EC/ME/BIOS Update via EFI Shell

Schenker Technologies GmbH, September 2019

This document will help you to get familiar with updating your EC, ME and BIOS-Firmware via EFI Shell.

FAQ – Frequently Asked Questions:

Q: What is EFI Shell?
A: EFI Shell is a Command-Line Interface similar to MS-DOS, PowerShell and Linux Bash. It is fully seperate from your operating system. EFI Shell is compatible with UEFI, which has been the most common BIOS architecture since 2012.

Q: What do I need?
A: You only need a USB Stick. It does not need to be empty. If the USB Stick is formatted in a different file system (exFat, NTFS), you need to format it in FAT32. If you decide to re-format, all data on the USB Stick would be deleted.

Q: Can I update my EC/BIOS in Windows instead?
A: Yes, some EC/BIOS updates include a Update Tool (Flash Tool) for Windows in 64-bit. This is usually done via AfuWin64 or FlashMEWinX64.bat or a similar Batch file. If you find such a file or folder in your EC/BIOS Update, it is OK to use it. However, we recommend using EFI Shell because EFI Shell is fully independent, therefor avoiding any potential risk of interference from Windows software and other background processes.

Phase 1: Prepare the USB Stick

1. Make sure that your USB Stick is formatted in FAT32.
2. Download the ZIP file Shell for EFI Flash.
3. Unpack it onto your USB-Stick.
4. Unpack the content of the EC/BIOS Update ZIP files onto your USB-Stick as well.

See the following screenshots for reference:

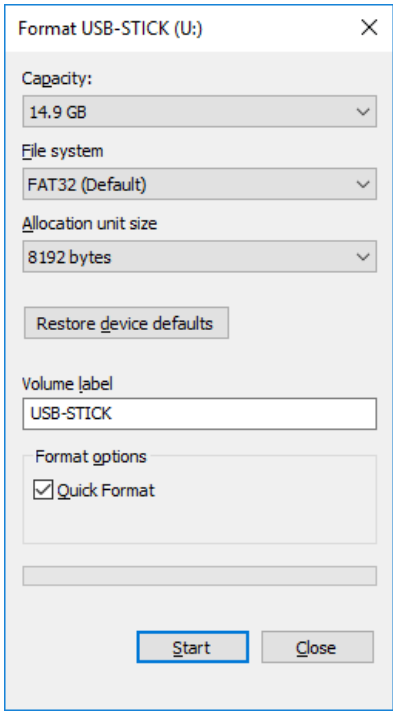

Figure 1: USB Stick formatted in FAT32

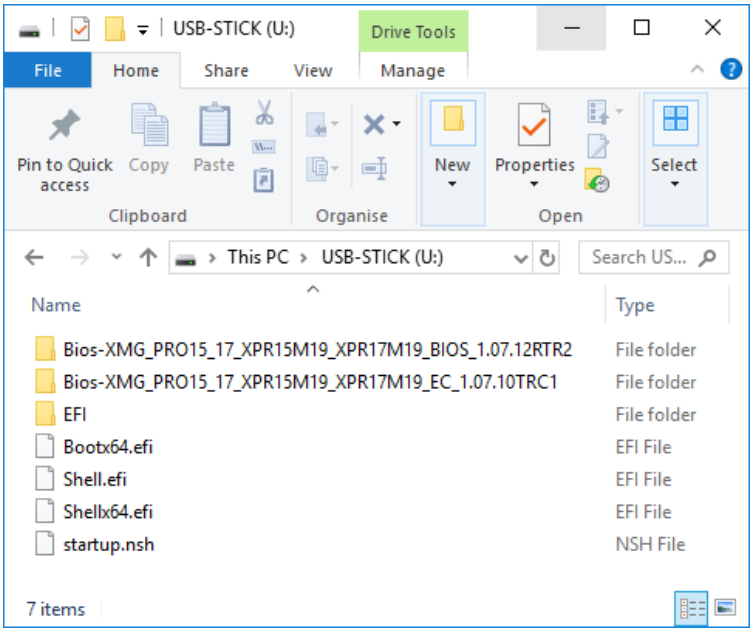

Figure 2: Typical directory layout of USB Stick with EFI Shell

Introduction: Aptio BIOS vs. Insyde BIOS

When entering BIOS Setup (F2), you will see either one of these two systems:

Aptio BIOS (American Megatrends, AMI)	Insyde BIOS
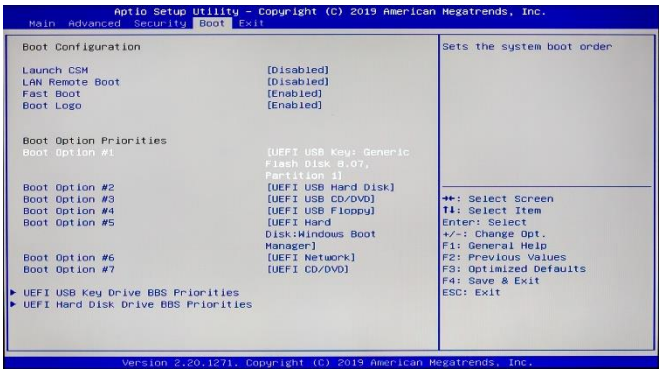	
Figure 3: Aptio BIOS	*Figure 4: inyde BIOS Welcome Screen*

Both systems are equally up to date and fully compliant with BIOS/UEFI standards. While the UI appear different on first look, the organisation and operation is identical.

Please remember these hotkeys:

F2	BIOS Setup Utility	*Gives you access to all UEFI/BIOS settings.*
F10	Save & Exit	*Stores the current UEFI/BIOS settings and reboots the system.*
F7	Boot Select Manager	*Enables you to select your boot device, including USB media.*

To enable **F2** (BIOS Setup) and **F7** (Boot Select), hold down the respective hotkey during early boot-up time.

Phase 2: Disable Secure Boot (optional)

For some Windows installation, a feature called „Secure Boot“ is enabled in the BIOS. However, “Secure Boot” needs to be temporarily disabled in order to boot EFI Shell from USB Stick.

1. Reboot and enter BIOS Setup Utility (F2)
2. Find and disable “Secure Boot”, if it is not disabled already
3. You will find it either in the “Security” category (Aptio) or in “Administer Secure Boot” item (insyde)
4. Go to “Exit” and “Save Changes and Reboot”

Phase 3: Boot your USB Stick

1. Make sure that your system is connected to external power.
2. Attach your USB Stick to one of the USB Ports.
3. Boot your system and hold down F7 to enter Boot Manager.
4. Select and confirm “EFI USB Device” or “Generic Flash Disk”

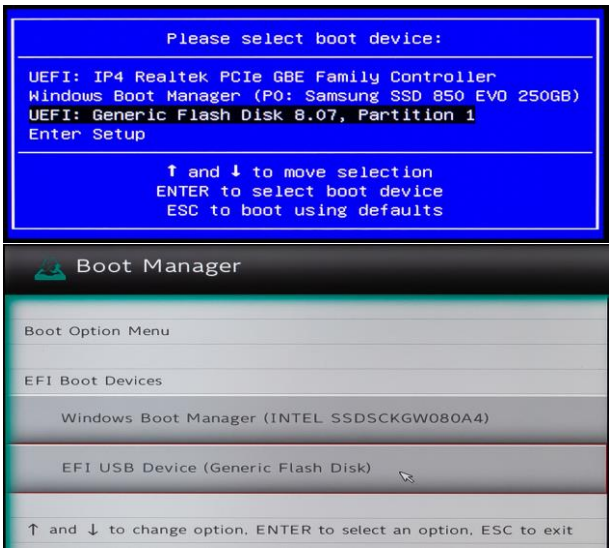

Figure 5: Boot Manager (F7) will look different, depending on your system. The function is the same on both systems.

Attention: EC and BIOS Updates might **automatically reboot** the system multiple times. The screen might even stay dark for a certain amount of time.
This is normal. Please be patient and let the update proceed without interruptions.

Do not *manually* shut down or reboot the system during the Update!
Do not remove the external power supply!

If the update asks you to confirm to continue the process, please read the instructions on the screen carefully and, if you want to proceed, confirm.

If you see any **Error** messages, please **take a picture** of the message and **send it to support**. A few common messages are explained at the end of this document.

Phase 4: Navigate the EFI Shell and start the Update

1. Your system should now boot into the EFI Shell.
2. There will be a countdown for startup.nsh - press ANY KEY to proceed. Do not press ESC (Escape).
3. You will see the following instruction on screen:

```
Welcome to EC/BIOS Update via EFI Shell.
You are already in the correct file system.

Please use commands 'dir' and 'cd' to navigate.
The command 'dir' will list the content of your current directory.
The command 'cd' (change directory) will navigate down to the next directory.
To navigate up to the parent folder again, use the command 'cd ..'

Use tabulator [Tab] key on your keyboard for auto-completion.
Example: 'cd Firmware' and then press [Tab] a few times.

After entering the appropriate folder, run the correct NSH file to Update.
NSH files in EFI Shell are the same as BAT files (Batch files) in MS-DOS.
To run an NSH file, simply type its name into the shell and hit [Return].
You can use [Tab] again to auto-complete the name of the NSH file.
Update files are named F.NSH, FLASH.NSH, FLASHME.NSH, ECFLASH.NSH or similar.

If your BIOS update contains an ME Update, please run MESET first.
If you wish to update both EC and BIOS, please run the EC Update first.
Typical update sequence: 1) EC Update, 2) MESET, 3) ME/BIOS Update.

You can use PageUp and PageDown keys on your keyboard to scroll up and down.
If you do not know how to proceed, please contact support.
```

Typical update sequence: 1) EC Update, 2) MESET, 3) ME/BIOS Update.

EC Update: EC Firmware is mostly responsible for power management, LED lights and keyboard control. If your EC is already up to date, you do not need to update it again. However, if you wish to update both EC and BIOS, it is recommended to **run the EC Update first**, before you proceed with ME/BIOS.

ME Update: Some BIOS Updates might include an ME Firmware-Update. “FLASHME.NSH” will typically run the ME Update first (if present), then automatically run the BIOS Update. However, before ME Update, you need to unlock the ME for write-access. This is done via **MESET Tool**, typically named MESET.EFI, MeSet.efi, or MeSetX64.efi.
If you find this tool in your BIOS Update folder, run it in EFI Shell. After MESET is complete, the system will reboot. During this reboot, the fans will run at high speed and it might take a few moments to finish rebooting. After reboot, you can launch EFI Shell again in order to continue with the ME/BIOS Update.

EC/BIOS Update via EFI Shell: Examples and Screenshots

The exact output on the screen will depend on your system and on each individual update. Please use the following screenshots for guidance.

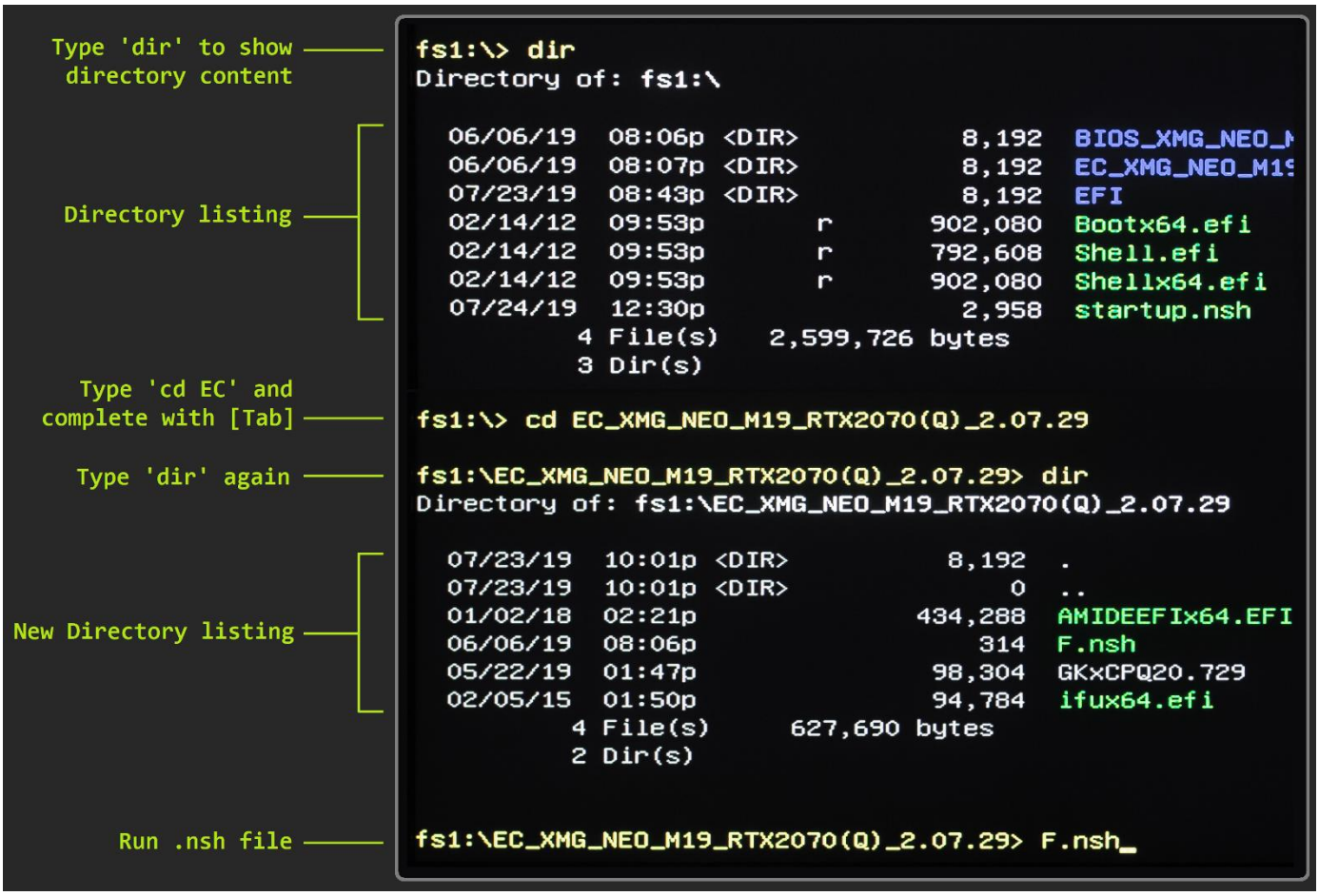

Figure 6: Navigating EFI Shell and starting NSH file for EC Update. The names of files and folder might appear different, depending on your update.

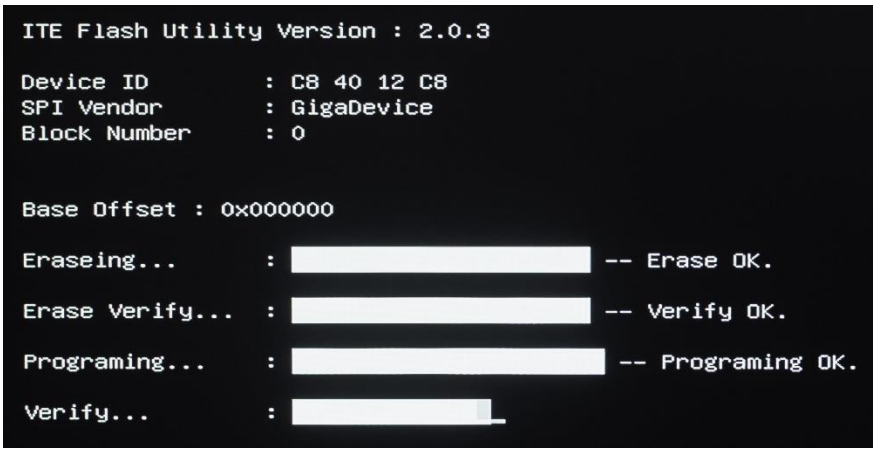

Figure 7: Typical example of screen output during EC Update.

Phase 5: Reset and Finish

After all Updates are completed successfully, it is strongly recommended to go back to the BIOS to restore all settings to factory default. This is usually described as “BIOS Reset” or “CMOS Reset”.

1. You can now remove the USB Stick from your system.
2. Enter BIOS Setup Utility (F2), go to “Exit” category.
3. Select and confirm “Load Optimized Defaults” / “Load Setup Defaults” (or similar)
4. If you have disabled “Secure Boot” earlier, please enable it again.
4. Press F10 and confirm for “Save and Exit”. Reboot and enjoy your updated system.

Finished. Update complete!

Thank you for updating EC/BIOS via EFI Shell.
If you have any question, please do not hesitate to contact us for support.

Common Warnings and Error messages

GbE Region does not exist

GbE Region contains code and configuration data for Gigabit Ethernet in the ME firmware. This region is usually not present if Booting over LAN is disabled in the BIOS. Can be ignored.

PDR Region does not exist

Platform Descriptor Region allows system manufactures to describe custom features for the platform. Usually not present in our system. Can be ignored.

Error 25: The host CPU does not have write access to the target flash area. To enable write access for this operation you must modify the descriptor settings to give host access to this region.

This indicates that the ME Firmware Region is protected against overwriting – it’s not a bug, it’s a feature.
If you encounter this error, please run MESET.EFI (or similar) as described in Phase 4 of this document.

End of document