How to flash AMIBIOS image (Signed/Unsigned) on AMD Platform

Background:

Since, windows8 OS, Microsoft requires all platform BIOS image to be secured/signed using sign server. Purpose of signed BIOS is to add a unique signature using sign server to prevent any kind of tempering of the BIOS F/W on the platform.

To bypass the Signing server image flashing user/OEM must use the BIOS Flash utility, which can support unsigned version of the BIOS flash. AMIBIOS Flash utility version 2.38 allows bypassing the Sign Server BIOS image to be flashed on AMD platform.

Flash utility:

AFU (AMI Firmware Update) is a package of utilities used to update the system BIOS under various operating systems.

Note: AFU only works for APTIO with SMI FLASH support. Compatible with Aptio 3, 4, 4.5

These packages include:

- AFUDOS 3.05.04

Flash utility can be downloaded from each platform landing page. After downloading the Amiflash.Zip from Landing page, unzip the file in local drive. "Local Drive:amiflash\amiflash\Aptio\afudos\afudos.zip. This utility will NOT allow to bypass the Sign Server. Therefore User/OEM MUST flash the BIOS image using Flash Programmer e.g. DediProg and others. After programming Signed BIOS using Flash programmer (first time), user/OEM can use this utility to flash the BIOS image on platform.

AFUDOS 2.38.00

Flash utility can be downloaded from each platform landing page. On landing page it is available as "AMI Unsigned Flash Update Utility**. After downloading the AMIUnsignedFirmwarepdate.zip from Landing page, unzip the file in local drive. This utility will allow to bypass the Sign Server. Therefore User/OEM MUST flash the BIOS image using this Flash utility if they do not have Flash Programmer.**

Usage applies to AFUDOS, AFUEFI and AFUEFI64...

AFUDOS <BIOS ROM File Name> [Option 1] [Option 2]
Or
AFUDOS <Input or Output File Name> <Command>
Or
AFUDOS <Command>

BIOS ROM File Name

The mandatory field is used to specify path/filename of the BIOS ROM file with extension.

Example: 0ACCV009.ROM

Commands

The mandatory field is used to select an operation mode.

- /O Save current ROM image to file
- /U Display ROM File's ROMID
- /S Refer to Options: /S
- /D Verification test of given ROM File without flashing BIOS.
- /OAD Refer to Options: /OAD
- /A Refer to Options: /A
- /CLNEVNLOG Refer to Options: /CLNEVNLOG

Options

The optional field used to supply more information for flashing BIOS ROM. Following lists the supported optional parameters and format:

- /Q Silent execution
- /X Don't Check ROM ID
- /CAF Compare ROM file's data with Systems is different or not, if not then cancel related update.
- /S Display current system's ROMID
- /HOLEOUT: Save specific ROM Hole according to RomHole GUID.
  NewRomHole1.BIN /HOLEOUT:GUID
- /SP Preserve Setup setting.
- /Rn Preserve SMBIOS type N during programming(n=0-255)
- /R Preserve ALL SMBIOS structure during programming
- /B Program Boot Block
- /P Program Main BIOS
- /K Program all non-critical blocks and ROM Holes.
- /N Program NVRAM
- /Kn Program n'th non-critical block or ROM Hole only(n=0-15).
- /HOLE: Update specific ROM Hole according to RomHole GUID.
  NewRomHole1.BIN /HOLE:GUID
- /L Program all ROM Holes.
- /Ln Program n'th ROM Hole only(n=0-15).
- /E Securely Flash Embedded EC at Runtime
  (If system supports. Can be overriden by other options)
- /OAD Delete Oem Activation key
- /A Oem Activation file
- /E Program Embedded Controller Block
- /ECUF Update EC BIOS when newer version is detected.
- /ME Program ME Entire Firmware Block.
- /MEUF Program ME Ignition Firmware Block.
- /CLNEVNLOG Clear Event Log.
- /CAPSULE Override Secure Flash policy to Capsule
- /RECOVERY Override Secure Flash policy to Recovery
- /EC Program Embedded Controller Block. (Flash Type)
- /REBOOT Reboot after programming.
- /SHUTDOWN Shutdown after programming.

Rules

- **Any parameter encolsed by < > is a mandatory field.**
- **Any parameter enclosed by [ ] is an optional field.**
- **<Commands> cannot co-exist with any [Options].**
- **Main BIOS image is default flashing area if no any option pre**

AFUDOS Flash command for DB-FP3 “Lamar”:

AFUDOS 0ACCV00X.ROM /P /B /N /K /X

- In 0ACCV00X.ROM indicates the version of the BIOS e.g. 0ACCV001.ROM, 0ACCV002.ROM, 0ACCV003.ROM….