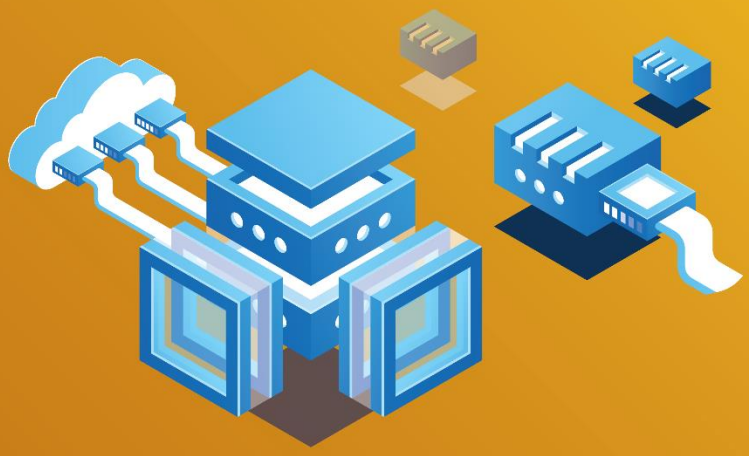
LiNKDOOD SECURED USB



Encryption protection which makes use of AES cryptography and authentication

Linkdood Secure USB

Who is the target user?

Any enterprise users who seek to pass the data to customer and worry about the data leaking. Especially for those who want to share the design to customer and open on customer side which really need to secure the data, in case those demonstration data leak to other parties.

BEYOND SECURITY LINKDOOD

Table of Content

Introduction

Linkdood Secure USB Stick system is a mobile storage device used for data security and operation audit. This system consists of three parts which is management software, application software and USB drive itself. The access control of the USB drive is secured by using password verification and encryption as security measure.

In architecture, this system uses dedicated microcontrollers unit and adopts USB standard protocol in exchanging data with the host.

In usage, this system uses different approach compared to conventional approach where users have to log into the USB drive and edit the file directly on the drive itself preventing data leakage effectively in the process. Real-time audit software records every operation on the drive and host environment where the drive is used. The recorded data is then stored in the log zone of the USB drive.

This system provides solution for data leakage due to the loss of USB drive and responsibility issue due to the usage of the USB drive.

Product Architecture

The structure of Linkdood Secure USB Stick system consists of the user and driver layer of the host computer, the memory, security control module and USB controller interface of the USB drive hardware layer. By connecting the USB drive to the host computer via USB port, the user of the host computer is able to interact or exchange data with the drive via standard USB bus (standard USB protocol).

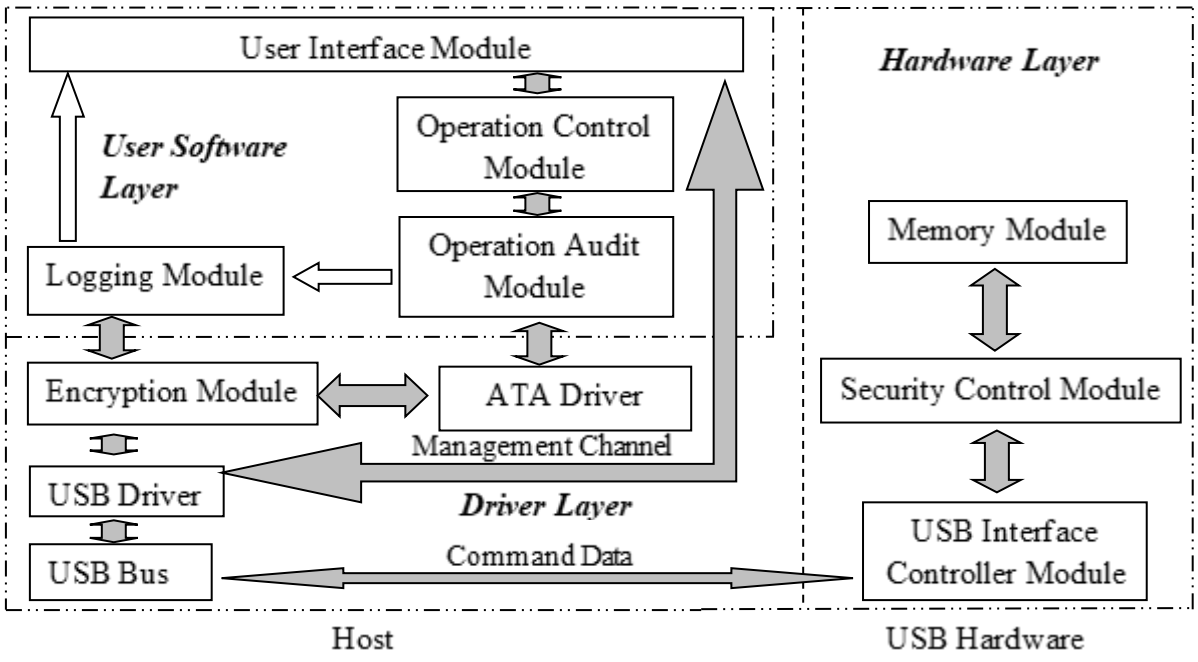


Figure 1

The below are the description for each component:

- User Layer

  This layer provides interface to control and monitor user operations, generate log data, read-write file data and interact with driver layer. User layer consists of user interface module, operation control module, operation audit module and logging module.

  User interface module provides user operation interface where this interface interacts with underlying file data through operation control and audit module. With operation control module, users are prevented from data leakage while working as their read-write operation are limited or restricted.
  User interface module is also able to read and display log information through logging module. Also, the user interface module directly controlling driver module to run read-write, device identity verification and more on the USB drive.

- Driver Layer

  This layer acts as an interface connecting user layer and hardware layer. It is also act as file system management and real-time encryption of the data operation between user layer and USB drive. This layer includes ATA driver module, file encryption module, transparent encryption module, redirect module and USB driver module. ATA driver module organizes incoming data stream file into file block according to file system and then encrypt the file block use encryption module. File encryption module encrypts all the incoming data log information from user layer and driver layer. Encrypted data then will set to bulk-only mode and generate USB data packet to interact with USB drive through USB drive module. Transparent encryption module encrypts temporary file that is generated during the edit process of files. Redirect module provides safe workspace for user to prevent data leakage. USB driver module receives direct command from user interface module to interact with USB drive through management channel.

- Hardware Layer (USB drive)

  USB drive consists of three parts: Memory module, USB controller interface module and security control module. It adopts standard USB protocol and it is equipped with USB drive security management function. Standard USB data packet is processed by USB controller interface module into commands and data. Commands and data is then sent to security control module for access permission verification with the current logged-in password and then process the incoming commands and data according to the corresponding access permission. After processed, the read-write instruction will be issued to the memory module and the result will be returned to the security control module for further processing.

- Logical Structure

  After the system logical structure is confirmed, we use layer-by-layer design to standardize the overall interfaces. With this, our system has a better scalability, inheritance, adaptability to meet more development needs and demands. The logical structure of the system consists of four parts as shown below.

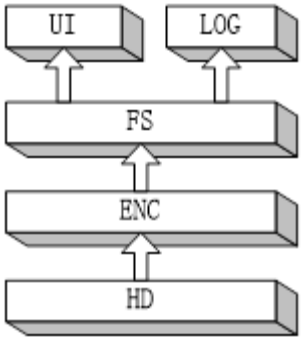


Figure 2

Below is the description and function of each layers:

- UI (User Interface Layer): Provides user operation input to retrieve file lists or read-write files.
- FS (File System Layer): Provides file system function like file lists, read file, write file, add file, delete file and etc.
- ENC (Encryption Layer): Provides encryption and user authentication on the data sector.
- HD (Hardware Layer): Provides read-write function on the data sector.
- LOG (Log Layer): Provides read-write log function and to simplify the design of log layer, LOG is placed on the upper layer of FS.

Product Modules

Linkdood Secure USB Stick system consists of user layer and driver layer on the host computer, USB drive, security control module and USB interface controller on the USB drive hardware. The functions of all the respective module function are described below:

1) User Software Layer

User layer provides interface to control and monitor user operations, generate log data, read-write file data and interact with driver layer. User layer consists of user interface module, operation control module, operation audit module and logging module.

- **User Interface Module**

This module creates interfaces such as operation, configuration and log management interface on the host computer which enable users to manage files, configure USB flash drive and manage log data. Operation interface are designed with operation buttons such as copy, delete, rename file and create new folder. It also has directory operation buttons for file management and manipulation like file browser to browse files on the local disks and the USB drive. Configuration interface enables user to directly access identity information on the USB drive through the driver layer. It also allows user to configure parameters through the management channel. Log management interface provides retrieve, search, analysis and delete function for user. This interface uses logging module directly through management channel.

- **Operation Control Module**

During data exchange between the host computer and USB drive, the user read-write access is limited by this module according to the policy or label configuration control. Hence, intended or unintended data leakage are then prevented.

- **Operation Audit Module**

This module captures all the user operations on the USB drive such as content details. timestamp and other relevant information as logging record and this record is then send to logging module for storing.

- **Logging Module**

This module will assemble the log information generated by the monitoring control module into a log entry. The log entry consists of operating time, host name, MAC address of each network cards, IP address, hard dish serial number, CPU type and etc. Thus, this module also makes specific operations on files for overall log information. Lastly, this module will organize this data into a fixed length log format and send to driver layer for encryption.

2) Driver Layer

Driver layer acts as an interface connecting user layer and hardware layer. It is also acting as file system management and real-time encryption of the data operation between user layer and USB drive. This layer includes ATA driver module, file encryption module, transparent encryption module, redirect module and USB driver module.

- **ATA Driver Module**

This module uses standard FAT file format where files and folders are organized into blocks and then send to encryption module. At the same time, it provides basic operations such as create, delete, copy, rename file, create directory and etc. to the user software layer.

- **File Encryption Module**

This module responsible for file encryption and decryption which uses AES-256 bits as the encryption algorithm or any other algorithms recognized domestically or internationally.

- **Transparent Encryption Module**

This module responsible for file cache encryption and decryption during the editing process and uses SEAL algorithm.

- **Redirect Module**

This module creates a safe working environment for the user during the editing process which is to prevent data leakage.

- **USB Driver Module**

This system uses standard USB enumeration and configuration protocol. Therefore, no additional drivers are needed when connecting the USB drive to host computer. In order to prevent host computer to take control on the data channel, this module added custom USB Mass Storage communication command so that the operating system of the host computer

unable to understand the data information on the data channel. To do so, the command code is same with the serial code on USB controller interface module.

The below is the main communication commands of the custom USB Mass Storage for this system:

- Standard command: ReadDisk, WriteDisk, TestUnitReady, DeviceInquiry.
- Log command: WriteLog, ReadLog, WriteBlock, ReadBlock, EraseBlock.
- Management command: Refer to read-write interface.

Under standard command, communication command uses non-standard protocol, randomize the data and add in the flag zone so that the USB controller interface module are able to differentiate the data. Therefore, the host operating system will not have any response to this data stream.

Log command is used to further encapsulate the standard command and add in the log flag so that the USB controller interface module can directly add the log entry to the log zone after it parses the command.

Management command is independent command where it goes through security control module for authentication and read-write the system configuration. It consists of password authentication, zone configuration, password configuration, clear log, sequence number setting and etc.

3) Hardware Layer (USB Drive)

USB drive consists of three parts: Memory module, USB controller interface module and security control module. It adopts standard USB protocol and it is equipped with USB drive security management function.

This system uses the firmware code of USB interface controller to generate its USB interface controller module and security control module. The USB drive controller uses a standard programmable chip and provides USB interface controller and NAND flash memory interface.

- **USB Interface Controller Module**

Comply with the built-in standard USB enumeration, configuration protocol and custom USB Mass Storage communication command for data exchange with the host computer, system configuration and etc.

This module will run automatically after USB drive is connected to the USB port of host computer. After connected, the host computer will show the drive as a standard read-only drive with small capacity size and its content is the portable software. Other partitions are hidden from the host operating system, and not accessible. Data zone is in a locked-state due to the difference of communication command and the security control module have yet to verify the identity of the user.

- **Security Control Module**

This module ensures the security access on the low-level hardware data information of the host software. Read-write or configuration command option will be granted on the partition after a successful password verification, else an error will be returned. Master key is generated by the system at user interface layer configuration then it is hashed and encrypted with user password and stored in the label information zone. Privilege security control module is responsible to allow or deny the data access request coming from the upper layer. This system has five privilege level as shown below:

Privilege level	Access permission
Administrator	Read-write label information, read-write device software, read and clear log zone.
Read-only Personal Storage	Read personal data storage and configure certain label information.
Read-Write Personal Storage	Read-write personal data storage and configure certain label information.
Read-only Log Zone	Read log entry.
Write-only Log Zone	Add log entry.

The process of security control module is as below:

- After USB drive is connected and powered up, the security control module will be turned on;
- User layer will issue an open command; error will be returned if fail. If open successfully, shared zone will be displayed. If user wanted to enter personal storage zone, then a login will be required;
- In the read-write process, log entry will be generated first, then only the operation been carried out.

Condition for USB drive lock down:

- Log Zone capacity is full and trigger the drive to be locked down. Only administrator can clear the log and unlock the device.
- Personal storage operation and user log view requires password input, if invalid password input reaches a preset number of times, the drive will be locked down. Only administrator is able to unlock the device.

- **Memory Storage**

  This system uses standard NAND flash just like the product of other vendors such as Samsung and Toshiba. NAND flash has a larger capacity and uses paging for storing which made it suitable for mass storage device.

  This system is divided into five zones which is label information zone, software zone, shared zone, personal storage zone and log zone as below:

  The below are the parameters of the stored label information which is then used by the security control module:

Parameter	**Description**

Flag zone	Tag of flag list, for verification use
Supplier name	Default setting
Product name	Default setting
Software zone capacity	Customizable by administrator
Shared data zone capacity	Set by administrator and customizable by user
Personal storage capacity	Set by administrator and customizable by user
Log zone capacity	Customizable by administrator
Log index zone capacity	Customizable by administrator
Serial number	Default setting
Password information	Hashed password information

The functions of each zone are as below:

- Software Zone:
- Storage for application software. If administrator is logged in, read-write function will be enabled for this zone. If it is user that is logged in, this zone will be available for read-only.

- Shared Data Zone and Personal Storage Zone:
- Both of these zones are for storage purpose which organize files using file system provided by ATA driver module. It is the same with normal USB drive, but Personal Storage Zone would have required the user password to access.

- Log Zone
- This zone uses sequential method to write the log, any operation on log is managed by Security Control Module to centralize controls and prevent log writing errors.

- The below is the organizational structure of Log Zone which consists of two major blocks: Block Zone and Log Zone.

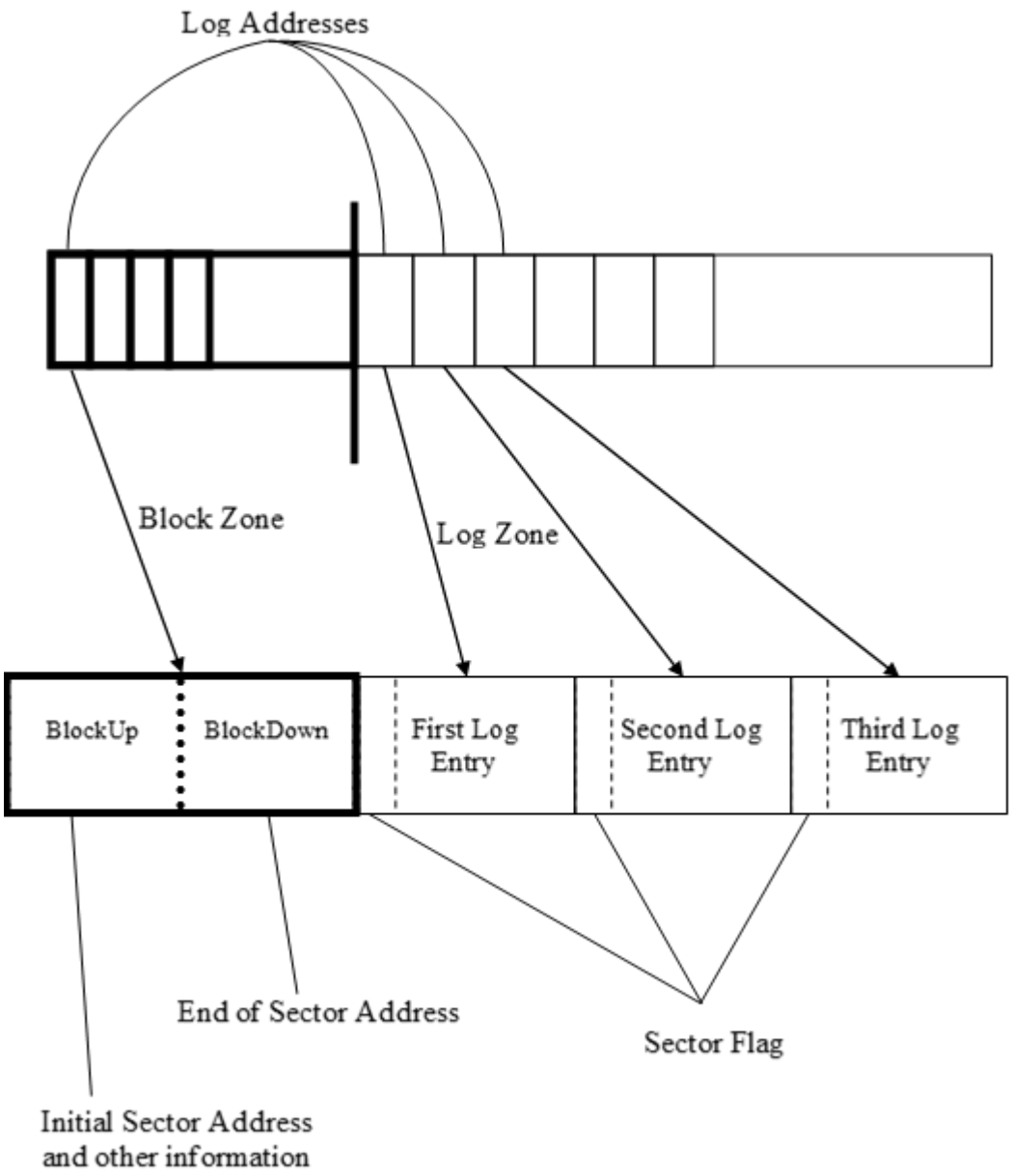


Figure 3

- Block Zone
  This zone is the index of Log Zone, space allocations are partitioned according to the data in the flag zone. The initial position of Block Zone is the initial position of Log Zone. Every times USB drive is plugged in and out will generate a Block which consists of BlockUp and BlockDown. BlockUp is generated when USB drive is opening and BlockDown is generated when USB drive is closing. To prevent the loss of BlockDown due to inappropriate closing, when opening the system, Block Zone will regenerate the BlockDown information.

  BlockUp consists of the following information: Startup time, host name, MAC address of each network cards, IP address, hard disk serial number and CPU type. Lastly, the corresponding initial address of the log.

  BlockDown consists of the following information: End time and the corresponding last address of the log.

- Log Zone
  This zone is the details of each log which consists of the following information: Time, operation directory (local disk is the path, USB drive is the shared data zone and personal storage zone), operation type (create, delete, copy in, copy out and rename).

  Logs are arranged in linear logic, so when reading the log, information is located based on description of the block.

  Every log entry included a sector use flag for security control module to identify which sector are not used yet.

  The below are the writing processes: After the device is opened, a binary search is used to look for the first empty sector in the Log Zone, then include the sector number to the block content and save the block. Lastly, save the log entry on the sector.

Products Functions

Linkdood Secure USB system uses mandatory encryption and hardware verification technique to prevent data storage from illegal access and leakage. The following are the functions and features:

1. Entire disk encryption: Mandatory encryption, no worries if USB drive is lost.
2. Password protection: If invalid password is input for a certain amount of times, the device will have locked itself.
3. Hardware verification: Password related information are hardware processing to prevent hackers or viruses attack.
4. Hierarchical management: Two layers of access permission management for respective responsibilities.
5. Ease of use: No extra installation as software already preinstalled on the disk with user-friendly interface.
6. Locate device: Log contents such as the host CPU ID, MAC address, hard disk serial number, username, username, computer name and IP address are saved.
7. Log accuracy: Contents such as data accessing, password verifying and every user operation are recorded accurately.
8. Uses dedicated control module to prevent unauthorized USB drive formatting.
9. Eliminate the viruses from copying itself to the USB drive by not using the operating system directly to read-write on the USB drive.
10. Support fine role-based in the access control mechanism, customizable data access and audit policies and provides multi domain level of security protection.

11. Use secured storage techniques to protect information storage and exchange security ensuring audit security of the use of information content.

12. Able to track the path of the information went by combining the collected multidimensional fingerprint of the host computer and able to analyze the audit of the data operations in detail.

13. Mandatory audit: Track and record every user operation, locate the computer device used by user, audit information recorded in the audit zone of the USB drive for later analysis.

Product Features

This is system is designed to ensure the security of important data on the USB storage by using mandatory log audit on the data read-write in real-time. With this, administrators are able to identify security risk through data mining of the log file and trace the responsible person through the audit when security incident happened. The following are the detail of features:

- **File Transfer Encryption**

In the process of data exchange between host computer and USB drive, this system will encrypt the data transfer in real-time. When the partition is loading, incoming data to the USB drive will be encrypted and outgoing data will be decrypted. This whole process is hidden from user and it only affect a small amount of the data transfer speed.

- **Custom Transfer Protocol**

Use custom USB Mass Storage transfer protocol which is completely different from Windows operating system and this also make Windows does not understand the underlying protocol. Therefore, the data transmission is hard to be eavesdropping and prevent viruses, remote control and etc.

- **User Authentication**

USB drive is partitioned into shared zone and personal storage zone for public and confidential data storage respectively. To access shared zone, user may directly operate the file, but to access personal storage zone, user will be required to input their password for authentication. If invalid password input reaches certain number of times, the USB drive will be locked and only administrator is able to unlock the drive.

- **Hardware Control Encryption Zone**

Except the shared zone, the other three zones are locked and hidden in Windows or Linux operating system. Only through the installed software on the USB drive, user can operate the file data on the other three zones.

- **Buffer Memory Protection**

In Windows operating system, data are placed in buffer memory first, then only write into storage after certain policies and this process needs to be protected to avoid data theft. Therefore, to protect all the commands and sensitive data in the buffer memory, buffer memory is locked, preventing page swap that will swap the data to the disk buffer memory. When the buffer memory unlocked, all the commands and sensitive data will be clear from the buffer memory.

- **Real-time Audit**

In usage, the software will record all the user operations and write the log into Log Zone in real-time. To uniquely identify the host computer and the user, the record includes the MAC address, IP address, hard disk serial number, CPU ID and logged-in user. The system will write the log first then only execute the operations, this is to ensure the reliability and integrity of the log information.

Product Model

Basic Specification

Parameter	Description
Product name	Linkdood Secure USB Stick
Capacity	4GB/8GB/16GB/32GB
Supporting operating system	Windows XP/ 2003/ Vista/ 7/ 8/ 10
Technical features	♦ Standard USB design ♦ Served as storage device and uses on-disk management tool for disk partitioning, disk formatting and data accessing etc. ♦ Customizable security for data access ♦ Uses 'Append-only' file system to store logs

Physical Appearance (Customizable)

Parameter	Description
Colour	Blue, White Silver
Weight (g)	25
Length (mm)	55.00
Width (mm)	20.30
Height (mm)	7.50

Working Environment

Parameter	Description
Working temperature	-5°C to 45°C
Working humidity	10 to 80%
Storage temperature	-8°C to 65°C
Storage humidity	8% to 95%