Advantech AE Technical Share Document

Date	2026/06/12	**Release Note**	☐ Internal ■ External
Category	■ FAQ ☐ SOP	**Related OS**	Windows 10 IoT Enterprise LTSC 2021 (21H2) or later; Windows 11
Abstract	This SOP describes the procedure for updating and verifying Microsoft Secure Boot 2023 certificates on Windows-based systems. The purpose of this document is to ensure system compatibility with Microsoft Secure Boot certificate migration requirements before the 2026 certificate expiration. This SOP includes Secure Boot key rollout procedures, verification methods, and related precautions for UEFI Secure Boot environments.		
Keyword	Secure Boot, UEFI, Microsoft CA 2023, KEK, DB, DBX, Secure Boot Migration, Windows 10, UEFI Variable, Certificate Update		
Related Product	POC-421/424 12th, POC-421/424 14th , POC-621/624 11th, POC-821/824 13th, HIT-515/518, USM-100H, USM-300 13th, USM-500 Gen2		

■ Background and Risk Description:

Microsoft Secure Boot certificates signed in 2011 will begin to expire starting in 2026. To maintain Secure Boot functionality and system security compliance, Microsoft has introduced new Secure Boot certificates signed by the 2023 Certificate Authority (CA).

Systems that continue using legacy Secure Boot certificates may encounter boot validation issues, Secure Boot incompatibility, or recovery media boot failures after future Microsoft Secure Boot policy updates.

This FAQ provides the procedure for deploying and verifying Microsoft Secure Boot 2023 certificates on supported Windows platforms. The document also includes related precautions and validation methods for UEFI Secure Boot environments.

■ Applicable Conditions

- System is configured in UEFI boot mode
- Secure Boot is enabled in BIOS
- Supported Windows operating system is installed
- Latest Windows cumulative updates are installed
- Administrator privilege is required
- Secure Boot update components are available in the OS

■ Preliminary Check

Before performing the Secure Boot CA 2023 migration procedure, verify the following conditions:

- System is configured in UEFI boot mode
- Secure Boot is enabled in BIOS
- Windows cumulative updates are installed
- Administrator privilege is available

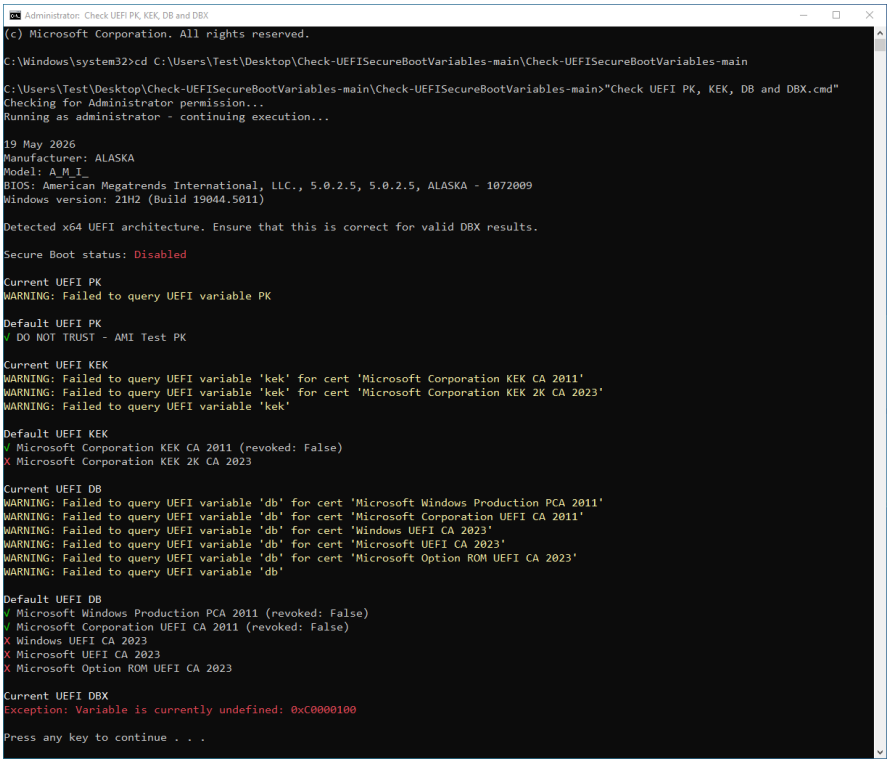
■ Required Tools and Conditions

Download the Secure Boot verification tool from Github:
https://github.com/cjee21/Check-UEFISecureBootVariables/archive/refs/heads/main.zip

■ Migration Procedure - Step by Step:

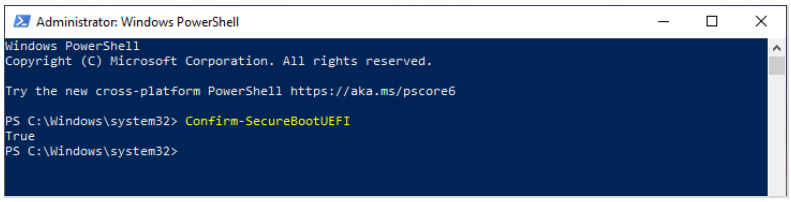
Verify Current Secure Boot Key Status

1. Run “Check UEFI PK, KEK, DB and DBX.cmd” from the downloaded “Check-UEFISecureBootVariables” package with administrator privilege.
2. Verify whether Microsoft Secure Boot 2023 certificates are already present in Current UEFI KEK and Current UEFI DB.
3. If the system has not completed the Secure Boot 2023 migration, the following conditions may be observed:
   - Secure Boot is disabled
   - Microsoft Secure Boot 2023 certificates are not present in Default UEFI KEK and Default UEFI DB

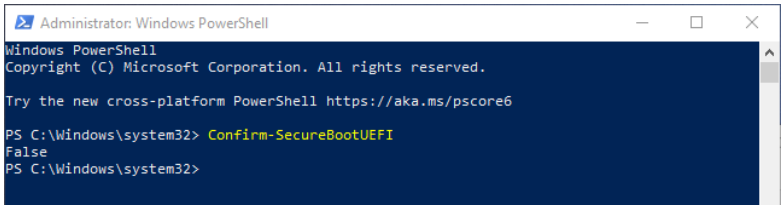


Confirm Secure Boot is enabled

1. Open Windows PowerShell with administrator privilege.
2. Run the following command:
   Confirm-SecureBootUEFI
3. The result should return:
   True

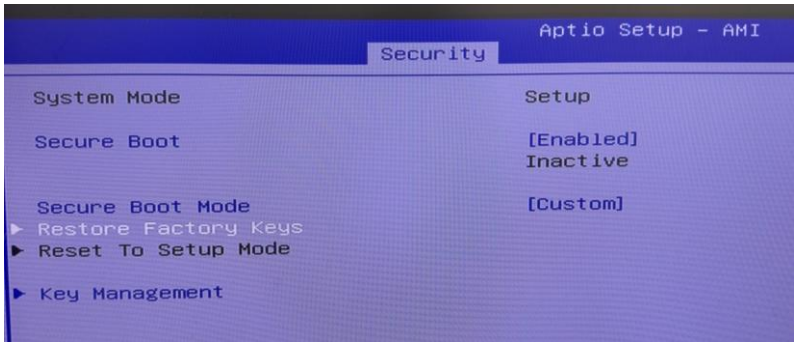


4. If the result is False, enable Secure Boot in BIOS before continuing the migration procedure.

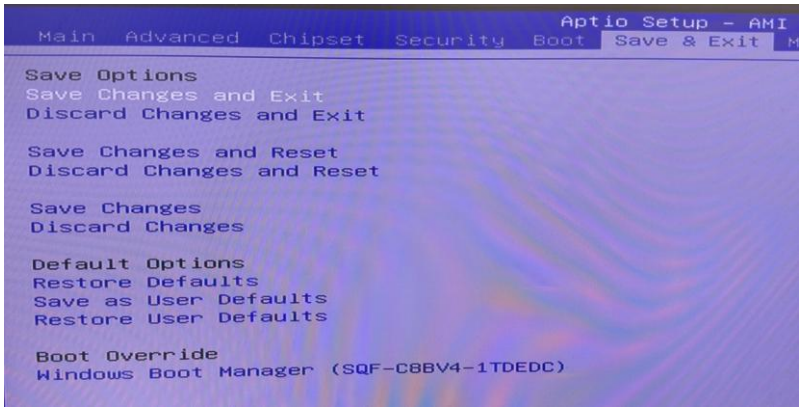


Verify Secure Boot settings

1. Enter BIOS Setup and configure the following Secure Boot settings:
   - Secure Boot = Enabled
   - Secure Boot Mode = Custom
2. Select “Restore Factory Keys” to enroll the default Secure Boot key database.

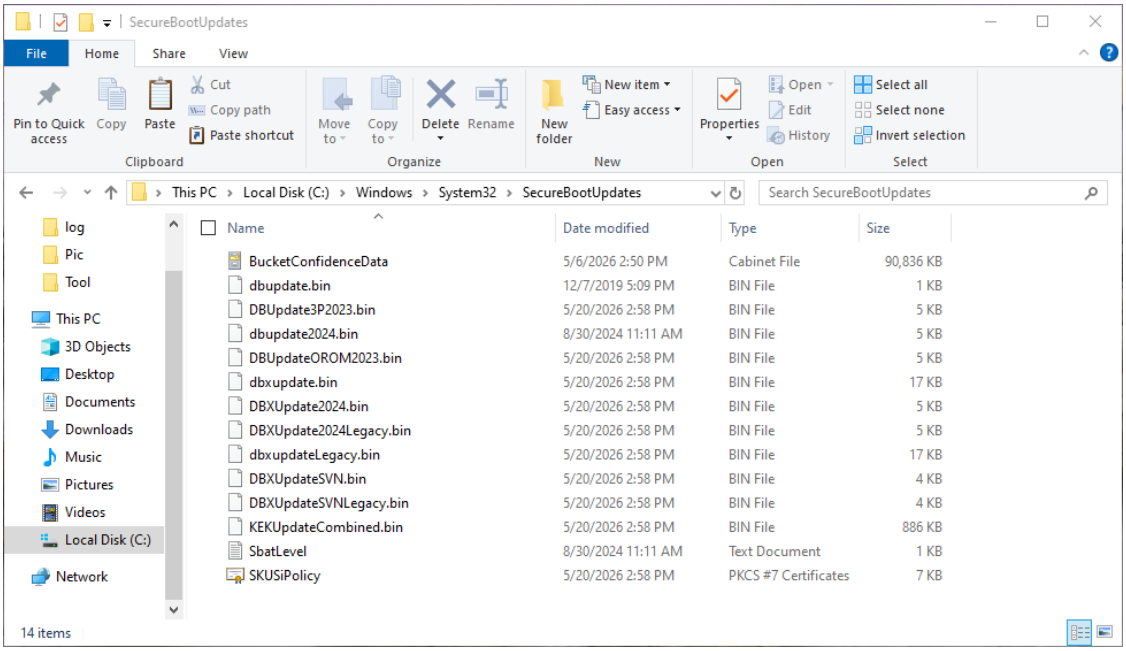


3. Go to ‘Save & Exit’ and choose ’Save Changes’, then choose ’Save Changes and Exit’



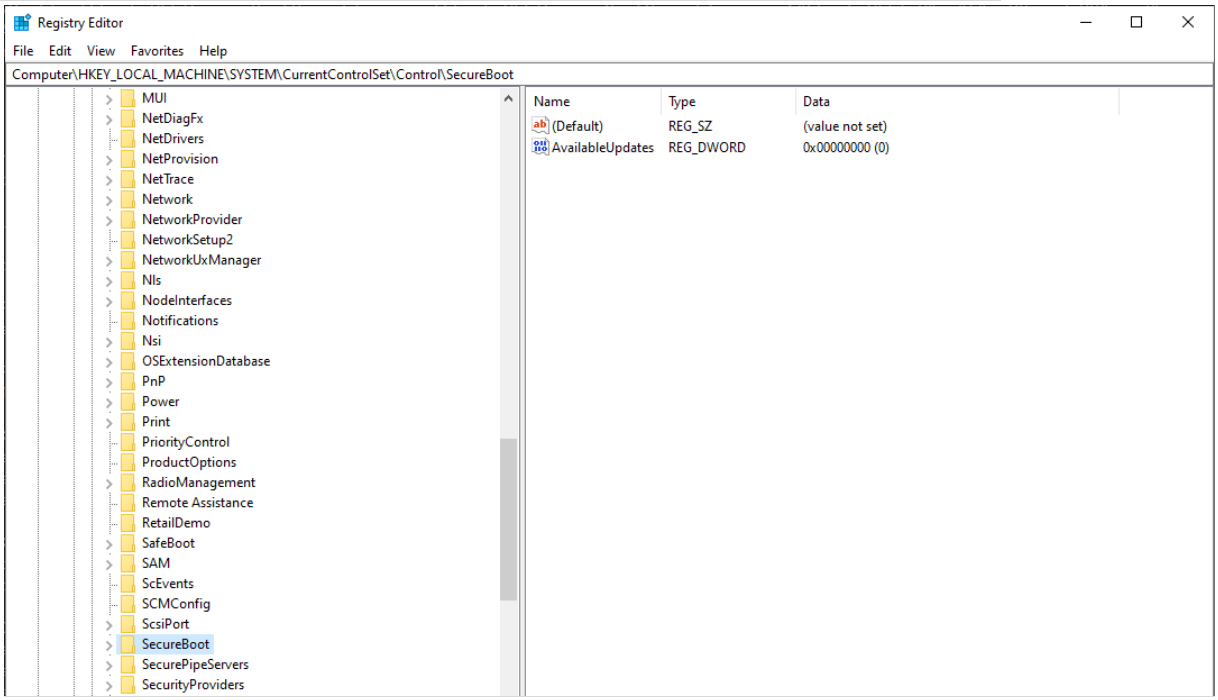
Verify Secure Boot Update Packages

1. Ensure the system has installed the latest Microsoft Windows updates.
2. Navigate to the following directory:
   C:\Windows\System32\SecureBootUpdates
3. Verify that Secure Boot update packages are present in the directory.

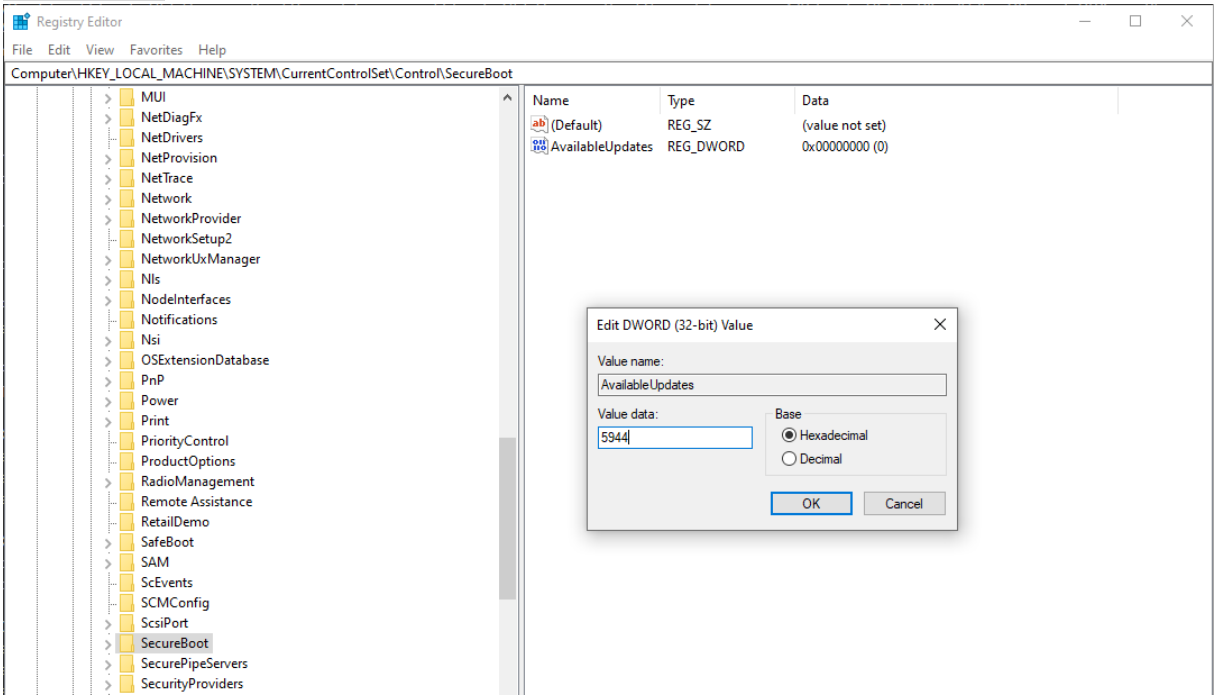


Configure Microsoft Secure Boot 2023 certificates

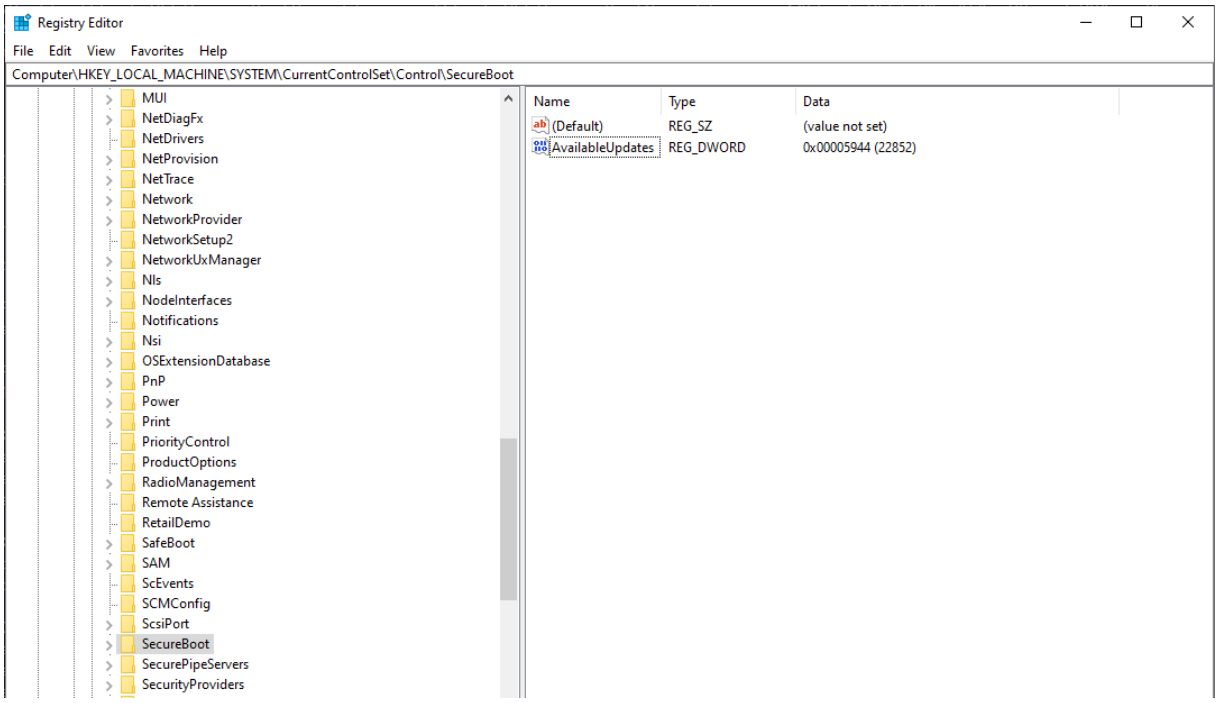
1. Open the Windows Registry Editor.
2. Navigate to the following registry path:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot



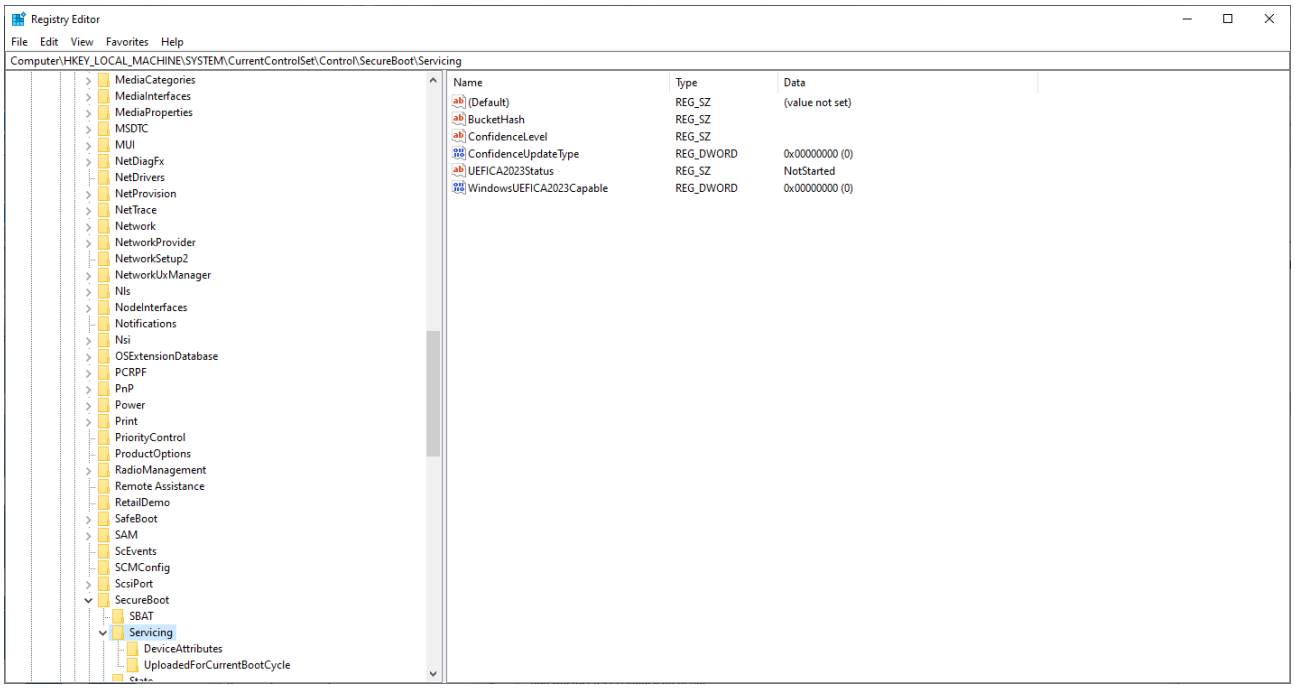
3. Modify the following registry value:
   Name: AvailableUpdates
   Value: 5944



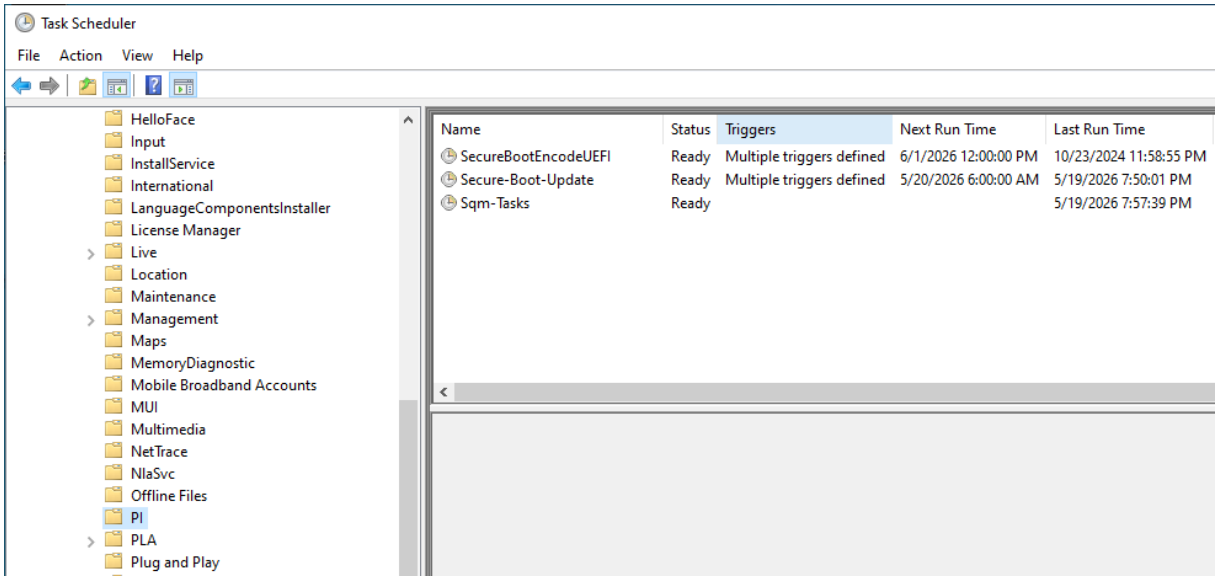
4. Press OK to save the setting.



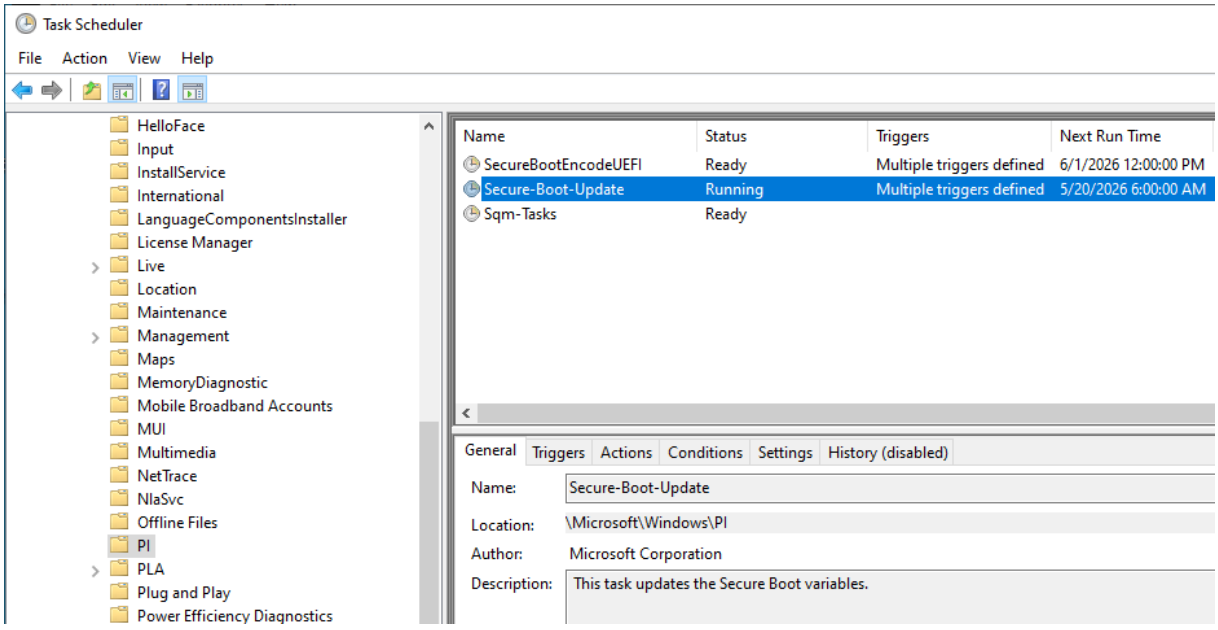
5. Navigate to the following registry path:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing
check the value of "UEFICA2023Status" first. The status may still show "NotStarted".



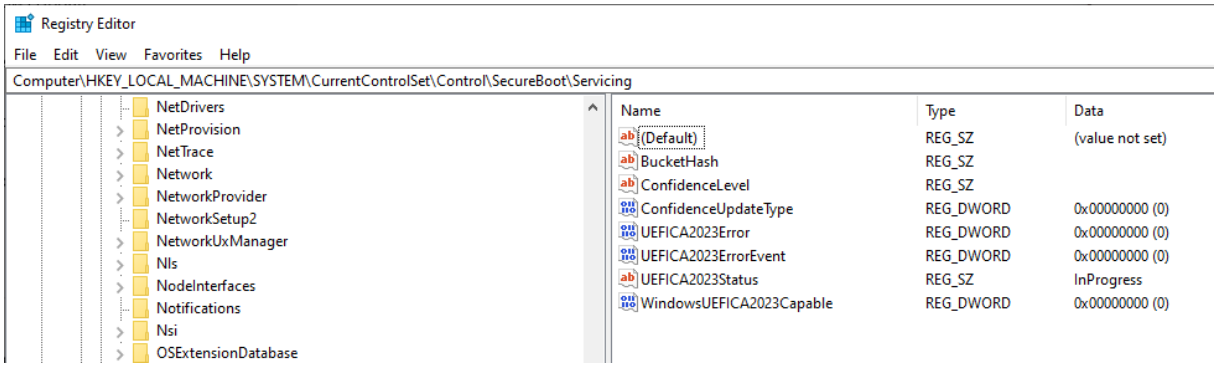
6. Open ‘Task Scheduler’ and navigate to:
   Task Scheduler Library → Microsoft → Windows → PI
7. Right-click the following task and select “Run”
   Secure-Boot-Update



8. The status will be changed to ‘Running’.

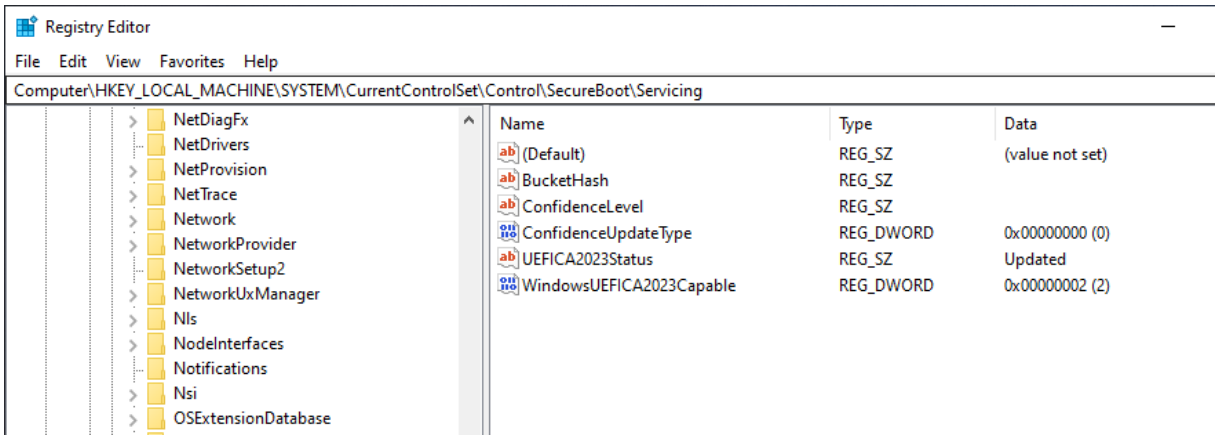


9. Navigate to the following registry path again:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing
   Check the value of "UEFICA2023Status". The status may show "InProgress",
   which indicates that the Secure Boot 2023 update process is currently running.
   If the status does not change immediately, wait a few minutes and reopen the registry to check the status again. Restart the system twice.

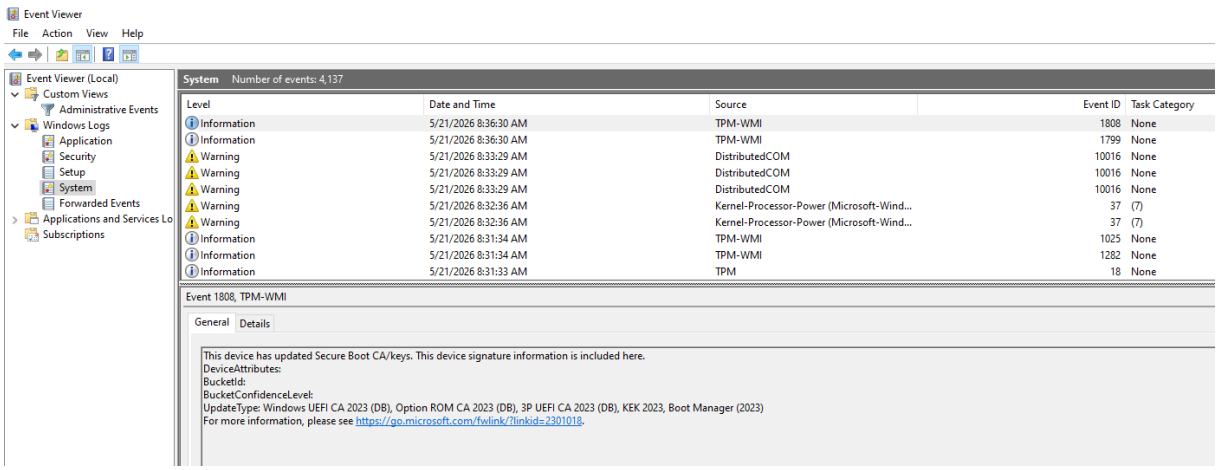


   If the value of "UEFICA2023Status" still does not change to "Updated" after several minutes and multiple system restarts, repeat Steps 1 through 10 and perform the migration procedure again.

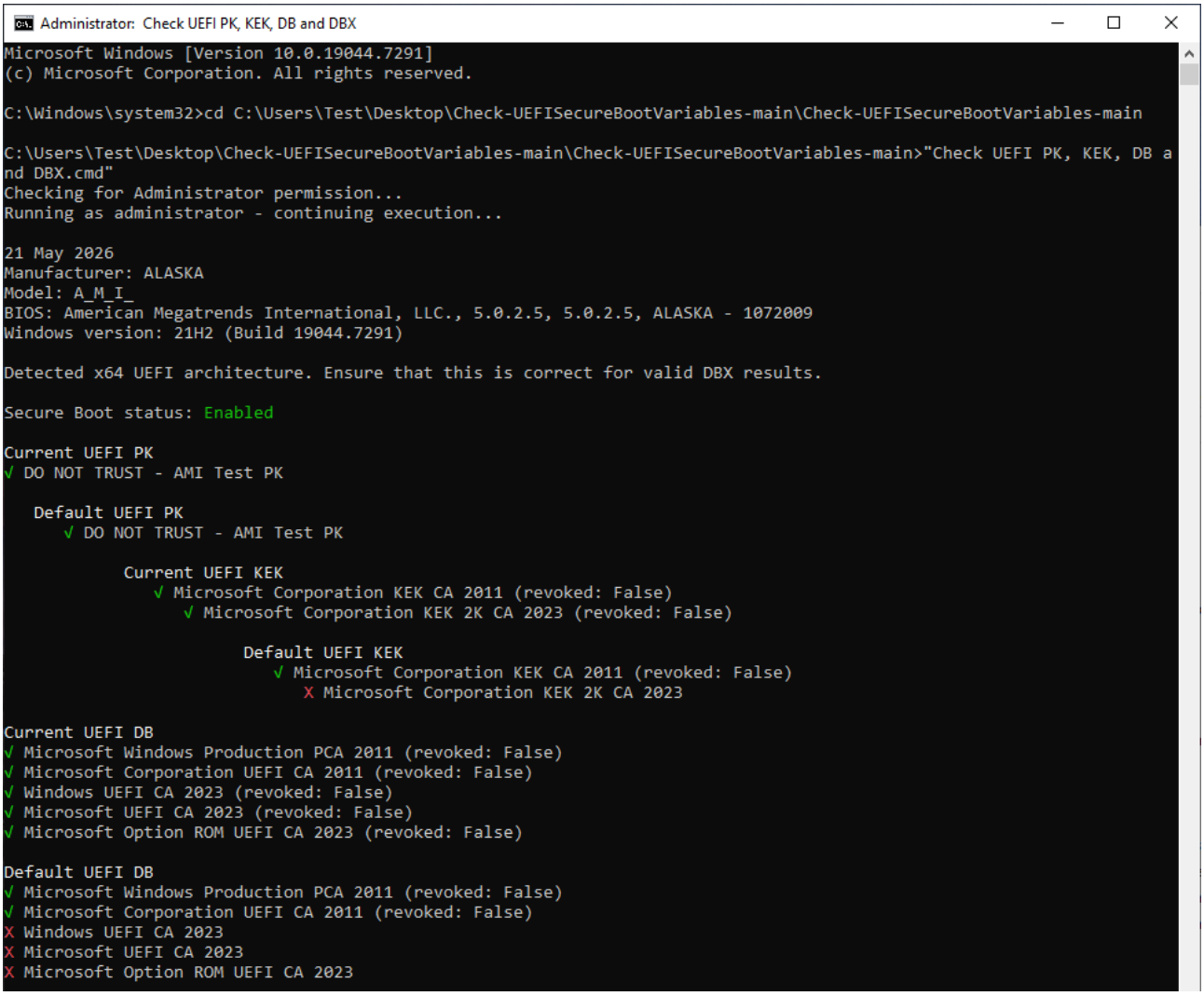
10. If the migration is completed successfully, the Data field of 'UEFICA2023Status' will change to "Updated".



11. Open Event Viewer and check System logs for Event ID 1808. The event indicates that the Secure Boot CA/key update process has completed successfully.



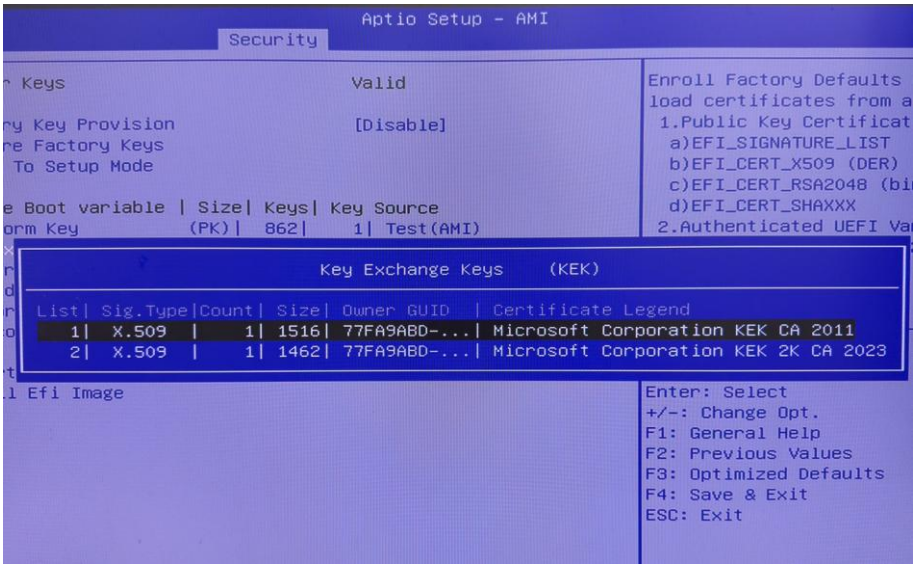
12. Run “Check UEFI PK, KEK, DB and DBX.cmd” again with administrator privilege.
    Verify that the following Microsoft Secure Boot 2023 certificates are present in Current UEFI KEK and Current UEFI DB:
    - Microsoft Corporation KEK 2K CA 2023
    - Windows UEFI CA 2023
    - Microsoft UEFI CA 2023
    - Microsoft Option ROM UEFI CA 2023



13. Enter BIOS Setup and navigate to the Secure Boot Key Management page.
    Verify that the following Secure Boot certificates are present in the BIOS database:

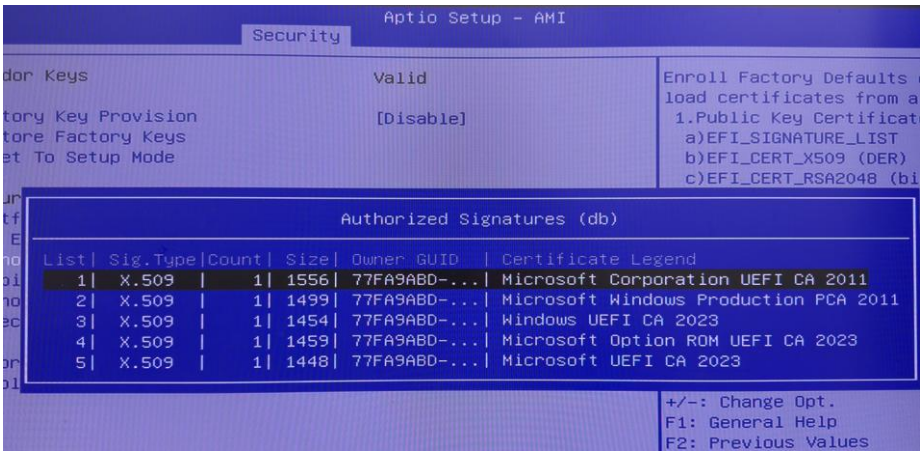
Key Exchange Keys (KEK)

- Microsoft Corporation KEK CA 2011
- Microsoft Corporation KEK 2K CA 2023



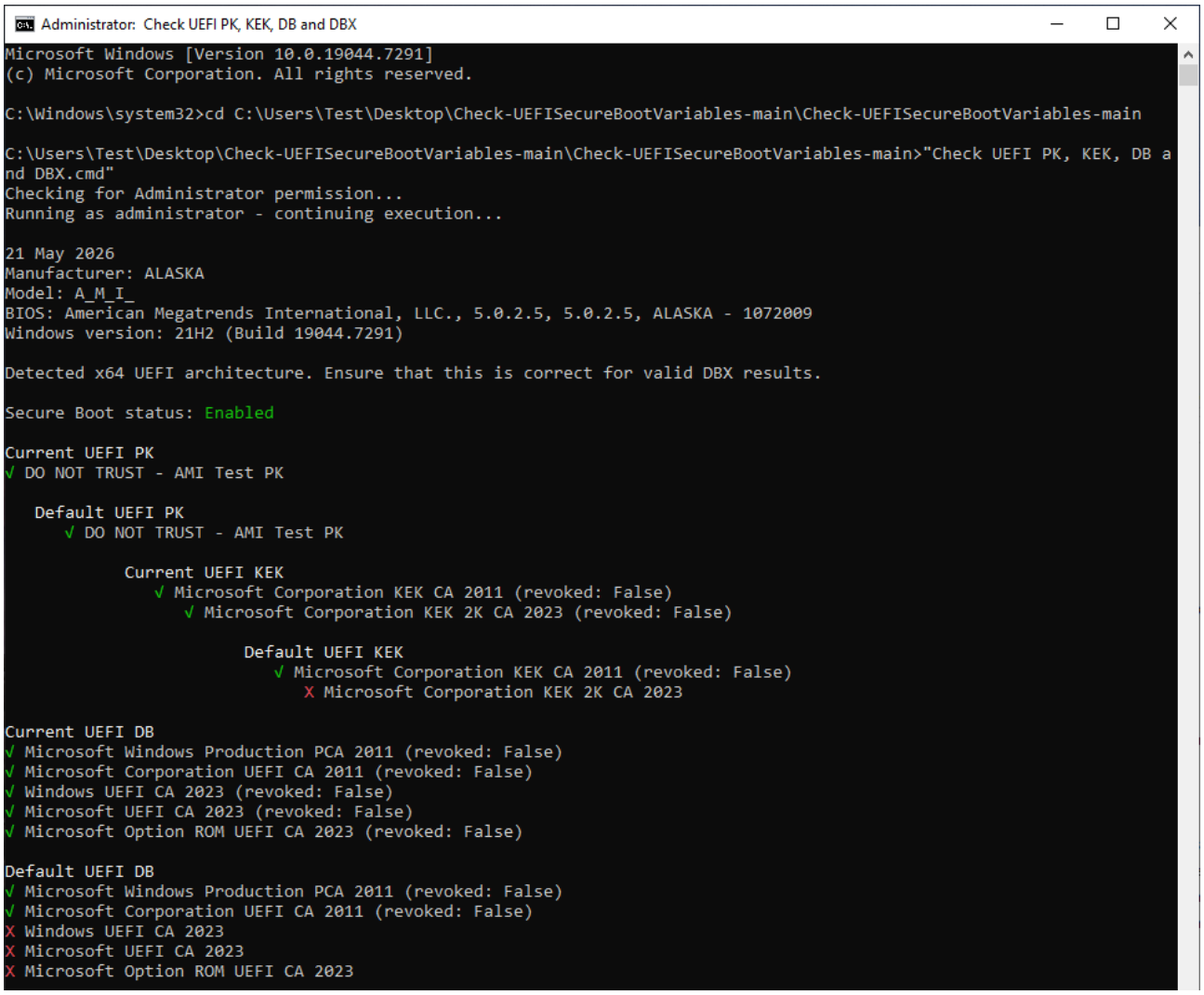
Authorized Signatures (db)

- Microsoft Corporation UEFI CA 2011
- Microsoft Windows Production PCA 2011
- Windows UEFI CA 2023
- Microsoft Option ROM UEFI CA 2023
- Microsoft UEFI CA 2023

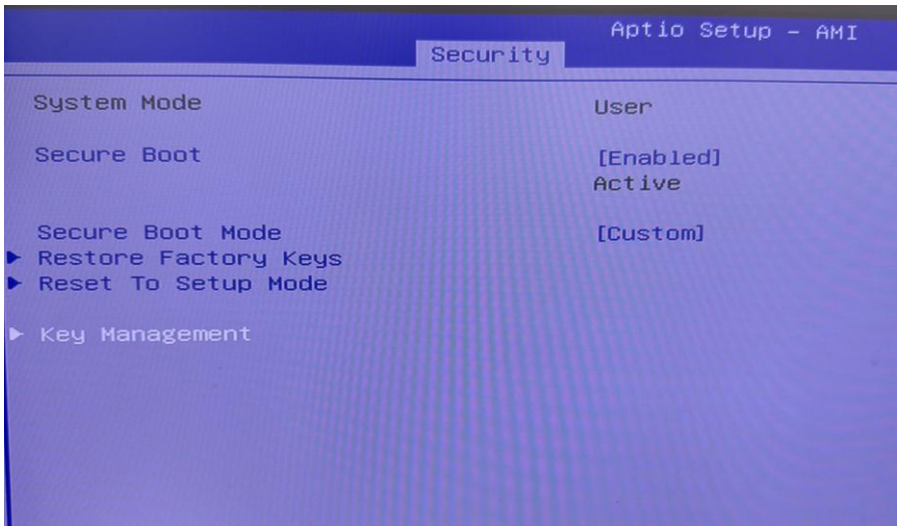


Replace AMI test PK with Advantech PK, KEK, DB

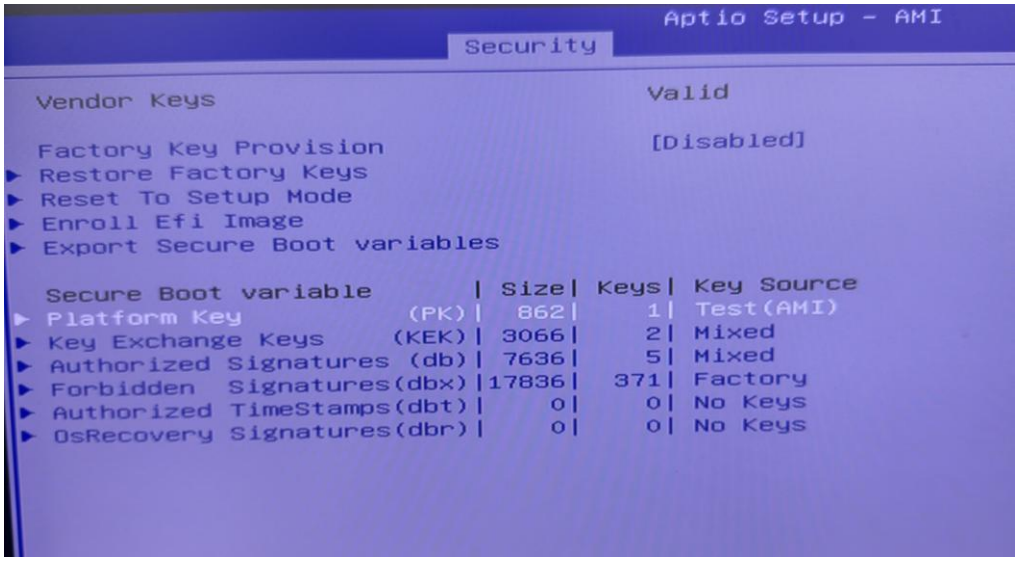
1. Put Advantech PK, KEK, DB into USB flash.
2. Power on system and enter the OS. Run “Check UEFI PK, KEK, DB and DBX.cmd” with administrator privilege.
   The Default UEFI PK is ‘AMI Test PK’



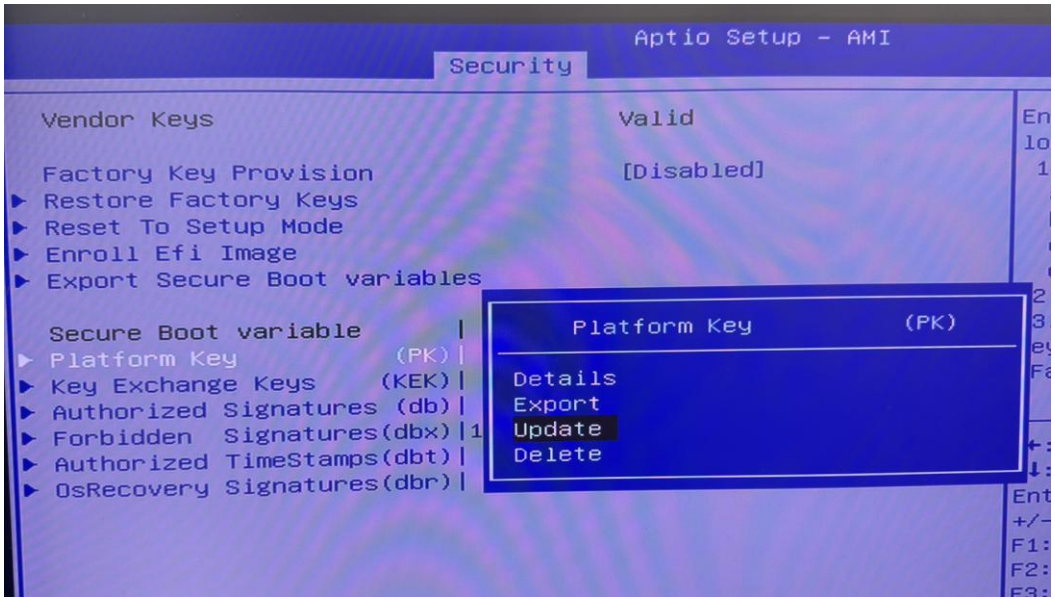
3. Go to BIOS setup menu -> Security tab.



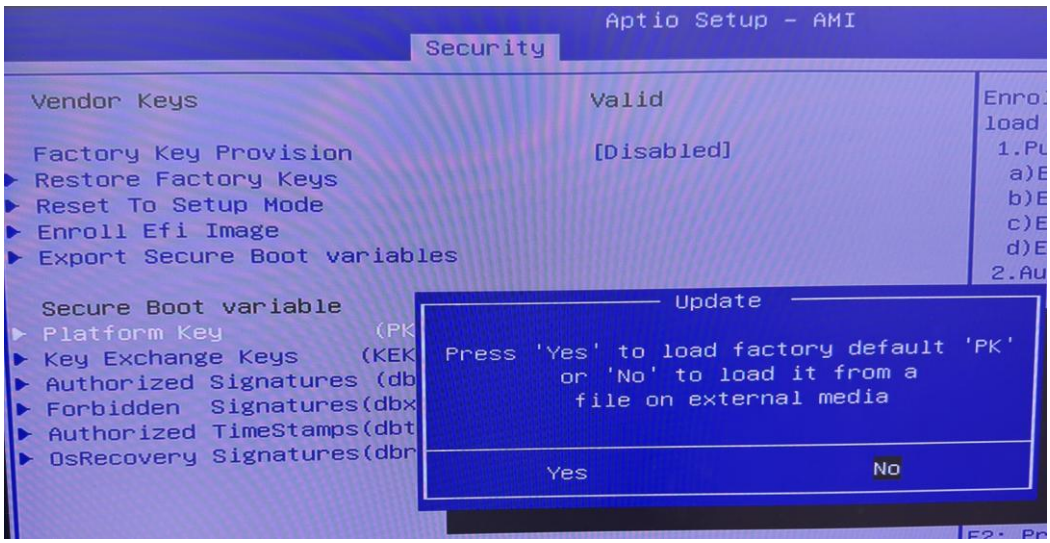
4. Choose ‘Platform Key’.



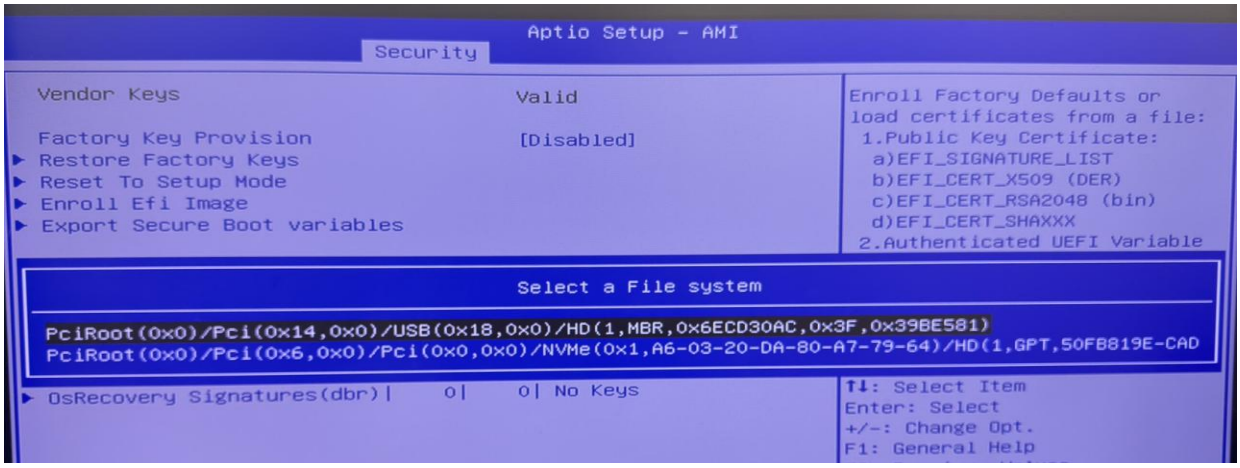
5. Choose ‘Update’



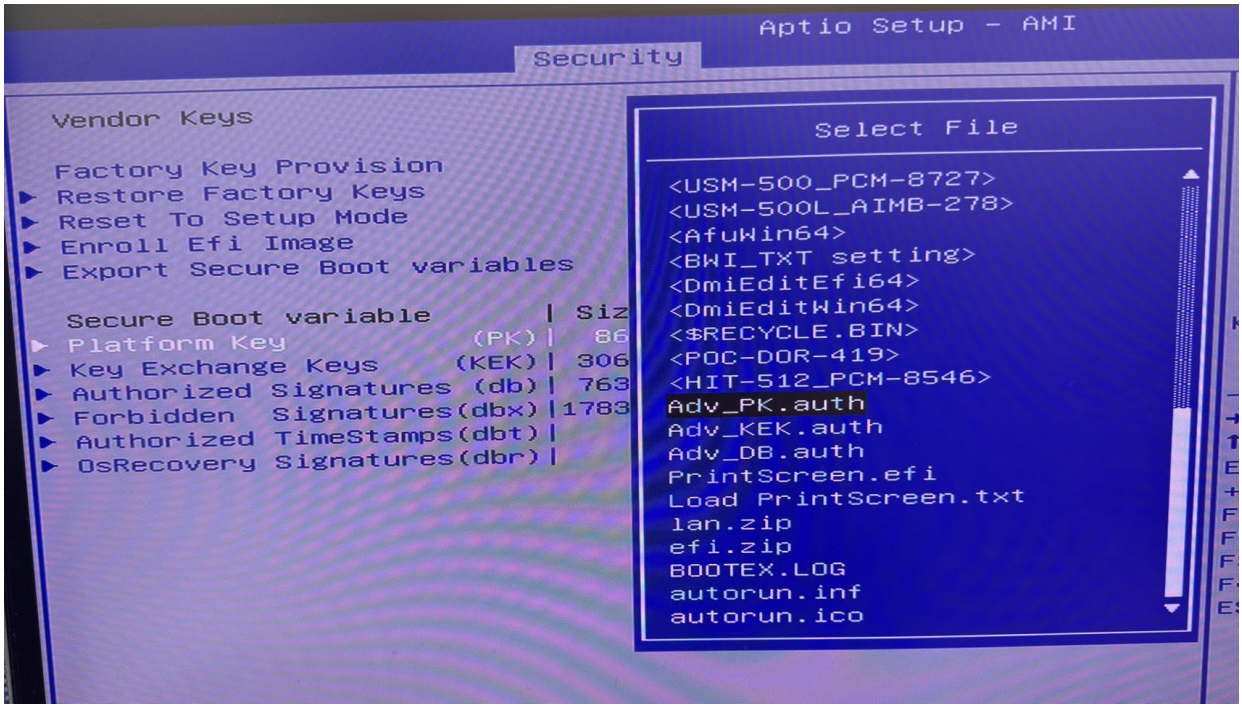
6. Choose ‘No’



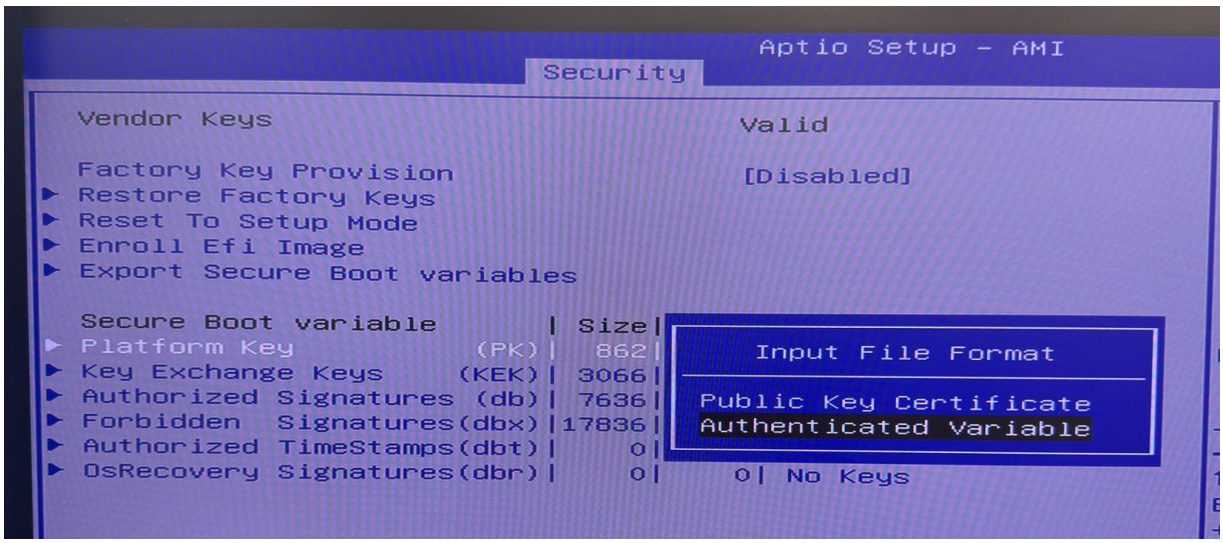
7. Choose your USB flash path



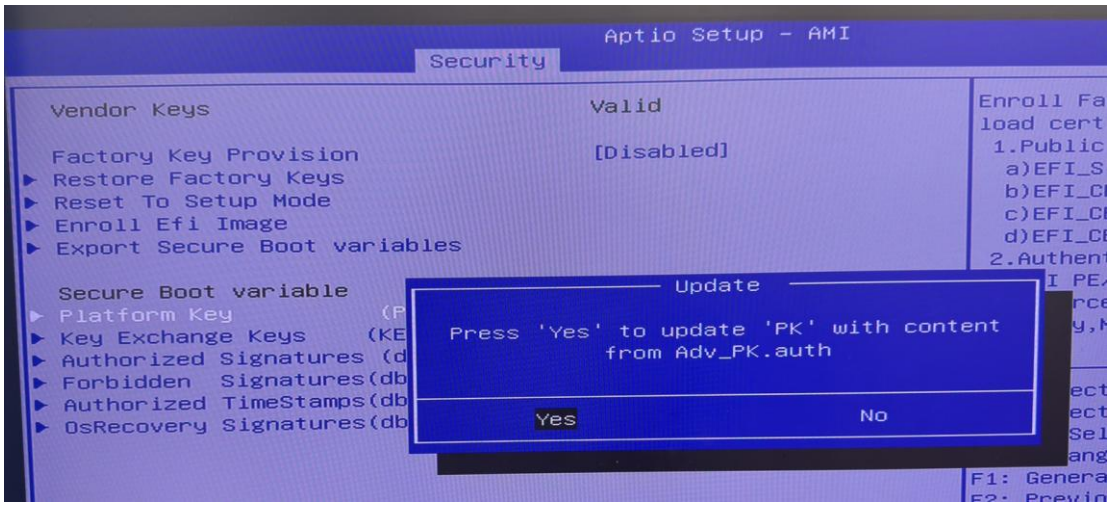
8. Choose the ‘Adv_PK.auth’



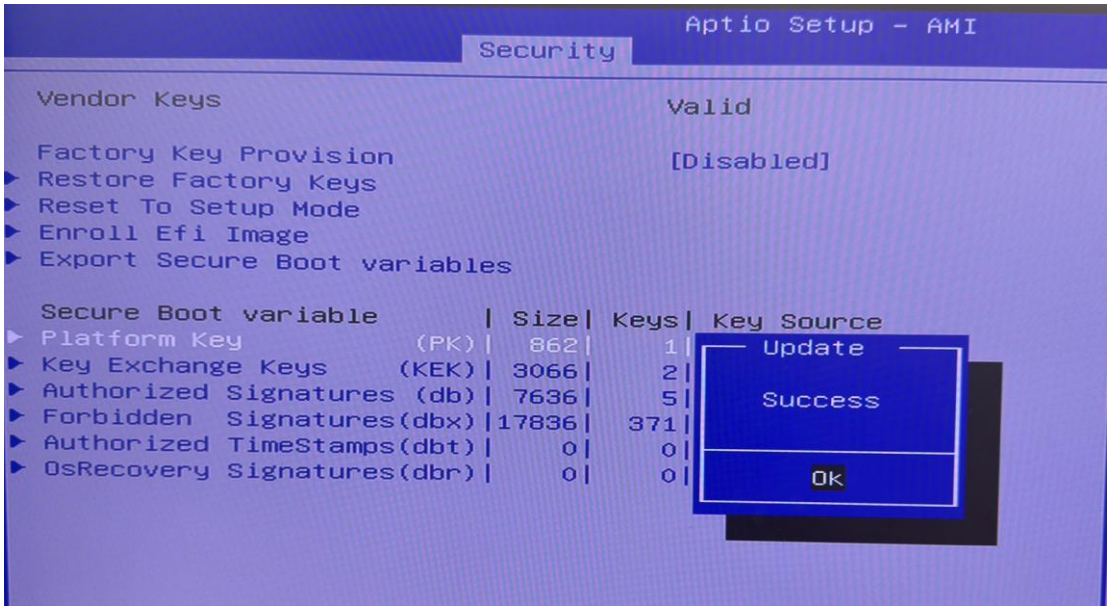
9. Choose ‘Authenticated Variable’



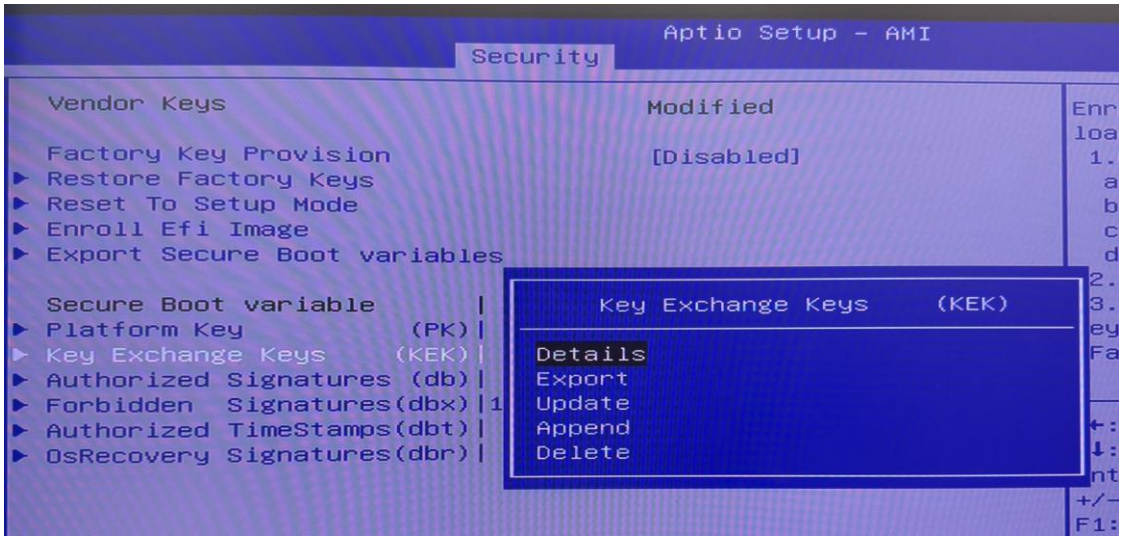
10. Choose ‘Yes’ to replace PK.



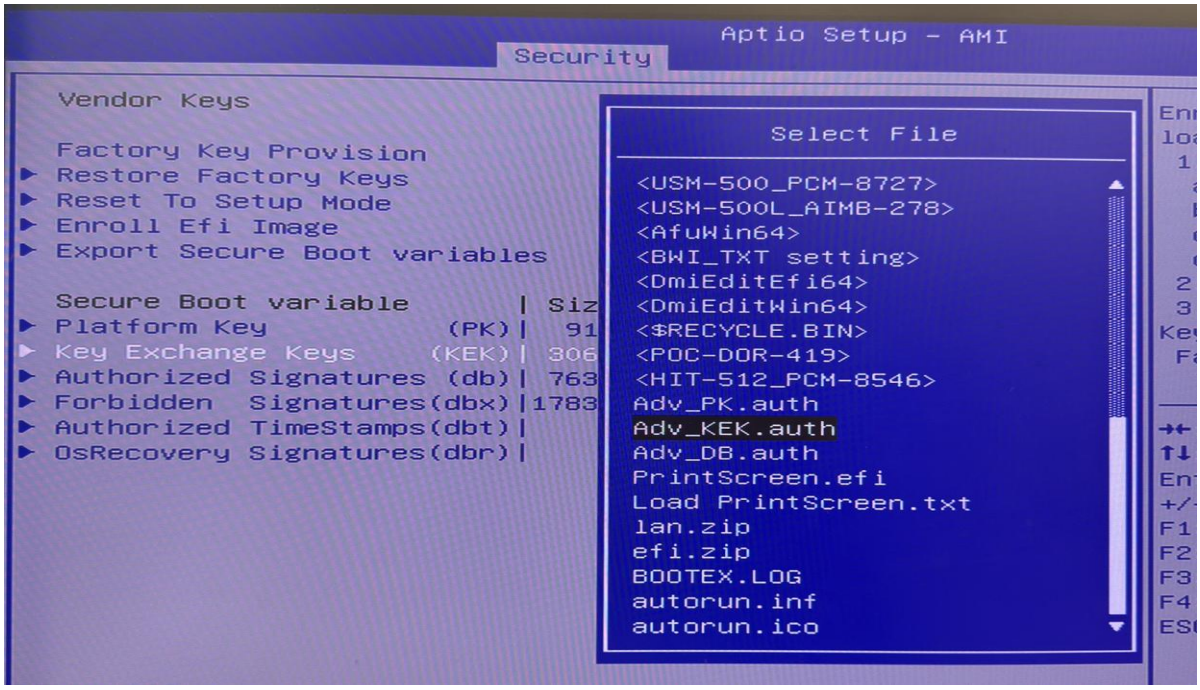
11. PK key was placed successfully.



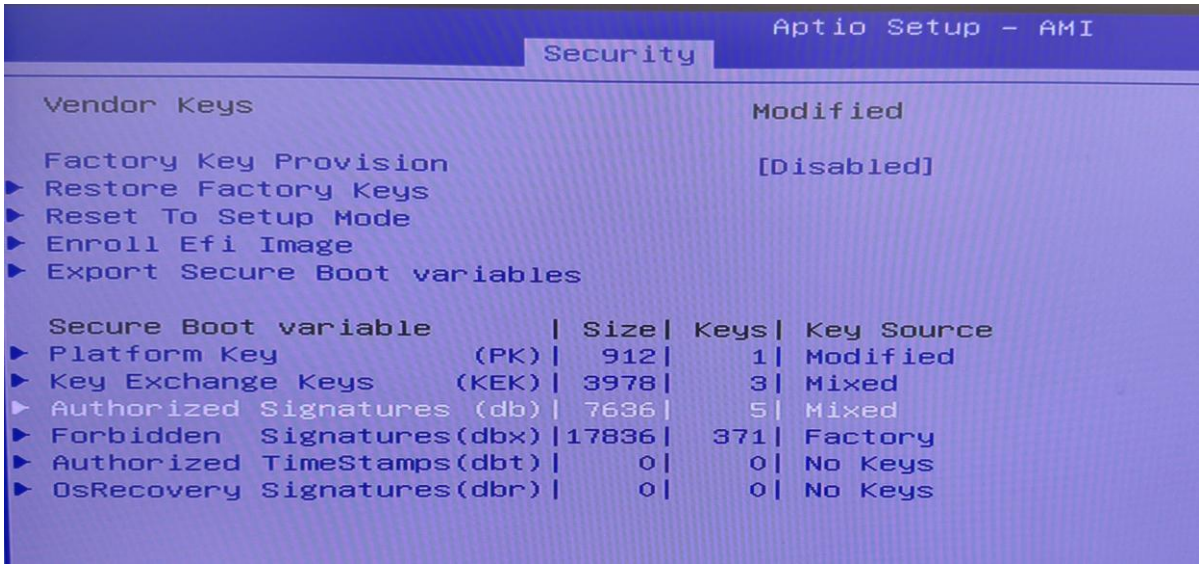
12. Use same method to replace KEK key



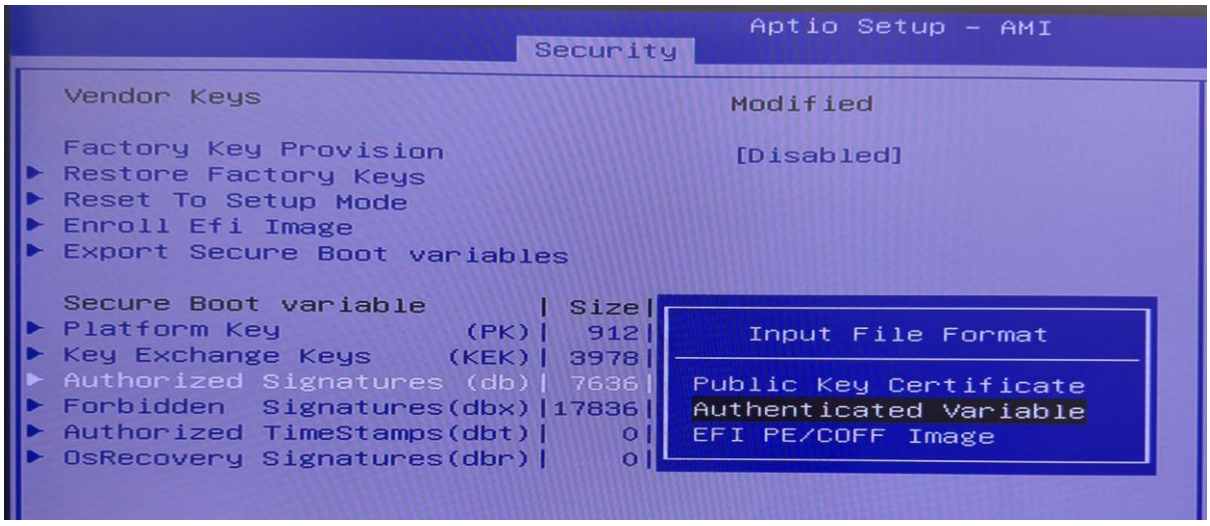
13. Choose ‘Adv_KEK.auth’



14. Use same method to replace DB key



15. Choose ‘Authenticated Variable’



■ **Reference**:

[1] Microsoft – Windows Secure Boot certificate expiration and CA updates
https://support.microsoft.com/en-us/topic/windows-secure-boot-certificate-expiration-and-ca-updates-7ff40d33-95dc-4c3c-8725-a9b95457578e

[2] Microsoft – Registry key updates for Secure Boot Windows devices with IT-managed updates
https://support.microsoft.com/en-au/topic/registry-key-updates-for-secure-boot-windows-devices-with-it-managed-updates-a7be69c9-4634-42e1-9ca1-df06f43f360d

[3] Microsoft – Updating Microsoft Secure Boot keys
https://techcommunity.microsoft.com/blog/windows-itpro-blog/updating-microsoft-secure-boot-keys/4055324

[4] GitHub – Check-UEFISecureBootVariables
https://github.com/cjee21/Check-UEFISecureBootVariables

■ **Contact Window and File Link**:

If you have any questions, please contact Jean Wang (JeanYC.Wang@advantech.com.tw)