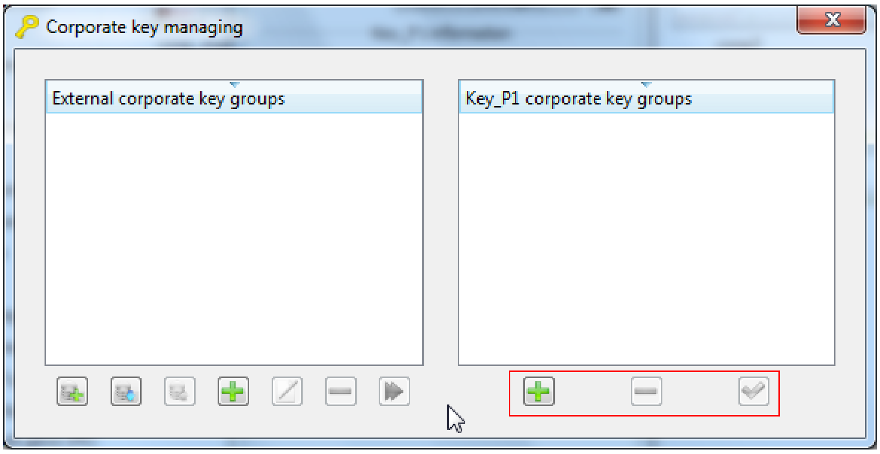
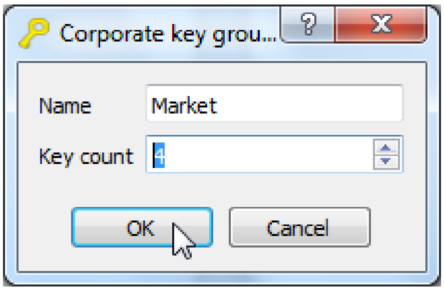


Figure 109: Corporate key management

1) **Add corporate key group in Key_P1 base** - adding corporate key to Key_P1 base. To do this operation necessary set group name and keyscount (fig. 110);


Corporate key grou...

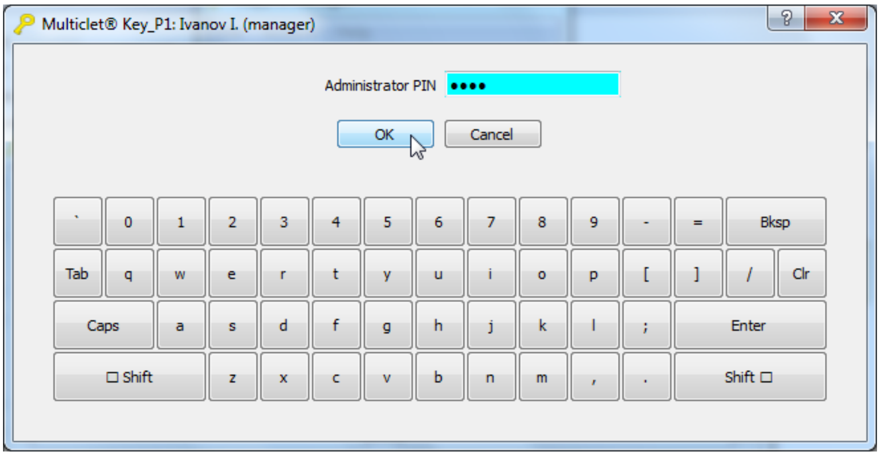
Name: Market

Key count: 4

Figure 110: Adding corporate keys group

2) **Delete corporate key group from Key_P1 base** - deleting corporate key group from Key_P1 base;

3) **Apply changing in Key_P1 base** - saving all changing in Key_P1 base. After complete this command necessary enter administrator PIN (fig. 111). Press button «OK» to continue.


Multiclet® Key_P1: Ivanov I. (manager)

Administrator PIN: ••••

?
X
OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 111: Enter administrator PIN

After changing apply in the corporate key group base management window will be as shown at the fig. 112. Thus in the device will be create "Market" group.

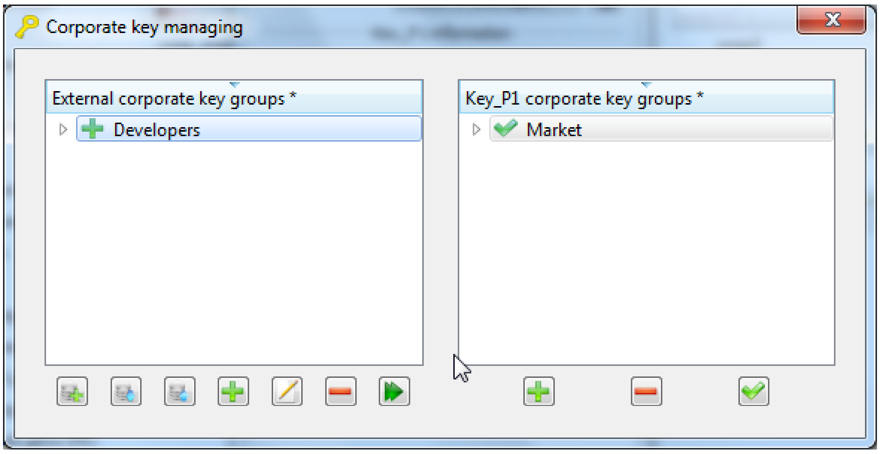

Corporate key managing
External corporate key groups *
Developers
Key_P1 corporate key groups *
Market

Figure 112: Corporate key management

3.6.1 Hierarchical access creating example

Consider the example about hierarchical access organization. Open window «Corporate key management»(tab Actions->Administration) and in the left section press button «Add corporate key group into database» , as shown at the fig. 113

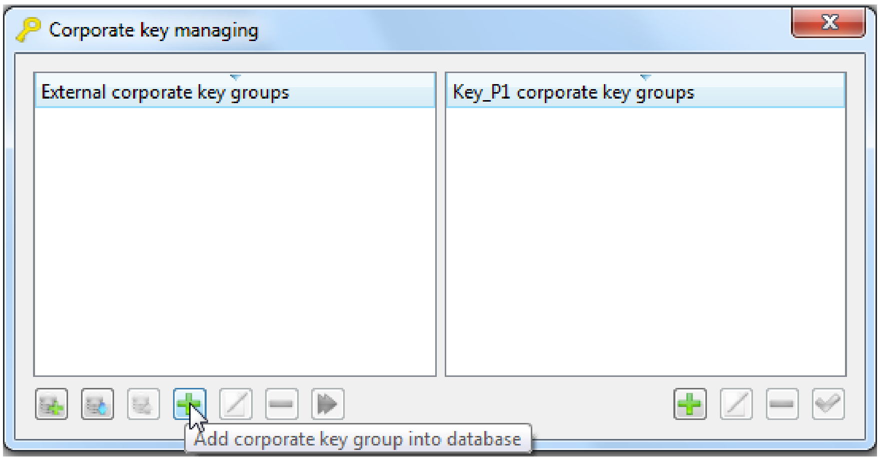
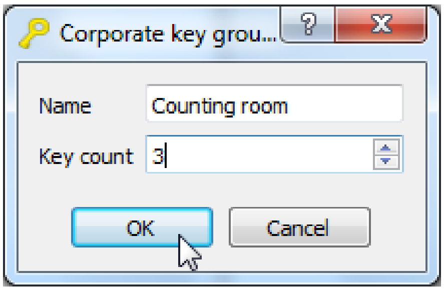

Corporate key managing
External corporate key groups
Key_P1 corporate key groups
Add corporate key group into database

Figure 113: Corporate key management

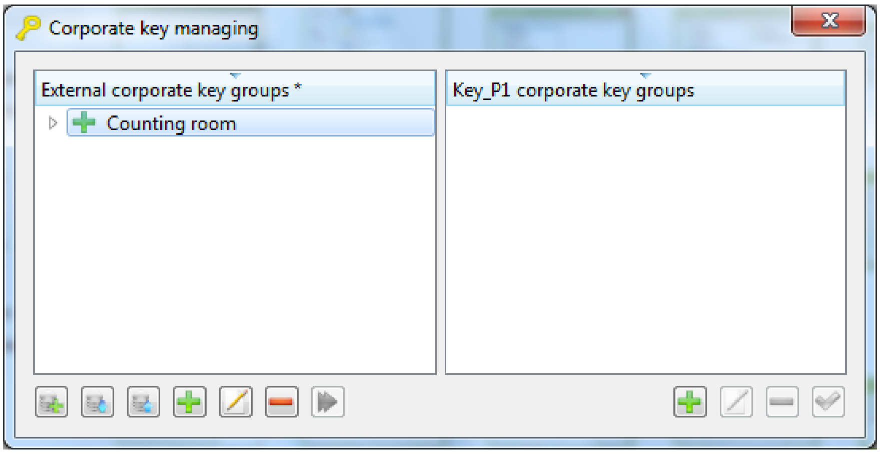
Create corporate key group «Counting room» and generate 3 keys for this group. Note that assignment several keys to this group does not complicate work, because device Key_P1 automatically recognize that user have or have not keys to decryption file for selected group name. Let us consider this point later. Corporate key group creation example shown at the fig. 114



Name: Counting room
Key count: 3

Figure 114: Corporate key group creation

After press button «Ok» this group will be display in the section external corporate key groups with icon «plus», means that corporate key group created, but not added into the external database, see fig. 115



Corporate key managing

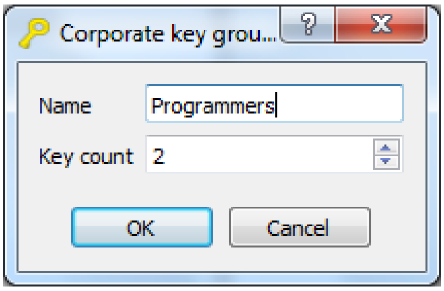
External corporate key groups *

- Counting room

Key_P1 corporate key groups

Figure 115: Corporate key group creation

Similarly add group «Programmers», assign for this 2 keys, which will be generate, see fig. 116



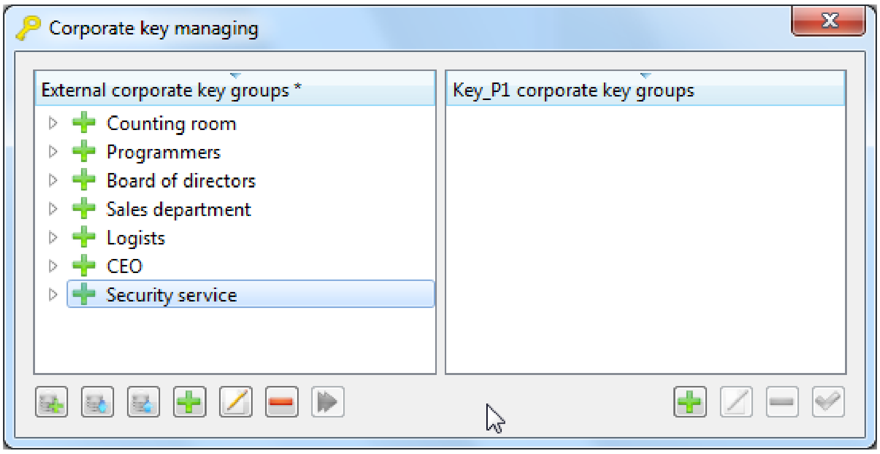
Corporate key grou...

Name: Programmers

Key count: 2

Figure 116: Corporate key group creation

Add all necessary groups into external corporate database, result see at the fig. 117



Corporate key managing

External corporate key groups *

- Counting room
- Programmers
- Board of directors
- Sales department
- Logists
- CEO
- Security service

Key_P1 corporate key groups

Figure 117: Corporate key group creation

In the next step save external database to file, as see at the fig. 118

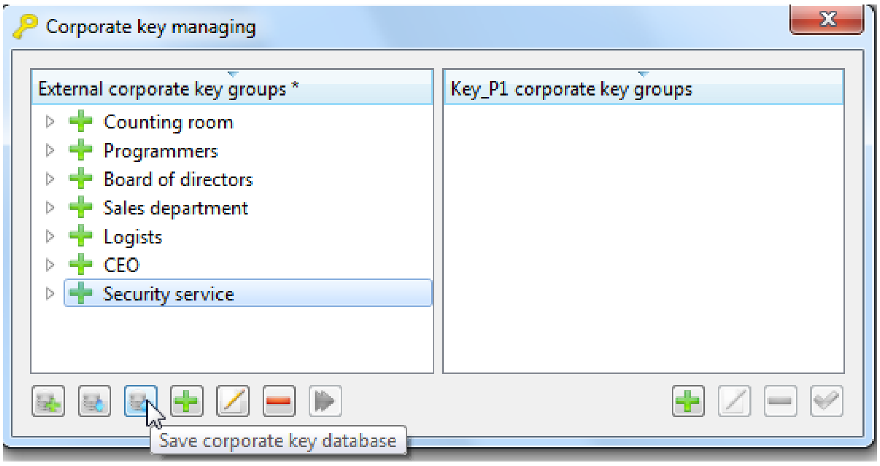
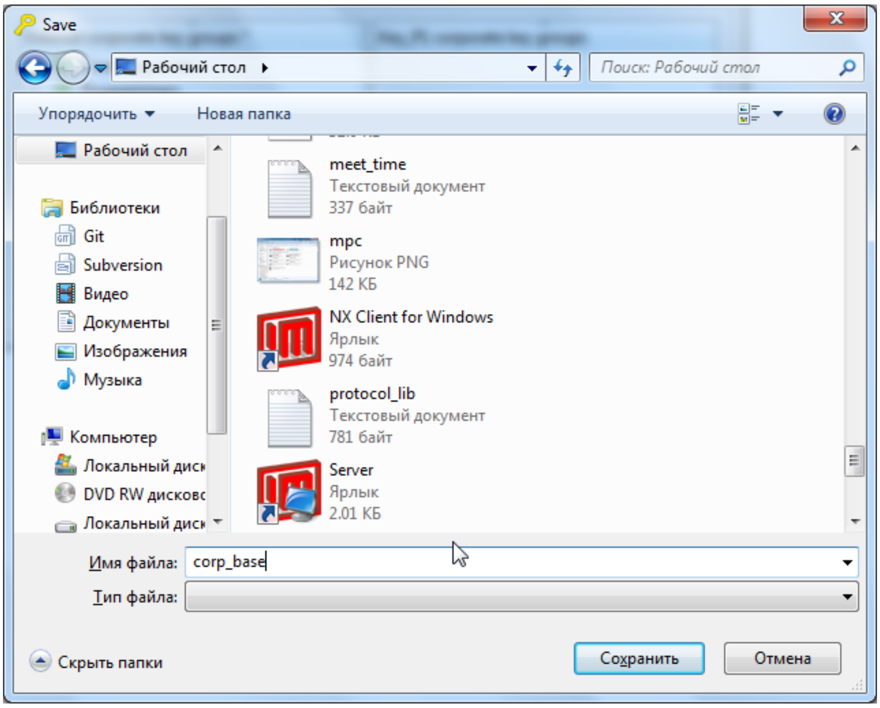


Figure 118: External corporate key database saving

After press button «Save external database» will be display window for setting file name and path to file, which will be contain database, see fig. 119



Имя файла: corp_base

Тип файла:

Figure 119: External corporate key database saving

Security administrator must keep corporate key database at trusted PC or at protected storage(for example in the private partition are created by Key_P1 device or this file may be enrypted with Key_P1). Hierarchical access organization is set by security administrator define composition corporate key group on user's devices Key_P1. Suppose that company director needed in data exchange with all company department, then security administrator open section «corporate key management» on director's Key_P1 device and press button «open external corporate key database», as shown at the fig. 120

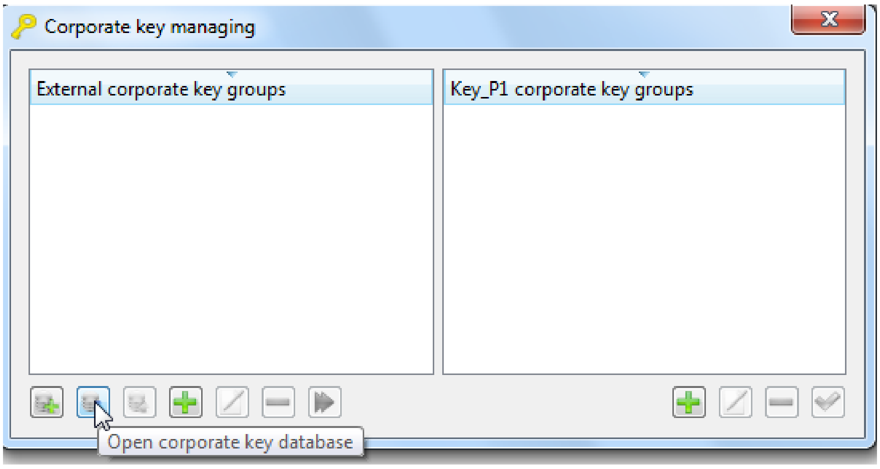

Corporate key managing
External corporate key groups
Key_P1 corporate key groups
Open corporate key database

Figure 120: Corporate key group management

Then security administrator choose file with corporate key database and press button «Open», as shown at the fig. 121

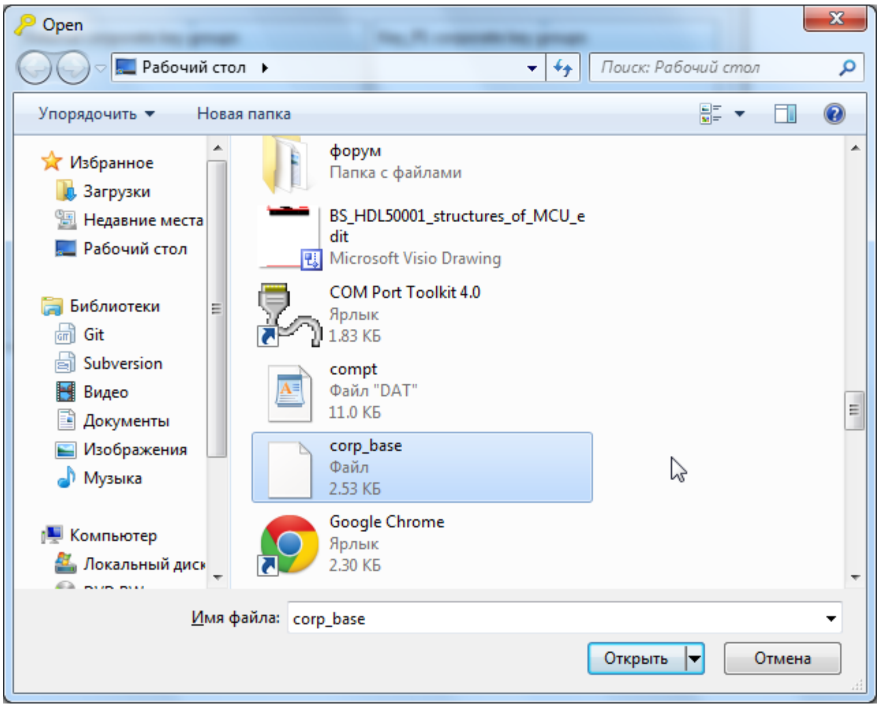


Figure 121: Opening external corporate key database

In the left section of the corporate key management window will be display list of available group from external database, see fig. 122

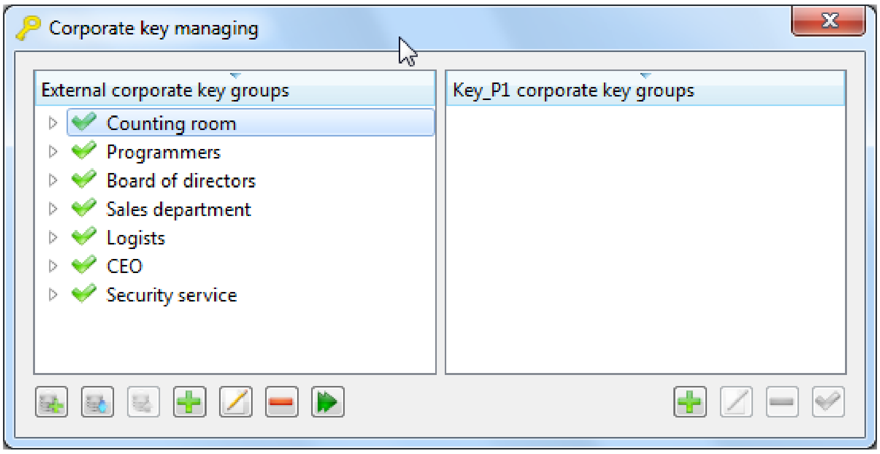


Figure 122: External database corporate key groups

Press button «Add corporate key group» to transfer group from external database to director's device Key_P1, see fig. 123

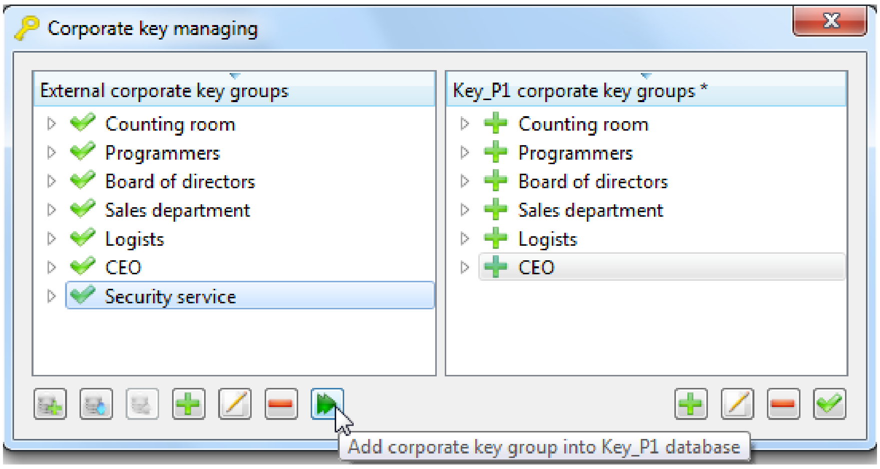
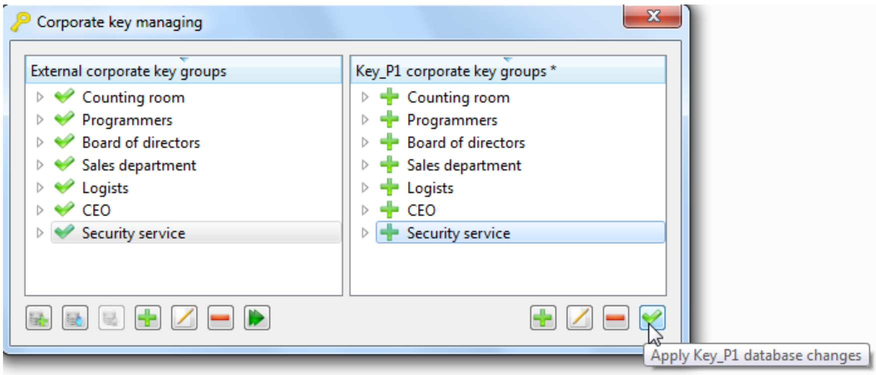


Figure 123: Setting corporate key groups to device from external database

After complete all corporate key transfers press button in the right section «Apply Key_P1 database changes», as shown at the fig. 124



External corporate key groups

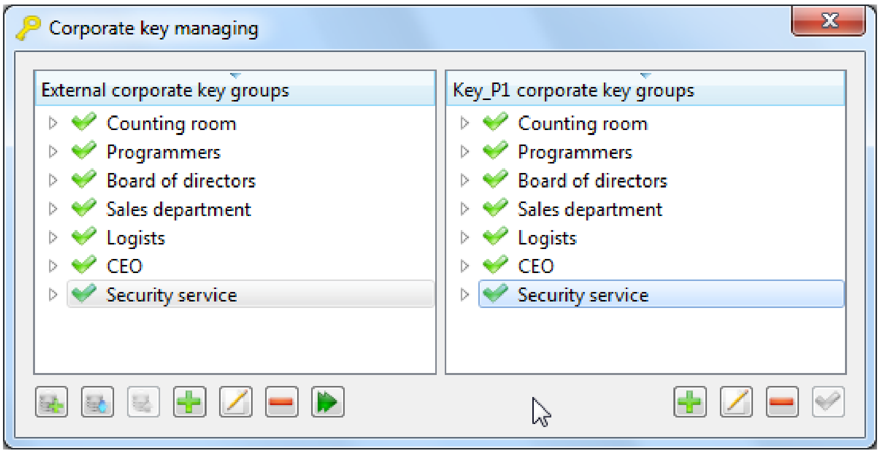
- Counting room
- Programmers
- Board of directors
- Sales department
- Logists
- CEO
- Security service

Key_P1 corporate key groups *

- Counting room
- Programmers
- Board of directors
- Sales department
- Logists
- CEO
- Security service

Figure 124: Setting corporate key groups to device

After success groups setting to device near all group will be display «check», see fig. 125



External corporate key groups

- Counting room
- Programmers
- Board of directors
- Sales department
- Logists
- CEO
- Security service

Key_P1 corporate key groups

- Counting room
- Programmers
- Board of directors
- Sales department
- Logists
- CEO
- Security service

Figure 125: Corporate key groups are installed to device

For users, for instance, «Counting room» department key groups install on device similarly. Add key groups that needed for «Counting room» department, see fig. 126

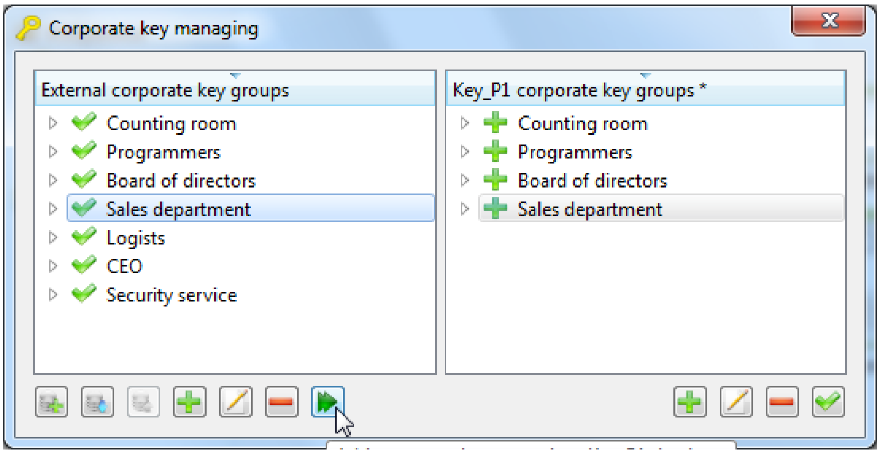


Figure 126: Corporate key groups for setting to device

Then press button «Apply Key_P1 database changes», as shown at the fig. 127

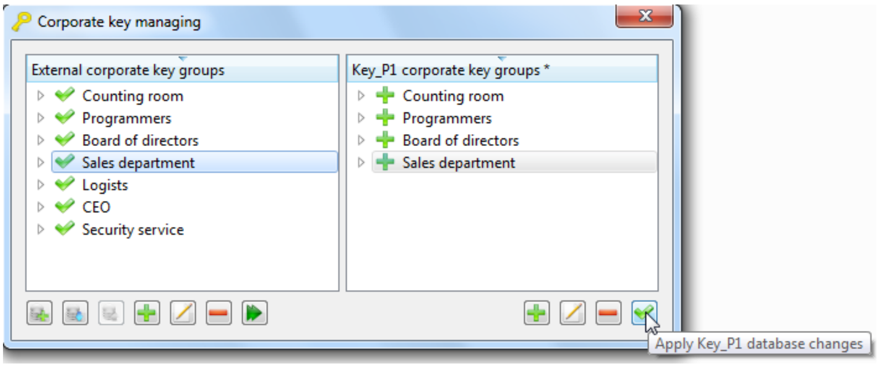


Figure 127: Corporate key groups setting on device

As a result will be display window, as shown at the fig. 128

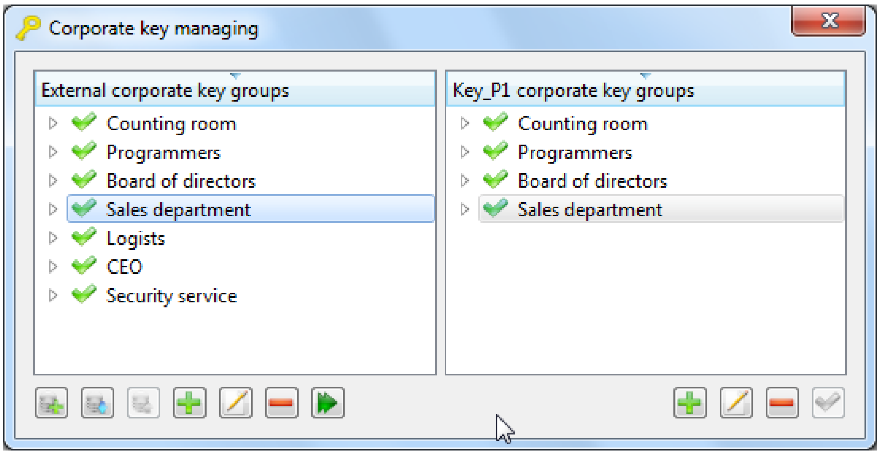


Figure 128: Corporate key groups on device

Security service fucntions about hierarchical access organization finish after set define list of corporate key groups for every users in department.

3.6.2 Enrypt data with corporate key

Data encryption with corporate key occur with universal window for data encryption with random, synchro, corporate keys. To do open window «Encrypt files» go to tab Actions->Encrypt files or with button in a toolbar, as shown at the fig. 129

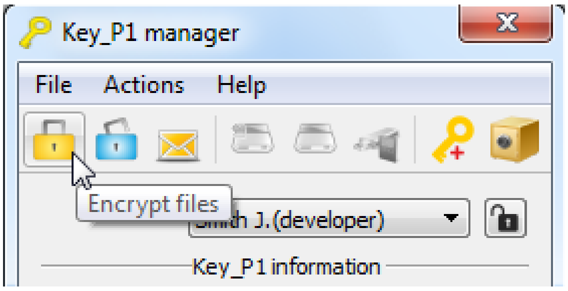
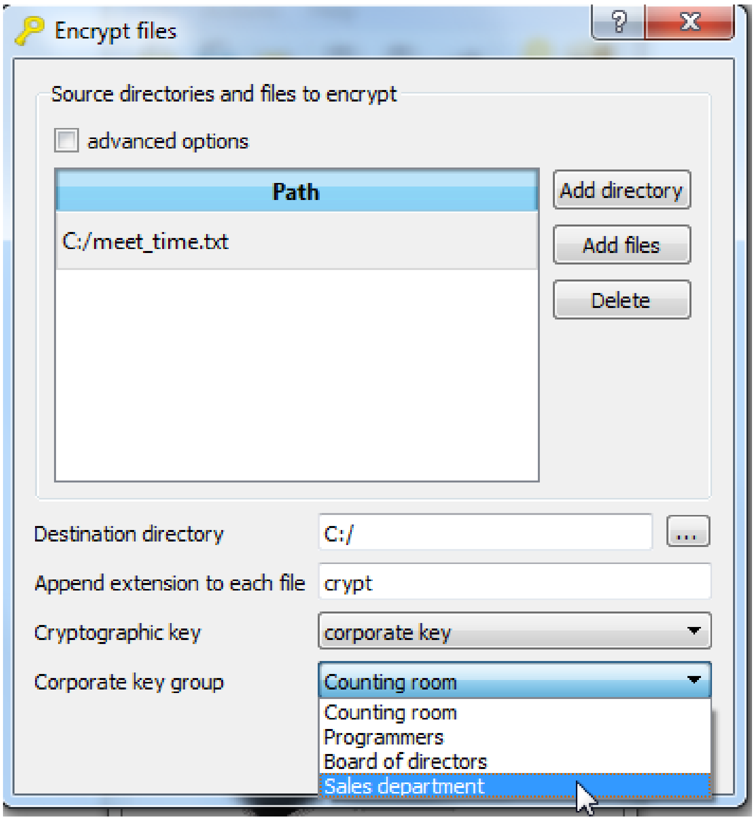


Figure 129: Data encryption

At the field crypthographic key necessary choose «corporate key», type user PIN code, after this choose corporate key for data encryption, for example «Sales department», see fig. 130



Source directories and files to encrypt

□ advanced options

Path
C:/meet_time.txt

Destination directory C:/

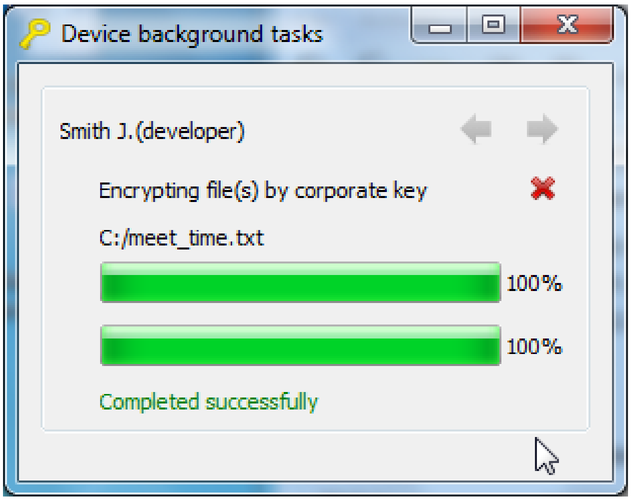
Append extension to each file crypt

Cryptographic key corporate key

Corporate key group Counting room

Figure 130: Data encryption window

Choice files or directories for ecnryption and destination directory in details described in the chapter 3.3(Files encryption). To start encryption process press button «Ok». Ecnryption progress display in the bacground operation window, as see at the fig. 131



Smith J.(developer)

Encrypting file(s) by corporate key

C:/meet_time.txt

100%

100%

Completed successfully

Figure 131: Data encryption progress

As a result in the destination directory will be file are ecnrypted with one from several keys for choosen department.

3.6.3 Decrypt data with corporate key

Data decryption with corporate key occur with universal window for data decryption with random, synchro, corporate keys. To do open window «Decrypt files» go to tab Actions->Decrypt files or with button in a toolbar, as shown at the fig. 132

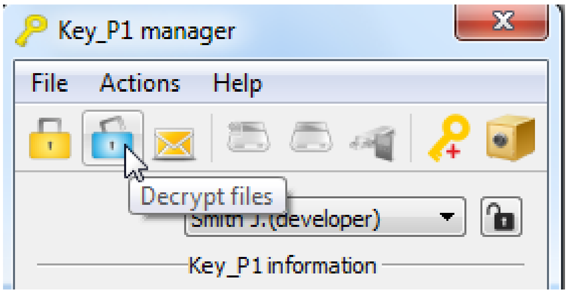
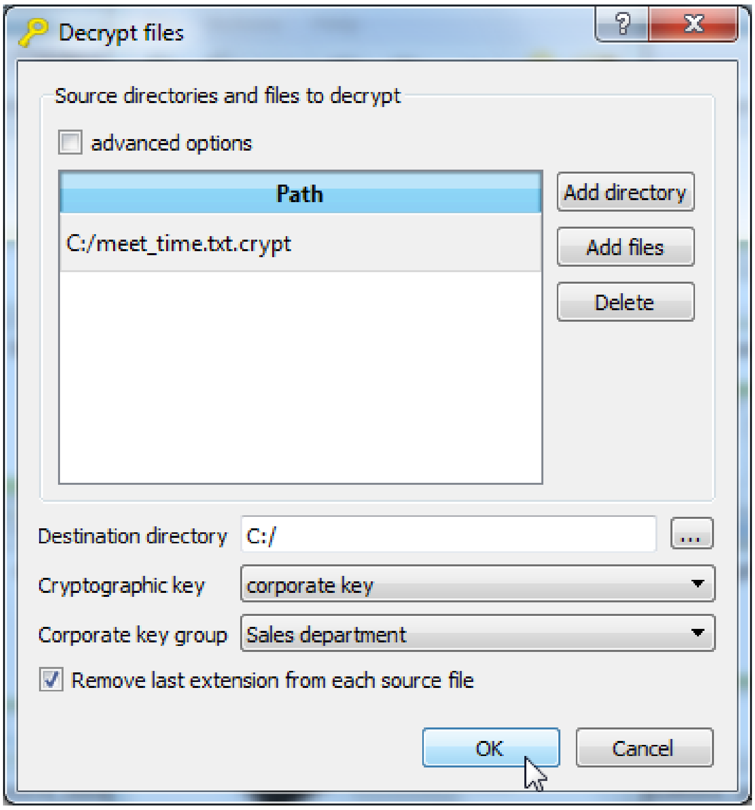


Figure 132: Data decryption

At the field crypthographic key necessary choose «corporate key», type user PIN code, after this choose corporate key for data decryption, for example «Sales department», see fig. 133



□ advanced options

C:/meet_time.txt.crypt

Destination directory C:/

Cryptographic key corporate key

Corporate key group Sales department

☑ Remove last extension from each source file

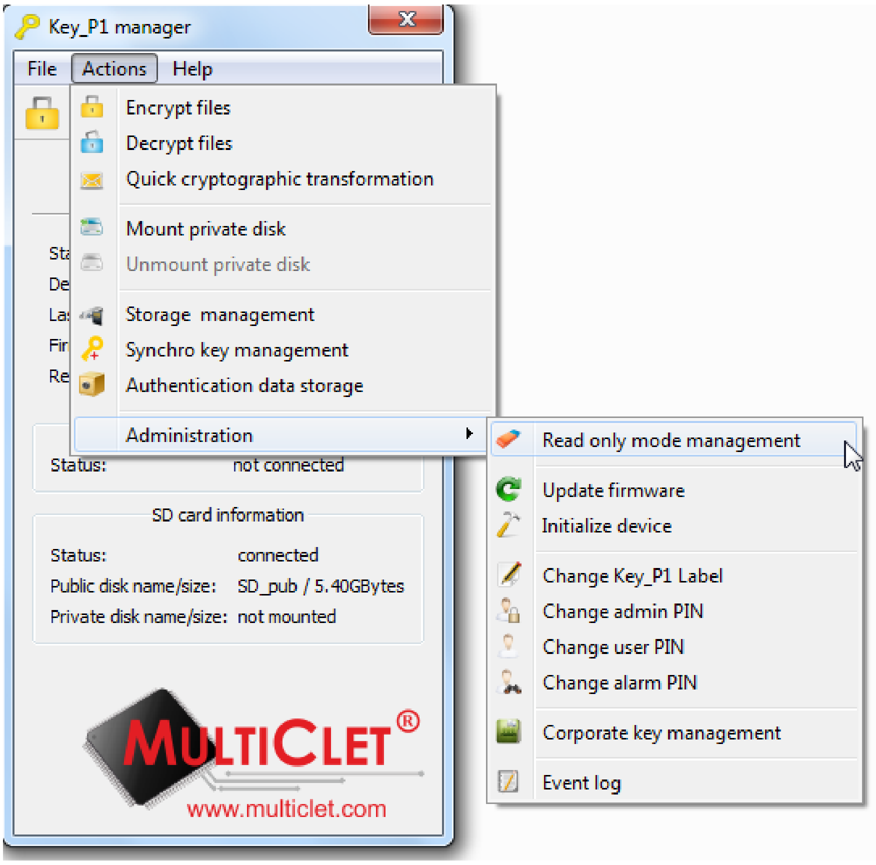
Figure 133: Data decryption window

Choice files or directories for decryption and destination directory in details described in the chapter 3.4(Decrypt files). To start decryption process press button «Ok». Ecnryption progress display in the bacground operation window. As a result in the destination directory will be file are decrypted with one from several keys for choosen department. Key_P1 device automatically detect if there is key for decryption after choosing department that send file, if Key_P1 device have key that file will be decrypt.

3.7 Limitation access to removable storages

Security service of the company may be block with internal security policy to lock a way write information from corporate PC on removable drives. For its can be set read only mode in order to Key_P1 will be lock on hardware level any unauthorized write of confidential data, viruses or other application on a storage. Write any information in this mode will be abort, user must have a permission to change read only mode or not active read only mode for write.

In order to set read only mode necessary consequentially choose tab **Actions** go to submenu **Administration** and choose **Read only mode management** (see fig. 134)



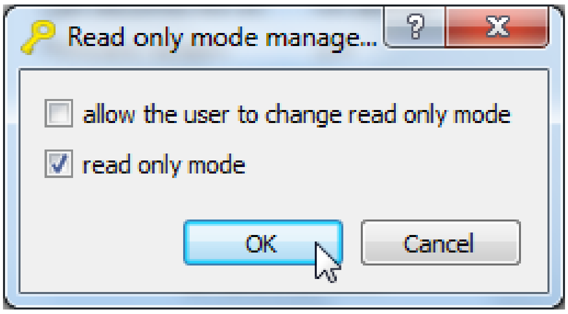
Status: not connected

SD card information

Status: connected
Public disk name/size: SD_pub / 5.40GBytes
Private disk name/size: not mounted

Figure 134: Read only mode management

After success entering administrator PIN window for read only mode management will be display. Administrator can allow access to read only mode management by user or set(unset) read only mode without user access to this management(fig. 135).



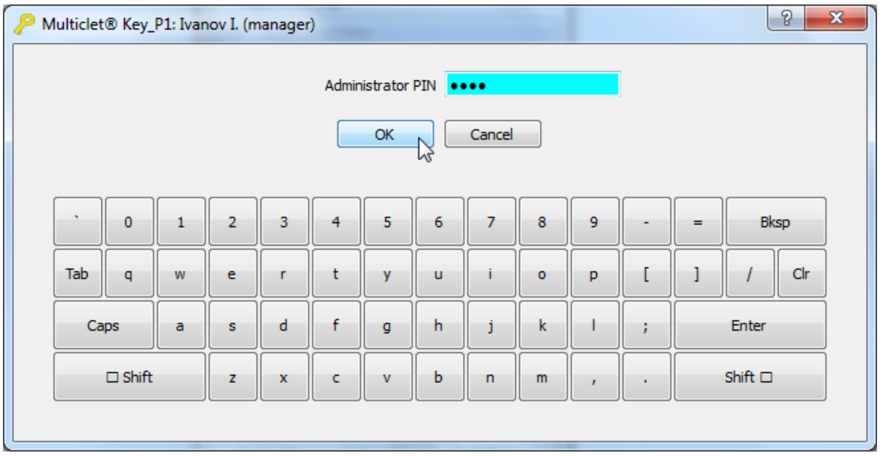
Read only mode manage...

□ allow the user to change read only mode

☑ read only mode

Figure 135: Entering administrator PIN

In case setting read only mode with the next enter administrator PIN (see fig. 136) in the main menu Key_P1 Manager user can see set checkbox at the field read only mode (see fig. 137)

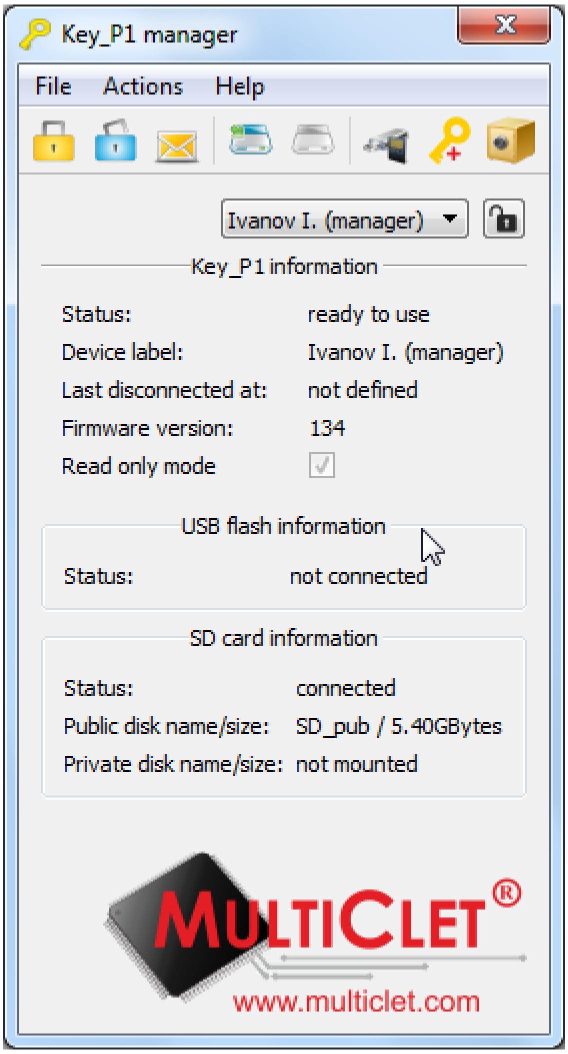


Multiclet® Key_P1: Ivanov I. (manager)

Administrator PIN ••••

OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 136: Entering administrator PIN



Key_P1 information

Status: ready to use

Device label: Ivanov I. (manager)

Last disconnected at: not defined

Firmware version: 134

Read only mode ☑

USB flash information

Status: not connected

SD card information

Status: connected

Public disk name/size: SD_pub / 5.40GBytes

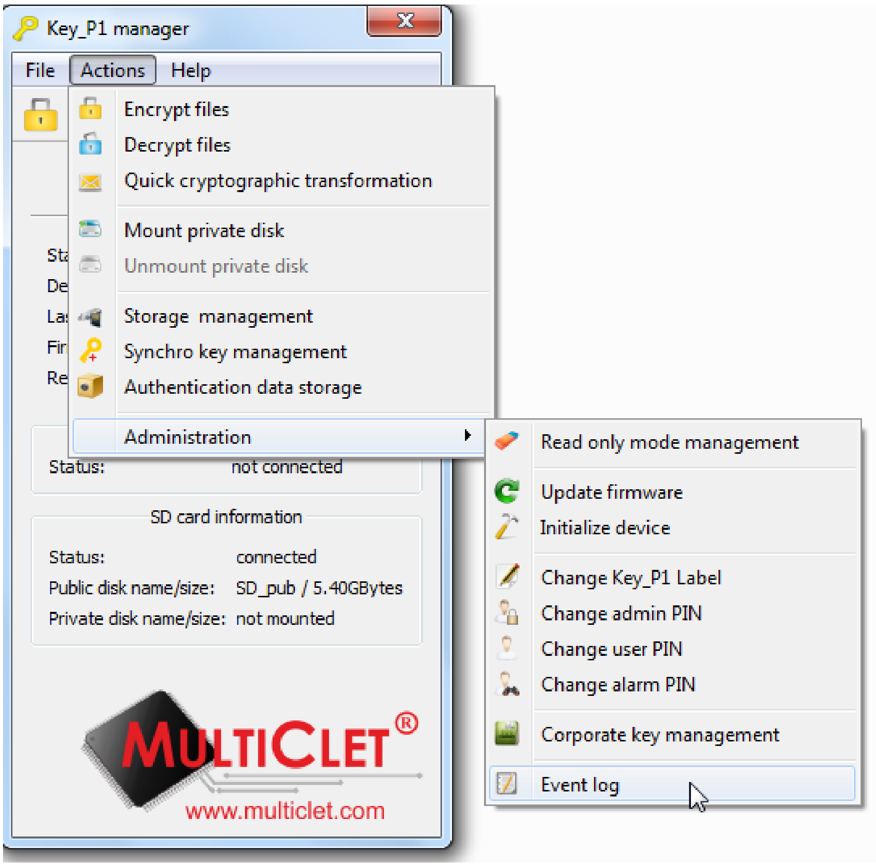
Private disk name/size: not mounted

Figure 137: Application main window

3.8 Event log

Key_P1 device leads event log of main actions. In the device event log record main actions with timestamp. Display device connection time, mount private partition and etc. Thus Key_P1 disconnect with unauthorized copy confidential information from corporate PC on internal storage, will be record (record stamp about time and date) and available to security service.

In order to open log event necessary consequentially choose tab **Actions** go to submenu **Administration** and choose **Log event** item (see fig. 138)



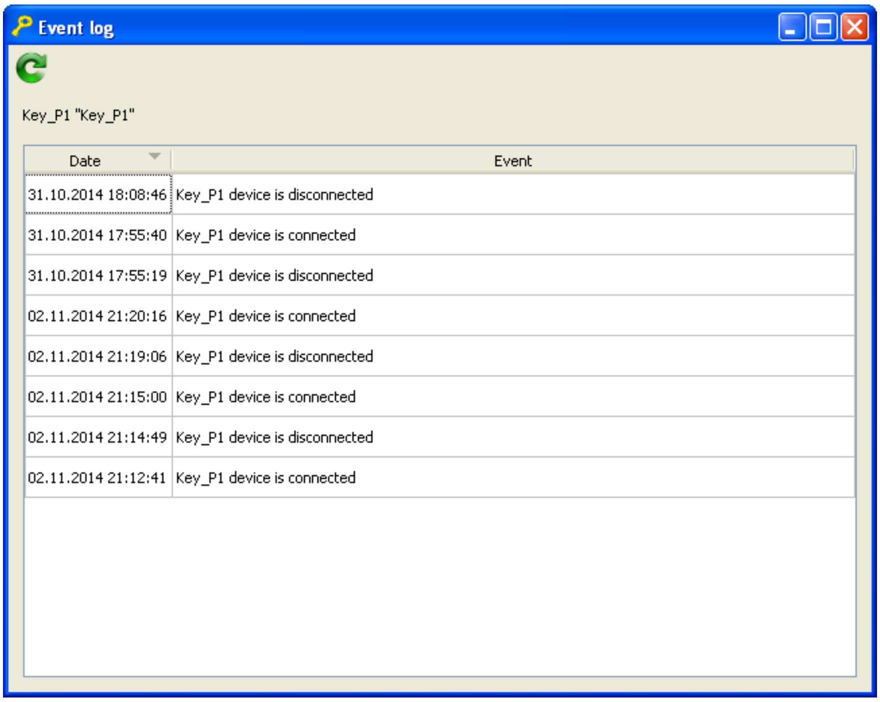
Status: not connected

SD card information

Status: connected
Public disk name/size: SD_pub / 5.40GBytes
Private disk name/size: not mounted

Figure 138: Log event

Event log section contain connection/disconnection Key_P1 device log and main user event log. Window with time log present at the fig. 139



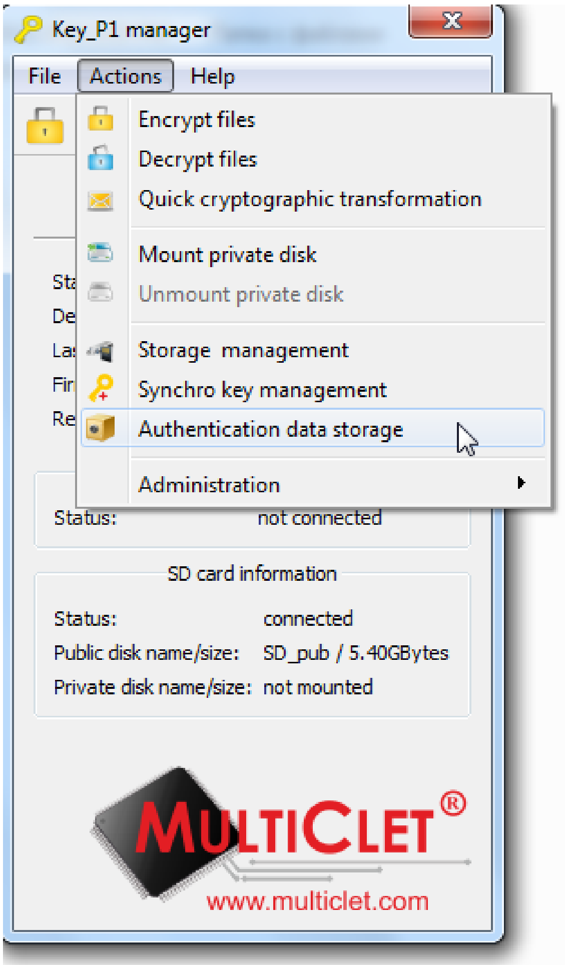
Key_P1 "Key_P1"

Date	Event
31.10.2014 18:08:46	Key_P1 device is disconnected
31.10.2014 17:55:40	Key_P1 device is connected
31.10.2014 17:55:19	Key_P1 device is disconnected
02.11.2014 21:20:16	Key_P1 device is connected
02.11.2014 21:19:06	Key_P1 device is disconnected
02.11.2014 21:15:00	Key_P1 device is connected
02.11.2014 21:14:49	Key_P1 device is disconnected
02.11.2014 21:12:41	Key_P1 device is connected

Figure 139: Log event

3.9 Autentication data storage

Device allow to save users passwords and logins on internal protected memory of the Key_P1 device. This function allow secure data to access on internet services: «Mail.ru», «Gmail.com», «Mail.yandex.ru» from unauthorized access, as it's happen at the autumn 2014 year with 6 million accounts other users. It's reach with settings sophisticated and long password. In order to use this functions necessary consequentially choose tab **Actions** and **Autentication data storage** item (fig. 140).



Status: not connected

SD card information

Status: connected

Public disk name/size: SD_pub / 5.40GBytes

Private disk name/size: not mounted

Figure 140: Autentication data storage

Login and password to information source is a autentication data. Window with user PIN field will be display. Press button «OK» to continue(fig. 141).

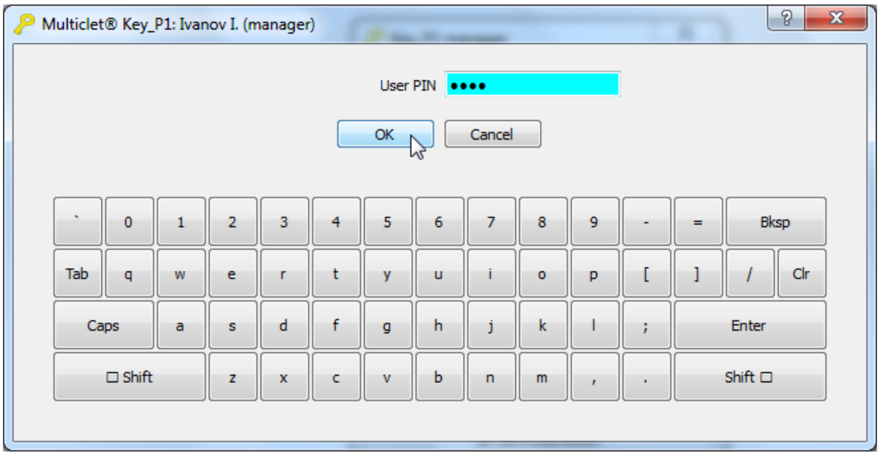

Multiclet® Key_P1: Ivanov I. (manager)
User PIN ••••
OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 141: Entering user PIN

Main window **Autentication data storage** will be display (fig. 142). Window consist from two part. In the left part user can create groups for logins and passwords for access to information services defined themes. In the right part user can record password, login and other information. Create new group «Mail». For it's necessary press button **Add** in the left part.

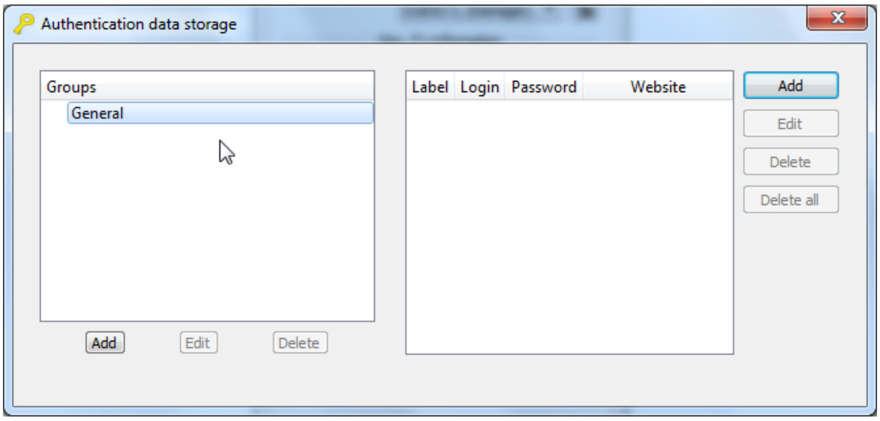


Figure 142: Data storage window

Window for setting label (name) new group will be display (fig. 143). Press button «OK» to continue.

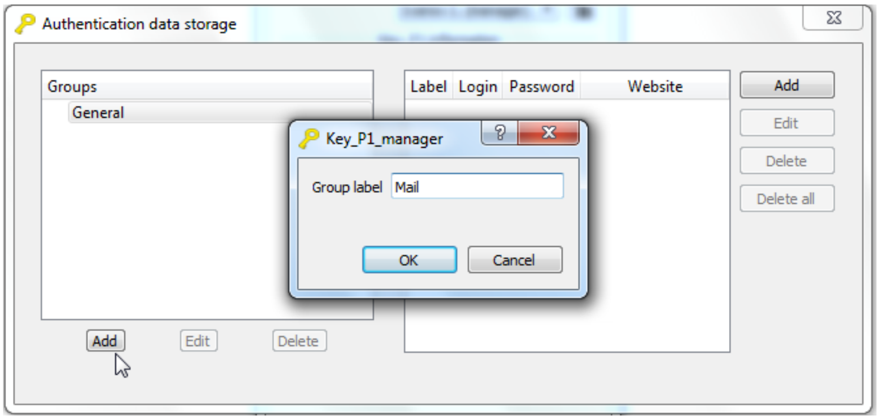


Figure 143: Group label

At the left part new group «Mail» appeared (fig. 144). Make adding new logins and passwords for email service «Mail.ru». To do this press button **Add** in the right part of the window.

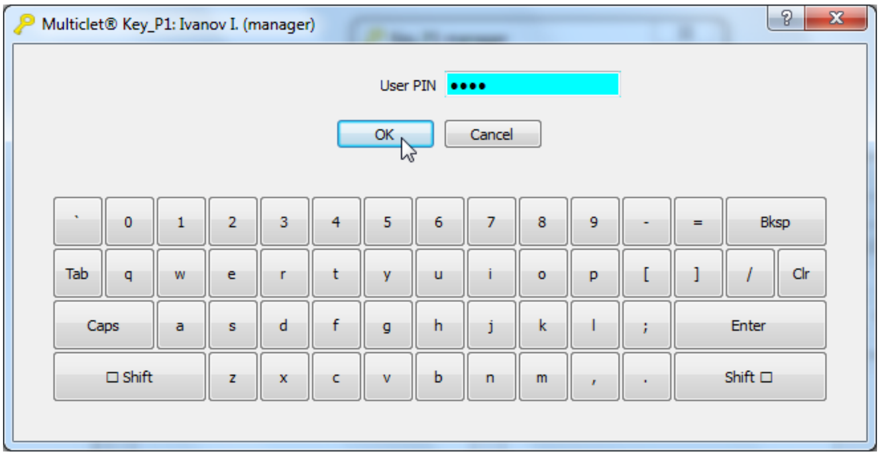
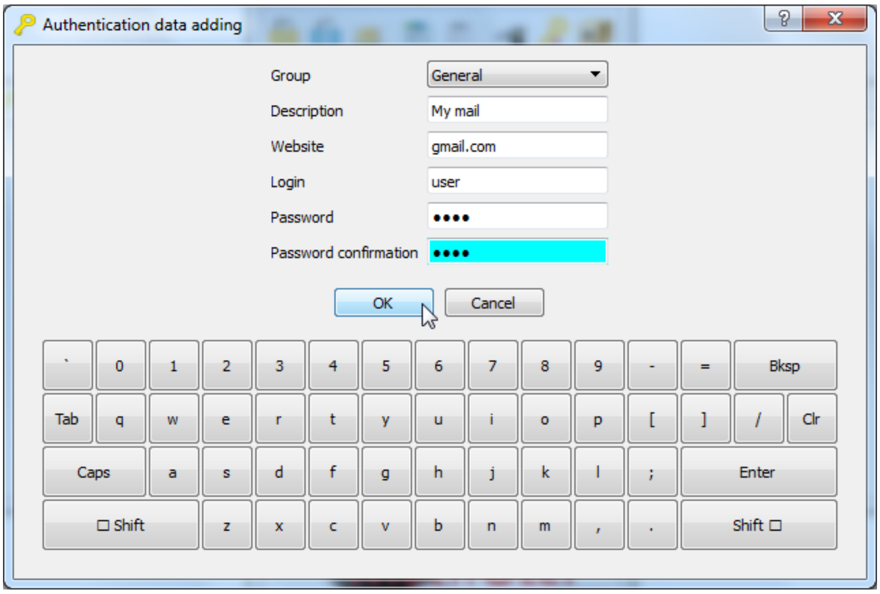

Multiclet® Key_P1: Ivanov I. (manager)
User PIN
••••
OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 144: Data storage window

Autentication data storage window will be display (fig. 145). At the **Group** field necessary choose group for information resource. At the **Description** field necessary add description or destination of information resource. At the **Site** field may add internet address for information resource. At the **Login** field may type login to access on information resource. At the **Password** field necessary type password to access on information resource. At the **Confirmation password** field type password. After all actions completed press button «OK».



Authentication data adding

Group: General

Description: My mail

Website: gmail.com

Login: user

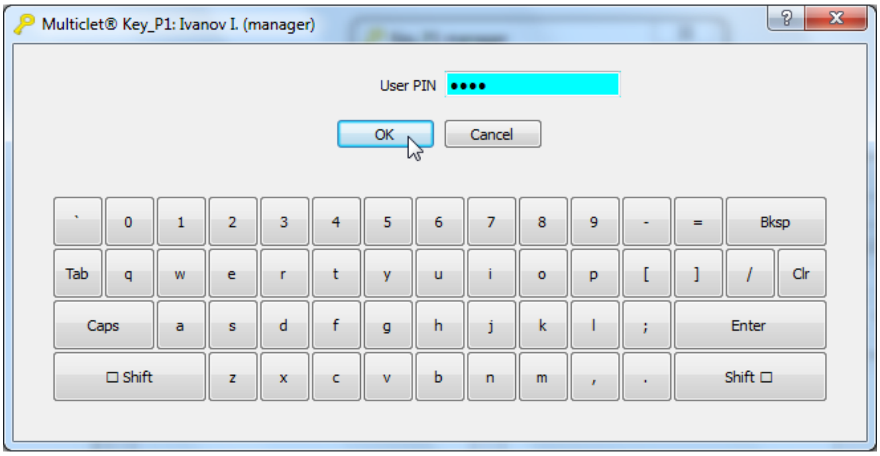
Password: ••••

Password confirmation: ••••

OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 145: Adding autentication data storage

Window for entering user PIN code will be display. After entering user PIN necessary press button «OK» (fig. 146).



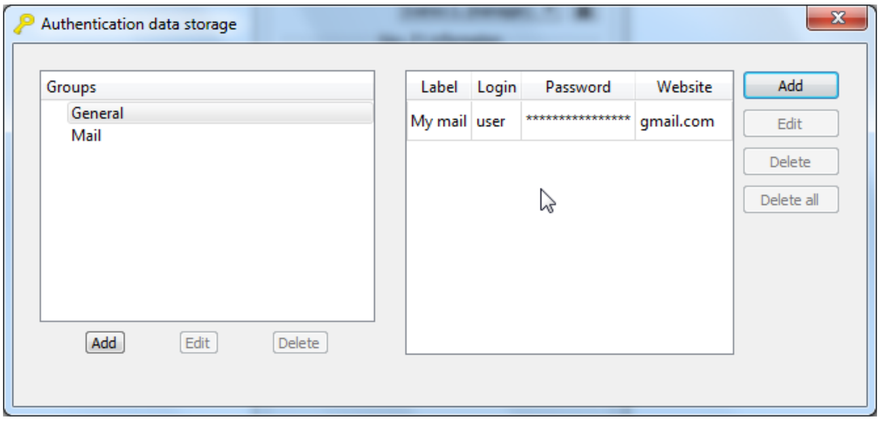
Multiclet® Key_P1: Ivanov I. (manager)

User PIN: ••••

OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 146: Entering user PIN

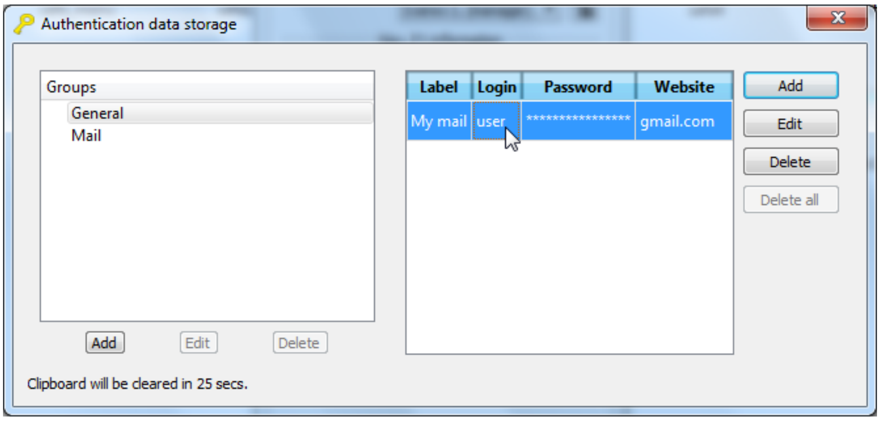
At the right part will be display information about «Mail.ru» (fig. 147).



Label	Login	Password	Website
My mail	user	****************	gmail.com

Figure 147: Data storage window

In order to make data copy and transfer it to window with autorized resource fields, initially necessary make copy resource URL - impose mouse cursor and on the field under title **Site** and with double click to make data capture (fig. 148). In the left part of the window will be display information about time before echange bufer will be clear.



Label	Login	Password	Website
My mail	user	****************	gmail.com

Clipboard will be cleared in 25 secs.

Figure 148: Data copy

Then necessary to use information resource URL. Open internet browser and paste URL at the address field, for example with mouse right button click choose command "Paste". After it necessary press key «Enter». Autorized window «Mail.ru» will appeared(fig. 149).

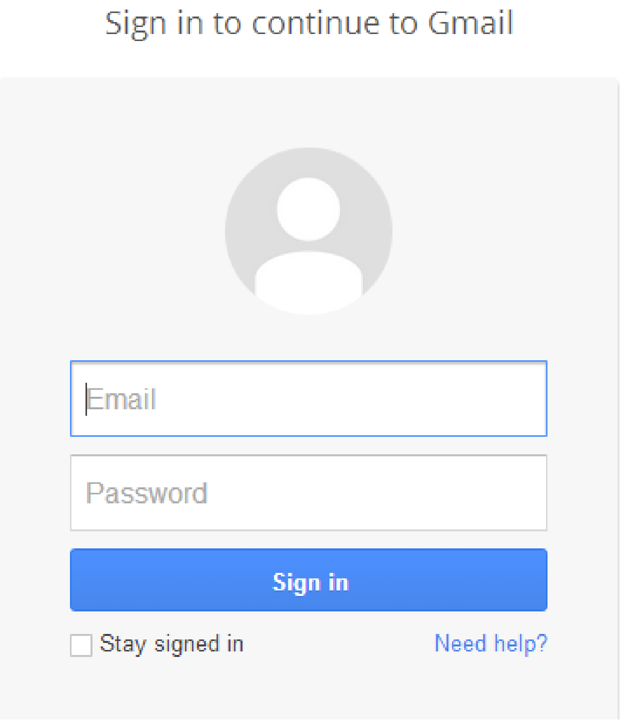
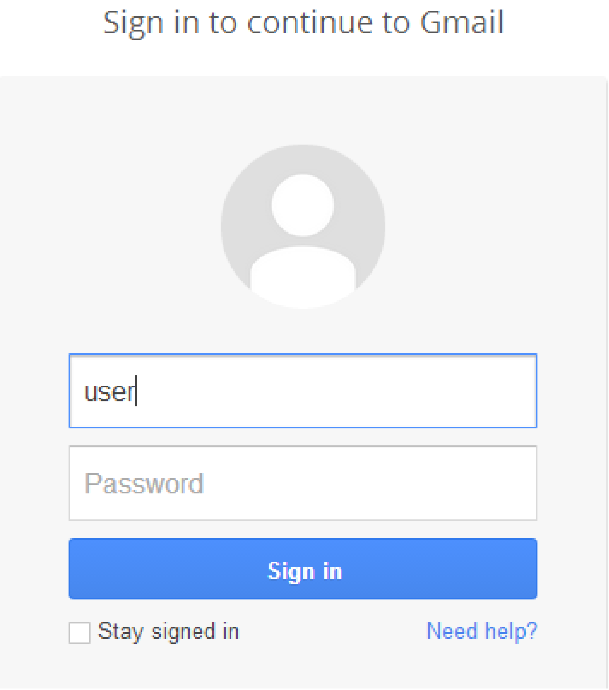


Figure 149: Autorized window

Then necessary to make copy login. To do this necessary impose mouse cursor at the field **Login** and with double click to make data capture (fig. 150). In the left part of the window will be display information about time before echange bufer will be clear. In the next step necessary impose mouse cursor in the autorized window at the field Login and press mouse right button and make command «Paste».

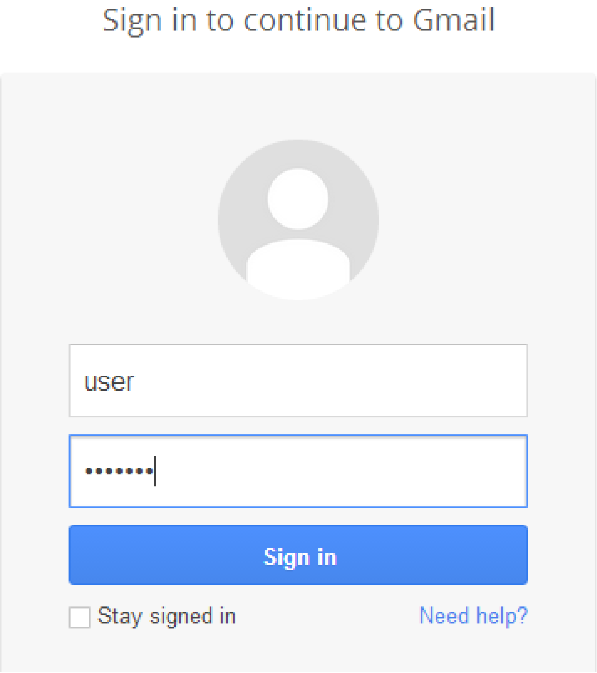


Sign in to continue to Gmail

user

Figure 150: Autorized window

Then necessary to make password copy. To do this necessary impose mouse cursor and at the **Password** field and with double click to make data capture (fig. 151). In the left part of the window will be display information about time before echange bufer will be clear. In the next step necessary impose mouse cursor in the autorized window at the field Login and press mouse right button and make command «Paste». After it may be press button "Enter" and occur autorization.



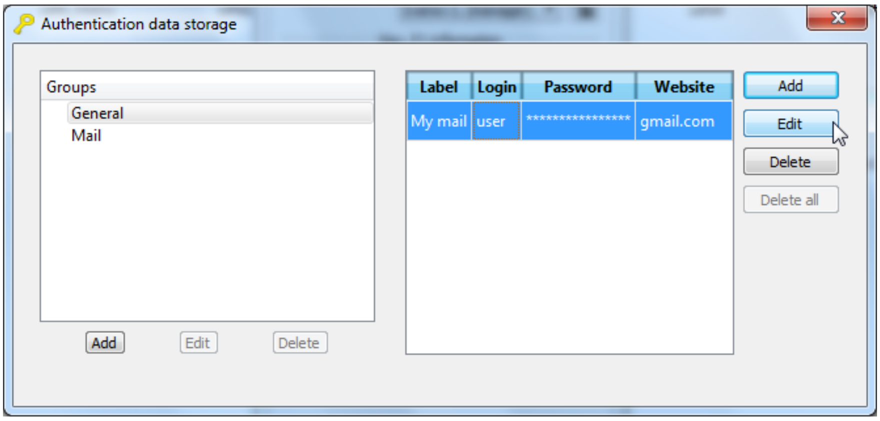
Sign in to continue to Gmail

user

•••••••

Figure 151: Autorized window

Any autentication data will be change. In order to perform this procedure necessary in the main window **Autentication data storage** click at the right part **Edit** (fig. 152).

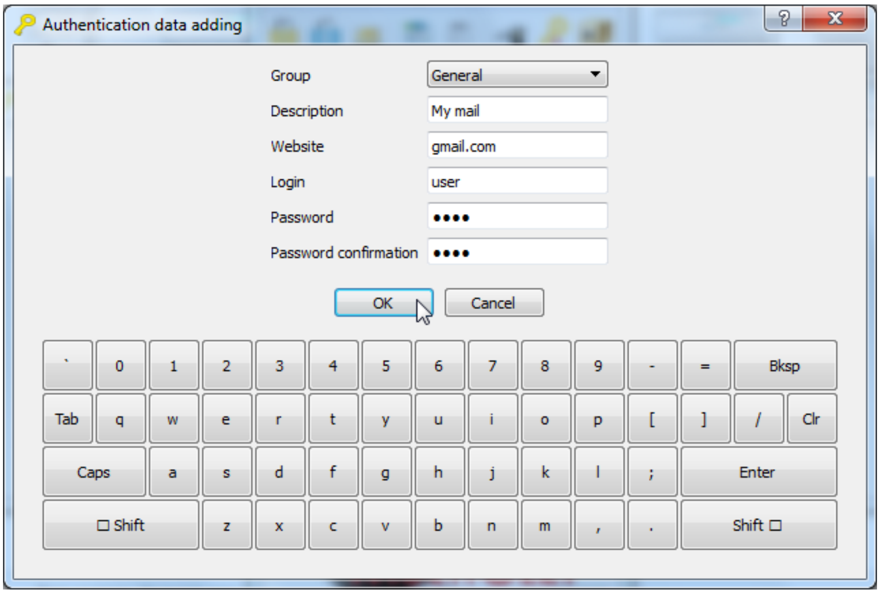


Authentication data storage

Label	Login	Password	Website
My mail	user	***************	gmail.com

Figure 152: Editing autentication data

Window for editing autentication data will be display (fig. 153). Any information may be change in this window. Press button «OK» to complete.



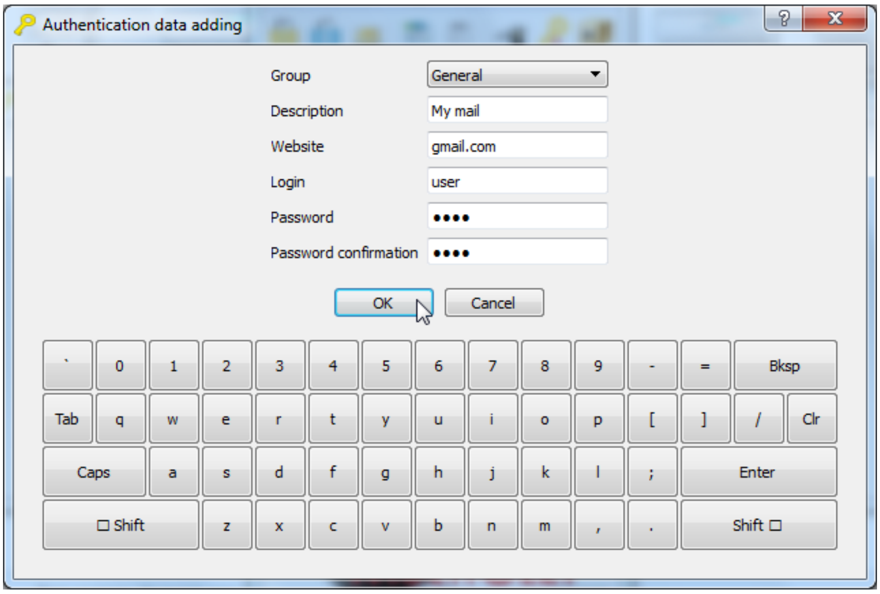
Authentication data adding

Group: General
Description: My mail
Website: gmail.com
Login: user
Password: ••••
Password confirmation: ••••

OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 153: Autentication data editing

Window for user PIN entering will be display. After entering PIN code necessary press «OK» (fig. 154).



Authentication data adding

Group: General
Description: My mail
Website: gmail.com
Login: user
Password: ••••
Password confirmation: ••••

OK
Cancel
` 0 1 2 3 4 5 6 7 8 9 - = Bksp
Tab q w e r t y u i o p [ ] / Clr
Caps a s d f g h j k l ; Enter
□ Shift z x c v b n m , . Shift □

Figure 154: Entering user PIN

4 Frequently asked questions

Question 1: *Is it possible to use and keep person confidential information on the device if this information is not a login or password?*

Answer: For example user can save credit card number at the «login» field and cvv number at the «password» field.

Question 2: *Where keys for encryption saved? Can I get keys from device?*

Answer: Keys for encryption saved in the protected memory of the device. As a security measure device not return any keys. But possible device recovery if in during device initialize process keys list was saved.