ThalesAlenia Space
A Thales / Finmeccanica Company

SecBox

A851 Ciphering station for computer data and mails

A851® is the safest way to guarantee confidentiality and integrity of highly sensitive data met in military or governmental applications (embassies, security services, …) and in some civil applications for highly confidential communications.

A851® is the ideal tool to protect your computer data while they are safeguarded or transported. It does not only allow to encrypt files and folders from Windows Explorer® but also to protect any sensitive part of a document, which has been created within a Windows® application.

Integrated in all existing electronic mail systems (Lotus Notes®, Outlook®, Hotmail®, Yahoo® ...) it also secures your mails exchanged over the Internet.

So easy to use

In a computer world where systems complexity evolves more and more quickly to the detriment of basic requirements for a quality security system, ***A851®*** is designed to allow an easy validation of its design and its right working.

The safest solution: *A851®* comes in the form of a rugged box that contains cryptographic algorithms as well as all sensitive information (secret keys, authentication, …). In any case this information cannot be accessed outside the box and a fortiori from the Internet network. It is automatically deleted in case of intrusion attempt or emergency system activation.

With a single key

A "User" access **control electronic key** physically introduced in ***A851®*** box restricts the cryptographic services to authorized people only. The loss or the equipment theft does not compromise the network security.

The ***A851®*** box is combined with the *SecClip®* software driving *SecBox®* device that is installed on the operator workstation (PC) to which it is connected by a high speed link.

The *KGS A857* system generates with complete confidence new secret keys, manages and attributes them to various users groups. Mechanisms of distribution and automatic renewal of keys are based on their validity periods (crypto-periods) which reduces the security manager interventions to a minimum.

Main advantages

- Polyvalent: product operational with all types of Windows® applications
- Very great facility of use
- High quality: solution of "military" quality
- Increased awareness of the users to the security policy
- Secret keys management made a lot easier thanks to the use of the KGS A857 system.
- Easy to evaluate by security authorities
- Access control reinforced by use of a physical access key per user (no password to memorize)
- Easy deployment on any type of PC (USB interface) without requiring an auxiliary supply

ThalesAlenia Space
A Thales / Finmeccanica Company

Technical Specifications

Operating Modes	◆ ASCII, binary, 8-bit data ◆ Baudot (on request) : possibility of a formatting compatible with Telex/TTY messages
Software	◆ Ciphering/deciphering of sensitive parts of documents which have to be protected, including when editing e-mails ◆ Ciphering/deciphering of folders and any type of files ◆ Easy selection of the secret key to use and activation of cryptographic functions by simple sequence of keyboard keying. ◆ Systematic shredding of the residual "clear" information on the user PC. ◆ Logbook of all operations and alarms ◆ Platform : PC with Windows® 98, Win NT4®, Win 2000® and Win XP® operating systems.
Algorithms	◆ DES, Triple-DES, AES-128, AES-256 or proprietary ◆ Other algorithm on request
Secret Keys	◆ Secret keys size : up to 256 bits depending on the algorithm chosen ◆ Up to 200 different secret keys stored in SecBox® device. ◆ Possibility for the user to introduce a personal secret key (only with the security manager agreement)
Keys Renewal	◆ Automatic on basis of crypto-periods defined by the security manager
Key Generation Station	◆ KGS Alcatel 857® : Secret keys generation and distribution software with time validity management
Access Control	◆ Strong user authentication and security manager via their physical access key ◆ Dimensions : 5.0 x 0.7 ∅ cm
Intrusion Detection	◆ Automatic destruction of sensitive parameters in case of intrusion detection or on voluntary action of the operator (KILL).
Security Certification	◆ Designed to meet the Common Criteria and FIPS-140 recommendations
Interfaces and Power Supply	◆ USB port (driver for Win NT4® available) ◆ No additional power supply.
Physical Characteristics	◆ 4 LEDS on SecBox® device to report the current use of the "User" or "Security Manager" cryptographic functions as well as alarms. ◆ Anti-theft : Designed for Key&Lock® (Kensington) fixing by cable
Size	◆ 6.8 x 11.8 x 1.9 cm
Reliability / Maintenance	◆ MTBF : 80.000 hours in operation - MTTR : 5 minutes

The Thales Alenia Space ETCA policy is one of continuous development and consequently the equipment may vary in detail from the description and specification in this publication.

Thales Alenia Space ETCA
101, rue Chapelle Beaussart
B-6032 Mont-sur-Marchienne – Belgium
Tel. : +32 (0) 71 44 22 11
Fax : +32 (0) 71 44 22 00
E-mail : etca.info@thalesaleniaspace.com
www.thalesaleniaspace.com

THALES