USBK™

CRYPTOBRIDGE
Unlimited Privacy

PROTECT YOUR PRIVACY

Your privacy is constantly in danger: USB sticks are extremely popular for transporting data. This is down to convenience in terms of their physical size and easy to use facility. Unfortunately their greatest asset is their greatest downfall: As small and convenient as they are, more likely to be lost or stolen. In any event, data in removable USB drives can be read easier than a postcard. Losing sensitive information on an open, unsecured USB stick could be disastrous for anyone. There are good reasons to protect trade secrets, work presentations, family photos or any other sensitive records, as doing so ensures shareholder value, public confidence and internal productivity.

USBK™ addresses these concerns and protects your privacy: You can turn your USB sticks and even your removable hard disks into a portable safe and securely carry your all sensitive data or work.

It is an on-the-fly encryption device featuring two USB ports, thereby provides encrypted link between host PC and peripheral USB stick or hard disk. All data is encrypted 100%, ensuring maximum security by hardware based encryption with freedom of using your own USB sticks or harddisks. Your USB stick got lost or stolen? In any event, your data is untouchable.

UNLIMITED CAPACITY

You notice something different from other recent entrants into this market:

USBK™ is a unique device as you can purchase today, that offers hardware-based 256-bit AES encryption and password protection, but without any internal storage area.

Create as much capacity as you like: Standard USB sticks are used, so you will be creating your capacity with your own standard USB stick and possible to encrypt many USB sticks by just one USBK™. All is at your discretion!

Features & Benefits

- **On-the-fly Encryption** — 256-bit and 128-bit AES hardware-based encryption is done during data transfer
- **Unlimited Capacity** — Use any USB stick or external harddisk in any capacity; no limited in anyway
- **Cost Effective** — Encryption cost per Gigabyte reaches to 0$ as there is no limit in capacity
- **Easy to use** — Just plug into USB port, activate and use. No need to install driver or software
- **User Authentication** — User password to prevent unauthorized access
- **Secure** — Zero foot-print on system and erases user password and encryption key after 3 wrong password attempts
- **Multiple Key Option*** — Create different encryption keys for work departments and personal data
- **Compatible on Multiple Platforms** — Possible to use on test and measurement equipments such as oscilloscope, EKG, etc.

Why is USBK™ secure?

- **Hardware-Based Encryption**
  - On-board hardware 256-bit and 128-bit AES encryption
  - Much more secure than software encryption
- **Strong Key Protection**
  - Encryption keys are managed in a chip – not USB Drive or PC
  - Encryption keys are also stored in AES encrypted
- **AES Encryption Mode**
  - Uses CBC mode of AES – the most secure AES mode available today and preferred by both NIST and NSA

* Multiple key option is available on model A103 only.

Technical Specifications

Security Features	
Encryption Type	256-bit and 128-bit AES (Advanced Encryption Standard)
Encryption Method	Hardware Based Encryption
AES Mode	CBC (Cipher Block Chaining) mode
AES Key	User initiated or Random Key Generator
Number of AES Keys	1 (for model A101) 3 (for model A103)
User Authentication	Password
Failed Password Procedure	Return back to fabric default after 3 wrong password attempts
System & Peripheral Features	
USB	USB 2.0 High Speed (USB 1.1 backward support) Plug&Play
Driver & Software Requirements	No need to install driver & Pop-up GUI for Windows (.net framework dependent)
Operating Systems	Supports Windows, Linux, MAC
Design Features	
Dimensions	10 x 20 x 75 mm
Connectors	USB A Type Plug for PC Side USB A Type Receptacle for USB Stick Side

Multiple Key Option

Customize your privacy policy with A103 model: There should be clear reasons to safeguard your work and personal data with different encryption keys

Model	Description
A101	1 encryption key is created
A103	Up to 3 Encryption keys can be created

Plug, Activate, Use

Host System
(Laptop, PC or any)

On-the-fly Encryption

Encrypted Data
(On USB removable disk)

10-point for selecting USBK™

1. As quick and easy to use as a normal USB Sticks
2. Does not require drivers or administrative privileges
3. Uses future-proof 128-Bit AES encryption
4. Uses transparent on-the-fly encryption that won't disturb the user when handling files
5. Built security features with standard USB Sticks or Harddisks
6. Uses any USB Stick or USB Harddisk in any capacity; not limited in anyway
7. Cost-efficient way of privacy due to unlimited capacity
8. Offers a custom password and encryption key
9. Configurable privacy policy with multi-key option
10. Compatible across multiple platforms, can be used on test and measurement equipments such as oscilloscope, EKG, etc.

Tamara Elektronik Ltd. Sti. Acibadem Cad. 34/3 Kadikoy Istanbul-Turkey P:+90 (216)418 9294 www.tamara.com.tr

USBK2v0_Datasheet_EN_4v1