SIR

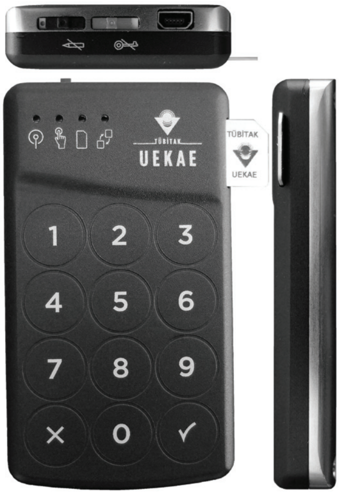
Secure USB Flash Memory Storage Device

TÜBİTAK

BİLGEM

CENTER OF RESEARCH FOR ADVANCED TECHNOLOGIES OF INFORMATICS AND INFORMATION SECURITY

SIR, Secure USB Flash Memory Storage Device



SIR is an encrypted USB flash memory storage device which protects data fulfilling the security requirements on a full hardware based architecture, operated by a single user. The device has the storage capacity options of 2GB/4GB/8GB flash memory with the ability of 10MB/s writing & reading speeds.

The device protects data stored on itself, not while reading from or writing to the host. Data security and device/user authentication requirements are provided by means of a user token and a user password.

The device employs a hardware implementation of a confidentiality protection algorithm type for providing data security for data classified as NATO SECRET and below. 256-bit hardware AES encryption block is used to provide data security. Device generates the keys used by the hardware AES encryption block using its own Random Number Generator, eliminating the need for key loading.

SIR supports plug and play operation when used with a wide range of operating systems of the host computer including Windows VISTA, Windows XP/2000/Me/98SE, MacOS 9.x, Linux Kernel 2.4 and higher versions. There is no need for any additional setup procedure for the usage of the device. It doesn't require any software application running on personal computers which the device is connected to; thus this approach results in non-vulnerability to threats related with user password and security parameters such as viruses or trojan horses.

Additional security precautions like emergency erase and tamper switches are employed in the device.

The user is informed about any change in the status of the device by the help of the visual indicators (login, keypressed, token, USB connected warnings) and an audio indicator.There is a write protect switch on the device to disable writing to the device if needed. The device is powered from one slot USB interface of the host computer, which it is connected to. There is an embedded battery inside which is charged via USB interface of the host, for supplying key memory for maximum 6 months period without any power.

Designed to be commercial grade, tactical, ruggedized, portable equipment, SIR is fully compatible with the COMSEC, EMI/ EMC, TEMPEST standards.

COMMUNICATION AND INFORMATION ASSURANCE

TECHNICAL SPECIFICATIONS	
Nato Stock Number	
Data Storage Capacity	2GB/4GB/8GB flash memory
Access Control:	• Two factor authentication with token and user password. • Equipment and user authentication with password protection & authorization and smart card as token.
Encryption	Real time hardware based offline encryption
Algorithms	256 -bit AES
Security	• Encryption architecture with 3 independent functional control blocks, 2 tamper switchs and BIT test. • Mechanical and electrical isolation depending on RED-BLACK separation.
Encrypted and stored Data Classification	NATO SECRET and below.
Key Generation & management	Self key generation, customizable user password.
Key Storage	• Split Key structure in three parts. • Embedded chargeable lithium battery for supplying key memory for maximum 6 months period without any power.
Access Security	No access to the system without token and password
Operating Systems	• Platform independent - Works on Windows, MAC and Linux platforms without the use of software. • Supports Windows VISTA, Windows XP / 2000 / Me / 98 / 98SE, MacOS 9.x, Linux Kernel 2.4 and higher version operating systems.
User Interface	12-key piezo ceramic keypad, 4 two coloured indicators, 1 buzzer, 1 emergency erase switch, 1 write protect switch
Host Interface	• Plug and Play - Hardware based security works without installing or running any software. • Interfaces supported: USB 2.0, USB 1.1, USB1.0
Read/Write Speed	10MB/s both.
Maintenance	• Power on controlled Built In Test -BIT, • Alarm management: login, keypressed, token, USB connected warnings, battery charge status warning (full or low levels), emergency erase.
Dimensions(WxDxH)	51 x 91 x 14 mm
Weight	90 g
Power Supply	5 V USB (one slot USB interface powered from the host.)
Power Consumption	<2.5W
Operating Temperature Range	Between +0°C and +50°C
Storage Temperature Range	Between -20°C and +65°C
Carriage Temperature Range	Between -40°C and +70°C
Relative Humidity	Between 10% and 90% relative humidity at 40°C
EMI/EMC	EN55022 ClassB.
TEMPEST	Compatibility to SDIP-27 Level A (AMSG-720B) standard, TEMPEST compatible to the TEMPEST standards of the host computers that the device is connected to.
Mechanical Architecture	Ruggedized aliminium case
Due to continuing product improvements, these specifications are subject to change without notice.	

TUBITAK BILGEM UEKAE
T: +90262 648 1000 • F: +90262 648 1100 • E: bilgem@bilgem.tubitak.gov.tr
W: http://www.bilgem.tubitak.gov.tr • A: P.BOX: 74, 41470, Gebze, Kocaeli, TURKEY