KEY™
SECUREPC

KeySecurePC

EMT140311UK

KEY™ SECUREPC

THE FIRST SYSTEM IN THE WORLD THAT REALLY MAKES THE DATA ON YOUR PC TOTALLY SECURE

100% PROTECTION OF DATA ON YOUR PC

TOTAL PROTECTION WITH AES256 ENCRYPTION FOR THE DATA INSIDE KEYSECUREPC

TOTAL PROTECTION BY WIPING: VOLUNTARY DATA DESTRUCTION

Actual size: cm 9,5x3,5x1,3

KEY™ SECUREPC

IT IS NOT AN ENCRYPTED PEN DRIVE
IT IS NOT DATA PROTECTION SOFTWARE

It is an external device that, in a very small space, contains an entire operating system, your programmes and your fully encrypted AES256 data.

A revolutionary system that guarantees a level of security far greater than any device you have ever seen:
no encrypted pen drive, no data security software
can give the same guarantee of protection.

EMT140311UK

IT IS NOT AN ENCRYPTED PEN DRIVE
IT IS NOT DATA PROTECTION SOFTWARE.

TO FULLY APPRECIATE THE KEYSECUREPC REVOLUTION, YOU FIRST NEED TO UNDERSTAND WHY TRADITIONAL SYSTEMS ARE NOT THAT EFFECTIVE.

We are all familiar with the traditional methods of data privacy protection

- Deleting confidential files;
- Transferring them to an external memory;
- Using encrypted systems such as pen drives or data protection software.

There are also people who believe that having an access password to a computer is a good system of defence, sufficiently adequate for their needs.

There are even those who are convinced they are protecting their privacy by periodically formatting the hard disk, in an attempt to delete every last trace of their data.

IN REALITY, ALL THESE SYSTEMS HAVE THE SAME WEAK POINT IN COMMON:

IT IS TRUE THAT THEY HIDE OR DELETE YOUR FILES, OR AT LEAST THE VISIBLE COPIES OF THE FILES THAT YOU WORK ON;

THEY DO NOT, HOWEVER, DELETE THE SO-CALLED "TEMPORARY FILES"; THOSE COPIES OF YOUR DATA THAT THE COMPUTER YOU ARE WORKING ON CREATES CONTINUALLY. THESE FILES ARE SAVED AUTOMATICALLY, WITHOUT YOU SEEING THEM, IN THE HARD DISK, OPERATING SYSTEM AND PROGRAMMES.

Despite the name, temporary files are stored for years inside the computer. These are "ghost" files, that you don't see but which remain hidden for years in the memory of your computer. They record and keep track of your Internet browsing habits, emails and files you manage or download.

RECOVERING TEMPORARY FILES FROM YOUR COMPUTER IS VERY EASY.

SIMPLE DATA RECOVERY SOFTWARE IS ALL THAT IS REQUIRED TO BRING BACK THE DATA THAT YOU WERE CONVINCED YOU HAD DELETED FOREVER.

That is why it is no use:

- deleting files
- moving them to an external memory
- saving them on encrypted pen drives

It is also no use repeatedly formatting the hard disk of your computer. Formatting, like standard deletion, does not actually delete files and/or data.

This is why the traditional systems, such as encrypted pen drives or data security software, do not offer the same total protection as KeySecurePC and give your adversaries the possibility of recovering your confidential data.

THE KEYSECUREPC SOLUTION: 100% PROTECTION FOR THE PC

KeySecurePC is the revolutionary system that guarantees absolute security for your PC, as it prevents the creation and storage of temporary files, blocking activity of the operating system, programmes and hard disk.

More precisely, as soon as you connect KeySecurePC to your computer, the system:

1 Replaces the hard disk of your computer, blocking the original operating system and programmes.
2 redirects all data management and storage inside the device, where an operating system and programmes run parallel to yours.

You continue working as normal: creating and editing documents, browsing on Internet, downloading files, receiving and sending emails… but while you work, the hard disk, operating system and programmes on your computer do not record anything. Consequently, not even temporary files are created on your computer: in fact, not a single trace of the work done is left as all data management has been redirected to KeySecurePC.

THE KEYSECURE PC SOLUTION: 100% PROTECTION FOR THE PC

KeySecurePC replaces the hard disk and operating system of your computer.

You use the keyboard and screen of the computer, but your data does not transit on your PC. Everything is managed within KeySecurePC, which functions as a parallel computer, using the operating system, programmes and memory contained inside the device, with total AES256 encryption.

Using KeySecurePC to replace the hard disk, operating system and programmes on your PC is the base of the first, real guarantee of total protection that KeySecurePC offers: in fact, no one could ever recover your data from a computer where it has never actually transited.

THERE IS NO SOFTWARE IN THE WORLD, HOWEVER SOPHISTICATED, THAT CAN RECONSTRUCT YOUR DATA BY RECOVERING IT FROM THE PC YOU WERE WORKING ON: YOU COULD GIVE THE COMPUTER DIRECTLY TO YOUR WORST ENEMY, CERTAIN THAT THEY WOULD NOT BE ABLE TO EXTRACT ANY DATA WHATSOEVER.

WHAT HAPPENS WITH ENCRYPTED PEN DRIVES OR DATA PROTECTION SOFTWARE?

When you use a traditional system such as an encrypted pen drive or data security software, you use the hard disk, operating system and programmes on your computer: this is the problem. While you browse online, create and edit files, receive or send emails, your computer continually creates temporary files, or those hidden traces that you don't see.

When you finish work, you delete the files that you want to protect or move them to an external memory device. You feel confident, because you NO LONGER SEE copies of your work on the computer. AS A MATTER OF FACT, YOU ARE LEAVING A CLEAR TRACE OF YOUR ACTIONS ON THE COMPUTER (IN THE HARD DISK, OPERATING SYSTEM, PROGRAMMES). THESE TRACES CAN EASILY BE RECOVERED USING SIMPLE DATA RECOVERY SOFTWARE.

Your encrypted pen drive does not give protection to the computer, which remains the real weak point in your security system. ONLY KeySecurePC, by blocking hard disk activity and redirecting all data management within the device, prevents the creation of temporary files and makes it impossible to recover your data.

IT IS VERY EASY TO USE

1 CONNECT IT TO THE PC AND ACTIVATE IT WITH A FEW CLICKS

2 YOU WORK AS NORMAL ON YOUR PC

3 AT THE END OF A WORK SESSION YOU DISCONNECT IT AND TAKE IT AWAY WITH YOU

KEY™ SECUREPC

IT IS VERY EASY TO USE

1 CONNECT IT TO THE PC AND ACTIVATE IT WITH A FEW CLICKS

2 YOU WORK AS NORMAL ON YOUR PC

3 AT THE END OF A WORK SESSION YOU DISCONNECT IT AND TAKE IT AWAY WITH YOU

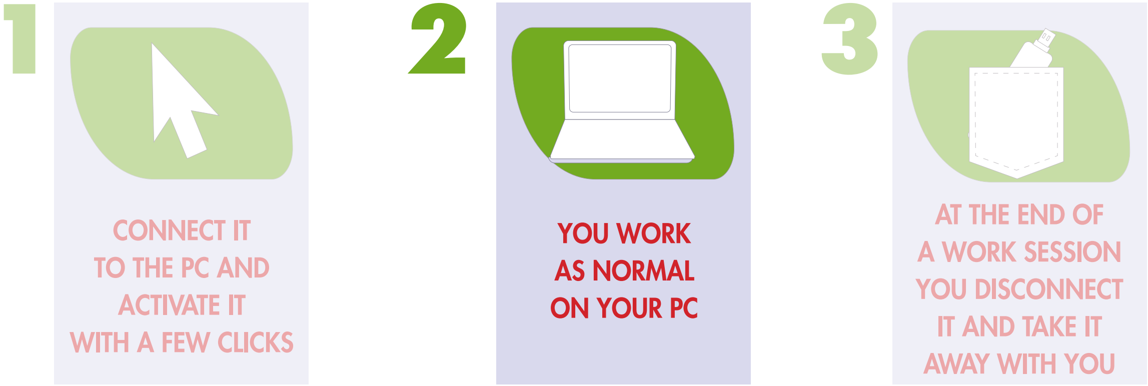
KeySecurePC connects to your computer via a USB port, like any other external memory device. Activating it is simple. There are 3 different ways to choose from.

- KEYSECUREPC IS ACTIVATED AUTOMATICALLY, as soon as it is plugged in, if your PC provides automatic booting from the USB port.

- IT IS ACTIVATED IN A FEW CLICKS, if you have installed the launch programme provided by KeySecurePC.

- IT IS ACTIVATED BY FOLLOWING THE "1° START UP PROCEDURE", if you have not installed the launch programme provided by KeySecurePC.

IT IS VERY EASY TO USE



1

CONNECT IT TO THE PC AND ACTIVATE IT WITH A FEW CLICKS

2

YOU WORK AS NORMAL ON YOUR PC

3

AT THE END OF A WORK SESSION YOU DISCONNECT IT AND TAKE IT AWAY WITH YOU

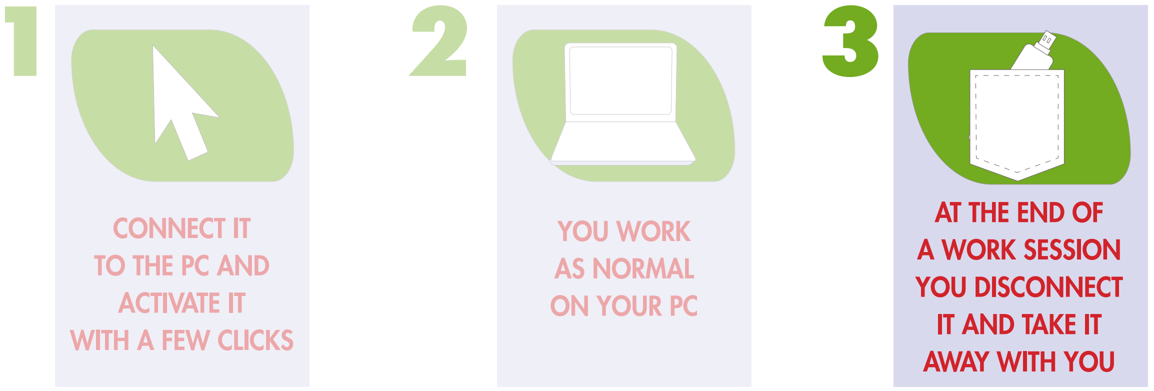
AFTER HAVING CONNECTED AND ACTIVATED KEYSECUREPC, YOU CARRY ON WORKING ON YOUR COMPUTER AS YOU NORMALLY DO.

KEYSECUREPC PROVIDES AN OPERATING SYSTEM AND A COMPLETE PACKAGE OF FREE PROGRAMMES AND APPLICATIONS.

There is a complete set of applications and software that enable you to use your computer in a comprehensive way: document preparation systems, spreadsheets, presentation programmes, Internet browsers, software for viewing images and videos or playing music, and much more.

Thanks to this operating system and the programmes already contained within the device, you can use your computer as you are accustomed to, in a fully comprehensive way.

IT IS VERY EASY TO USE



1 CONNECT IT TO THE PC AND ACTIVATE IT WITH A FEW CLICKS

2 YOU WORK AS NORMAL ON YOUR PC

3 AT THE END OF A WORK SESSION YOU DISCONNECT IT AND TAKE IT AWAY WITH YOU

At the end of a work session, disconnect KeySecurePC from the computer and take it away with you.
It is such a small object that you can carry it in a bag or even in your pocket, and you can easily store it in a safe or any other secure place.
When you take KeySecurePC away with you, you can leave your PC unattended on the desk with the absolute certainty that nobody could ever extract the data: this is because the data has never actually transited on the computer but instead has been entirely managed and stored within KeySecurePC.

It is a simple and ingenious solution that enables you to work without leaving a single trace on the PC.
Your privacy is totally guaranteed and you will no longer have reason to dread hackers, competitors or adversaries: nobody will be able to access your data without your consent.

HOW IT GUARANTEES ABSOLUTE PROTECTION.

1

100% PROTECTION OF DATA ON YOUR PC

2

TOTAL PROTECTION WITH AES256 ENCRYPTION

3

TOTAL PROTECTION BY WIPING: VOLUNTARY DATA DESTRUCTION

KEY™ SECUREPC

HOW IT GUARANTEES ABSOLUTE PROTECTION.

1 100% PROTECTION OF DATA ON YOUR PC

2 TOTAL PROTECTION WITH AES256 ENCRYPTION

3 TOTAL PROTECTION BY WIPING: VOLUNTARY DATA DESTRUCTION

As soon as KeySecurePC is connected to your computer, the system:

1 Replaces the hard disk, operating system and programmes on your computer.

2 redirects all data management and storage inside the device, where an operating system and programmes run parallel to yours.

You continue working as normal: creating and editing documents, browsing on Internet, downloading files, receiving and sending emails... but while you work, the hard disk, operating system and programmes on your computer are blocked and do not record anything, and all data management is redirected to KeySecurePC. Above all, your computer does not create or save temporary files: this is why no trace of your work is left on the computer.

YOUR PC IS 100% SAFE: NO ONE COULD EVER RETRIEVE ANY DATA WHATSOEVER FROM IT, NOT EVEN WITH THE MOST SOPHISTICATED SOFTWARE, BECAUSE DATA NO LONGER TRANSITS ON YOUR COMPUTER.

HOW IT GUARANTEES ABSOLUTE PROTECTION.

1

100% PROTECTION OF DATA ON YOUR PC

2

TOTAL PROTECTION WITH AES256 ENCRYPTION

3

TOTAL PROTECTION BY WIPING: VOLUNTARY DATA DESTRUCTION

KeySecurePC replaces the hard disk and operating system of your PC and redirects all data management within the device, where an operating system and programmes run parallel to those of your computer.

THE OPERATING SYSTEM AND PROGRAMMES CONTAINED WITHIN KEYSECUREPC ARE FULLY AES256 ENCRYPTED. THE ACRONYM AES STANDS FOR "ADVANCED ENCRYPTION STANDARD", AND REFERS TO A BLOCK CIPHER ALGORITHM WHICH TO DATE HAS NOT BEEN CRACKED AND IS CONSIDERED UNBREAKABLE WITH CURRENT COMPUTING POWER.

Only those who know your password can access your data. Anyone else would first have to crack the AES256 encryption which, as we have already mentioned, is currently considered virtually unbreakable.

KEY™ SECUREPC

HOW IT GUARANTEES ABSOLUTE PROTECTION.

1

100% PROTECTION OF DATA ON YOUR PC

2

TOTAL PROTECTION WITH AES256 ENCRYPTION

3

TOTAL PROTECTION BY WIPING: VOLUNTARY DATA DESTRUCTION

The only possibility for a potential perpetrator, would be to “guess” your password, trying every single combination of letter and numbers, perhaps using specialised software.

Another important factor is that KeySecurePC does not encrypt single files, as the encrypted pen drives that many use often do, but goes beyond that, encrypting the ENTIRE OPERATING SYSTEM and, consequently, all programmes and all data managed within the device.
It is impossible to access a single file without knowing the password. To do so, you would have to force the entire system: a practically impossible feat considering the security level guaranteed by total AES256 encryption.

HOW IT GUARANTEES ABSOLUTE PROTECTION.

1 100% PROTECTION OF DATA ON YOUR PC

2 TOTAL PROTECTION WITH AES256 ENCRYPTION

3 TOTAL PROTECTION BY WIPING: VOLUNTARY DATA DESTRUCTION

KEYSECUREPC IS ONE OF THE VERY FEW SYSTEMS IN THE WORLD EQUIPPED WITH A WIPING FUNCTION, THAT IS AN OPTION FOR THE VOLUNTARY AND IRREVERSIBLE DESTRUCTION OF DATA.

A function that may seem excessive, but that many professionals and entrepreneurs appreciate because, in extreme cases, data destruction is preferable to letting it fall into others' hands, even if it is encrypted and inaccessible.

The KeySecurePC Wiping function not only removes single files but the entire operating system, making it impossible to retrieve data.

THE WIPING FUNCTION IS ANOTHER IMPORTANT DIFFERENCE BETWEEN KEYSECUREPC AND TRADITIONAL SYSTEMS SUCH AS ENCRYPTED PEN DRIVES OR DATA SECURITY SOFTWARE, WHICH NORMALLY DO NOT INCLUDE THIS FUNCTION AS AN OPTION FOR CLIENTS.

ADVANTAGES OF KEYSECUREPC

1) Data confidentiality

2) Lightweight

3) Speed

4) Portability

5) Recovery of old hardware in disuse

6) Protection of ideas and intellectual property

7) Invulnerability to spyware, adware and telematics tracking in general

8) Invulnerability to viruses (with consequent savings on antivirus and other devices)

ADVANTAGES OF KEYSECUREPC

9) Development of tailor made applications for individual businesses and professions (common to all platforms)

10) Compatibility with the highest number of software professionals and businesses offline

11) Total compatibility with SaaS business and professional applications and online in general

12) Quick and trouble free management of external devices, such as and including obsolete printers

13) Protection of sensitive data (in compliance with the legislative norm 196/03) even in case of theft or fraudulent removal

14) Wiping in two minutes (voluntary data destruction)

NO ENCRYPTED PEN DRIVE, NO DATA SECURITY SOFTWARE CAN GIVE YOU THE SAME GUARANTEE AS KEYSECUREPC.

IN SUMMARY: WHY KEYSECUREPC IS SAFER THAN AN ENCRYPTED PEN DRIVE

KeySecurePC gives absolute protection to the data on the PC because it does not use the hard disk, operating system or programmes and redirects all data management within the device.
A normal encrypted pen drive leaves traces on the hard disk, in the operating system and in the programmes because it uses them without preventing the creation of temporary files, which keep track of your activities for years.

KeySecurePC adds the guarantee of AES256 protection for the data saved within the device: an encryption algorithm that to date has not been cracked and is considered unbreakable.
A normal encrypted pen drive usually has a weaker encryption than AES256 which, therefore, could be cracked more easily.

KeySecurePC is one of the very few devices equipped with Wiping, voluntary data destruction.
An encrypted pen drive is not usually equipped with a data destruction system.

IN SUMMARY: WHY KEYSECUREPC IS SAFER THAN AN ENCRYPTED PEN DRIVE

KeySecurePC contains an entire operating system, programmes and applications: for all intent and purposes it is like a tiny computer that you can carry around with you, which means that you always have your desktop, files, emails, videos with you (in a word: your computer...). All you need to do is connect it to any PC and you'll find your desktop and files ready for work as if it were your own computer, but always in maximum security conditions.

A normal encrypted pen drive only contains your files. Every time you connect it to a different computer, you take a big security risk.

IN SUMMARY: WHY KEYSECUREPC IS SAFER THAN AN ENCRYPTED PEN DRIVE

KeySecurePC is a revolutionary system. It is easy to use, partly thanks to an entirely new system of icons inspired by your user friendly smartphone and the most advanced tablet PCs. It provides thousands of programmes free of charge and can offer you a completely new experience: an easier and more immediate way of working, with the guarantee of absolute data protection for your computer.

KEY™ SECUREPC

KEYSECUREPC S.P.A.
Exclusive Right to Sell
P.IVA 11213071001
Via Lungotevere delle Navi, 20 - 00196 Rome
19925 Stevens Creek Blvd. - Cupertino CA 95014

Swiss patent pending N. 0363/11
c/o Swiss Federal Institute of Intellectual Property
Stauffacherstrasse 65/59g, CH-3003 Bern

KEY™
SECUREPC

Actual size: cm 9,5x3,5x1,3

Contact:

www.keysecurepc.com
info@keysecurepc.com