Secure Boot Variable Update

Secure Boot is a security mechanism defined by the UEFI (Unified Extensible Firmware Interface) specification. It ensures the authenticity and integrity of the operating system and drivers during system boot, preventing malicious or unauthorized software from loading. Secure Boot works by verifying the signature of each boot component using a set of trusted keys (PK, KEK, DB, DBX).

The significance of updating Secure Boot variables (such as PK/KEK/DB/DBX) includes:

- **Enhancing System Security**: Regularly updating Secure Boot variables ensures that only the latest and most secure keys and certificates are trusted, preventing the use of outdated or compromised keys.
- **Preventing Malware Intrusion**: If Secure Boot variables are tampered with or injected with untrusted keys, attackers may bypass the boot verification mechanism. Updating can remove untrusted or expired keys.
- **Compatibility and Compliance**: Some operating systems or hardware vendors periodically update keys to ensure compatibility with the latest security standards and policies.
- **Vulnerability Patching**: If a key or certificate is found to have security issues, updating allows timely patching to reduce risks.

Therefore, it is recommended to regularly check and update Secure Boot variables, and always back up the original settings before updating for future recovery.

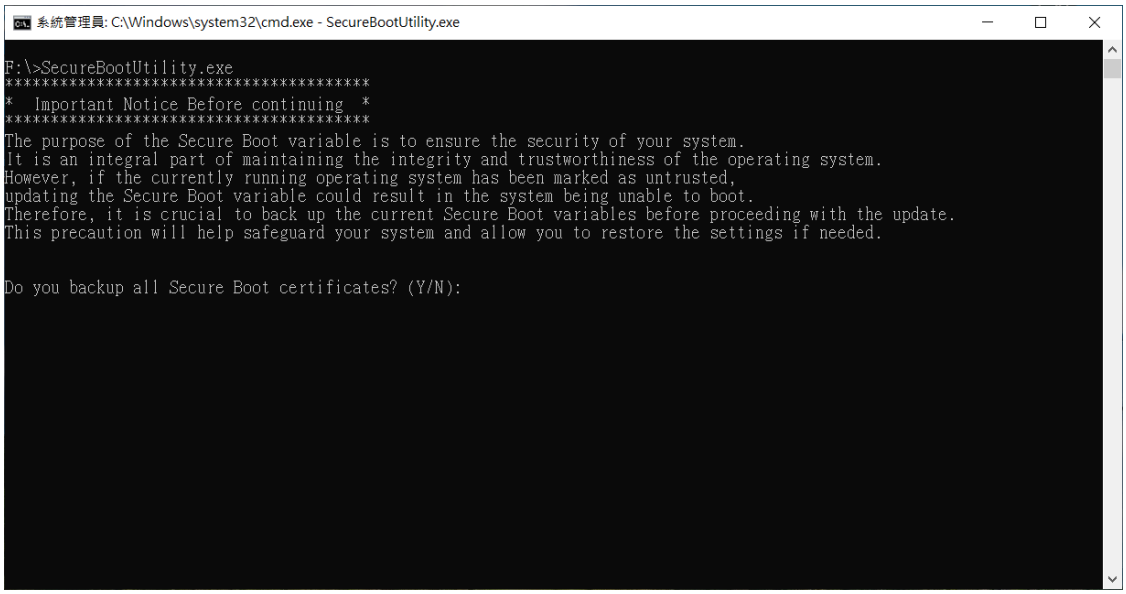
Windows Update Tool

SHA256 (SecureBootUtility.exe):
dea9c21d021a3a3114d516f96972131845b4d979a563f7544f00a63f424ba016

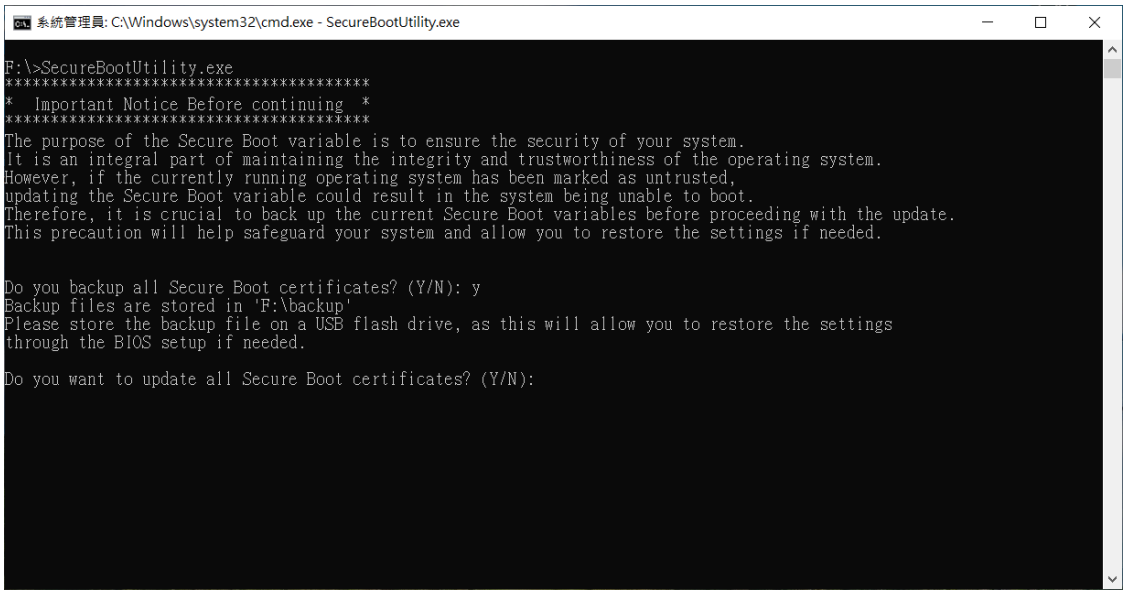
Requirements: Windows 10/11, administrator privileges required

Operation Steps

1. Open Command Prompt (CMD) as an administrator and run the tool by entering `SecureBootUtility`.

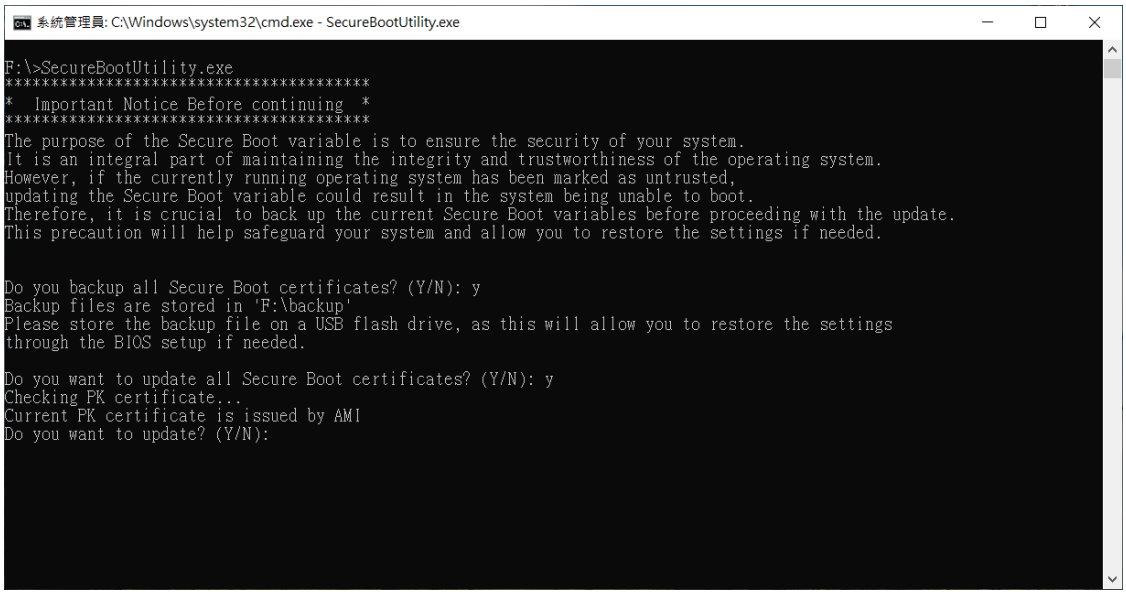


2. **Strongly recommended**: Before the first operation, back up the current Secure Boot variables to an external storage device for future recovery.

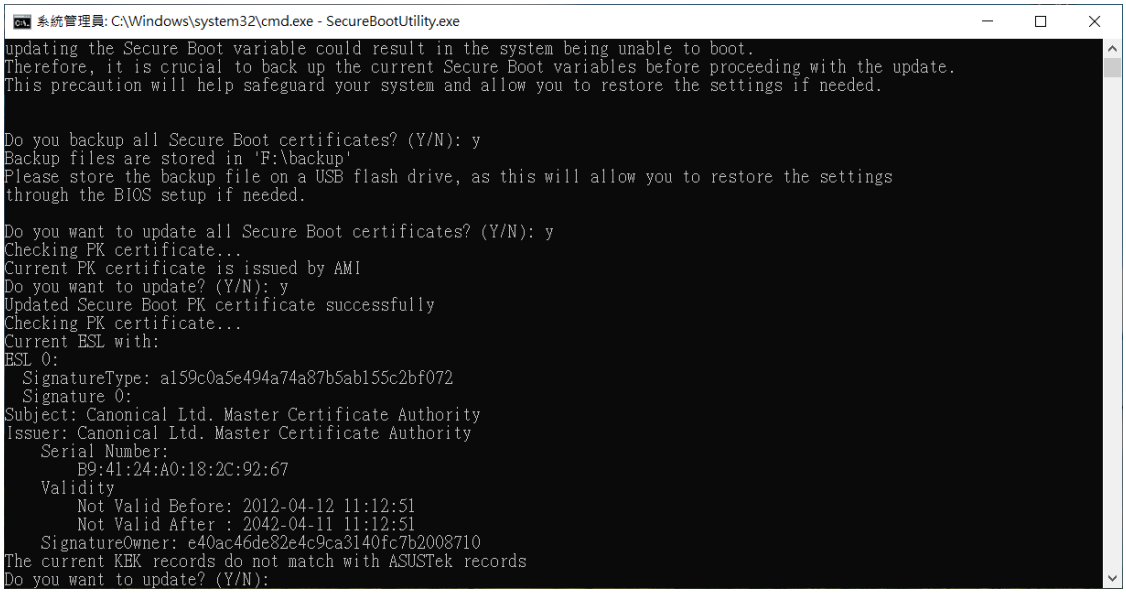


   After backup, the files will be automatically saved in the `backup` folder in the same directory as the tool, including `PK.esl`, `KEK.esl`, `DB.esl`, and `DBX.esl`. Please keep them safe.

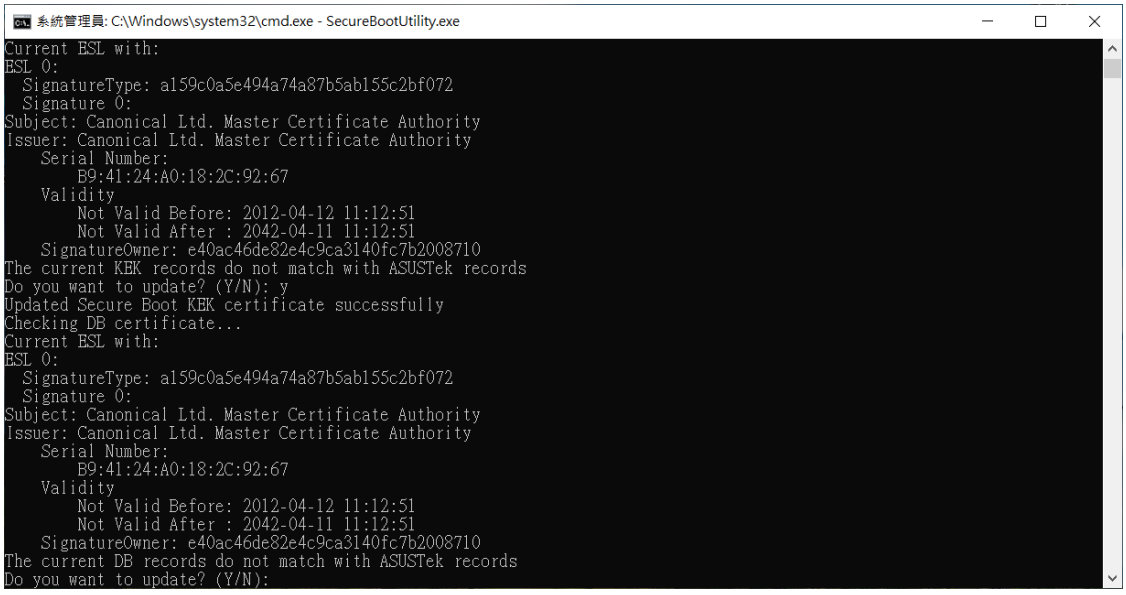
3. During execution, the tool will automatically determine whether PK/KEK/DB need to be updated. If an update is required, detailed differences will be displayed and you will be asked for confirmation before proceeding.



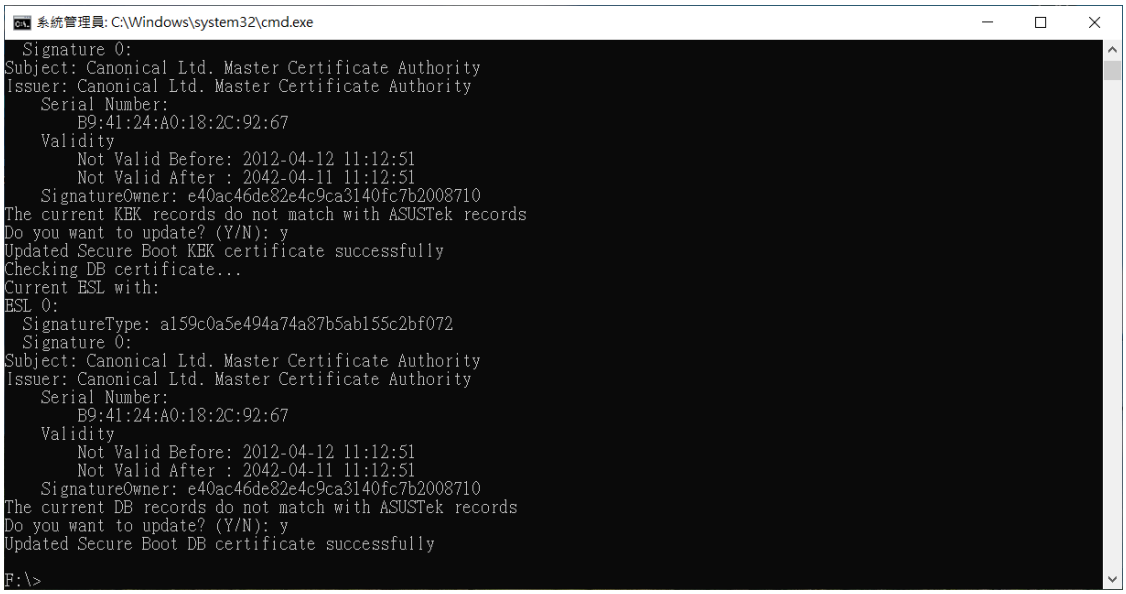
4. KEK is different from PK and DB, and usually contains multiple certificates. If untrusted or expired certificates are detected, the tool will list the abnormal content and prompt for update confirmation.



5. DB may also contain multiple certificates. If any abnormality is detected, a prompt will be shown as well.

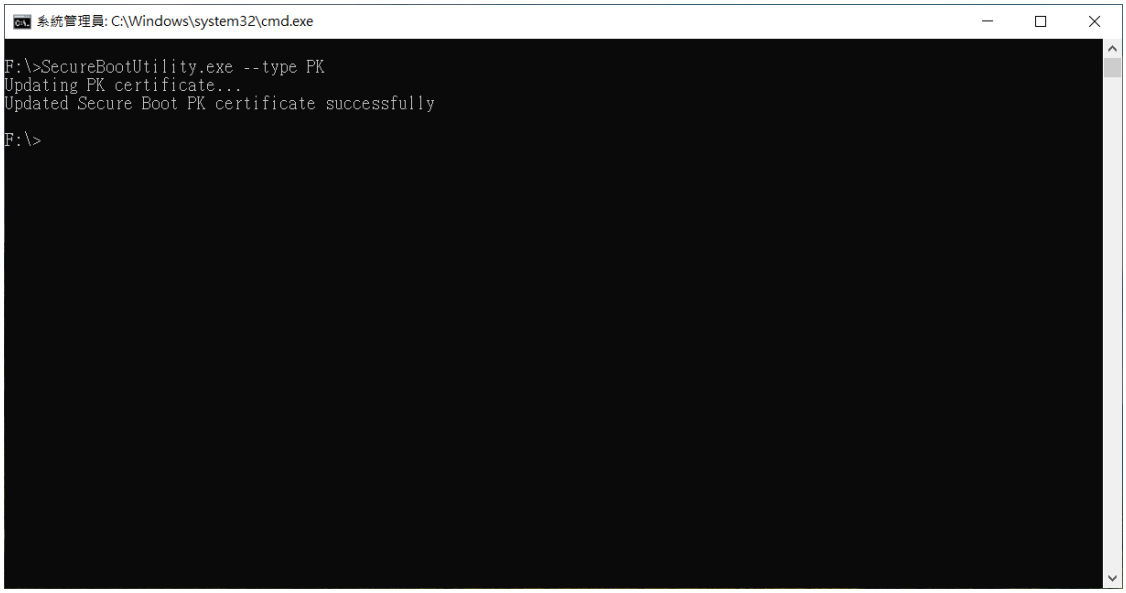


6. If PK/KEK/DB all match ASUS recommended security settings, no update will be performed.



7. To update a specific Secure Boot variable only, add the `--type {PK, KEK, DB}` parameter when running the tool. For example, to update only PK:

```
SecureBootUtility --type PK
```



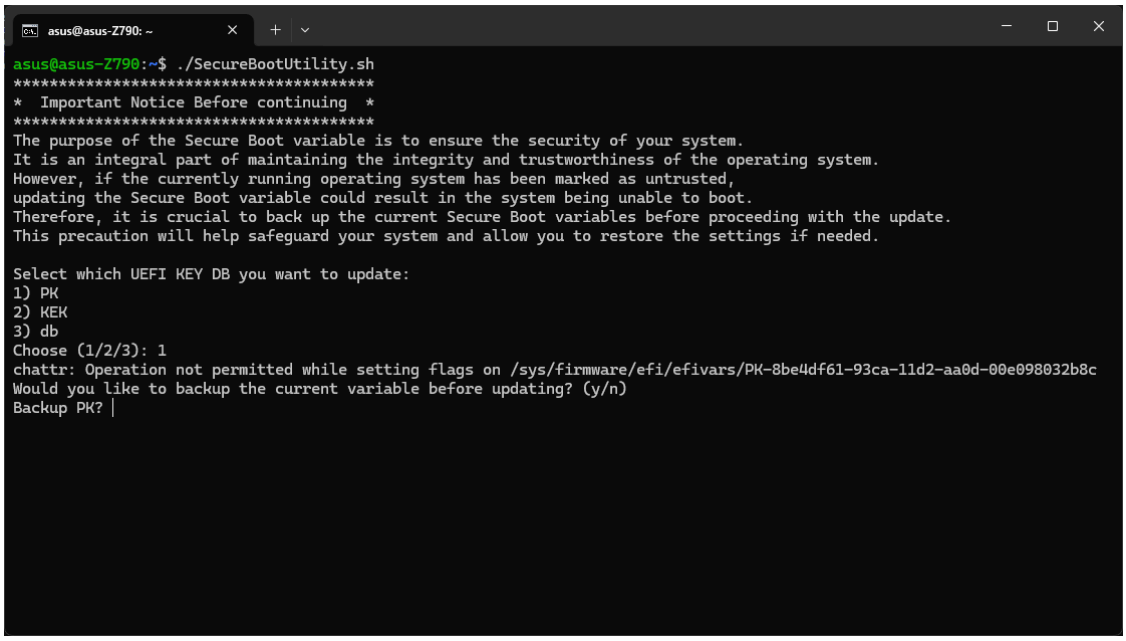
Linux Update Tool

SHA256 (SecureBootUtility.sh):
83c081a3c1e5859dd6819a43a1469d62d984234bfe80b714b86d7154ab6d49fd

Requirements: efi-updatevar package installed, root privileges required

Operation Steps

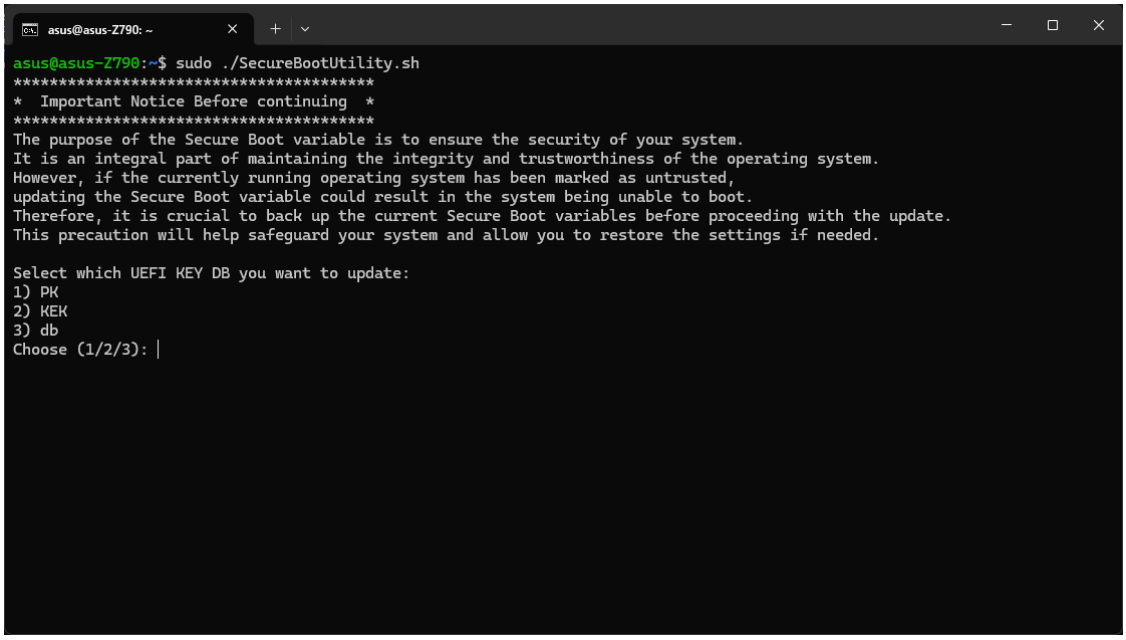
1. Run the tool with root privileges, otherwise you will not be able to modify Secure Boot variables. If insufficient privileges, an error message will appear:



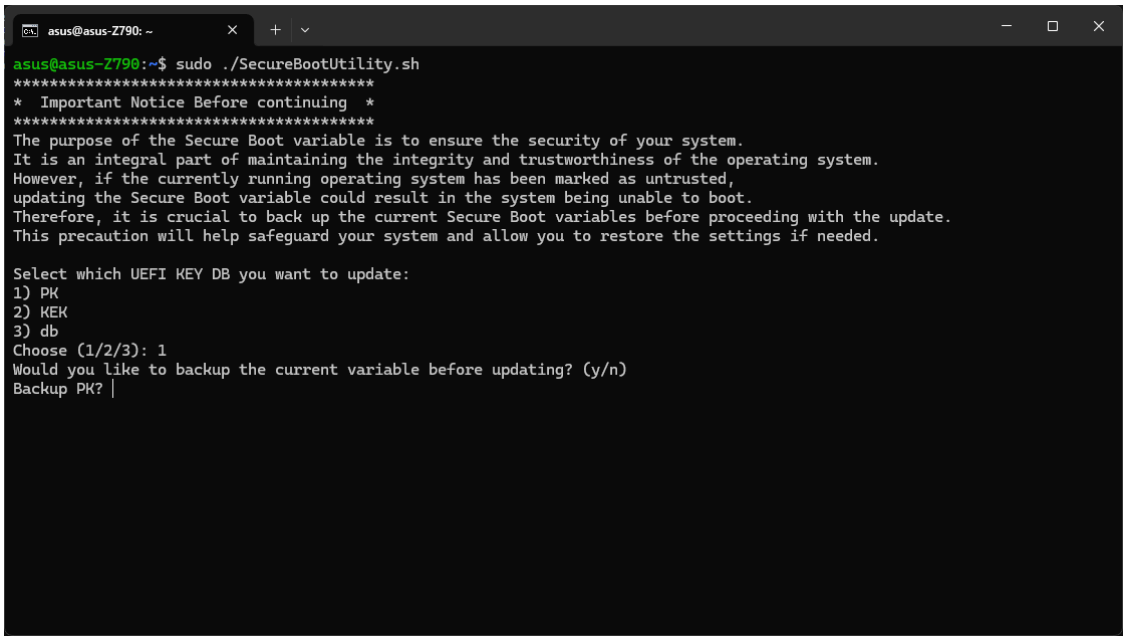
2. It is recommended to use sudo to execute, for example:

   ```
   sudo ./SecureBootUtility.sh
   ```

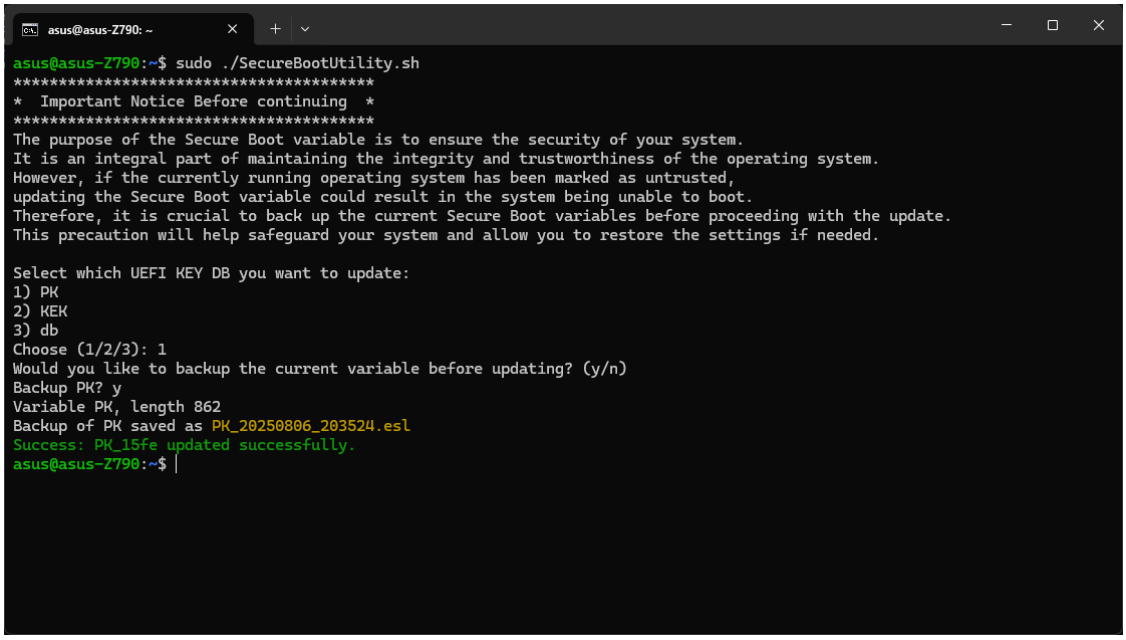
   After execution, follow the on-screen instructions to enter 1/2/3 to select the variable to update (PK/KEK/DB).

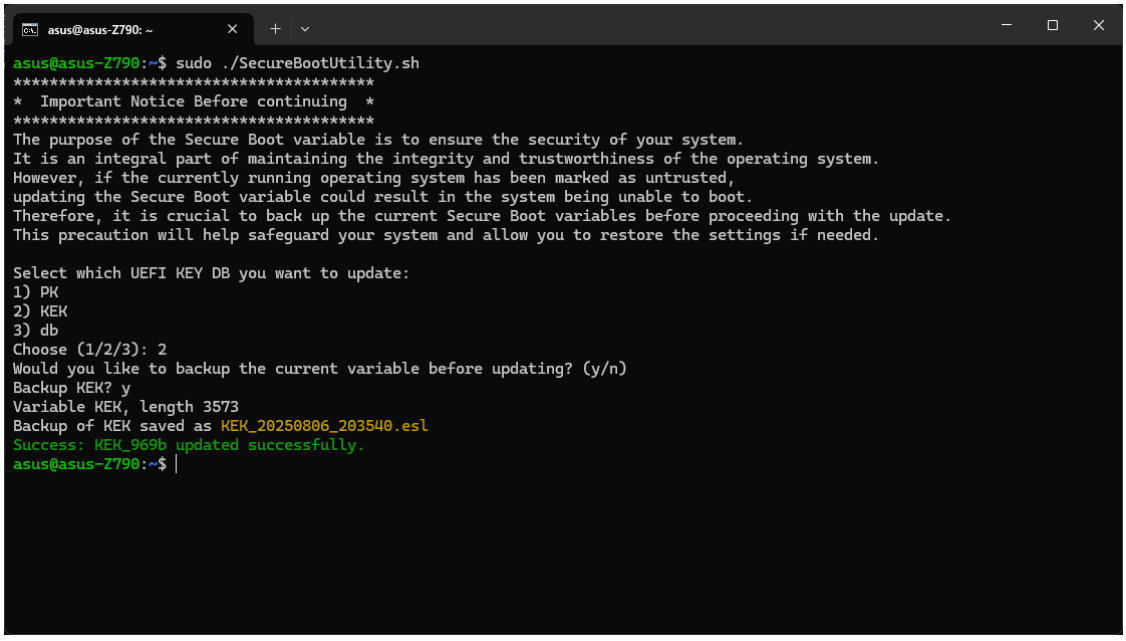


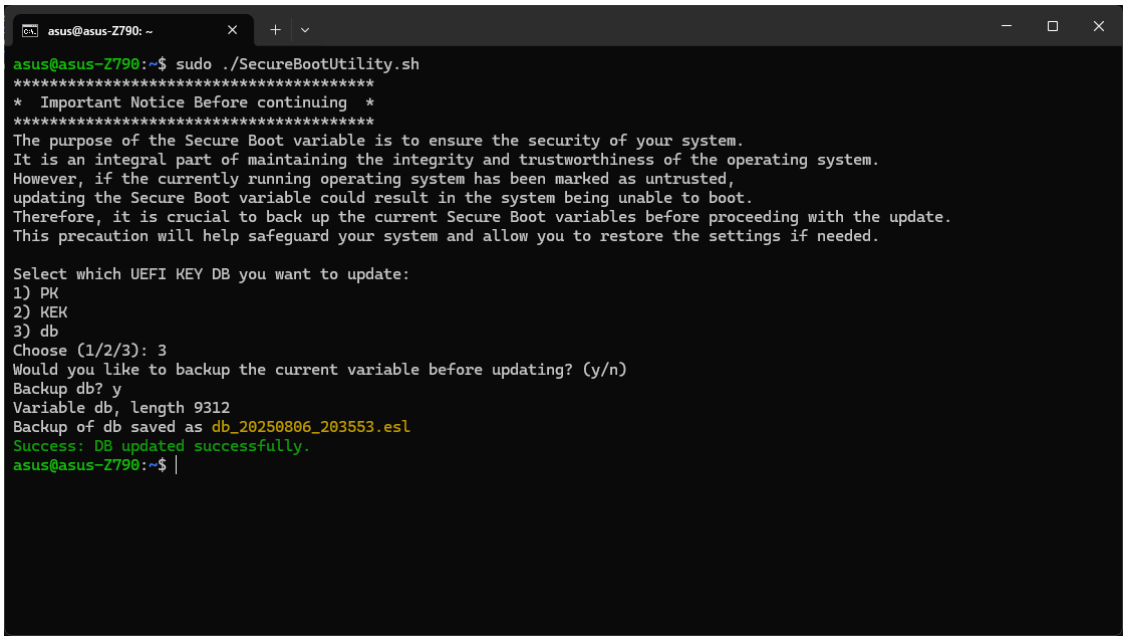
3. **Strongly recommended**: Before operation, back up the current variables to an external storage device for future recovery.



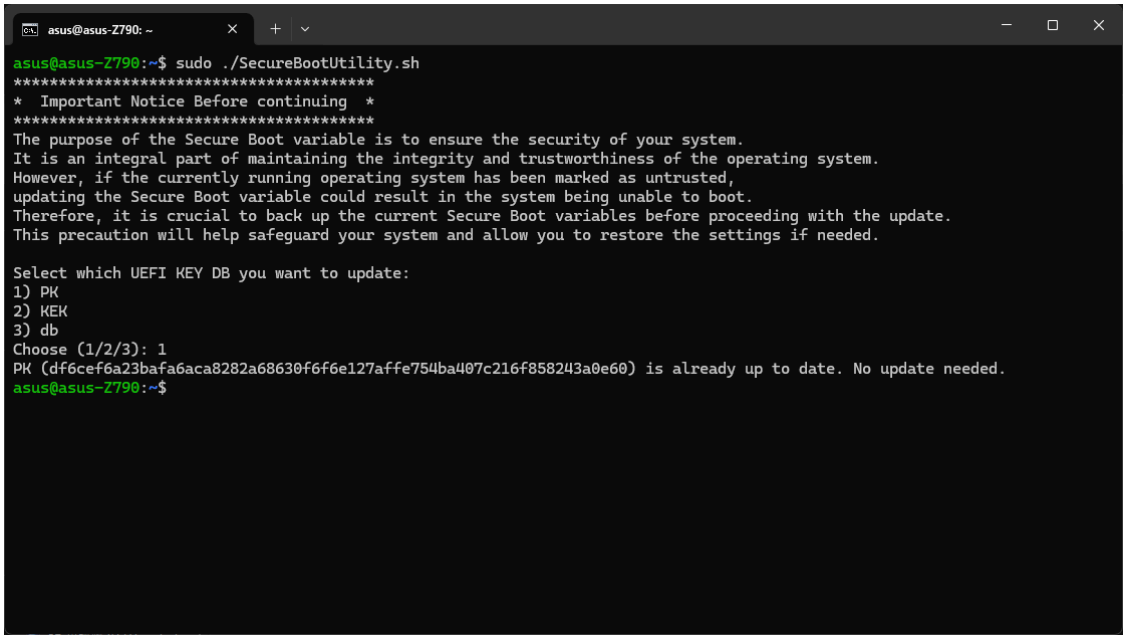
4. After choosing whether to back up, the tool will automatically perform the backup and update process.







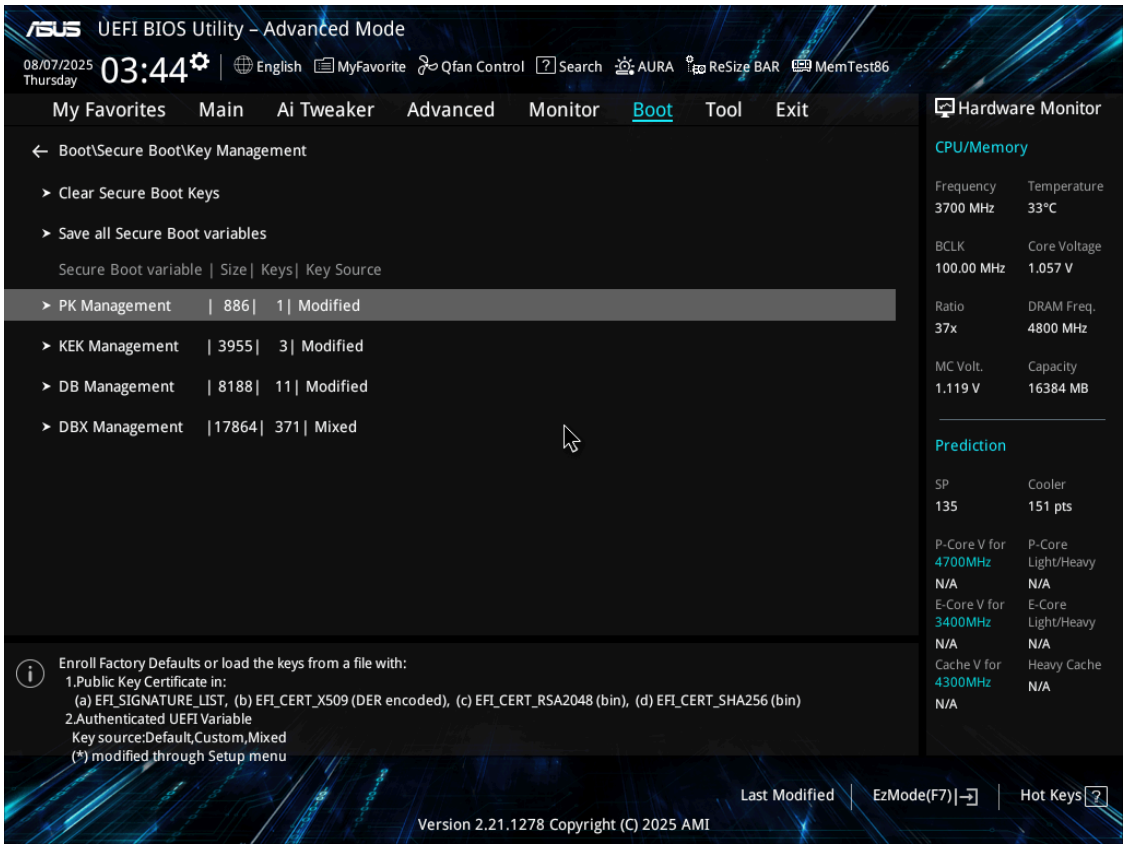
5. If the current variable content already matches the recommended settings, a "No update needed" message will be displayed.



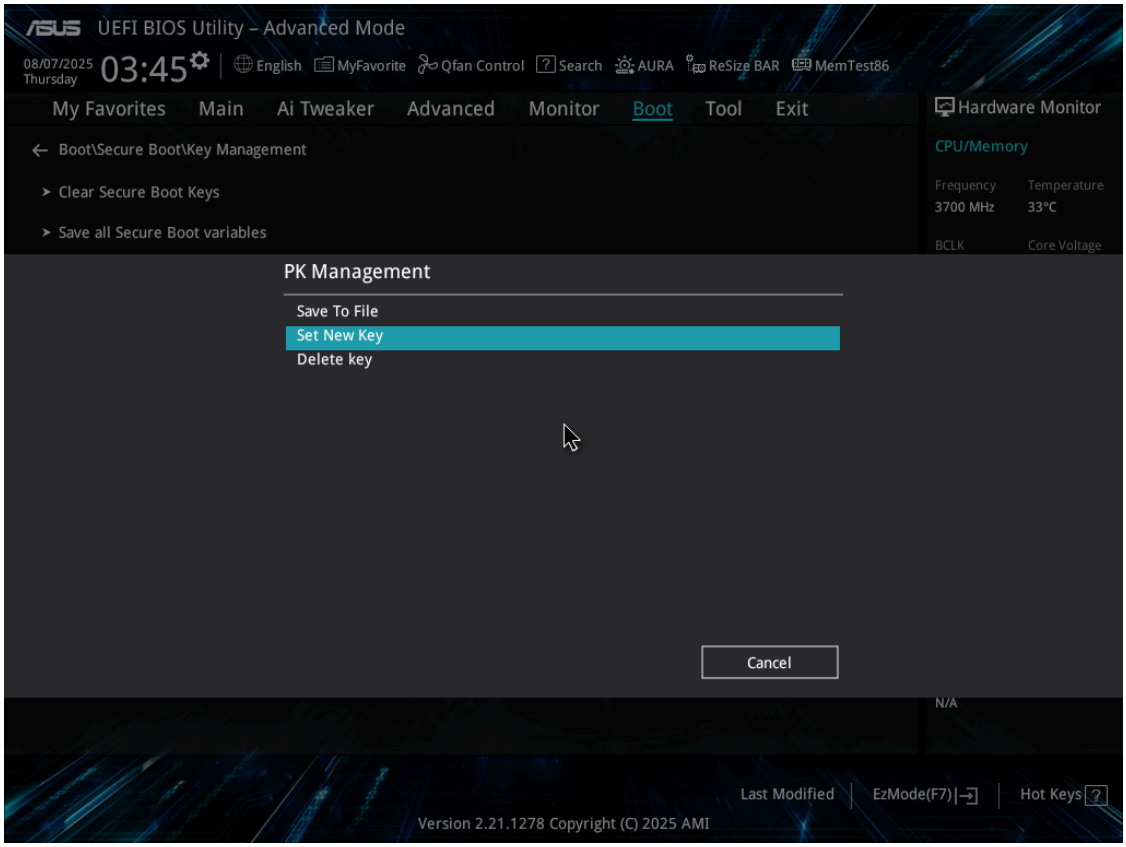
Recovery Steps

1. Files backed up by this tool can only be restored via the BIOS setup interface. Please refer to the product manual.

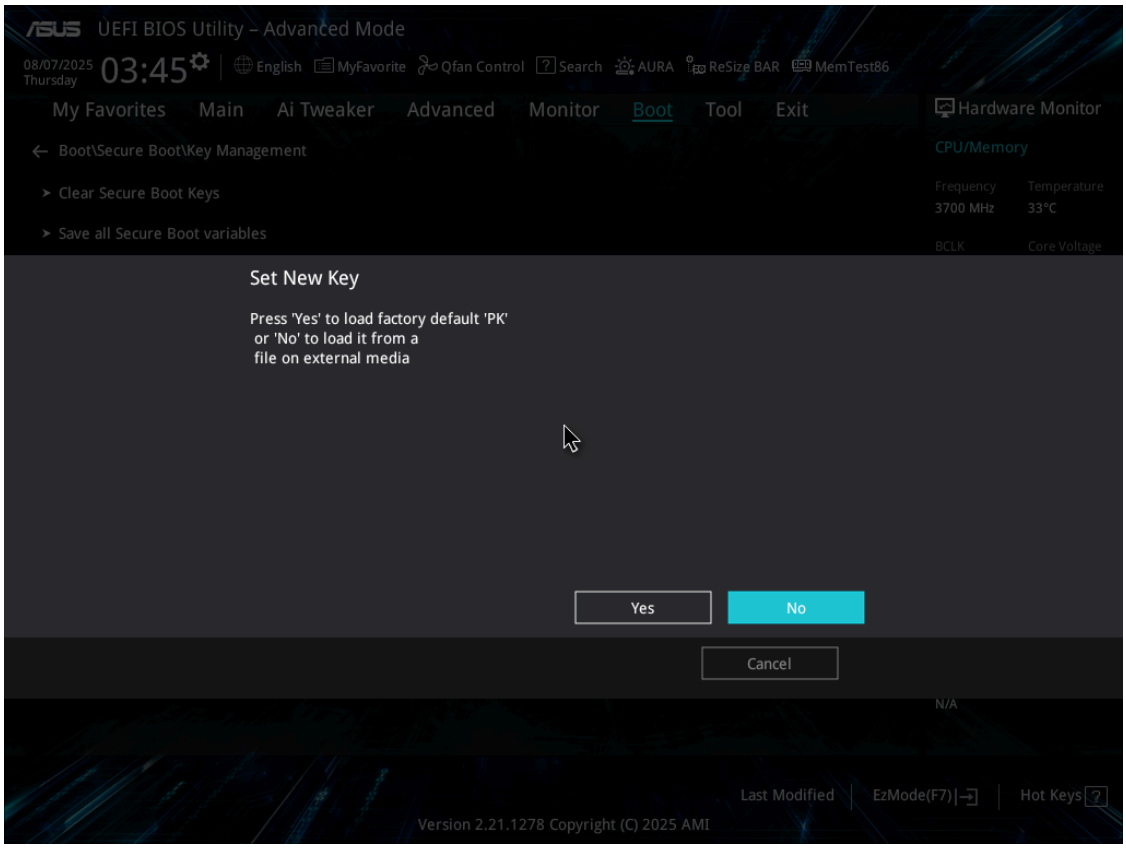
2. Enter BIOS, select the variable to restore and press `Enter` (example: PK):



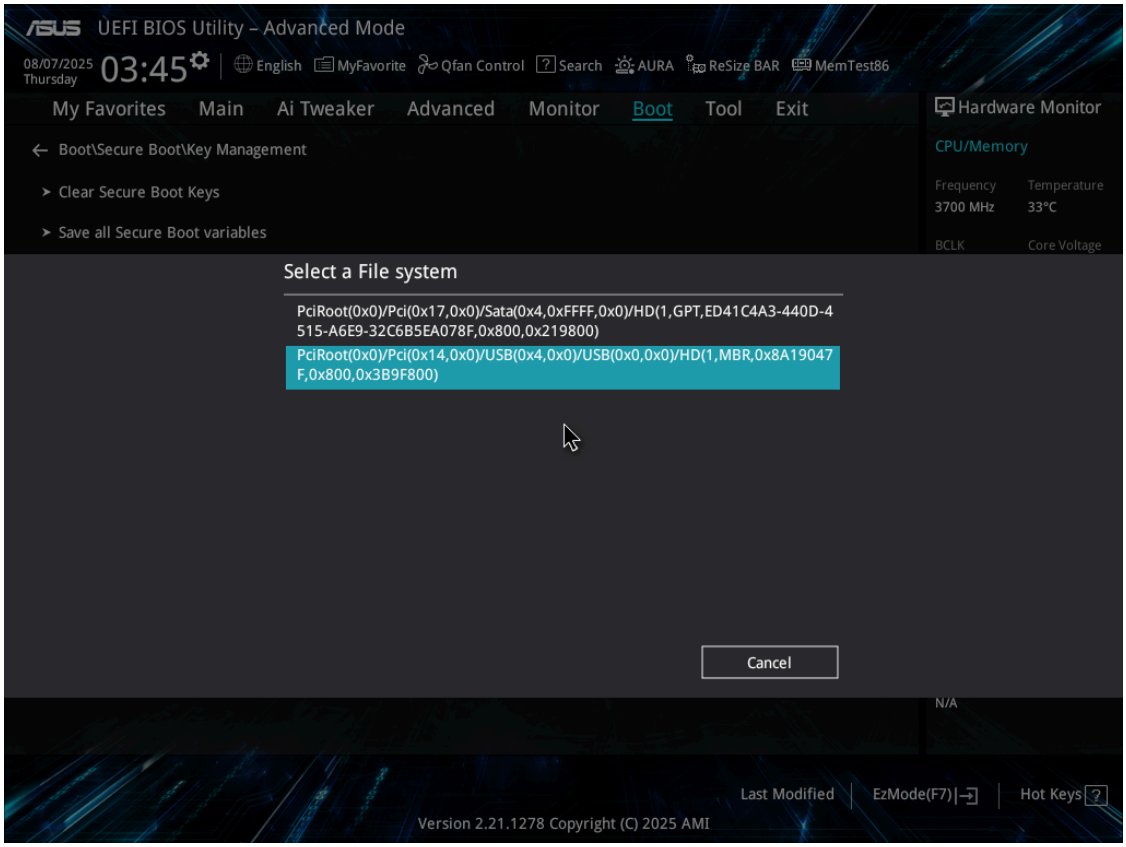
3. Select Set New Key to restore the backup setting.



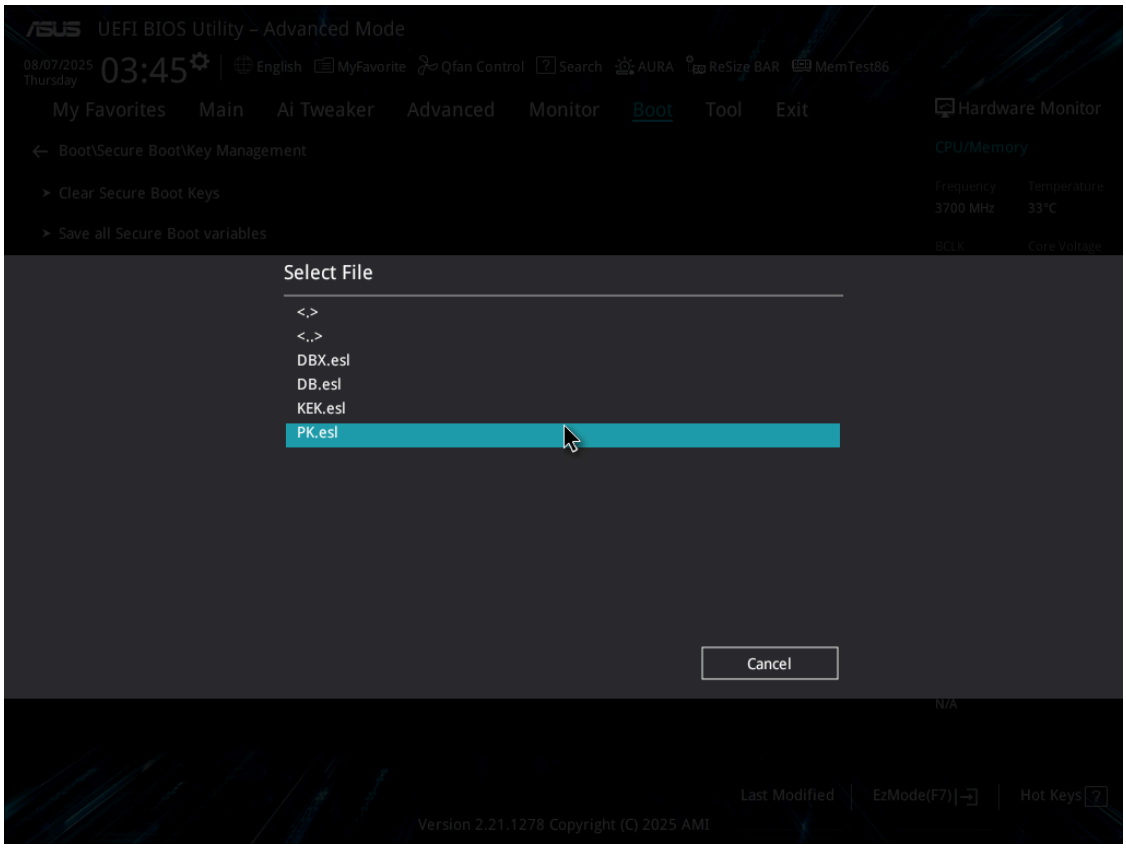
4. Select No (depending on the situation).



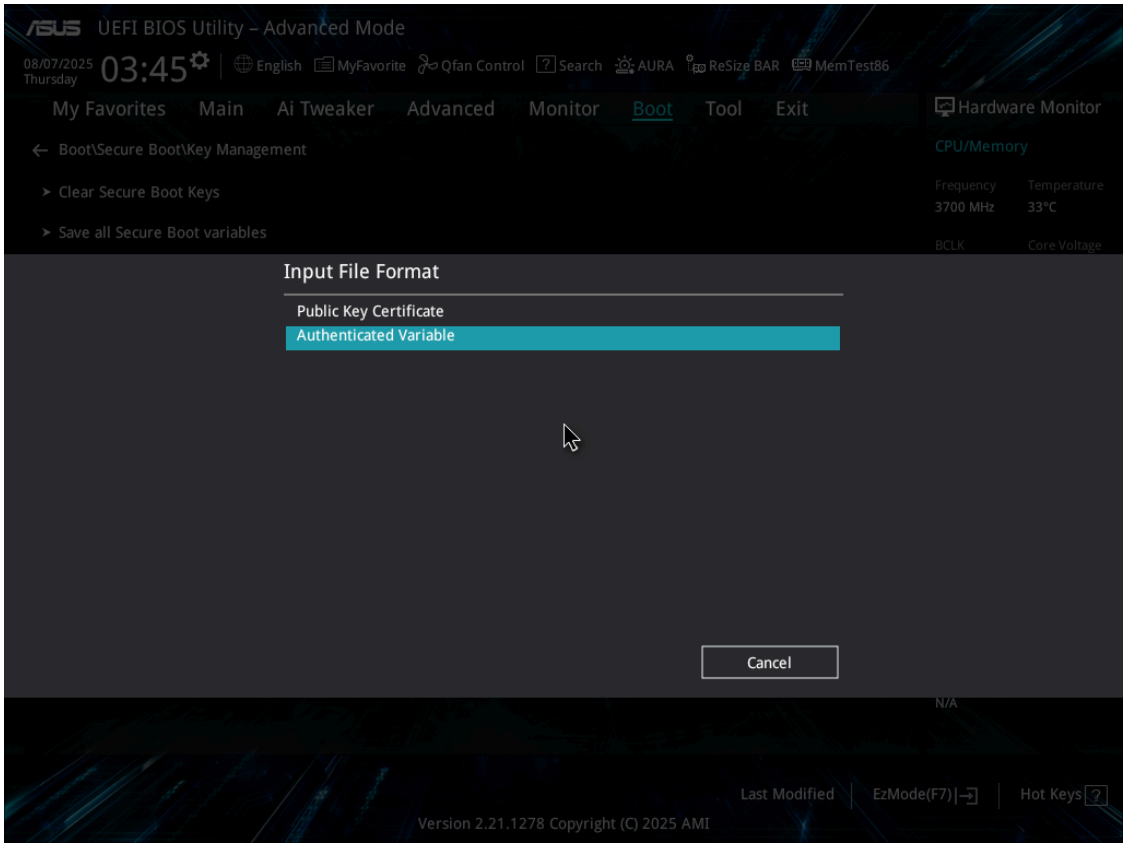
5. Select the storage device containing the backup file.



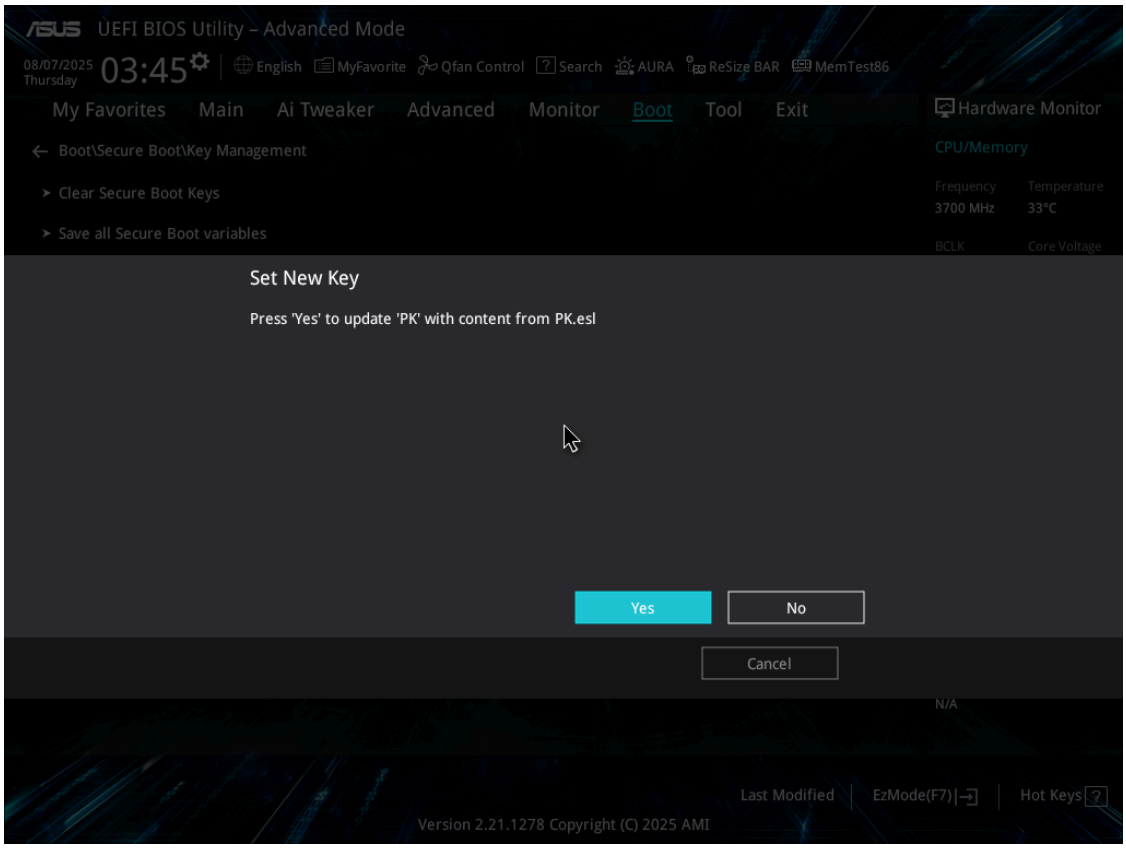
6. Select the previously backed up file (for PK, select `PK.esl`).



7. Select `Authenticated Variable`.



8. Select `Yes` to continue the update.



9. After a successful update, repeat the process to restore KEK/DB and other variables as needed.

