SmartPico

Overview version 1.0

CE

This hardware key is in compliance with the following test specification:

CEI EN 61000-4-2; CEI EN 61000-4-3; CISPR22

as required by:

CEI EN 61000-6-1, CEI EN 61000-6-2, CEI EN 61000-6-3, CEI EN 61000-6-4

which are specified for the following test:

- "ESD Immunity test"
- "Radiated radio-frequency and electromagnetic field immunity test"
- "Radiated Emission Verification"

In compliance with the "Essential Requisites" for the EMC Directive 89/336/EEC.

FC

FCC ID: TFC-AAG

Eutronsec S.p.A.
SmartPico
Supply: 5V DC
Absorption: 250 mA

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

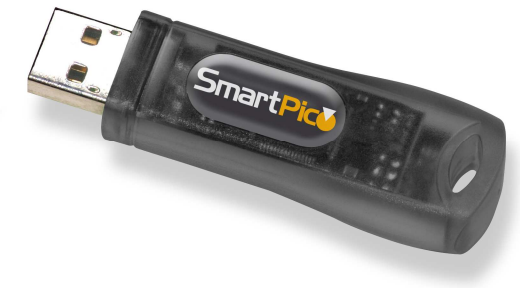
Caution: changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

IMPORTANT REMARKS

Due to the limited space on the product shell, all FCC certification references are on this technical manual.

Changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

1. Introduction

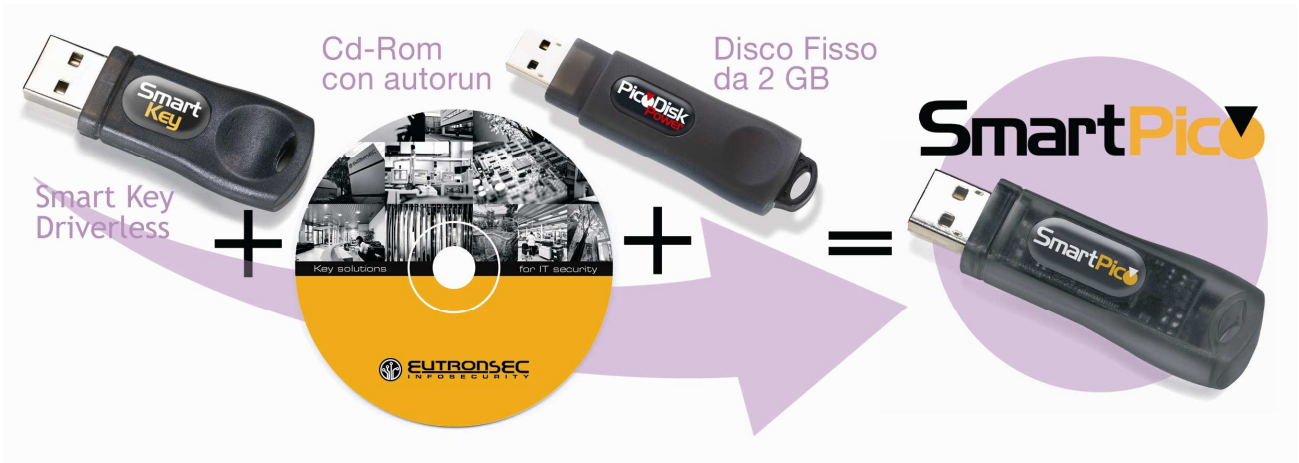


SmartPico is a driverless device that combines the SmartKey's software protection characteristics with the handiness and data transport features. The core of the device is represented by SmartKey, the dongle for software protection against piracy, and mass storage memory where to upload the software itself.

SmartPico's software protection section is fully plug & play; it does not require any installation on the computer as it exploits drivers that are already available in Windows installation. This part is always characterized by one unique code that identifies the software house.

By means of the included application it is possible to partition the flash memory into various units according to one's needs. It is possible to create one partition with a CD functionality in order to manage Windows autorun and store the ISO image, one mass storage partition at the end-user's disposal, one write-protected partition, for a "secure" use and one fully encrypted partition. Besides it is possible to reserve a memory area which is hidden to the operating system but that can be accessed by addressing it with proper commands.

The application can be then directly installed on SmartPico, protected by any unauthorized copy and run, also automatically, directly from the device thus making the solution completely portable.
The User will only have to insert it in the USB port of any computer and the application will be immediately available.



2 DEVICES IN 1

- software protection like with Smartkey without having to install any driver (using the SDK of the SmartKey)
- partitionable flash memory with the possibility of creating up to 4** partitions with the following functionalities:

- Standard Mass Storage, where data can be stored and visualized
- CD-ROM, with Autorun function
- Encrypted Mass Storage, with AES 256 bit
- Write-protected Mass Storage, that is a read-only partition

(**) Hidden area to the OS

2. Features

High security: the use of microprocessors makes hardware cloning of the dongle impossible.

Driverless: the dongle drivers are already present in Windows installation.

Algorithmic query: algorithmic query processes, and not only fixed response based, are present

Identification Code: each dongle is customized with an ID code which is preset during the manufacture and different for every User.

Data Protection: it allows to encrypt data files associated with the proctected applications.

Internal Memory: up to 896 bytes of non volatile secure password protected memory for reading and writing operations.

Programmable security codes: the user can program a double 16+16 access code through the utilities supplied.

Remote control: additional libraries allow to identify, read and write the dongle installed on an Internet client.

Languages: complete support of programming languages and environments (Visual C++, Visual Basic, Autocad, Solaris, Delphi, .NET, ecc).

Flash memory capacity: 256MB - 512MB - 1GB - 2GB.

SDK: constantly updated on the website.

3. Technical specifications

- USB Spec. 1.1 - USB 2.0 High Speed
- Green LED (power on/connected)
- Data reading speed of the flash memory: 18 MB/s
- Data writing speed on the flash memory: 11 MB/s
- Certifications: FCC/CE