USBK - CryptoBridge

USER GUIDE

Version: 1.2

Models: A101
A103

For more product information, please visit
www.usb-k.com

Contents

Contents 2

Introduction 6

Technical & Security Notes 7

Key things to know about your USBK- CryptoBridge 7

Best Practices 8

Overview 9

Security Label (Sticker) as Seal 9

Package Content 9

Identifying Parts 9

About USBK Models 10

Introducing USBK 10

Definitions 10

States (Modes) of USBK 10

Types of Users 11

How USBK protects your data 11

System Requirements 11

Getting started 13

Before You Begin 13

About Drive Mapping 13

Control Panel of USBK Management Software 13

Initializing with a USBK 14

Personalizing a USBK 14

Starting with your BackDisk 17

Day to Day Using of USBK 19

Activate / Deactivate your USBK 19

Activate your USBK 19

Deactivate your USBK 19

Usage of BackDisk 20

Understanding USBK status via LEDs 20

Managing User Authentication 22

Changing your password 22

Forgetting your password 23

Auto-Activation Property 23

Managing USBK(s) 25

Recycling a USBK **25**

Changing Device (USBK) Name **25**

Changing Key Name(s) on USBK **26**

Viewing device information **26**

Using USBK on Linux ***28***

Getting started for Linux **28**

Installing Linux CLI Software 28

Using USBK Linux CLI Software 29

Initializing with a USBK **29**

Personalizing a USBK 29

Starting with your BackDisk 31

Day to Day Using of USBK **31**

Activate / Deactivate your USBK 31

Usage of BackDisk 32

Changing your password 32

Forgetting your password 32

Auto-Activation Property 32

Changing Device (USBK) Label 33

Changing Only Key Name(s) on USBK 34

Using USBK with Text Editor ***35***

Getting Started **36**

Personalizing a USBK 36

Starting with your BackDisk 39

Day to Day Using of USBK **40**

Activate / Deactivate your USBK 40

Usage of BackDisk 41

Changing your password 42

Forgetting your password 42

Auto-Activation Property 42

Changing Device (USBK) Name 43

Changing your encryption key(s) 44

Viewing device information 45

Using USBK with a USB Hub ***46***

Troubleshooting (FAQ) ***47***

USBK.exe program doesn't work. What can I do? **47**

How can I recover my Encryption Key if I forget it? **47**

My BackDisk plugged-in USBK recognized as unformatted. Why? **47**

The file that I saved to USBK disk is lost. Why? **47**

I have two partitions on my BackDisk. Can I use one partition encrypted with USBK and other partition as regular? **47**

How long does it to format my 300GB external harddisk by USBK? **47**

How can I read data on my BackDisk if I lost my USBK? **47**

Who are we? *48*

Contact Information *48*

Appendix: USBK policy settings *49*

Revision History

Version	Date	Comments
Ver: 1.0	23.03.2011	Initial Publication
Ver: 1.1	24.03.2011	"About USBK Models" part of this guide is revised
Ver: 1.2	23.05.2011	"Using USBK on Linux" and "Using USBK with Text Editor" parts of this guide is revised.

NOTE: Please visit our website www.usb-k.com to obtain the latest version of this document.

Introduction

Thank you for your interest in USBK - CryptoBridge. This document will help you become familiar with it.

USBK - CryptoBridge offers the following benefits:

- Built security features on ordinary USB flash drives and USB external harddisks.
- Secures your removable data by hardware-based encryption (AES 128-bit and AES 256 bit).
- Offers you unlimited capacity as there is no restriction on quantity and size of USB drives that you use with your USBK.
- Compatible with a wide range of hosts, independent from operating system.
- Does not require installation driver or software on host.
- Possible to use on test & measurement equipments such as oscilloscope, EKG, etc. with its auto-activation property.
- Easy-to-use and affordable.

This guide provides instructions for Windows. Procedures that are OS-specific (Operating System specific) carry the OS name. Procedures that do not specifically mention the OS apply to Windows.

Additionally, this guide is valid for all models of USBK on page 10. Procedures that are specific for model is emphasized with comments including the model name.

We made use of special conventions which will guide you throughout the entire document. The purpose of each convention is explained below:

! CAUTION: This convention is used when there is a topic related to data security and/ or situation which may result in loss of data and vulnerability.

NOTE: This convention is used when a topic has a helpful note or additional information that is possibly essential or complements the main text.

Tip: This convention is used when there's an alternative way to do so with expressed instructions.

Technical & Security Notes

Key things to know about your USBK- CryptoBridge

! On-the fly Encryption – Always

When you use your USBK, all data encryption/decryption is performed automatically and absolutely transparent to you. It cannot be disabled.

! Fabric Default

You must personalize your before you start to use it. You are forced to set new password at first usage.
After this password setting, random encryption key(s) is assigned on your USBK. That's why, it is strongly recommended to set your encryption key(s) and take in care the notes here at Encryption key(s).

! Password protected

Do not share your password with anyone- keep it secret.

! It's Self-destruct

After 3 wrong password attempts, USBK erases all your encryption key(s) and password, returns back to Fabric Default. You are forced to set new password same as at first usage. Take in care the notes here at Fabric Default.

! Encryption key(s)

After setting/changing your encryption key(s), write down encryption key(s) in note for future reference, but remember to keep it confidential. There's no way to recover encryption key(s) as they are never exported or displayed during usage of USBK. A lost of encryption keys results in lost of data on BackDisk. Therefore, it is very important that you remember the encryption key(s) or store it in a safe place.

! Format at first-time use of BackDisk

You must format your BackDisk (USB stick / USB external harddisk) when it is the first time use with your new encryption key(s).

! Use only on trusted HostSytems

HostSystem should be protected against virus, trojan, malware or any type of network attacks which can compromise the security of data transfer between the HostSystem and USBK. Operational environment should also be trusted.
Any person, any application or software that use the open platform of computer can access the BackDisk and become a user when USBK is in "**Activate**" state.

! Take more care when your USBK in 'Auto-Activation"

If you carry and lose your BackDisk plugged-on your USBK in "Auto-Activation Enabled", any user can access your data on your BackDisk when he plug in the computer as no password is asked to verify user. Just carry only your USBK when "Auto-Activation Enabled" for the security of data on your BackDisk.

Best Practices

☆Physically securing

You can physically secure your USBK on keychain or use lanyard provided.

☆ Read user guide

This document will help you become familiar with your USBK and secure usage. You can obtain the latest version of user guide on our website www.usb-k.com.

☆Renaming your USBK

You can optionally change the name of your USBK so that you will be able to identify them easily when you plug.

☆Giving name to encryption key(s)

You can optionally give name for your encryption key(s) for easy usage.

☆ Encryption keys per your BackDisks

Keep in mind which encryption key is used for your each BackDisk in order to prevent disk confusion. There is no support on USBK for this point.

Overview

Security Label (Sticker) as Seal

Check the security label and examine the packaging.

USBK carton box has a security label as seal that need to be cut or removed before it can be opened. The label is positioned over the opening port of the carton box to ensure that you are purchasing a genuine USBK.

If you see that the security label is removed or damaged, please contact with your supplier immediately.

Package Content

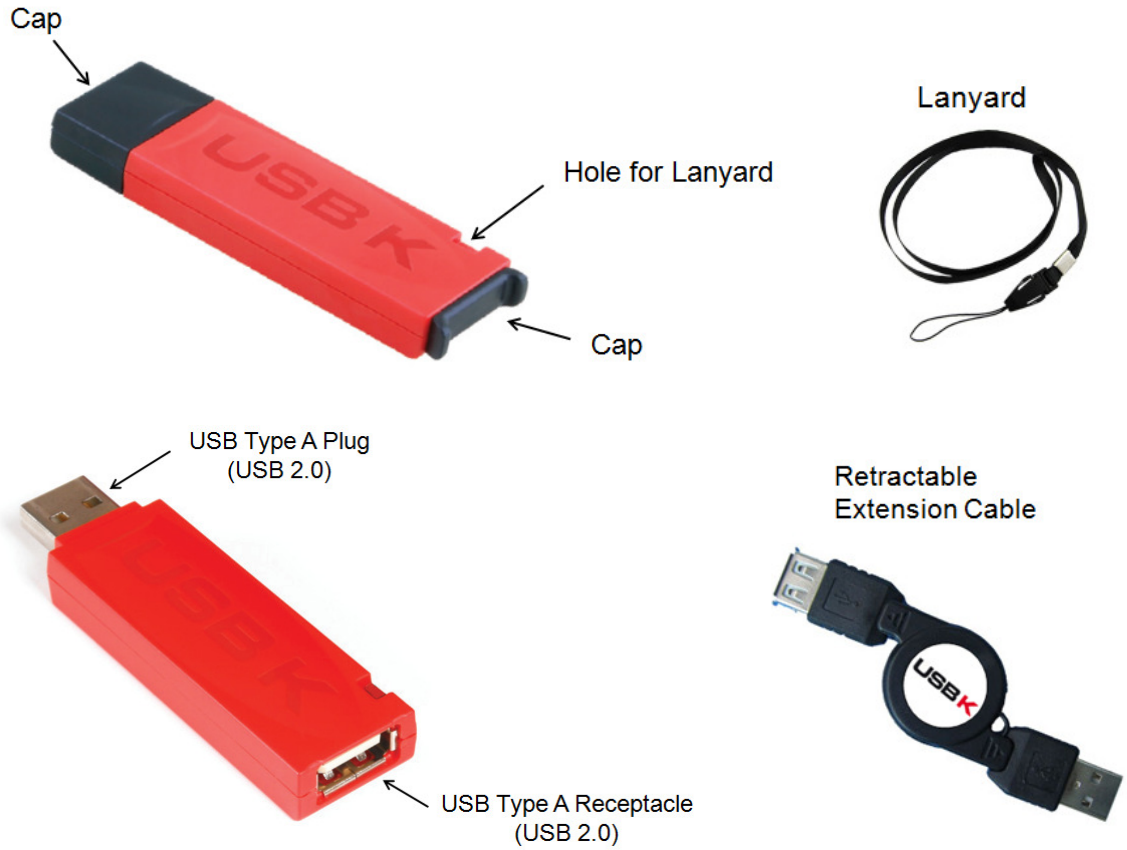
Your USBK package includes:

Accessory	Qty
USBK-CryptoBridge	1
Removable Lanyard	1
USB (A male to A female) Retractable Extension Cable 2.0	1
Download Instruction for User Guide	1

If any item is missing or damaged, please contact with your supplier immediately.

Identifying Parts

This part helps you to become familiar with your USBK – CryptoBridge and its parts.



About USBK Models

The following table provides a brief description about each USBK models.

Device	Model	Description
	A101	1 encryption key is created
	A103	Up to 3 Encryption keys can be created 3 adet şifreleme anahtarı desteklenir

Introducing USBK

USBK - CryptoBridge is an on-the-fly encryption device featuring two USB ports which establish and maintain encrypted link between HostSystem and BackDisk. It is equipped with a USB Type A receptacle for attaching your BackDisk, a USB Type A plug for attaching to your HostSystem.

Definitions

HostSystem: The system on which the USBK is plugged and used. It can be a desktop PC, laptop PC or test & measurement equipment such as oscilloscope, EKG, etc.

BackDisk: All kind of USB flash drives and USB external hard drives plugged into the USBK for secure data transfer. The capacity/ size of USB drive is not important, it can be in any size in any brand name. Additionally, file system of USB drive is also not important. It can be NTFS FAT/ FAT32 or EXT3/EXT4.

NOTE: USBK is not compatible with USB storage disks with multiple LUNs. The BackDisk should be single LUN.

On-the-fly Encryption: It means that encryption is made always automatically and transparently without user intervention and cannot be disabled. Data can be copied to/from a mounted BackDisk at back of USBK just like they are copied to/from any normal USB drive (for example, by simple drag-and-drop operations). Data that are being written or copied to the BackDisk are automatically being encrypted on the fly. Similarly, data is automatically being decrypted on the fly while it is being read or copied from a BackDisk.

States (Modes) of USBK

- **Fabric Default (Initial State):** This is the state that USBK is in Fabric Default. In this state, the user is forced to set new password.
- **Deactivate State:** This is the state that, any user who knows the user password can perform the tasks of USBK such as Deactivate key, setting/changing password, setting/changing key(s) and key name(s), setting/changing device name (label) and setting Auto- Activation property. 3 failed password attempts during these settings,

the USBK erases all your encryption key(s) and password; and returns back to Fabric Default(Initial State).

- **Activate State:** This is the state that the BackDisk is accessible and used securely. In this state, user has privileges just to perform Activate key Types of Users

Types of Users

With USBK - CryptoBridge, one user type is present as general users. General users are typical device user who can authenticate USBK and save data securely to BackDisk.

General users have all privileges to perform all tasks of USBK such as Activate/Deactivate key, setting/changing password, setting/changing key(s) and key name(s), setting/changing device name(label) and setting Auto- Activation property.

! CAUTION: Any person, any application or software that use the open platform of computer can access the BackDisk and become a user when USBK is in "**Activate**" state.

How USBK protects your data

In general, the USBK – CryptoBridge includes two main areas of protection:

1. **Access to the USBK:** controlled by the authentication mechanisms with password to verify user. Password makes practically impossible for unauthorized people to access your USBK and consequently your data on BackDisk.
   For the password protection you are required to set a password on the first use.
   Also, to protect against brute force password attacks, after 3 consecutive incorrect password attempts, USBK securely erases all onboard data (your encryption key(s) and password)
2. **Protection of private data on BackDisk:** provided by encrypting the data using AES algorithm (FIPS PUB 197). USBK – CryptoBridge uses hardware-based encryption and entire file system is encrypted for advance security. All USBK models support the following AES key sizes: 128-bit and 256-bit. You are required to choose the key size, set encryption key(s) accordingly. Encrypted data stored on your BackDisk cannot be read (decrypted) without using correct encryption key(s).

System Requirements

USBK – CryptoBridge does not require installation of driver or software on HostSystem.

The following list describes the requirements of HostSystem and BackDisk that you need to use your USBK:

HostSystem

USB Port

- USB 1.1 or USB 2.0 (should be High Speed or Full Speed as Low Speed does not support MSD interface)

Operating Systems

- All operating systems that support FAT16 file system and have a text editor such a Notepad or any other
- Windows XP, 2000, Vista, 2007 (.NET 2.0 Framework dependent for windows GUI)
- Linux (Ubuntu 10.10 for Linux CLI)

! CAUTION: HostSystem should be protected against virus, trojan, malware or any type of network attacks which can compromise the security of data transfer between the HostSystem and USBK. Operational environment should also be trusted.

BackDisk

USB Port

- USB 1.1 or USB 2.0

MSD (Mass Storage Device)

- All kind of USB flash drives and USB external hard drives as registered as USB MSD having SCSI interface with a single LUN.

Getting started

Before You Begin

Before you use your USBK for the first time, it is important to understand how Windows maps the USBK to your computer and how the software on the USBK is run.

About Drive Mapping

The USBK is mapped to the host file system using two drive letters. These drive letters are assigned dynamically on a free letter basis.
One drive is labeled "**USBK**". It contains the software for Windows GUI and 'Text Menu' directory for operation of USBK via a text editor such a Notepad or any other.
The other Drive is labeled as "Removable Disk".

Before

- initializing your USBK at first time usage,
- user authentication at day to day usage,

the "Removable Disk" is inaccessible. When you try to access it, the following message displays, "insert a disk into drive E:" where E is for the drive letter associated with your BackDisk. After successful user authentication, it opens for read/write as your BackDisk.

Control Panel of USBK Management Software

USBK contains the USBK Management Software for Windows GUI. The "Control Panel" supplies you simple-to-use interface for USBK operations and settings.

See below the main page of USBK Management Software for Windows GUI and will be referred as Control Panel at the instructions hereafter.

Initializing with a USBK

Personalizing a USBK

You must personalize a new USBK the first time you use it as it is in Fabric Default. Personalizing USBK involves two main steps - setting your password and creating your encryption key(s).

You are automatically prompted to set new password at first usage. After this password setting, random encryption key(s) is assigned on your USBK. That's why, it is strongly recommended to set your encryption key(s).

To personalize a USBK

1. Plug the USBK into the USB port of the computer.
   When USBK is plugged in computer, the operating system recognizes automatically and the AutoRun window appears.

2. Select **Run USBK Management Software** and double-click.

NOTE: This screen may not appear if computer does not allow the devices to autorun. For this case; double-click on the **USBK disk** icon in **My Computer** and run **USBK.exe**.

To set your password

1. Type your password on dialog boxes **New Password** and **New Password Again**, and click **OK**.

   When you click **Cancel**, this Change Password window is closed without completing password setting and the Control Panel of USBK appears.

NOTE: Password should be minimum 4 characters long and not exceed 16 characters. It may contain three different types of characters: letters, numbers and special characters such as punctuation marks, etc..

NOTE: After new password setting, random encryption key(s) is generated by USBK and assigned on it. That's why, it is strongly recommended to set your encryption key(s).

To set your encryption key(s)

1. On the Control Panel of USBK, click **Encryption Keys** in **Settings**.

2. Select the key that you want to set from **Key** combobox. (Valid for A103 model. If you are using A101 model, pass directly to the next step).

NOTE: You can optionally type a name for your key in box **Key Name**. It is not mandatory nd see “Changing Key Name(s) on USBK” part of this guide for more info. Be sure that "Change Only Key Name" checkbox is not signed at this stage as it disables the generating AES key.

3. Select the key size from **Key Size** combobox.
4. Select key type **Text** or **Decimal**, enter your key to **AES Key** box accordingly and click **OK**.

NOTE: For 128-bit AES key size; encryption key in ‘Text’ type must be 16 characters long with letters, numbers and special characters such as punctuation marks, etc. Decimal is formed of 16 numeric digits between 0 and 255, each digit separated with a dot. You can follow up shown examples below **AES Key** box.

NOTE: For 256-bit AES key size; encryption key in ‘Text’ type must be 32 characters long with letters, numbers and special characters such as punctuation marks, etc. Decimal is formed of 32 numeric digits between 0 and 255, each digit separated with a dot. You can follow up shown examples below **AES Key** box.

NOTE: USBK can generate the encryption key(s) on behalf of user. If you wish that, click **Generate** button. Then, USBK generates a random encryption key and shows the generated key on **AES Key** box. ***It is just one time the key is showed you and will not be displayed again during daily usage of USBK.*** Therefore, memorize or store the generated key in a safe (For example; write it down in note to remember in future)

! CAUTION: After setting/changing your encryption key(s), write down encryption key(s) in note for future reference, but remember to keep it confidential. There’s no way to recover encryption key(s) as they are never exported or displayed during usage of USBK. A lost of encryption keys results in lost of data on BackDisk. Therefore, it is very important that you remember the encryption key(s) or store it in a safe place.

5. Type your password in appeared password window and click **OK**.
   If the password is correct, setting your encryption key(s) on USBK is done successfully. Bubble message on notification area indicates this setting as “Changed Successfully”.

Starting with your BackDisk

After you personalize your USBK, it is needed to format your BackDisk with your USBK.

NOTE: You must format your BackDisk when it is the first time use with your new encryption key(s).

! CAUTION: Formatting your BackDisk erases all data on it. Before formatting it, be sure to back up your files on it.

To start with your BackDisk

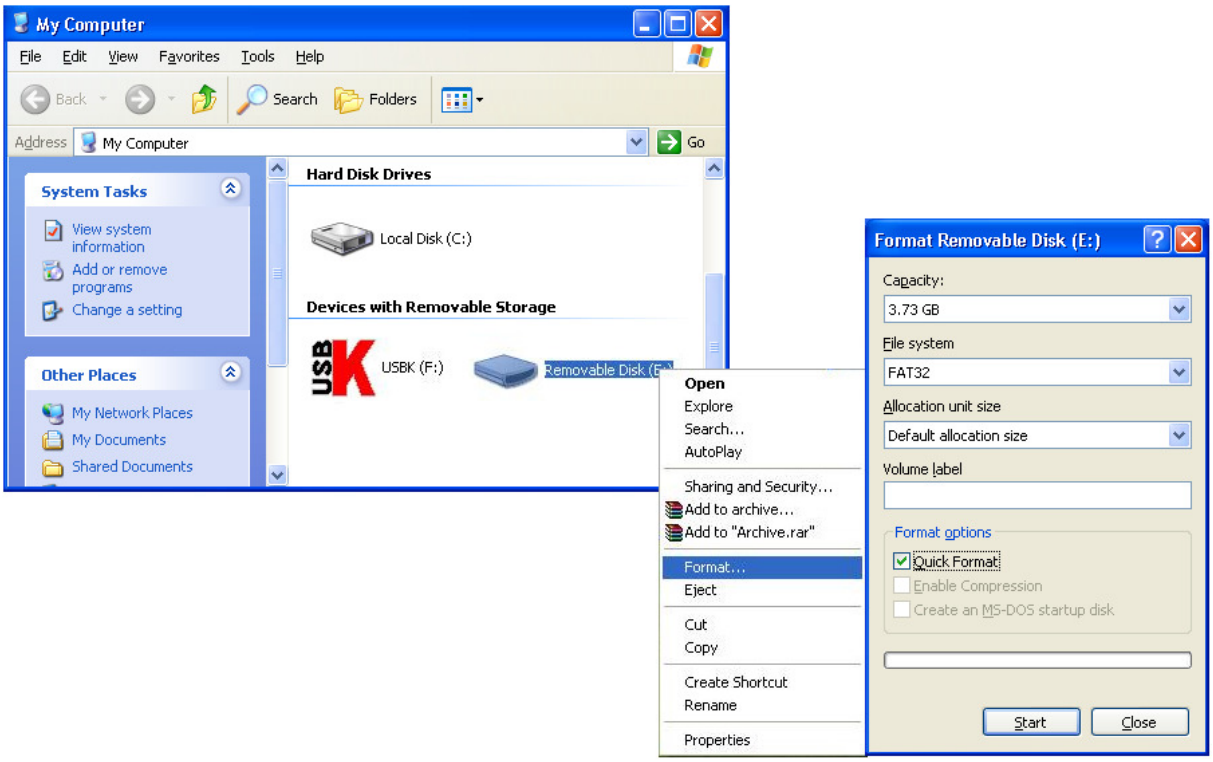
1. Plug your BackDisk port of your USBK.
2. Activate your USBK. To activate your USBK;
   2.1. On the Control Panel of USBK, click **Activate Key**.
   2.2. Select the key that you want to activate from **Key** combobox and click **Select**.(Valid for A103 model. If you are using A101 model, pass directly to the next step).
   2.3. Type your password in appeared password window and click **OK**.
   If the password is correct, activating your USBK is done successfully. Bubble message on notification area indicates this as “Activated”.

   Tip: You can also activate your USBK by right-clicking the USBK icon on the notification area and clicking **Activate Key.** And then, follow up the same instructions explained above starting from 2.2 Step.
3. Find **Removable Disk** in **My Computer**. When you double-click **Removable Disk**, the operating system recognizes it as unformatted.
4. Format it by using one of following methods:

1. Disk Formatting Method

1. Right-click on labeled **Removable Disk** in **My Computer**, select **Format**.
2. There is a checkbox for **Quick Format**. Check it and click **Start** button.

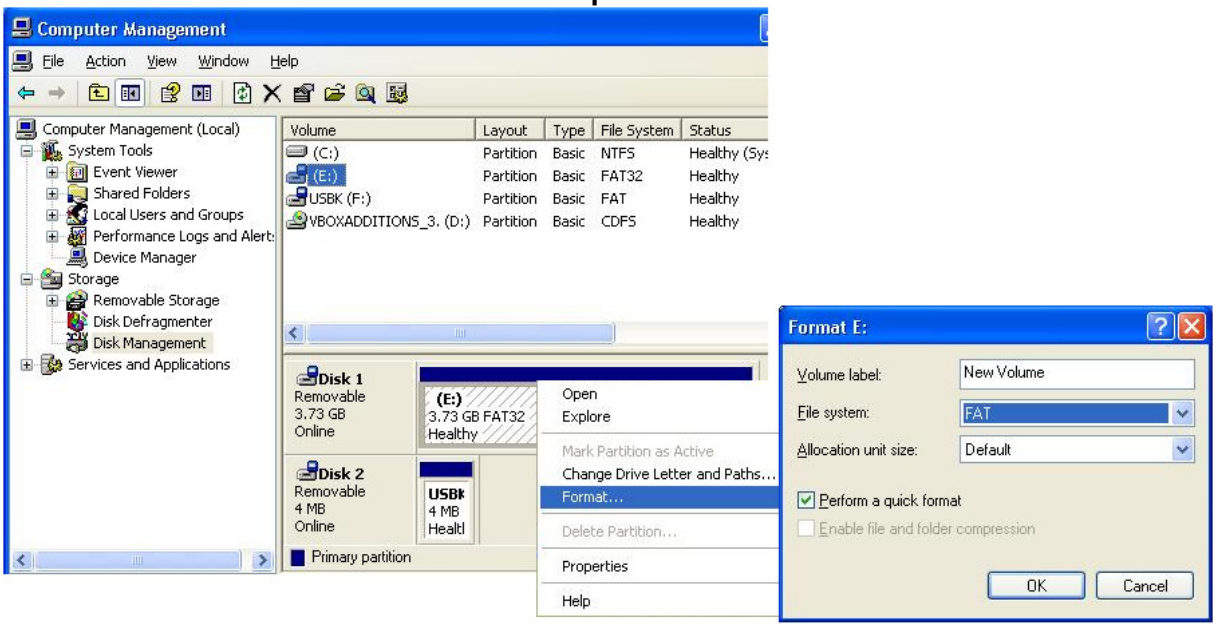
! CAUTION: If you are formatting a used BackDisk which contains data currently, Quick Format leaves file tracks on it. To clear all tracks from your Backdisk, not check the Quick Format option



NOTE: If the 1. disk format method is not successful in anyway, try 2. disk format method explained below.

2. Disk Formatting Method

1. Right-click on **My Computer**, select **Manage** and **Computer Management** window appears.
2. Click **Disk Management** in the left pane of **Computer Management** window.
3. Choose your removable disk, right-click it and select **Format**.
4. There is a checkbox for **Perform a quick format**. Check it and click **OK**.



At this point, you are ready to use your USBK and your BackDisk encryption key(AES key) activated here in this part of guide at step 2.2.

Day to Day Using of USBK

After you initialized your USBK, you can securely use your BackDisk together with USBK at any time.

Activate / Deactivate your USBK

Activate your USBK

Activate your USBK, before you use your BackDisk and access the information on it.

To activate your USBK

1. On the Control Panel of USBK, click **Activate Key**.
2. Select the key that you want to activate from **Key** combobox and click **Select**.(Valid for A103 model. If you are using A101 model, pass directly to the next step).
3. Type your password in appeared password window and click **OK**.
   If the password is correct, activating your USBK is done successfully. Bubble message on notification area indicates this as " Activated".

Tip: You can also activate your USBK by right-clicking the USBK icon on the notification area and clicking **Activate Key.** And then, follow up the same instructions explained above starting from 2. Step.

You can check the status of your USBK at on the Control Panel of USBK. It is represented as **Activate** in green.

Deactivate your USBK

Deactivate is tantamount to removing your BackDisk. It is equivalent in effect with removing your BackDisk although it is plugged-in your USBK.

Deactivate your USBK, before you

- leave your USBK plugged-on your computer,
- want to use 'Settings' menu
- activate another key(Valid for A103 model)

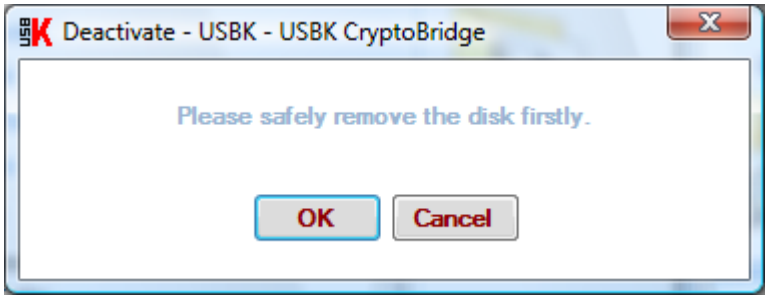
To deactivate your USBK

1. On the Control Panel of USBK, click **Deactivate Key**. Bubble message on notification area indicates this change as "Deactivated".

Tip: You can also deactivate your USBK by right-clicking the USBK icon on the notification area and clicking **Deactivate Key.**

You can check the status of your USBK at on the Control Panel of USBK. It is represented as **Deactivate** in red.

NOTE: If you deactivate your USBK before removing your BackDisk safely, a warning message displays, “Please safely remove the disk firstly” as below. Click **Cancel** and remove your BackDisk safely. For safely remove, right-click on your BackDisk and click **Eject.**



! CAUTION: Disconnecting the devices either accidentally or on purpose, without using the safely remove hardware operation, could corrupt the data on the devices.

NOTE: If you try to access your BackDisk when the status of your USBK is **Deactivate**, the following message displays, “insert a disk into drive E:” where E is for the drive letter associated with your BackDisk.

Usage of BackDisk

Once you activate your USBK, you can save files to your BackDisk same as regular usage of ordinary USB sticks. USBK encrypts data transferred to/from your BackDisk using the AES algorithm (FIPS PUB 197). Data is automatically decrypted when you open the file.

Data can be copied to/from a mounted BackDisk at back of USBK just like they are copied to/from any normal USB drive (for example, by simple drag-and-drop operations or right click send etc.)

NOTE: To access to your BackDisk, the status of your USBK must be “**Activate**”. If it is “**Deactivate**” and you try to access your BackDisk, the following message displays, “insert a disk into drive H:” where H is sample for the drive letter associated with your BackDisk.

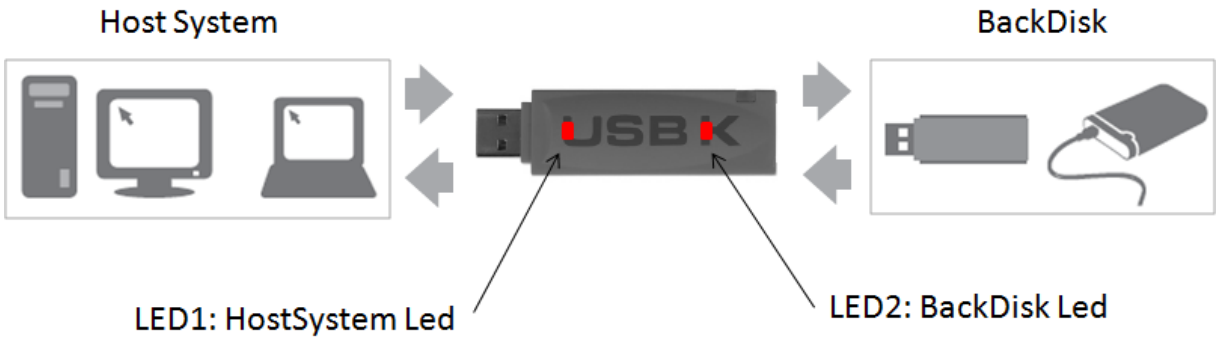
! CAUTION: Any person, any application or software that use the open platform of computer can access the BackDisk and become a user when USBK is in “**Activate**” state

! CAUTION: If you leave your USBK plugged-on your computer in “**Activate**” state, any user can access your data on your BackDisk while you are away from the computer.

Understanding USBK status via LEDs

USBK has two LEDs in red color for indicating its operational status.

The positions of LEDs are as following figure and states are explained in Table 1- Led Status of USBK.



LED1: HostSystem Led	LED2: BackDisk Led	Description
ON	ON	USBK in error
OFF	OFF	USBK is ready (deactivated)
ON	OFF	-
OFF	ON	-
Blink	OFF	USBK is activated w/o BackDisk
OFF	Reverse Blink	
Blink	Reverse Blink	USBK is activated with BackDisk
Twinkle	Blink	Indicates a data transfer activity, writing to BackDisk with encryption
Blink	Twinkle	Reading from BackDisk with decryption

Table 1 - Led Status of USBK

Managing User Authentication

You can authenticate to your USBK using a password.

Password should be minimum 4 characters long and not exceed 16 characters. It may contain three different types of characters: letters, numbers and special characters such as punctuation marks, etc.

Changing your password

You can change your password in any time.

NOTE: To change your password, the status of device must be "**Deactivate**". You can check the status of your device on the Control Panel of USBK. If the status is **Activate** in green, click **Deactivate Key** button. **Settings** menu will be enabled and get color in red.

To change your password

1. On the Control Panel of USBK, under **Settings**, click **Password**.
2. Type your password on dialog boxes **New Password** and **New Password Again**, and click **OK**.

3. Type your old password in appeared password window and click **OK**.

If the password is correct, changing your password is done successfully. Bubble message on notification area indicates this as "Changed Successfully".

Tip: You can also change your password by right-clicking the USBK icon on the notification area, then dragging your mouse on to **Settings** and clicking **Password**. Then, follow up the same instructions explained above starting from 2. Step.

Forgetting your password

There is no support on USBK for forgotten password.

If you forget your password, you can set a new password by taking your USBK to Fabric Default. After 3 wrong password attempts, USBK erases all your encryption key(s) and password, returns back to Fabric Default. You are forced to set new password same as at first usage.

! CAUTION: After this password setting, random encryption key(s) is assigned on your USBK. That's why; set your encryption key(s) same with old(s) in order to access data on your BackDisk and prevent data lost.

Auto-Activation Property

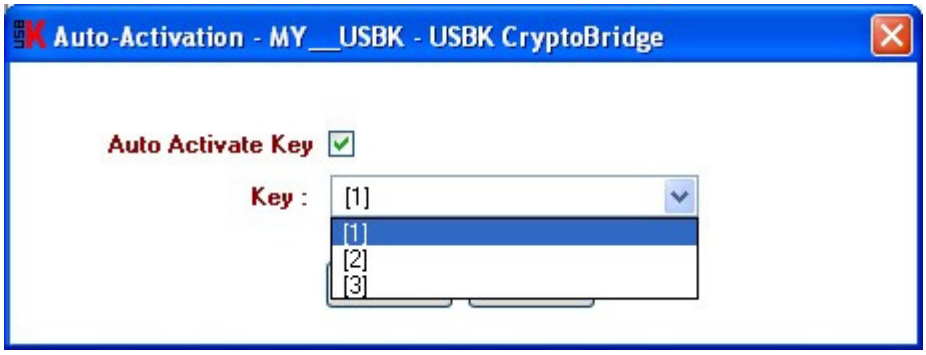
With Auto-Activation property, you configure your USBK to automatically start when you plug it in a HostSystem. So, you can use your USBK on hostsytems which do not have any user interface for password entry.

When Auto-Activation is enabled, USBK does not ask for password confirmation to verify user. Thence, it can be used directly on test & measurement equipments such as oscilloscope, EKG, etc.

NOTE: To enable Auto-Activation, the status of device must be "**Deactivate**". You can check the status of your device on the Control Panel of USBK. If the status is **Activate** in green, click **Deactivate Key** button. **Settings** menu will be enabled and get color in red.

To enable Auto-Activation

1. On the Control Panel of USBK, under **Settings**, click **Auto-Activation**.
2. Check the **Auto Activation Key** checkbox.
3. Select the key that you want to auto-activate from **Key** combobox.(Valid for A103 model. If you are using A101 model, pass directly to the next step).



4. Click **OK**.
5. Type your password in appeared password window and click **OK**.
   If the password is correct, auto-activation of your USBK is done successfully. Bubble message on notification area indicates this as " Auto-Activation Enabled".

Tip: You can also enable Auto-Activation of your USBK by right-clicking the USBK icon on the notification area, then dragging your mouse on to **Settings** and clicking **Auto-Activation**. Then, follow up the same instructions explained above starting from 2. Step.

! CAUTION: If you carry and lose your BackDisk plugged-on your USBK in "Auto-Activation Enabled", any user can access your data on your BackDisk when he plug in the computer as no password is asked to verify user. Just carry only your USBK when "Auto-Activation Enabled" for the security of data on your BackDisk.

To disable Auto-Activation

1. On the Control Panel of USBK, under **Settings**, click **Auto-Activation**.
2. Remove the sign in **Auto Activation Key** checkbox, click **OK**.
3. Type your password in appeared password window and click **OK**.
   If the password is correct, disable of auto-activation property is done successfully. Bubble message on notification area indicates this as " Auto-Activation Disabled".

Tip: You can also disable Auto-Activation property of your USBK by right-clicking the USBK icon on the notification area, then dragging your mouse on to **Settings** and clicking **Auto-Activation**. Then, follow up the same instructions explained above starting from 2. Step.

Managing USBK(s)

Recycling a USBK

Recycling a USBK removes all user private data such as encryption key(s) and password from the device and returns it to the Fabric Default. You must personalize the device after you recycle it. For more information, see “Personalizing a USBK” part of this guide.

To Recycle a USBK

1. Reach the maximum number of failed password attempts. After 3 consecutive invalid password attempts, your USBK will self-destruct and return to the Fabric Default.

Changing Device (USBK) Name

You can optionally change USBK name to identify your device. For example, you can type your name or company name in “Device Label” to make it distinctive.

Additionally, the “Device Label” as nickname helps you distinguish between different USBK devices since you can have multiple USBKs.

NOTE: To change your device (USBK) name, the status of device must be “**Deactivate**”. You can check the status of your device on the Control Panel of USBK. If the status is **Activate** in green, click **Deactivate Key** button. **Settings** menu will be enabled and get color in red.

To change device name

1. On the Control Panel of USBK, under **Settings**, click **Device Label**.
2. Type a name in **Device Label** window and click **OK**.
3. Type your password in appeared password window and click **OK**. If the password is correct, “REMOVE AND RE-PLUG THE USBK” message window appears as below. Click **OK**.

All buttons on the Control Panel of USBK “Control Panel” are disabled in gray color and the status is “**Force Remove**”. Additionally, bubble message on notification area indicates this status as “Force Remove”.

4. Un-plug your device(USBK)
5. When you plug it, you see your device with new name instead of USBK as default name. New name is also indicated at **Device** on the Control Panel of USBK.

Changing Key Name(s) on USBK

You can optionally change Key Name(s) on USBK for easy usage. Key name(s) is represented with number(s) by default.

NOTE: To change your device(USBK) name, the status of device must be "**Deactivate**". You can check the status of your device on the Control Panel of USBK. If the status is **Activate** in green, click **Deactivate Key** button. **Settings** menu will be enabled and get color in red.

To change key name

1. On the Control Panel of USBK, under **Settings**, click **Encryption Keys**.
2. Select the key that you want to name from **Key** combobox.(Valid for A103 model. If you are using A101 model, pass to the next step)
3. Type a name in **Key Name** box, sign **Change Only Key Name** checkbox and click **OK**.

4. Type your password in appeared password window and click **OK**.
   If the password is correct, changing key name is done successfully. Bubble message on notification area indicates this setting as "Changed Successfully".

Viewing device information

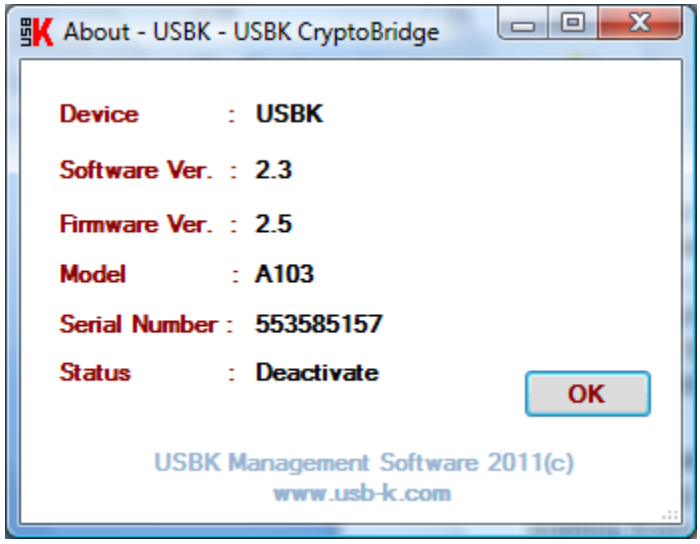
You can view information about your USBK on the Control Panel of USBK.

All information is viewed in following categories:

- **Device:** The name of your device. USBK is fabric default name and viewed with the new name after you change the device label.
- **Software ver:** Software version associated with your USBK
- **Firmware ver:** Firmware version associated with your USBK

- **Model:** Model of your USBK
- **Serial Number:** Serial Number of your USBK. This is a unique number for each USBK.

Tip: You can also view device information by right-clicking the USBK icon on the notification area and clicking **About**.



Using USBK on Linux

Linux CLI will allow you to use your USBK, if you prefer to use on a Linux computer.

Getting started for Linux

The CLI software exists for managing USBKs in Linux Operation Systems. This software provides some services for Linux such as listing, configuring and controlling USBK plugged to host system. Before you use Linux CLI software for the first time, it is important to know where this software is obtained and how the software is installed on host system and then run.

Linux CLI software is open source project. The newest version of software can be downloaded from our web site www.usb-k.com on pages Support => Downloads. The installation packages of some Linux distributions are available in this web site.

NOTE: "$" is normal user and "#" is user who has all super user privileges.

NOTE: USBK has two LEDs for indicating its operational status. The states of these LEDs are explained herein this guide at Table-1 Led Status of USBK on page 21.

Installing Linux CLI Software

Please be sure you have installed GCC compiler tool before installation. You should download from our website www.usb-k.com on pages Support => Downloads. You should enter project directory and below command should be executed in command line to configure, build and install for your Linux system:

```
$ wget http://www.usb-k.com/files/files/usbk_driver/usbk-1.1.tar.gz

$ tar xzf usbk-1.1.tar.gz

$ cd usbk-1.1/

$ ./configure

$ make

$ sudo make install
```

Moreover, .deb package for debian which is installer package can be downloaded from our website www.usb-k.com. To install USBK Linux CLI Software to your Linux System, below commands should be executed in command line:

For debian

```
# dpkg -i usbk-x.x.x.deb
```

Using USBK Linux CLI Software

After installed, you should confirm the successful installation by version checking. The below command is executed for showing the version of installed USBK Linux CLI Software.

```
$ usbk -v
```

If this command is executed successfully, the software is installed and works fine.

Initializing with a USBK

Personalizing a USBK

You must personalize a new USBK the first time you use it as it is in Fabric Default. Personalizing USBK involves two main steps - setting your password and creating your encryption key(s). Before these, you will need to find device name of USBK plugged on your host system.

To find device name

In this step, all USBKs plugged to host system are listed and some information of USBKs is given as device label, device name, BackDisk device name, product name, model, serial number and firmware version. Moreover, the information whether the installed software supports the USBK or not is shown in response of this command.

The command to list all USBKs in your host system is below:

```
# usbk -s
```

The device name can be learn for specific USBK by matching device label, product name, model, serial number and firmware version.

To show more detail information about specific USBK

After finding the device name, you can get more detail information about this USBK such as device label, BackDisk device name, product name, model, serial number, firmware version, USBK label, status, retry number, existence of BackDisk, auto-activation setting and name of key(s).

To get more detail information about USBK, below command should be executed in command line:

```
# usbk -u DEVICENAME -i
```

To personalize your USBK

At first usage, the status of USBK is “Fabric Default”. In this status USBK has no password and no encryption key(s). Firstly, you must set your own password and encryption key(s) to personalize your USBK.

To set your password

Below command is used to set password to USBK in Fabric Default:

```
# usbk -u DEVICENAME -c PASSWORD
```

NOTE: Password must be minimum 4 characters long and not exceed 16 characters. It may contain three different types of characters: letters, numbers and special characters such as punctuation marks, etc.

NOTE: After new password setting, random encryption key(s) is generated by USBK and assigned on it. That's why, it is strongly recommended to set your encryption key(s).

To set your encryption key(s)

After setting your password, the status of USBK is "Deactive" status. Now, you should set encryption key(s). To set encryption key and key name for a key of USBK, below command should be used:

```
#usbk -u DEVICENAME -p PASSWORD -k KEYNO -m KEYNAME -f KEYFORMAT -F
KEYSIZE -x NEWKEY
```

NOTE: The "-F" parameter related to AES key size should be either "128" or "256".

NOTE: For 128-bit AES key size; encryption key in 'Text' type must be 16 characters long with letters, numbers and special characters such as punctuation marks, etc. Decimal is formed of 16 numeric digits between 0 and 255, each digit separated with a dot. You can follow up shown examples below **AES Key** box.

NOTE: For 256-bit AES key size; encryption key in 'Text' type must be 32 characters long with letters, numbers and special characters such as punctuation marks, etc. Decimal is formed of 32 numeric digits between 0 and 255, each digit separated with a dot.

NOTE: USBK can generate and set random encryption key automatically in decimal format. Below command should be used to set random encryption key:

```
#usbk -u DEVICENAME -p PASSWOD -k KEYNO -m KEYNAME -F KEYSIZE -X
```

NOTE: The random encryption key is generated and set and then the Linux CLI software shows this encryption key to you. Please note this encryption key down in note to remember in future

NOTE: The "-F" parameter related to AES key size should be either "128" or "256".

! CAUTION: After setting/changing your encryption key(s), write down encryption key(s) in note for future reference, but remember to keep it confidential. There's no way to recover encryption key(s) as they are never exported or displayed during usage of USBK. A lost of encryption keys results in lost of data on BackDisk. Therefore, it is very important that you remember the encryption key(s) or store it in a safe place.

Starting with your BackDisk

After you personalize your USBK, it is needed to format your BackDisk with your USBK since the host system senses this BackDisk as unformated disk.

NOTE: You must format your BackDisk when it is the first time use with your new encryption key(s).

! CAUTION: Formatting your BackDisk erases all data on it. Before formatting it, be sure to back up your files on it.

To start with your BackDisk

1. Plug your BackDisk port of your USBK.
2. Activate your USBK.

```
#usbk -u DEVICENAME -p PASSWOD -a -k KEYNO
```

NOTE: if you execute the command to get more detail information, you will see the status of USBK as activate [#EK].

3. After activation, the BackDisk should be formatted by disc tools of Linux and then the you use BackDisk securely.

Day to Day Using of USBK

After you initialized your USBK, you can securely use your BackDisk together with USBK at any time.

Activate / Deactivate your USBK

Activate your USBK

Activate your USBK, before you use your BackDisk and access the information on it.

For data transfer in ecryption/decryption form between BackDisk and Host System, the USBK should be activated with a specific encryption key. To activate your USBK;

```
#usbk -u DEVICENAME -p PASSWOD -a -k KEYNO
```

NOTE: if you execute the command to get more detail information, you will see the status of USBK as activate [#EK].

Deactivate your USBK

Deactivate is tantamount to removing your BackDisk. It is equivalent in effect with removing your BackDisk although it is plugged-in your USBK.

Deactivate your USBK, before you

- leave your USBK plugged-on your computer,
- want to set some settings
- activate USBK with another key(Valid for A103 model)

To deactivate your USBK:

```
#usbk -u DEVICENAME -d
```

NOTE: if you execute the command to get more detail information, you will see the status of USBK as deactivate.

! CAUTION: Before deactivating USBK, you must be sure that the disks of BackDisk are unmount ; otherwise deactivation without unmounting could corrupt the data on the devices.

Usage of BackDisk

Once you activate your USBK, you can save files to your BackDisk same as regular usage of ordinary USB sticks. USBK encrypts data transferred to/from your BackDisk using the AES algorithm (FIPS PUB 197). Data is automatically decrypted when you open the file.

Data can be copied to/from a mounted BackDisk at back of USBK just like they are copied to/from any normal USB drive.

NOTE: To access to your BackDisk, the status of your USBK must be "**Activate**". If it is "**Deactivate**" and you can not access your BackDisk.

! CAUTION: Any person, any application or software that use the open platform of computer can access the BackDisk and become a user when USBK is in "**Activate**" state

! CAUTION: If you leave your USBK plugged-on your computer in "**Activate**" state, any user can access your data on your BackDisk while you are away from the computer.

Changing your password

You can change your password in any time when the status of USBK is "**Deactivate**"

To change your password

Below command is used to change password:

```
# usbk -u DEVICENAME -p PASSWORD -c NEWPASSWORD
```

NOTE: Password should be minimum 4 characters long and not exceed 16 characters. It may contain three different types of characters: letters, numbers and special characters such as punctuation marks, etc

Forgetting your password

The instructions are same as expressed herein this user guide in 'Forgetting your password' section on pages 23 with taking in care the cautions therein.

Auto-Activation Property

With Auto-Activation property, you configure your USBK to automatically start when you plug it in a HostSystem. So, you can use your USBK on HostSytems which do not have any user interface for password entry.

When Auto-Activation is enabled, USBK does not ask for password confirmation to verify user. Thence, it can be used directly on test & measurement equipments such as oscilloscope, EKG, etc.

NOTE: To enable Auto-Activation, the status of device must be "**Deactivate**". If the status is **Activate** , you must deactive USBK for changing Auto-Activation setting.

To enable Auto-Activation

Below command is used to enable Auto-Activation

```
# usbk -u DEVICENAME -p PASSWOD -k KEYNO -t
```

! CAUTION: If you carry and lose your BackDisk plugged-on your USBK in "Auto-Activation Enabled", any user can access your data on your BackDisk when he plug in the computer as no password is asked to verify user. Just carry only your USBK when "Auto-Activation Enabled" for the security of data on your BackDisk.

To disable Auto-Activation

Below command is used to disable Auto-Activation

```
# usbk -u DEVICENAME -p PASSWOD -T
```

Changing Device (USBK) Label

You can optionally change USBK label to identify your device. For example, you can type your name or company name in "Device Label" to make it distinctive.

Additionally, the "Device Label" as nickname helps you distinguish between different USBK devices since you can have multiple USBKs.

NOTE: To change your device (USBK) label, the status of device must be "**Deactivate**". If the status is **Activate**, you have to deactive USBK for changing Device Label.

To change device label

Below command is used to change device label:

```
# usbk -u DEVICENAME -p PASSWOD -n DEVICELABEL
```

After changing device label, the status of USBK is "**Force Remove**". In this status, You can not do any setting. You must unplug USBK from Host system and then re-plug for appying this change and doing any settings.

Changing Only Key Name(s) on USBK

You can optionally change Key Name(s) on USBK for easy usage. Key name(s) is represented with number(s) by default.

NOTE: To change key name, the status of device must be "**Deactivate**". If the status is **Activate**, you must deactive USBK for changing Key Name.

To change key name

Below command is used to change key name:

```
#usbk -u DEVICENAME -p PASSWORD -k KEYNO -m KEYNAME
```

To obtain more information about USBK Linux CLI software

To get help about the parameters of USBK CLI software, from command line you can use the help parameter in below form:

```
#usbk -h
```

Moreover, if you want to obtain more detail information about USBK CLI software, the manual page of USBK CLI including more detail about parameters and some explanation related to usage of these parameters. Below command is used to show manual page of USBK CLI in command line:

```
$man usbk
```

Using USBK with Text Editor

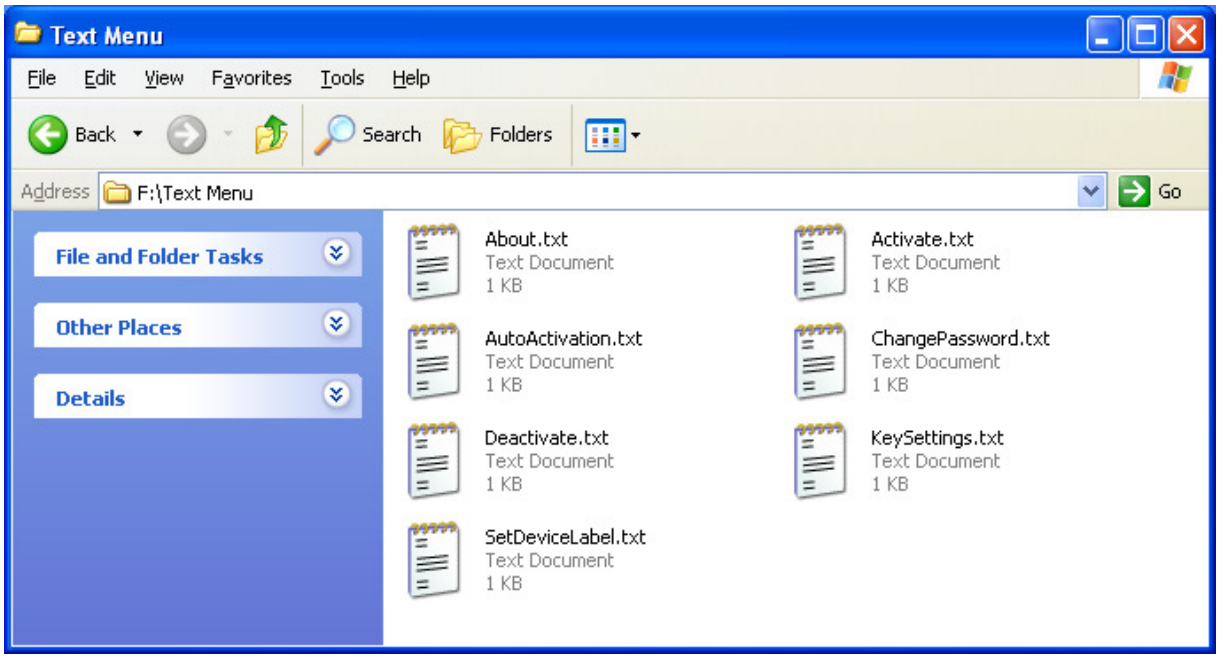
You can use your USBK in any operating systems that have a text editor such a Notepad or any other. It contains 'Text Menu' directory for operation of USBK via a text editor.

To use your USBK with Text Editor

Double-click on the **USBK disk** icon in **My Computer** and use the files in **Text Menu**

Text Menu directory contains the following files for operation of USBK.

- Activate.txt
- AutoActivation.txt
- ChangePassword.txt
- Deactivate.txt
- KeySettings.txt
- SetDeviceLabel.txt



Due to the characteristics of Text Menu, it cannot enforce the user for a proper scenario. That's why; it is important to understand the modes (states) of USBK expressed on page 8 in this guide and follow it up via LEDs.

The following table indicates each file (command) and indicates the states (modes) of USBK on which these files (commands) can be applied.

State (mode) of USBK	File (Command)
Fabric Default (Initial State)	• ChangePassword.txt
Deactivate State	• Activate.txt • AutoActivation.txt • ChangePassword.txt • KeySettings.txt

	• SetDeviceLabel.txt
Activate State:	• Deactivate.txt

Text Menu directory contains the 'About.txt' for viewing device information. User can use this file in any time.

Open the related txt. file to set function. Each .txt file contains examples for what to do. Follow up the examples, set your instructions and save the file in order to use your USBK accordingly.

! CAUTION: The operating system uses cache to serve faster for future requests. Your security data such as password and encryption keys can be read from a cache after your data entry. In order to clean the cache, clear your entry and save it again. So, any security object that resides in the cache is considered as expired.

Getting Started

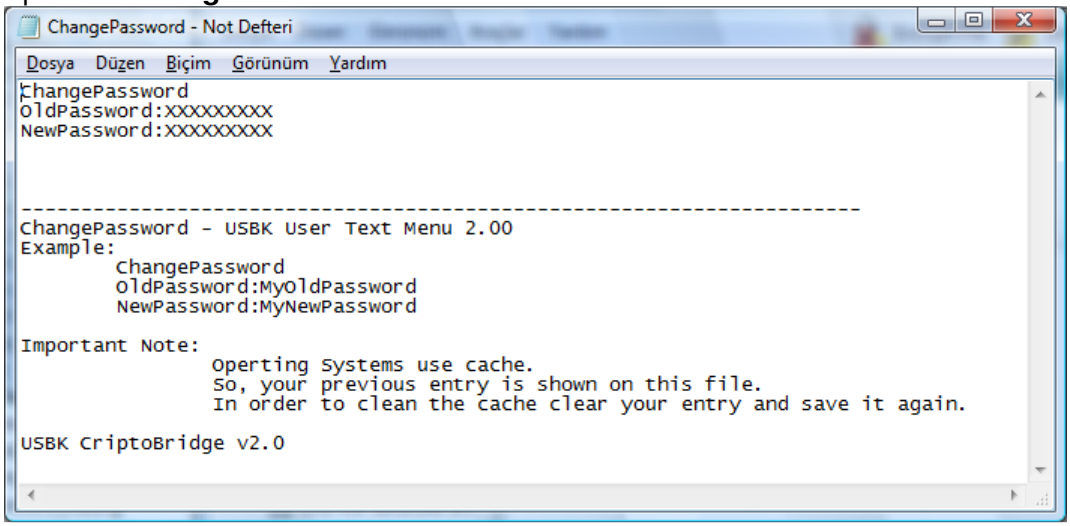
Personalizing a USBK

You must personalize a new USBK the first time you use it as it is in Fabric Default. Personalizing USBK involves two main steps - setting your password and creating your encryption key(s).

After this password setting, random encryption key(s) is assigned on your USBK. That's why, it is strongly recommended to set your encryption key(s).

To set your password

1. Double-click on the **USBK disk** icon in **My Computer** and use the files in **Text Menu**
2. Open the **ChangePassword.txt** file



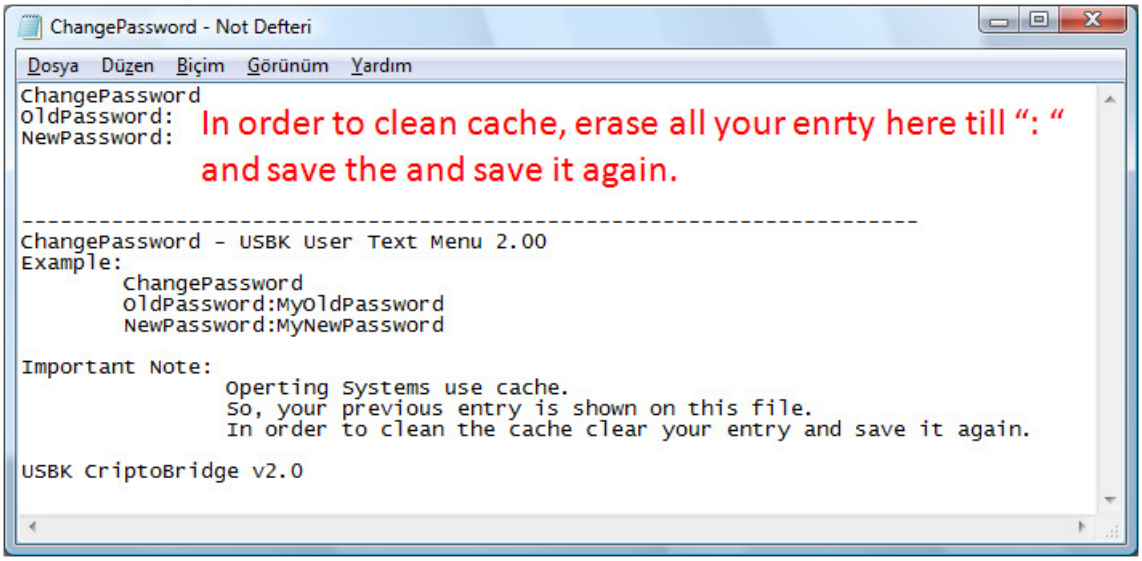
3. Erase all '**xxx**' letters till '**:**' and type your password near **OldPassword:**
4. Erase all '**xxx**' letters till '**:**' and type your password near **NewPassword:** again.
5. Save the file in order to execute these changes.
   If all your entry is valid, setting on USBK is done successfully. You can follow it up via LEDs. The LEDs indicates as follows when setting is done successfully.

LED1: HostSystem Led	LED2:BackDisk Led
Blink	OFF

If any of your entry is wrong, the LEDs indicate as follows:

LED1: HostSystem Led	LED2:BackDisk Led
Blink twice	OFF

! CAUTION: The operating system uses cache to serve faster for future requests. Your password can be read from a cache after your data entry. In order to clean the cache, erase your entry (erase till ':' in keeping the 'OldPassword:' and 'NewPassword:' titles) and save it again. So, any security object that resides in the cache is considered as expired.



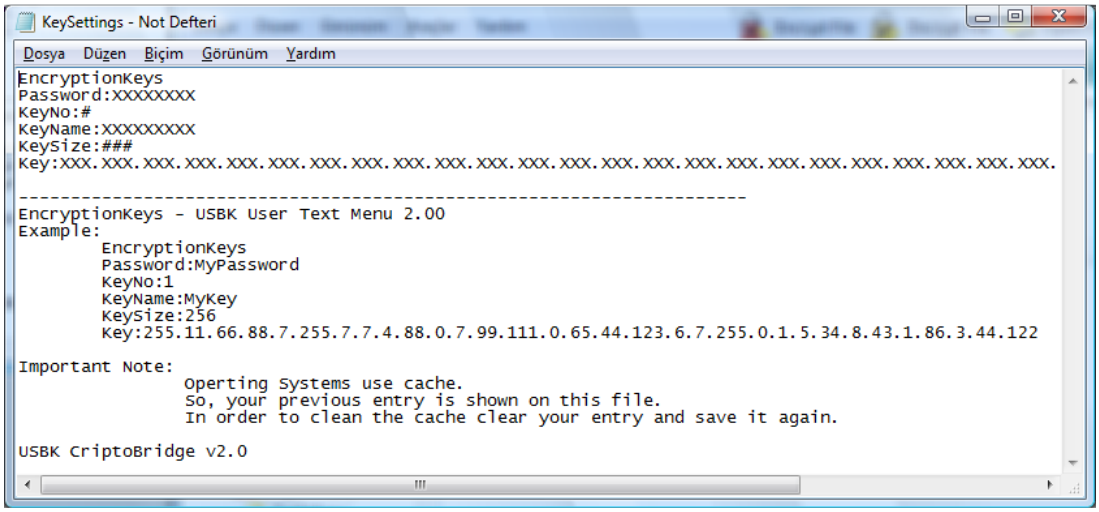
NOTE: Password should be minimum 4 characters long and not exceed 16 characters. It may contain three different types of characters: letters, numbers and special characters such as punctuation marks, etc..

NOTE: After new password setting, random encryption key(s) is generated by USBK and assigned on it. That's why, it is strongly recommended to set your encryption key(s).

NOTE: Each file contains related example. You can follow up shown example below broken line.

To set your encryption key(s)

1. Double-click on the **USBK disk** icon in **My Computer** and use the files in **Text Menu**
2. Open the **KeySettings.txt** file



3. Erase all '**xxx**' letters till '**:**' and type your password near **Password:**
4. Erase '**#**' letters till '**:**' and type the key number that you would like to set near **KeyNo:**. The KeyNo is 1 for A101 models and can be either 1 or 2 or 3 for A103 models.
5. Erase all '**xxx**' letters till '**:**' and type a name for your key near **KeyName:** Key name is not mandatory; you can optionally type a name for your key.
6. Erase '**###**' letters till '**:**' and type the key size that you would like to set near **KeySize:**. The KeySize can be either 128 or 256 refer to 128-bit AES and 256-bit AES.
7. Erase all '**xxx.xxx**' letters till '**:**' and type your encryption key near **Key:** in decimal format. Decimal is formed of numeric digits between 0 and 255 and also each digit separated with a dot. Key is formed of 16 numeric digits for 128-bit AES key size and 32 digits for 256-bit AES.
8. Save the file in order to execute these changes.
   If all your entry is valid, setting on USBK is done successfully. You can follow it up via LEDs. The LEDs indicates as follows when setting is done successfully.

LED1: HostSystem Led	LED2:BackDisk Led
Blink	OFF

If any of your entry is wrong, the LEDs indicate as follows:

LED1: HostSystem Led	LED2:BackDisk Led
Blink twice	OFF

! CAUTION: The operating system uses cache to serve faster for future requests. Your security data such as password and encryption keys can be read from a cache after your data entry. In order to clean the cache, erase your all entries erase till ':' in keeping the titles and save it again. So, any security object that resides in the cache is considered as expired.

! CAUTION: After setting/changing your encryption key(s), write down encryption key(s) in note for future reference, but remember to keep it confidential. There's no way to recover encryption key(s) as they are never exported or displayed during usage of USBK. A lost of encryption keys results in lost of data on BackDisk. Therefore, it is very important that you remember the encryption key(s) or store it in a safe place.

NOTE: Each file contains related example. You can follow up shown example below broken line.

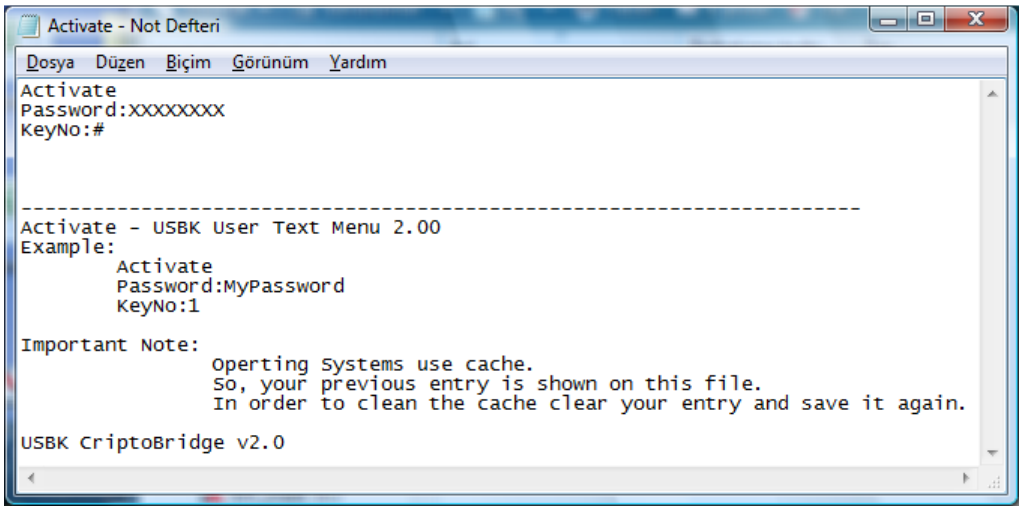
Starting with your BackDisk

After you personalize your USBK, it is needed to format your BackDisk with your USBK.

! CAUTION: Formatting your BackDisk erases all data on it. Before formatting it, be sure to back up your files on it.

To start with your BackDisk

1. Plug your BackDisk port of your USBK.
2. Activate your USBK. To activate your USBK;
   2.1. Double-click on the **USBK disk** icon in **My Computer** and use the files in **Text Menu**
   2.2. Open the **Activate.txt** file



   2.3. Erase all '**xxx**' letters till '**:**' and type your password near **Password:**
   2.4. Erase '**#**' letters till '**:**' and type the key number that that you want to activate near **KeyNo:**. The KeyNo is 1 for A101 models and can be either 1 or 2 or 3 for A103 models.
   2.5. Save the file in order to execute these changes.
   If all your entry is valid, activating your USBK is done successfully. You can follow it up via LEDs. The LEDs indicates as follows when activating is done successfully and when your USBK is in Activate State.

LED1: HostSystem Led	LED2:BackDisk Led
Blink	Reverse Blink

If any of your entry is wrong, the LEDs indicate as follows:

LED1: HostSystem Led	LED2:BackDisk Led
Blink twice	OFF

3. Find **Removable Disk** in **My Computer**. When you double-click **Removable Disk**, the operating system recognizes it as unformatted.
4. Format it by using one of the formatting method expressed herein this user guide on pages 17-18 with taking in care the cautions and notes therein.

! CAUTION: The operating system uses cache to serve faster for future requests. Your password can be read from a cache after your data entry. In order to clean the cache, erase your all entries erase till ':' in keeping the titles and save it again. So, any security object that resides in the cache is considered as expired.

NOTE: Each file contains related example. You can follow up shown example below broken line.

NOTE: You must format your BackDisk when it is the first time use with your new encryption key(s).

Day to Day Using of USBK

After you initialized your USBK, you can securely use your BackDisk together with USBK at any time.

Activate / Deactivate your USBK

Activate your USBK

Activate your USBK, before you use your BackDisk and access the information on it.

To activate your USBK

1. Double-click on the **USBK disk** icon in **My Computer** and use the files in **Text Menu**
2. Open the **Activate.txt** file
3. Erase all '**xxx**' letters till '**:**' and type your password near **Password:**
4. Erase '**#**' letters till '**:**' and type the key number that that you want to activate near **KeyNo:**. The KeyNo is 1 for A101 models and can be either 1 or 2 or 3 for A103 models.
5. Save the file in order to execute these changes.

   If all your entry is valid, activating your USBK is done successfully. You can follow it up via LEDs. The LEDs indicates as follows when activating is done successfully.

LED1: HostSystem Led	LED2:BackDisk Led
Blink	Reverse Blink

If any of your entry is wrong, the LEDs indicate as follows:

LED1: HostSystem Led	LED2:BackDisk Led
Blink twice	OFF

! CAUTION: The operating system uses cache to serve faster for future requests. Your password can be read from a cache after your data entry. In order to clean the cache, erase your all entries erase till ':' in keeping the titles and save it again. So, any security object that resides in the cache is considered as expired.

NOTE: Each file contains related example. You can follow up shown example below broken line.

You can check the status of your USBK via LEDs in any time. The LEDs indicates as below table when your USBK is in Activate State.

LED1: HostSystem Led	LED2: BackDisk Led	Description
Blink	Reverse Blink	USBK is activated with BackDisk(plugged BackDisk)
Blink	OFF	USBK is activated w/o BackDisk (un-plugged BackDisk)

Usage of BackDisk

Once you activate your USBK, you can save files to your BackDisk same as regular usage of ordinary USB sticks. USBK encrypts data transferred to/from your BackDisk using the AES algorithm (FIPS PUB 197). Data is automatically decrypted when you open the file.

Data can be copied to/from a mounted BackDisk at back of USBK just like they are copied to/from any normal USB drive (for example, by simple drag-and-drop operations or right click send etc.)

NOTE: To access to your BackDisk, your USBK must be in "**Activate** State". If you try to access your BackDisk when it is in "**Deactivate** State" and, the following message displays, "insert a disk into drive H:" where H is sample for the drive letter associated with your BackDisk.

! CAUTION: Any person, any application or software that use the open platform of computer can access the BackDisk and become a user when USBK is in "**Activate** State".

! CAUTION: If you leave your USBK plugged-on your computer in in "**Activate** State", any user can access your data on your BackDisk while you are away from the computer.

Deactivate your USBK

Deactivate is tantamount to removing your BackDisk. It is equivalent in effect with removing your BackDisk although it is plugged-in your USBK.

Deactivate your USBK, before you

- leave your USBK plugged-on your computer,
- want to make settings using the files 'AutoActivation.txt', 'ChangePassword.txt', 'KeySettings.txt' and 'SetDeviceLabel.txt'
- activate another key(Valid for A103 model)

To deactivate your USBK

1. Double-click on the **USBK disk** icon in **My Computer** and use the files in **Text Menu**
2. Open the **Deactivate.txt** file
3. Save the file in order to deactivate your USBK.
   You can follow it up via LEDs. The LEDs indicates as below table when your USBK is in Deactivate State.

LED1: HostSystem Led	LED2:BackDisk Led
OFF	OFF

Changing your password

You can change your password in any time.

NOTE: To change your password, your USBK must be in "**Deactivate** State". You can check it via LEDs.

To change your password

1. Double-click on the **USBK disk** icon in **My Computer** and use the files in **Text Menu**
2. Open the **ChangePassword.txt** file
3. Erase all '**xxx**' letters till '**:**' and type your current password near **OldPassword:**
4. Erase all '**xxx**' letters till '**:**' and type your new password near **NewPassword:**.
5. Save the file in order to execute these changes.
   If all your entry is valid, setting on USBK is done successfully. You can follow it up via LEDs. The LEDs indicates as follows when setting is done successfully.

LED1: HostSystem Led	LED2:BackDisk Led
Blink	OFF

If any of your entry is wrong, the LEDs indicate as follows:

LED1: HostSystem Led	LED2:BackDisk Led
Blink twice	OFF

! **CAUTION:** The operating system uses cache to serve faster for future requests. Your new password can be read from a cache after your data entry. In order to clean the cache, erase your entry (erase till ':' in keeping the 'OldPassword:' and 'NewPassword:' titles) and save it again. So, any security object that resides in the cache is considered as expired.

NOTE: Password should be minimum 4 characters long and not exceed 16 characters. It may contain three different types of characters: letters, numbers and special characters such as punctuation marks, etc..

NOTE: Each file contains related example. You can follow up shown example below broken line.

Forgetting your password

The instructions are same as expressed herein this user guide in 'Forgetting your password' section on pages 23 with taking in care the cautions therein.

Auto-Activation Property

With Auto-Activation property, you configure your USBK to automatically start when you plug it in a HostSystem. So, you can use your USBK on hostsytems which do not have any user interface for password entry.

When Auto-Activation is enabled, USBK does not ask for password confirmation to verify user. Thence, it can be used directly on test & measurement equipments such as oscilloscope, EKG, etc.

NOTE: To enable Auto-Activation, your USBK must be in "**Deactivate** State". You can check it via LEDs.

To enable Auto-Activation

1. Double-click on the **USBK disk** icon in **My Computer** and use the files in **Text Menu**
2. Open the **AutoActivation.txt** file
3. Erase all '**xxx**' letters till '**:**' and type your current password near **Password:**
4. Erase '/**Disable**' in '**Enable**/**Disable**' as '**Enable**' will stand alone.
5. Erase '**#**' letters till '**:**' and type the key number that that you want to activate near **KeyNo:**. The KeyNo is 1 for A101 models and can be either 1 or 2 or 3 for A103 models.
6. Save the file in order to execute these changes.
   If all your entry is valid, auto-activation of your USBK is done successfully. You can follow it up via LEDs. The LEDs indicates as follows when setting is done successfully.

LED1: HostSystem Led	LED2:BackDisk Led
Blink	OFF

   If any of your entry is wrong, the LEDs indicate as follows:

LED1: HostSystem Led	LED2:BackDisk Led
Blink twice	OFF

! **CAUTION:** The operating system uses cache to serve faster for future requests. Your password can be read from a cache after your data entry. In order to clean the cache, erase your entry (erase till ':' in keeping the 'OldPassword:' and 'NewPassword:' titles) and save it again. So, any security object that resides in the cache is considered as expired.

! **CAUTION:** If you carry and lose your BackDisk plugged-on your USBK in "Auto-Activation Enabled", any user can access your data on your BackDisk when he plug in the computer as no password is asked to verify user. Just carry only your USBK when "Auto-Activation Enabled" for the security of data on your BackDisk.

NOTE: Each file contains related example. You can follow up shown example below broken line.

To disable Auto-Activation

NOTE: To disable Auto-Activation, your USBK must be in "**Deactivate** State". If not, deactivate your USBK before using the instruction herein this guide on page 41.

1. Double-click on the **USBK disk** icon in **My Computer** and use the files in **Text Menu**
2. Open the **AutoActivation.txt** file
3. Erase all '**xxx**' letters till '**:**' and type your current password near **Password:**
4. Erase '**Enable**/' in '**Enable**/**Disable**' as '**Disable**' will stand alone.
5. Do nothing on '**KeyNo: #**'. No need to erase '**#**' letter till '**:**' and type the key number.
6. Save the file in order to execute these changes.
   If all your entry is valid, disable of auto-activation property is done successfully.

NOTE: Each file contains related example. You can follow up shown example below broken line.

Changing Device (USBK) Name

The device name is described as "Device Label" and device label is USBK in Fabric Default. To identify your device, you can optionally change Device Label The "Device Label" as

nickname helps you distinguish between different USBK devices since you can have multiple USBKs.

NOTE: To change/set Device Label, your USBK must be in "**Deactivate** State". If not, deactivate your USBK before using the instruction herein this guide on page 41.

To change device name

1. Double-click on the **USBK disk** icon in **My Computer** and use the files in **Text Menu**
2. Open the **SetDeviceLabel.txt** file
3. Erase all '**xxx**' letters till '**:**' and type your current password near **Password:**
4. Erase all '**xxx**' letters till '**:**' and type a name for your device near **Name:**
5. Save the file. If your password is valid, The LEDs indicates as below table:

LED1: HostSystem Led	LED2:BackDisk Led
ON	ON

   It means that you should remove and re-plug your USBK for changing to be applied.
6. Un- plug your device (USBK)
7. When you plug it, you see your device with new name instead of USBK as default name. New name is also indicated at **About.txt** near **Device Label:**

! CAUTION: The operating system uses cache to serve faster for future requests. Your password can be read from a cache after your data entry. In order to clean the cache, erase your entry (erase till ':' in keeping the 'OldPassword:' and 'NewPassword:' titles) and save it again. So, any security object that resides in the cache is considered as expired.

Changing your encryption key(s)

You can change your encryption key(s) in any time you want.

! CAUTION: You can not read current data on your Backdisk with your new encryption key. Before changing your encryption key, be sure to back up your files in your BackDisk used with your current encryption key.

NOTE: To change your encryption key(s), your USBK must be in "**Deactivate** State". You can check it via LEDs.

To change/set your encryption key(s)

1. Double-click on the **USBK disk** icon in **My Computer** and use the files in **Text Menu**
2. Open the **KeySettings.txt** file
3. Erase all '**xxx**' letters till '**:**' and type your password near **Password:**
4. Erase '**#**' letters till '**:**' and type the key number that you would like to set near **KeyNo:**. The KeyNo is 1 for A101 models and can be either 1 or 2 or 3 for A103 models.
5. Erase all '**xxx**' letters till '**:**' and type a name for your key near **KeyName:** Key name is not mandatory; you can optionally type a name for your key.
6. Erase '**###**' letters till '**:**' and type the key size that you would like to set near **KeySize:**. The KeySize can be either 128 or 256 refer to 128-bit AES and 256-bit AES.
7. Erase all '**xxx.xxx**' letters till '**:**' and type your encryption key near **Key:** in decimal format. Decimal is formed of numeric digits between 0 and 255 and also each digit

separated with a dot. Key is formed of 16 numeric digits for 128-bit AES key size and 32 digits for 256-bit AES.

8. Save the file in order to execute these changes.
   If all your entry is valid, setting on USBK is done successfully. You can follow it up via LEDs. The LEDs indicates as follows when setting is done successfully.

LED1: HostSystem Led	LED2:BackDisk Led
Blink	OFF

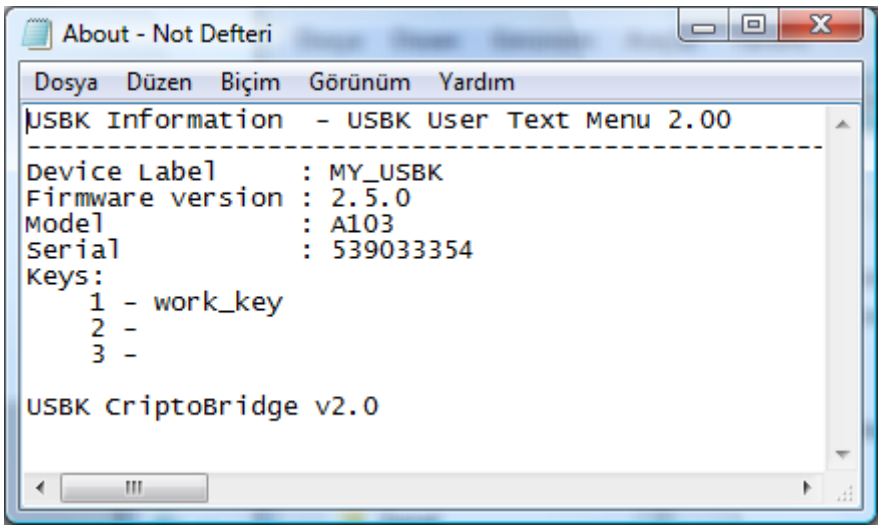
! CAUTION: The operating system uses cache to serve faster for future requests. Your security data such as password and encryption keys can be read from a cache after your data entry. In order to clean the cache, erase your all entries erase till ':' in keeping the titles and save it again. So, any security object that resides in the cache is considered as expired.

! CAUTION: After setting/changing your encryption key(s), write down encryption key(s) in note for future reference, but remember to keep it confidential. There's no way to recover encryption key(s) as they are never exported or displayed during usage of USBK. A lost of encryption keys results in lost of data on BackDisk. Therefore, it is very important that you remember the encryption key(s) or store it in a safe place.

NOTE: You must format your BackDisk when it is the first time use with your new encryption key(s).

Viewing device information

You can view information about your USBK on **About.txt** .

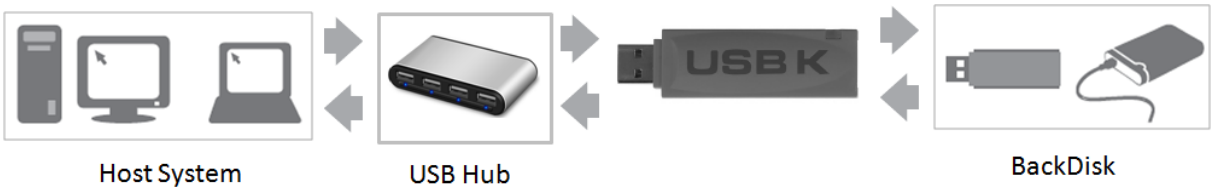


All information is viewed in following categories:

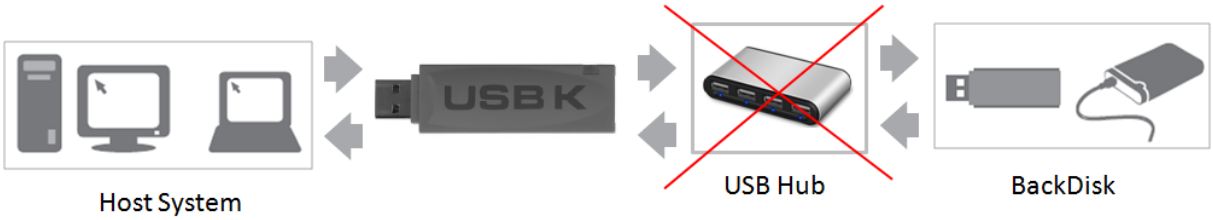
- **Device Label:** The name of your device. USBK is fabric default name and viewed with the new name after you change the device label.
- **Firmware ver:** Firmware version associated with your USBK
- **Model:** Model of your USBK
- **Serial Number:** Serial Number of your USBK. This is a unique number for each USBK.
- **Keys:** Key names are viewed here.

Using USBK with a USB Hub

You can use your USBK over a hub plugged to your computer.



NOTE: You can not plug any USB hub to backport of your USBK.



Troubleshooting (FAQ)

If you have problems using your USBK, you may find a solution in one of the following questions and scenarios. To obtain the latest version of FAQ, please visit 'FAQ' at 'Support' page of our website www.usb-k.com.
For further technical assistance, contact us or submit your problem to support@usb-k.com.

USBK.exe program doesn't work. What can I do?

It is .Net framework dependent. That's why, you should install "Microsoft .NET Framework Version 2.0" on your computer. You can download it from following link.
http://www.microsoft.com/downloads/en/details.aspx?FamilyID=0856eacb-4362-4b0d-8eddaab15c5e04f5&displaylang=en

How can I recover my Encryption Key if I forget it?

If you forget your encryption key, there is no way to get it back except you remember it. After your key setting, it is securely saved in your device and never exported or displayed during usage of USBK. Therefore, it is very important that you remember the encryption key or store it in a safe place.

My BackDisk plugged-in USBK recognized as unformatted. Why?

There are two possibilities:

1. If it is the first time that you are using your BackDisk with your USBK; it will be recognized as unformatted disk. You should format your BackDisk when you are using it with your USBK the first time.
2. If you have an A103 model, be sure that you activate right key that you used before with your BackDisk.

The file that I saved to USBK disk is lost. Why?

USBK is not a real disk and has no flash memory on. It uses ordinary USB flash drives as data storage area. Although you can copy small sized file on it, it is deleted when you remove your USBK. You cannot save any file to your USBK. Save data to only your BackDisk.

I have two partitions on my BackDisk. Can I use one partition encrypted with USBK and other partition as regular?

No, you cannot use. You should format all your disk with your USBK and all disk is used in encrypted form.

How long does it to format my 300GB external harddisk by USBK?

There is approximately %30 slowdown. It will be %30 slower than normal formatting of your harddisk.

How can I read data on my BackDisk if I lost my USBK?

If your USBK is lost/broken, you can buy a new USBK and make it identical with lost/broken one to read your encrypted data. It is enough to remember your encryption key on lost/broken one and define the same key on your new USBK. Names of Encryption keys need not to be the same, but encryption keys must be same.

Who are we?

USBK and USBK logo is trade mark of Tamara Elektronik Ltd. Şti.

Since its establishment in 1996, Tamara Elektronik Ltd. Şti. has been a company specialized in the design of hardware products. We have hardware/software design skills required to develop a wide variety of electronics based products for IT security market.

With USBK, we mixed our security expertise with product design that emphasizes usability, simplicity and accessibility. Our mission is to create innovative products by making them easy-to-use, affordable and available to everyone.

Your feedback really matters to us, and we carefully review all feature requests, ideas, suggestions and customer feedback for prioritization of our next features and products.

Contact Information

TAMARA Elektronik Ltd. Şti.

Address: Acibadem Cad. 34/3 Kadikoy 34718 Istanbul - TURKEY

Phone: +90 216 418 92 94

e-mail: info@usb-k.com
support@usb-k.com
tamara@tamara.com.tr

Appendix: USBK policy settings

The policy settings that are available vary according to the model of USBK.
The following table describes each policy setting and indicates the models to which these options apply.

Policy setting	Description	Applicable Models
AES Key Size	128-bit and 256 bit	All models
Encryption Key Type	The type of key that user can specify when creating a valid encryption key. It can be in two different types: “Text” or “Decimal”. For 128-bit AES key size; • Text must be 16 characters long with letters, numbers and special characters such as punctuation marks, etc. • Decimal is formed of 16 numeric digits between 0 and 255, each digit separated with a dot. For 256-bit AES key size; • Text must be 32 characters long with letters, numbers and special characters such as punctuation marks, etc. • Decimal is formed of 32 numeric digits between 0 and 255, each digit separated with a dot.	All models
Type of Encryption Key Generation	This is for how the user creates its encryption keys. It can be in two different types: “User initiated” or “Random Key Generator”. For “User initiated”, the user creates itself the encryption key(s). For “Random Key Generator”, USBK generates the encryption key(s) on behalf of user.	All models
Number of Encryption Key	Total number of creating different encryption keys	A101: 1 A103: 3
Password Length	Min.-max. number of characters that user can specify when creating a valid password. The length of password can range from 4 to 16 characters. User can increase the level of security by creating a strong password.	All models
Password Retry Limit	A retry limit is the number of wrong password attempts allowed the user before USBK returns back to Fabric Default. Password retry limit will block unauthorized user after 3 failed attempts.	All models

Table 2 - USBK Policy Settings