KLC GROUP

KLC Advantech Drives

Firmware Version: SCPB13.0/ECPB13.0

Common Criteria Guide

Version 1.1

June 2024

Document prepared by

www.lightshipsec.com

Table of Contents

List of Tables

1 About this Guide

1.1 Overview

1. This guide provides supplemental instructions to achieve the Common Criteria evaluated configuration of the KLC Advantech Drives and related information.

1.2 Audience

2. This guide is intended for system administrators and the various stakeholders involved in the Common Criteria evaluation.

1.3 About the Common Criteria Evaluation

3. The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) is an international standard for security certification of IT products and systems. More information is available at https://www.commoncriteriaportal.org/

1.3.1 Protection Profile Conformance

4. The Common Criteria evaluation was performed against the requirements of the collaborative Protection Profile for Full Drive Encryption – Encryption Engine, v2.0 + Errata 20190201 (referenced within as CPP_FDE_EE) available at https://www.niap-ccevs.org/Profile/PP.cfm

1.3.2 Evaluated Firmware and Hardware

5. The physical boundary of the TOE encompasses the KLC firmware running on the SEDs identified in Table 1.

Table 1. TOE Hardware/Firmware

Series	CC Listed P/N & Version	Advantech P/N & Version	Form Factor	Controller	FW Version
840F	SQF-2020-1TSCB	SQFFS25V8-1TSC	2.5" SATA	PS3112-S12	SCPB13.0
840F	SQF-2020-512SCB	SQFFS25V8-512GSC	2.5" SATA		
840F	SQF-2020-256SCB	SQFFS25V4-256GSC	2.5” SATA		
840F	SQF-2020-128SCB	SQFFS25V2-128GSC	2.5” SATA		
840F	SQF-2020-1TSCM	SQFFSM8V4-1TSC	M.2 SATA		
840F	SQF-2020-512SCM	SQFFSM8V4-512GSC	M.2 SATA		

Series	CC Listed P/N & Version	Advantech P/N & Version	Form Factor	Controller	FW Version
840F	SQF-2020-256SCM	SQFFSM8V4-256GSC	M.2 SATA	PS3112-S12	SCPB13.0
840F	SQF-2020-128SCM	SQFFSM8V2-128GSC	M.2 SATA		
920F	SQF-2040-1TECM	SQFFCM8V4-1TEC	M.2 NVMe	PS5012-E12	ECPB13.0
920F	SQF-2040-512ECM	SQFFCM8V4-512GEC	M.2 NVMe		
920F	SQF-2040-256ECM	SQFFCM8V4-256GEC	M.2 NVMe		

1.3.3 Evaluation Assumptions

6. The following assumptions were made in performing the Common Criteria evaluation. The guidance shown in the table below should be followed to uphold these assumptions in the operational environment.

Table 2: Evaluation Assumptions

Assumption	Guidance
Communication among and between product components (e.g., AA and EE) is sufficiently protected to prevent information disclosure. In cases in which a single product fulfils both cPPs, then the communication between the components does not extend beyond the boundary of the TOE (e.g., communication path is within the TOE boundary). In cases in which independent products satisfy the requirements of the AA and EE, the physically close proximity of the two products during their operation means that the threat agent has very little opportunity to interpose itself in the channel between the two without the user noticing and taking appropriate actions.	The Authorization Acquisition (AA) component, and the Encryption Engine (EE) component should be within a close physical proximity.
Users enable Full Drive Encryption on a newly provisioned storage device free of protected data in areas not targeted for encryption. It is also assumed that data intended for protection should not be on the targeted storage media until after provisioning. The cPP does not intend to include requirements to find all the areas on storage devices that potentially contain protected data. In some cases, it may not be	Drives should be formatted prior to use with the TOE.

Assumption	Guidance
possible – for example, data contained in "bad" sectors. While inadvertent exposure to data contained in bad sectors or unpartitioned space is unlikely, one may use forensics tools to recover data from such areas of the storage device. Consequently, the cPP assumes bad sectors, un-partitioned space, and areas that must contain unencrypted code (e.g., MBR and AA/EE pre-authentication software) contain no protected data.	
Users follow the provided guidance for securing the TOE and authorization factors. This includes conformance with authorization factor strength, using external token authentication factors for no other purpose and ensuring external token authorization factors are securely stored separately from the storage device and/or platform. The user should also be trained on how to power off their system.	Administrators should ensure that TOE users are aware of organizational password policies.
The platform in which the storage device resides (or an external storage device is connected) is free of malware that could interfere with the correct operation of the product.	Administrators should ensure that the TOE is protected from malware.
The user does not leave the platform and/or storage device unattended until the device is in a Compliant power saving state or has fully powered off. This properly clears memories and locks down the device. Authorized users do not leave the platform and/or storage device in a mode where sensitive information persists in non-volatile storage (e.g., lock screen or sleep state). Users power the platform and/or storage device down or place it into a power managed state, such as a "hibernation mode".	A module in unlock state shall never be left unattended. The User shall lock or power off the module before leaving the module unattended.
All cryptography implemented in the Operational Environment and used by the product meets the requirements listed in the cPP. This includes generation of external token authorization factors by a RBG.	The TOE makes use of FIPS validated cryptography.
The platform is assumed to be physically protected in its Operational Environment and not subject to physical attacks that compromise the security and/or interfere with the platform's correct operation.	Ensure that the device is hosted in a physically secure environment, such as a locked server room.

1.4 Conventions

7. The following conventions are used in this guide:

a) `CLI Command <replaceable>` - This style indicates to you that you can type the word or phrase on the command line and press [Enter] to invoke a command. Text within <> is replaceable. For example:

Use the `cat <filename>` command to view the contents of a file

b) [key] or [key-combo] – key or key combination on the keyboard is shown in this style. For example:

The [Ctrl]-[Alt]-[Backspace] key combination exits your graphical session and returns you to the graphical login screen or the console.

c) **GUI => Reference** – denotes a sequence of GUI screen interactions. For example:

Select **File => Save** to save the file.

d) [REFERENCE] *Section* – denotes a document and section reference from relevant supporting documents (if applicable).

1.5 Terminology

8. Below defines terms and acronyms that are not commonly known.

Table 3: Terminology

Term	Definition
AA	Authorization Acquisition
AES	Advanced Encryption Standard
BEV	Border Encryption Value
BIOS	Basic Input Output System
CBC	Cipher Block Chaining
CC	Common Criteria
CEM	Common Evaluation Methodology
CMOS	Complementary Metal-Oxide Semiconductor
CPP	Collaborative Protection Profile
DAR	Data At Rest
DEK	Data Encryption Key
DRBG	Deterministic Random Bit Generator
DSS	Digital Signature Standard
EE	Encryption Engine
EEPROM	Electrically Erasable Programmable Read-Only Memory
FIPS	Federal Information Processing Standards
FDE	Full Drive Encryption
HMAC	Keyed-Hash Message Authentication Code
HW	Hardware
IEEE	Institute of Electrical and Electronics Engineers
IT	Information Technology
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission

Term	Definition
IV	Initialization Vector
KEK	Key Encryption Key
KMD	Key Management Description
MBR	Master Boot Record
NIST	National Institute of Standards and Technology
OS	Operating System
OTP	One-Time Programmable
PBKDF	Password-Based Key Derivation Function
PRF	Pseudo Random Function
RBG	Random Bit Generator
RNG	Random Number Generator
RSA	Rivest Shamir Adleman Algorithm
SAR	Security Assurance Requirements
SED	Self-Encrypting Drive
SHA	Secure Hash Algorithm
SFR	Security Functional Requirements
ST	Security Target
SPD	Security Problem Definition
TOE	Target of Evaluation
TSF	TOE Security Functionality
USB	Universal Serial Bus
XOR	Exclusive or
XTS	XEX (XOR Encrypt XOR) Tweakable Block Cipher with Ciphertext Stealing

2 Configuration

2.1 Obtaining the TOE

9. The TOE hardware is delivered to customers via trusted courier with the firmware preinstalled.

2.2 User Data Protection Configuration

10. Refer to section 3.1 of this document for information on how to turn the cryptographic module into FIPS-approved mode.

2.3 Management Functions

11. The DEK can only be changed by generating a new one. Refer to section '*Cryptographic Key Generation* > *Change DEK*' of this document for more information on how to generate and re-generate the data encryption key.

12. Users of the TOE must contact the vendor to obtain firmware updates. Firmware updates are manually installed by authorized administrators.

13. When the user triggers the TOE update, the TOE compares a hash of the public key with the stored hash of the public key, and then verifies the digital signature. If the digital signature verification succeeds, the upgrade process is carried out. If the digital signature verification fails, the upgrade process is aborted, and an error is displayed to the user.

14. Key recovery is not supported by the TOE.

2.4 Power Saving States

15. The TOE does not support any non-compliant power saving states. The TOE only supports D3 power on and power off, which is a compliant power saving state. The time it takes for the TOE to fully transition into the compliant power saving state is dependent on the host platform. In the evaluated configuration, after power is removed from the TOE, it takes approximately two seconds for DRAM to completely power down.

16. **Note**: No methods of inactivity timeout are supported by the TOE.

2.5 Prepare and Install the PBA Software

17. These instructions will show you how to create a bootable USB thumb drive, when to install your operating system or virtual machine during the PBA software installation process, how to activate the PBA capability, as well as how to log in using the PBA software.

2.5.1 Download the PBA Software

18. Download the KLC CipherDrive PBA installation package from the KLC customer portal and save it to a place on your computer.

2.5.2 Create A Bootable USB Thumb Drive

19. Refer to section 2.6.2.1.

2.5.3 Configure UEFI/BIOS Settings

20. You will need to properly configure your BIOS or UEFI in order to properly boot from the thumb drive. To do so, follow these steps to ensure your computer's BIOS or UEFI settings are configured correctly. To access the BIOS or UEFI, you may have to press Delete, Esc, F2, or F12 repeatedly while your computer boots.

    1) If you have an option for "UEFI Boot Path Security" or something like it, be sure to change it to '**Never'**.
    2) If you have an option to allow OPAL hard drive SID authentication, be sure to **enable it.**
    3) Ensure that your "SATA Operation" is set to '**AHCI'** or **'RST'** mode**.** Please note that RST mode is supported only for SATA or NVMe SEDs using VMD for Intel® 11th Generation platforms or newer.
    4) If you have a system that supports CPUs with high core counts, such as a server, the UEFI will likely have an option for "X2Apic Mode" in its processor settings section. Set "X2Apic Mode" to '**Disabled'**.
    5) If you have a discrete video card, ensure your primary display detection is set to '**Auto'**.
    6) Disable "**Secure Boot**".

       Note: Secure Boot is supported, but only once the PBA software is completely installed. You may re-enable Secure Boot after you have completed installation of the PBA software and your operating system.

2.5.4 How to Boot Into the Thumb Drive

21. Refer to section 2.6.2.2.

2.5.5 Install the PBA Software

22. To install the PBA software:

    1) Boot into the thumb drive using the steps above.
    2) Type in the following command,

       Please note that the following text is case sensitive

       CAUTION: The following commands will only work when your SSD is the only drive installed in the system. If you have multiple drives, please ensure you are using the correct Linux boot path (examples: /nvme0, /nvme1, /sda for your SSD. To do so, type *sedutil-cli --scan* and press Enter. Please note that with this version of the PBA software, only the drive you select during this process will be protected by pre-boot authentication and encryption.

       CipherDriveInstaller -d /dev/nvme0 -p <password> -lic <license filename>

       Note: <password> is the Administrator password. The default Administrator password is Administrator, and it is case-sensitive. <license filename> is the filename of the license you added to the boot disk in the steps above.

       Important: If you are using the Administrator password shown as an example in the manual, then you must change it as soon as possible by logging into the PBA software's Management Console.

    3) The computer will shut down automatically. Remove the USB thumb drive and reboot the system. The PBA software has been installed! You can now start using the pre-boot authentication feature.

2.6 Upgrading the PBA Software

23. The PBA software can be upgraded via the management console or through a USB boot disk while using a command line utility

2.6.1 Management Console

1) Go to the KLC customer portal and download the latest version of the KLC CipherDrive PBA software that you have a license for.
2) Open the ZIP file containing the PBA software you downloaded and extract the folder inside to your computer's desktop.
3) Navigate into the folder you extracted and copy the contents to the thumb drive, including any individual files as well as the “EFI” folder.

   IMPORTANT: Do not copy the folder itself over to the thumb drive. Your system will be unable to boot from it if you do.
4) If there are any changes in customization information (your organization name, your IT support number, or disclaimer), then copy the license file you received from Technical Support to the root location of the thumb drive as well. Otherwise, continue onto the next step.
5) Insert the thumb drive into the computer with the SSD you are upgrading.
6) On the Settings Console, go to the Maintenance > PBA Upgrade screen.
7) Choose the thumb drive that contains the PBA software from the Device Name drop-down box. It may take a few seconds for the list of available devices to appear.
8) Check the Custom Signed Bootloader checkbox if you know you are using a custom signed bootloader. Otherwise, continue to the next step.
9) Click the Upgrade PBA button.
10) A dialog box will pop up. Enter an Administrator password and click Continue.
11) The SSD will now be upgraded. After the upgrade is complete, the computer will power off.

2.6.2 Command Line Utility

2.6.2.1 Create A Bootable USB Thumb Drive

1) Insert a USB thumb drive into your computer.
2) Format the USB thumb drive to the FAT32 file system.

   Caution: Be sure to backup any files on the drive because they will be erased!

   Important: Ensure that no other partitions or files exist on the thumb drive! If you have multiple partitions on the thumb drive, you may have to use other tools to delete them such as "Disk Management" which is built into Windows.
3) Open the ZIP file containing the PBA software you downloaded and extract the folder inside to your computer's desktop.
4) Navigate into the folder you extracted and copy the contents to the thumb drive, including any individual files as well as the “EFI” folder.

   Important: Do not copy the folder itself over to the thumb drive. Your system will be unable to boot from it if you do.

5) Copy the license file that you received upon purchasing the SSD to the root of the thumb drive.

   Note: Make note of the license file's filename because you will need it later to install the PBA software.

6) You now have a bootable thumb drive.

2.6.2.2 How to Boot Into the Thumb Drive

1) Ensure that the computer is turned off.
2) Insert the bootable USB drive you created in the steps above into the computer and turn it on.
3) Continually press the key for accessing your motherboard's boot menu while the computer starts up. The key to access it differs on different models, but the most common keys are F2, F10, F12, or Esc.
4) The motherboard's boot menu will appear. Choose the USB thumb drive from the list of boot options.
5) A Linux BASH prompt will load. Press Enter to activate the console.

2.6.2.3 Execute the Upgrade

1) Type in the following command:

   CipherDriveUpgrade -p <password>

   Note: <password> is the Administrator password.

2) The software will now be updated. When you see the message "CipherDrive upgrade is successful", power off the computer.

2.7 Upgrading Disk Firmware

24. Disk firmware can be updated through an application utility provided by the vendor. This application runs on the Windows operating system.

25. To upgrade the firmware of a hard drive, connect the drive to the Windows computer and execute the update utility. Next, select ‘Run’ or ‘Upgrade’ to perform the upgrade.

3 Cryptography

3.1 Initialization

26. The Drive Owner needs to follow these steps to turn the cryptographic module into FIPS approved mode after having received the KLC Advantech Drives.

1. Examine the tamper evidence and check the module has not been tampered.
2. StartSession SID of AdminSP with MSID password, and then set new password for SID password. The new password shall be at least 20 bytes.
3. Disable AdminSP “Makers” Authority.
4. Execute `TCG activate` command to have the module enter TCG active mode.
5. StartSession Admin1 of LockingSP with new password of SID in Step2, and then set new password for Admin1-4 passwords and User1-9 passwords of LockingSP. The new passwords shall be at least 20 bytes.
6. Configure all LockingRanges of LockinSP by setting **ReadLockEnabled** and **WriteLockEnabled** columns to `TRUE`.
7. Power cycle the module.
8. Check if the module is in the FIPS approved mode by using the Identify command response data byte 506 bit1 (SATA) or the Identify controller command response data byte 4093 bit1 (NVMe). The bit1 shall be set to 1.
9. Check the module’s firmware version using the Identify command response data dword 23-26 (SATA) or the Identify controller command response data byte 64-71 (NVME). The firmware version shall be an approved version as described in the Security Target.

3.2 Cryptographic Key Generation

3.2.1 Change DEK

27. The data encryption key (DEK) size is determined during a TOE Firmware license request. By default, the key size is 256-bits. Only 256-bit keys are used in the evaluated configuration.

28. The DEK can be changed within the PBA GUI by rebooting the computer and checking the ‘Login to Management Console’ box at the Pre-Boot Authentication Login screen. Then navigate to ***‘Maintenance > Change DEK’***

The “Change DEK” screen allows an administrator to change the protected drive’s data encryption key (DEK). This is the actual key used to encrypt the data on the protected drive.

1) On the "Maintenance" > "Change DEK" screen, enter your password into the password field.
2) Click the Change DEK button.
3) A window will pop up warning that the operation will cryptographically and irreversibly erase the protected drive(s). Click Yes to change the DEK and erase the drive contents.

3.2.2 Change AK

29. The AK can be changed within the PBA GUI by rebooting the computer and checking the 'Login to Management Console' box at the Pre-Boot Authentication Login screen. Then navigate to ***'Maintenance > Change AK'***

The "Change AK" screen allows an administrator to change the authentication keys (AK's) for all users. An AK ensures that a user is who they say they are. An administrator should change the AK's if they suspect an AK to be compromised.

1) On the "Maintenance" > "Change AK" screen, enter your password into the password field.
2) Click the Change AK button.
3) A window will pop up warning that the operation will change the AK's used to access the protected drive(s) and that the change is non-destructive and all of the content on the protected drive(s) will remain intact. Click Yes to change the AK.

3.3 Cryptographic Key Destruction

30. All DEKs are stored encrypted in NAND flash. DEKs are overwritten by SP800-90A HMAC-SHA256-DRBG in NAND when the *Change DEK* option is executed via the GUI.

31. The TOE erases cryptographic keys and key material from volatile memory when transitioning to a Compliant power saving state. Keys are erased in two stages. First, the old key is overwritten with the new key value and then stored in a new location in memory. The old block location (where the original key was stored) is erased using a wear-leveling program.

32. The TOE has only two states, namely power on and power off. The TOE does not support any non-compliant power saving states. The TOE does not delay key destruction of keys under any circumstance.

3.4 Validation

33. The TOE requires the validation of the BEV (Authentication key) prior to allowing access to TSF data after exiting a Compliant power saving state.

34. After a configurable number of failed authentication attempts is reached, the system will lockout the user account and stop responding until it is rebooted at which point the lockout counter is reset. An administrator can set this threshold to a value between 1 and 10 failed attempts.

35. Administrators can configure the number of '*Failed Logins Before Lockout'* setting via the GUI by navigating to **Settings** > **Configuration > Security** and then entering a value between 1 and 10 in the '***Failed Logins Before Lockout'*** field.

Note: The '*Failed Logins Before Lockout'* setting addresses the lockout functionality described and tested in the evaluated configuration and is distinctly different from the '*Failed Logins Before Disk Erase'* setting.

3.5 Cryptographic Operations

36. When in FIPS mode, the TOE only uses the SHA-256 hash algorithm. It is not configurable.

3.6 Random Bit Generation

37. See section 3.1 of this document for information on how to enable FIPS mode. While in FIPS mode the TOE will use the selected DRBG mechanism.