



## Check UEFI Secure Boot KEK & DB Certificates

### Document Control

Version	Note	Date	Author
1.0	Original version	24/09/2025	PW

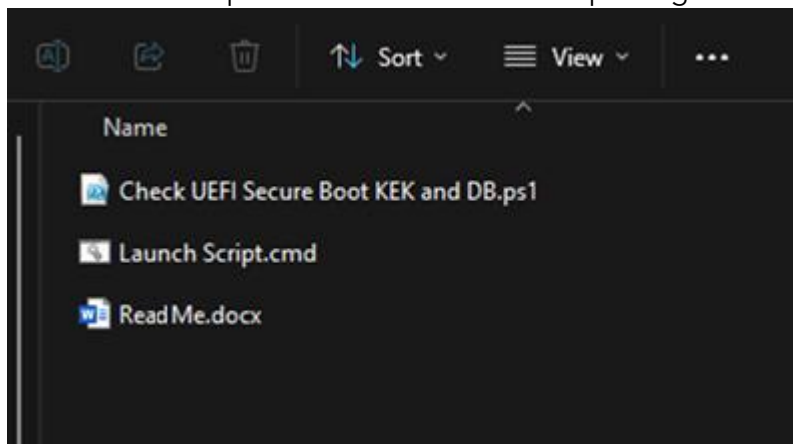
### Overview

This document is provided alongside a script which allow users and IT administrators to query the Secure Boot certificates contained within their device(s), to identify where systems require an update.

The script will also assist with identifying device models and will provide an output in the console for quick visual confirmation and will also append the results to a .CSV file in the directory the script is run from

### Steps

1. Extract the all the files from the zip archive to the same directory.
2. Run 'Launch Script.cmd' with Administrator privileges.



3. Observe the output on screen.

Example:

```
Administrator: Check UEFI Secure Boot KEK and DB
Checking for Administrator permission...
Running as administrator - continuing execution...

25 September 2025
Manufacturer: OEGStone
Model: BOAMOT-529
BIOS: 1405
Baseboard: Pro Q870M-C
Windows version: 24H2 (Build 26100.6584)

Secure Boot status: Enabled

Current UEFI KEK
✓ Microsoft Corporation KEK CA 2011 (revoked: False)
✓ Microsoft Corporation KEK 2K CA 2023 (revoked: False)

Default UEFI KEK
✓ Microsoft Corporation KEK CA 2011 (revoked: False)
✓ Microsoft Corporation KEK 2K CA 2023 (revoked: False)

Current UEFI DB
✓ Microsoft Windows Production PCA 2011 (revoked: False)
✓ Microsoft Corporation UEFI CA 2011 (revoked: False)
✓ Windows UEFI CA 2023 (revoked: False)
✓ Microsoft UEFI CA 2023 (revoked: False)
✗ Microsoft Option ROM UEFI CA 2023

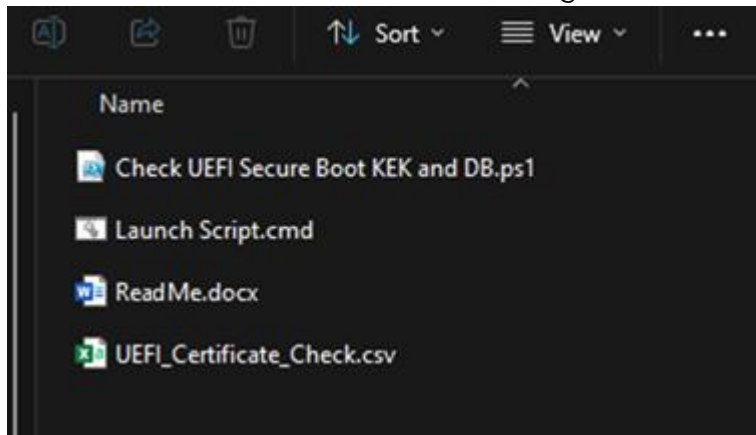
Default UEFI DB
✓ Microsoft Windows Production PCA 2011 (revoked: False)
✓ Microsoft Corporation UEFI CA 2011 (revoked: False)
✓ Windows UEFI CA 2023 (revoked: False)
✓ Microsoft UEFI CA 2023 (revoked: False)
✗ Microsoft Option ROM UEFI CA 2023

CSV log updated/appended:

Press any key to continue . . .
```



4. Check the 'UEFI\_Certificate\_Check.csv' log file.



### Identifying certificates

The information provided in the console and logfile, will show which certificates are currently active and which exist (default) in the respective KEK and DB certificate stores.

```
Secure Boot status: Enabled

Current UEFI KEK
✓ Microsoft Corporation KEK CA 2011 (revoked: False)
✓ Microsoft Corporation KEK 2K CA 2023 (revoked: False)

Default UEFI KEK
✓ Microsoft Corporation KEK CA 2011 (revoked: False)
✓ Microsoft Corporation KEK 2K CA 2023 (revoked: False)

Current UEFI DB
✓ Microsoft Windows Production PCA 2011 (revoked: False)
✓ Microsoft Corporation UEFI CA 2011 (revoked: False)
✓ Windows UEFI CA 2023 (revoked: False)
✓ Microsoft UEFI CA 2023 (revoked: False)
X Microsoft Option ROM UEFI CA 2023

Default UEFI DB
✓ Microsoft Windows Production PCA 2011 (revoked: False)
✓ Microsoft Corporation UEFI CA 2011 (revoked: False)
✓ Windows UEFI CA 2023 (revoked: False)
✓ Microsoft UEFI CA 2023 (revoked: False)
X Microsoft Option ROM UEFI CA 2023
```





### Identifying device model

The information provided in the console and logfile can assist you with cross checking against the supported products matrix provided in our knowledge base article titled '[Expiry of 2011 Secure Boot Certificates & Replacement with 2023 Certificates](#)'.

The below information (also contained in the log file) shows our internal identifier 'model' and unique motherboard 'baseboard' strings, both of which can be checked against our support matrix.

The BIOS version is also shown.

```
25 September 2025
Manufacturer: OEGStone
Model: BOAMOT-529 ←
BIOS: 1405 ←
Baseboard: Pro Q870M-C ←
Windows version: 24H2 (Build 26100.6584)
```

