KEY SECUREPC

KEYSECUREPC
USER MANUAL

N.B.: PRIOR TO READING THIS MANUAL, YOU ARE ADVISED TO READ THE FOLLOWING MANUAL:

“GENERAL OPERATING PRINCIPLES”

EMA100511_UK

Dear Customer,

KeySecurePC is an innovative product that uses a patented technology: on purchasing this device you have chosen to protect your sensitive data with the highest level of security available today.

This manual provides instructions for your first start-up and initialization of KEYSECUREPC, along with instructions for common tasks such as data backup. Please read and follow it carefully, as it will help you to rapidly proceed with the boot procedure of your KEYSECUREPC and to quickly familiarise yourself with this new tool.

We also advise you to carefully read the Manual entitled **"General Operating Principles"** before initializing KeySecurePC to help you better understand how your device was designed and developed.

We would like to thank you once again for buying our product and remind you that our customers may also receive assistance and additional information by contacting us:

- via email at support@keysecurepc.com
- through our website at www.keysecurepc.com

KeySecurePC

EMA100511_UK

KEY™ SECUREPC

INDEX

EMA100511_UK

FIRST USE: HOW TO BOOT.

INTRODUCTION

Each time you start your computer, it automatically launches your operating system without the need for any input from you. This startup is called the **BOOT** process, and the software that controls this process is called the **BOOT MANAGER**.

KeySecurePC steps in during this boot phase, preventing the computer from launching its internal operating system and redirecting the **BOOT** process to launch our operating system (see the manual called "General Operating Principles").

In order to allow KeySecurePC to carry out this operation, select the **BOOT** mode on your PC (this information is usually provided in the computer's instruction booklet or available online at the manufacturer's website).

AUTO BOOT FROM USB PORT

If your computer is set to **AUTO BOOT FROM USB PORT**, insert KeySecurePC in your computer and go directly to section 3: Initialising KeySecurePC.

INSTALLING THE KEYSECUREPC SOFTWARE TO BOOT FROM USB PORT

If your computer is NOT set to AUTO BOOT FROM USB PORT you will need to install the **USB PORT BOOT MANAGER**, a programme comprised in your KeySecurePC, by following the simple instructions found in Chapter 2 of this Manual.
We highly recommended this option because, once installed, this programme will allow KeySecurePC to boot quickly every time.

MANUAL BOOT CONFIGURATION

Finally, if your computer is NOT set for AUTO BOOT FROM USB port, and you do NOT wish to install the USB PORT BOOT MANAGER on your computer, you can follow the procedure outlined in the manual called "MANUAL BOOT CONFIGURATION", which you can download from the "DOWNLOAD" section on our website. Although this procedure takes longer, it also allows KeySecurePC to boot correctly on your computer.

INSTALLING USB PORT BOOT MANAGER.

Software compatible with Windows 98, Windows ME, Windows XP, Windows Vista, Windows 7.

a Start your computer.

b Insert your KeySecurePC into a USB port.

c The Autoplay window will appear showing two options:
"General Options" and "Install or run programmes".
Select "Install" and click Start.

d This opens the "KeySecurePC Boot Manager" window: click on "Install".

e If your computer asks for an administrator password, enter it as required.

f This opens the "Confirmation" window: click OK.

g THE BOOT PROGRAM IS INSTALLED; THE COMPUTER MUST BE RESTARTED TO LAUNCH KEYSECUREPC.
Your PC may restart automatically or following your confirmation, depending on the operating system installed on your PC.

h After restarting, the "Windows Boot Manager" screen will appear, asking you to choose whether to launch KeySecurePC or run the computer's operating system: select KeySecurePC using the arrow keys and pressing Enter.

i Now, your computer will launch KeySecurePC.
The windows "Detecting device" and "Starting device" appear in succession. Wait until the KeySecurePC password prompt window appears before entering any input.

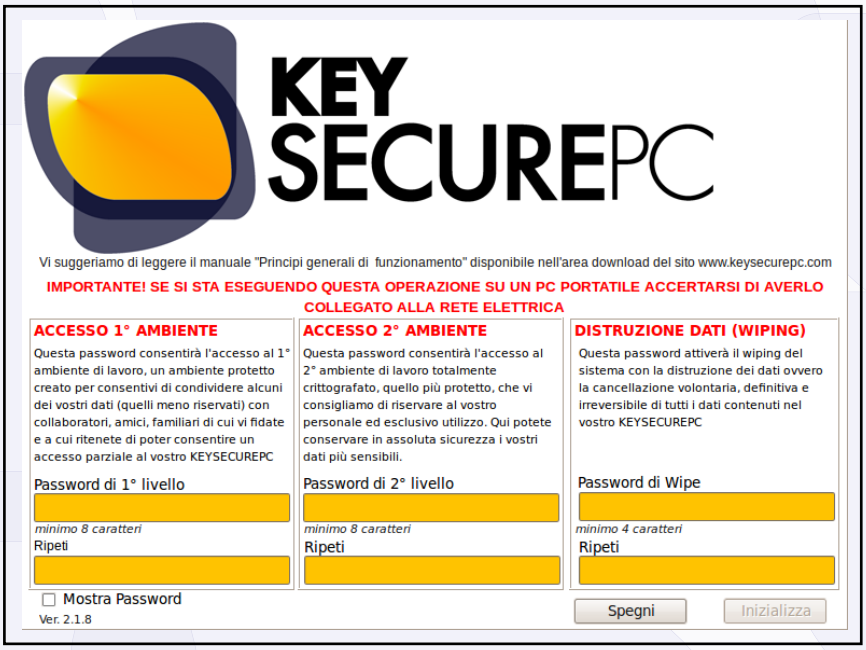
l KeySecurePC is ready to be initialized: proceed with initialization according to the instructions in section 3.

FIRST USE: INITIALISING AND ENTERING THE 3 REQUIRED PASSWORDS.

Before you enter your 3 passwords, we would like to remind you that these passwords are an integral part of KeySecurePC's security system and should be chosen with particular care.
If you have not already done so, please read the Manual entitled "General Operating Principles" available in the "DOWNLOAD" section on our website before initializing and entering your 3 passwords.

a Launch KeySecurePC on your computer according to one of three BOOT procedures described in the previous sections.

b The initialization window appears requesting 3 passwords: enter these by following the instructions on the window and click "CONFIRM"



c The KeySecurePC initialization procedure starts and takes approximately 5 minutes (depending on the KeySecurePC model you have chosen). As indicated in the initialization window, you should not shut down the computer or press any keys to avoid disturbing initialization.

d Following initialization, a window opens asking you restart your computer: click "RESTART".

e Once the computer restarts, your KeySecurePC is ready for use. A window will appear requesting entry of a single password: go to section 4 entitled SUBSEQUENT USE to see how to proceed.

SUBSEQUENT USE.

a Insert KeySecurePC into your computer.

b Start your computer.

c You will see the "Windows Boot Manager" screen asking you to choose between launching KeySecurePC and running the computer's internal operating system: select KeySecurePC using the arrow keys and press Enter.

d Your computer will now launch KeySecurePC.
The windows "Detecting device" and "Starting device" appear in succession. Wait until the KeySecurePC password prompt window appears before entering any input.

e Enter one of the 3 passwords, depending on whether:
- you want to access the 1st environment,
- you want to access the 2nd environment,
- you want to carry out the wiping procedure (deliberate destruction of data).

f After entering the password, click "Confirm": KeySecurePC launches and opens your Desktop (pictured below). Now you can carry on freely with your work session.

RE-INITIALISING / CHANGING PASSWORD.

You will lose the data stored on KeySecurePC when you re-initialise. In order to save such data, we suggest you carry out the following steps before re-initialising:

- transfer your data to a device such as KeySecurePC Backup;
- re-initialise;
- retrieve your data from the Backup device and transfer it to your KeySecurePC.

a Launch KeySecurePC and go to your desktop.

b Click the START button and from the pop-up menu, select the option "KeySecurePC" and "Initialise Device".

c A window appears asking if you want to proceed with re-initialisation: click to confirm.

d Your computer restarts.

e The initialisation window appears requesting your 3 passwords: enter them by following the instructions on the window and press "CONFIRM".

The KeySecurePC re-initialisation process starts and lasts around 5 minutes (depending on the KeySecurePC model you have chosen). As indicated in the initialisation window, do not shut down your computer or press any keys to avoid disturbing re-initialisation.

HOW TO CHANGE YOUR PASSWORD.

a You must re-initialise the entire system to change your KeySecurePC password. This is due to the fact that your passwords are an integral part of KeySecurePC's security technology. Once entered into the system, they are encrypted and influence the AES256 encryption algorithm, thereby making your system increasingly secure. Changing your passwords would open a potential flaw in the security technology of our device and make it susceptible to attack.
If you wish to change your passwords for security reasons, you must re-initialise the entire system by following the instructions above.

DATA BACKUP.

a Launch KeySecurePC and go to your desktop.

b Insert a backup device such as KeySecurePC Backup into a USB port on your computer.

c Click the START button and, from the pop-up menu, select the option "KeySecurePC" and "Backup".

d This opens the "KEYSECUREPC BACKUP" window: The window toolbar displays the message "KEYSECUREPC DEVICE DETECTED". If your device is not found, click "REFRESH".

e In the window, under "DEVICES DETECTED", locate "KEYSECUREPC BACKUP": check the box "MANAGE DEVICES".

f Once again from the window toolbar, click the button "INITIALISE SELECTED DEVICE".

g This opens the "CONFIRMATION" window, which warns you that any data previously stored on the backup device will be deleted. If you agree, click "CONFIRM".

h This opens the password prompt window: enter your password and wait for the message indicating that your KEYSECUREPC is ready.

i Return to the window toolbar and click "START BACKUP PROCEDURE": the system automatically starts to transfer all the data contained in your KEYSECUREPC to the Backup device.

l When the Backup is complete, return to the window toolbar and click the "CLOSE" button: you can now remove your Backup device.

IMPORTING YOUR FILES TO KEYSECUREPC.

Importing a file from your PC to KeySecurePC is easy: you can simply cut and paste, or drag and drop the files to KeySecurePC.

You must however bear in mind that folders are renamed when they are imported to KeySecurePC and you may not therefore immediately recognise them. We recommend that you import files according to the following instructions:

a combine all your files in one folder and put the folder on your computer's hard drive "C".

b Return to the KeySecurePC desktop and click on the "My Computer" icon: this opens a window displaying various icons, including one for the hard drive "C" which has been renamed by the system.

c Locate the hard drive "C" by opening all of the icons.

d Once you have located hard drive "C" with its new name and you have located your folder therein, import your files by "Copy and Paste" or by dragging and dropping them to KeySecurePC.

WIPING – DELIBERATE DESTRUCTION OF DATA.

The process of WIPING, or the deliberate and irreversible destruction of data, is one of KeySecurePC's special features.

Wiping overwrites the headers of encrypted volumes and the partition table to make them inaccessible, thus deleting the internal disk structure of KeySecurePC. At the end of this process, your device no longer works and can no longer be reused.

The wiping process can be implemented in one of two ways:

a upon starting KeySecurePC, enter your 3rd password or the password you selected for data wiping in the password prompt window. The wiping process immediately commences without further confirmation, the bar goes back and forth and everything is destroyed in just a few minutes.

b Alternatively, the same wiping process can be implemented by clicking on the "Wiping" icon that appears on the desktop. This will open the password prompt window; simply enter your password and confirm to implement the wiping process.