

Open Source Firmware status on AMD platforms 2022 - 3rd edition





FOSDEM'22 - Open Source Firmware, BMC and Bootloader
devroom

Michał Żygowski





Michał Żygowski
Firmware Engineer

-  [@_miczyg_](https://twitter.com/_miczyg_)
-  michal.zygowski@3mdeb.com
-  linkedin.com/in/miczyg
-  facebook.com/miczyg1395
- Braswell SoC, PC Engines and Protectli maintainer in coreboot
- OpenPOWER System Software Technical Workgroup chair
- 4 years in Open Source Firmware
- interested in advanced hardware and firmware security features

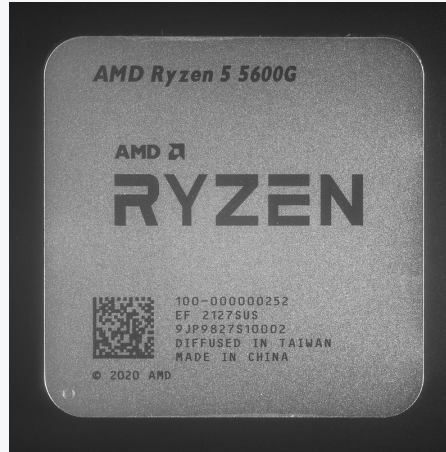


- coreboot licensed service providers since 2016 and leadership participants
- UEFI Adopters since 2018
- Yocto Participants and Embedded Linux experts since 2019
- Official consultants for Linux Foundation fwupd/LVFS project since 2020
- IBM OpenPOWER Foundation members since 2020

- AGESA - **A**MD **G**eneric **E**ncapsulated **S**oftware **A**rchitecture AMD processor initialization source code
 - we can easily call it FSP for AMD, but requires NDA and sometimes "special relations"
 - despite being compliant with UEFI reference implementation (edk2) it does not support open source toolchains (GCC or LLVM)
 - from AMD OSF group: AGESA goes through modifications to support GCC
 - see our [FOSDEM2020 presentation](#) for AGESA history and versions
- AMD Security Processor - (commonly referred to as PSP - **P**latform **S**ecurity Processor AMD's equivalent of Intel ME), a coprocessor on the chipset performing similar operations to the ME (security, crypto, CPU bringup, etc.)

Processor codenames and architecture names explained on [wikipedia](#) and [cpu-world.com](#).

- **Puma** - Steppe Eagle core architecture, AMD 2nd Gen G series embedded SoCs (APU2)
- **Bulldozer** - Interlagos core architecture, AMD Opteron 6200 series (server), KGPE-D16
- **Piledriver** - Abu Dhabi core architecture, AMD Opteron 6300 series (server), KGPE-D16
- **Piledriver** - Trinity core architecture, AMD A{4,6,8,10} series APUs(laptop), Lenovo G505s
- **Picasso** - Zen+ core architecture, Ryzen 3000 APU series with RX Vega (desktop & laptop)
- **Cezanne** - Zen3 core architecture, Ryzen 5000 series (desktop & laptop), **new in coreboot**
- **Sabrina** - family 17h models A0h-AFh, **new in coreboot**



[Ryzen photo](#) by Fritzchens Fritz, CC0 1.0 Universal Public Domain Dedication

- Under review
 - [initial patches for AMD Cezanne support \(AMD Ryzen 5000\)](#)
 - [initial patches for AMD Majolica support \(FP6 APU\)](#)
- Due to groundbreaking change to architecture it takes a lot of time and effort to make it land into the main tree in usable form

- Picasso and Cezanne complete and usable (Cezanne FSP not public yet)
- PSP BIOS A/B recovery in amdfwtool support WIP:
 - <https://review.coreboot.org/c/coreboot/+/57131>
 - <https://review.coreboot.org/c/coreboot/+/56773>
- [PSP FW extraction in amdfwtool support WIP](#)
- [First patches for Sabrina SoC](#)
- Community sentiment in 2021 was rather more on negative side then positive regarding the old AMD open platforms already (see [coreboot mailing list](#) and [leadership meeting minutes](#))

AMD server status - last year vs now



[AMD EPYC photo](#) by Raysonho @ Open Grid Scheduler / Grid Engine, CC0, via Wikimedia Commons

2021:

- From coreboot leadership meeting: There is a chance that AMD servers will also get OSF support
- [Pure open source on AMD EPYC 7002 "Rome" by Ron Minich](#)

2022:

- No updates about the OSF on servers unfortunately. Neither on oreboot
- OSFW Slack channels you can find concerning information about AMD OSF support on servers.

2021:

- ~~many platforms are being dropped due to coreboot release requirements~~
- ~~community aligns with the work and push updated board support~~
- much clean-up and fixes to do, most of the code landed in the repository as copy-paste

Very lax in accepting vendorcode early on. We hoped that AMD would clean up the codebases. Promises to maintain the code didn't happen

Official explanation of coreboot leadership why the code ended up in such state.

2022:

- new coreboot releases come with new feature/option deprecation announcements
- many older AMD boards do not implement the newest coreboot platform initialization interfaces (features/options) and as a result are getting dropped
- thanks to the companies like PC Engines (who support open source development through 3mdeb), the platforms keep living in coreboot
- family14 in review and family16 support is upstream for the newest interfaces
- Trinity and Kabini lack support for the new interfaces (donations welcome)

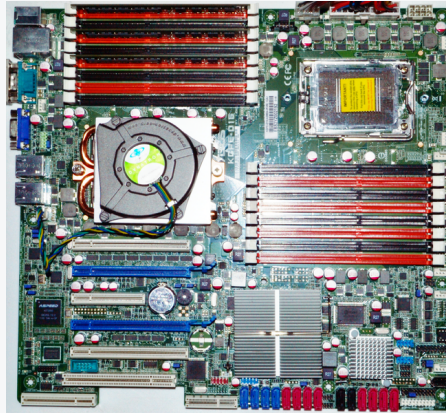


[Padlock photo](#) CC0 1.0 Universal (CC0 1.0), Public Domain Dedication

- Modern AMD based hardware enables Platform Secure Boot by fusing the platform keys to the CPU
- Such CPU cannot be used in another platform with different firmware key
- Causes a serious vendor lock-in and steals the user's freedom of firmware modifications (cannot change the CPU allowlist or freely replace CPUs)
- [Lenovo automatically locks CPUs](#)

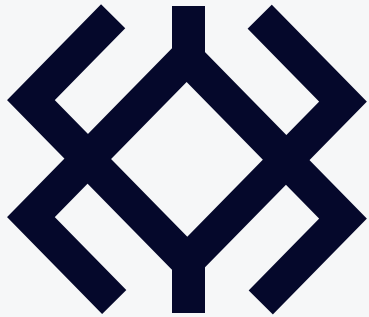


Dasharo is open source firmware distribution, we prefer clean and simple code, long term maintenance, privacy-respecting implementation, liberty for the owners, and trustworthiness for all.



FSF RYF photo from ryf.fsf.org
[KGPE-D16 photo](#) coreboot wiki

- ASUS KGPE-D16 FSF RYF platform revival sponsored by [Immunefi](#)
- Hardware donated by [Vikings](#)
- [Ready to flash binaries for various configurations](#)
- [based on coreboot 4.14-2078-g03aef28f16 \(September 30th, 2021\)](#)
- complies to all current coreboot requirements (to be upstreamed soon)



Immunefi

- [Immunefi](#) as main sponsor of ASUS KGPE-D16 platform revival
- Leading bug bounty and security services platform for Web3
- **Goal: have a secure and trustworthy machine for blockchain developers**
- Improved security with vboot and TPM 2.0 support
- Additional work to support flash write protection enabling in flashrom
- Exchange the DIP8 flash with a bigger SOIC8 flash with an adapter containing WP pin jumper

- ASUS KCMA-D8 and Supermicro H8SCM use the same common silicon code as KGPE-D16, all blobless platforms
- Donations (not only financial but hardware or hands as well) welcome to get the support for these platforms
- We will present Dasharo plan for long term stable and sustainable support for older platforms soon
- Sign up to [Dasharo newsletter](#) to get up to date information about supported platforms and the their status



- After the devroom we invite for an [virtual after-party](#).
- Next [Dasharo vPub](#) coming 17th February where we will discuss about open source firmware

Q&A