Open Source Firmware status on AMD platforms 2024 - 5th edition

FOSDEM’24 - Open Source Firmware, BMC and Bootloader devroom

Michał Żygowski

3MDEB

whoami

Michał Żygowski
Firmware Engineer

- @_miczyg_
- michal.zygowski@3mdeb.com
- linkedin.com/in/miczyg
- facebook.com/miczyg1395

- Braswell SoC, PC Engines, Protectli, MSI PRO Z690-A boards maintainer in coreboot
- dedicated to open-source firmware since 2017
- interested in advanced hardware and firmware security features

Who we are ?

- 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

AMD microarchitetcures in coreboot

- **Puma** - Steppe Eagle core architecture, AMD 2nd Gen G series embedded SoCs (PC Engines apu2)
- **Bulldozer** - Interlagos core architecture, AMD Opteron 6200 series (server), KGPE-D16
- **Piledriver** - Abu Dhabi core architecture, AMD Opteron 6300 series (server), KGPE-D16
- **Picasso** - Zen+ core architecture, Ryzen 3000 APU series with RX Vega (desktop & laptop), AMD Family 17h, Model 18h
- **Cezanne** - Zen3 core architecture, Ryzen 5000 series (desktop & laptop), AMD Family 19h, Model 50h
- **Mendocino** - Zen2 core architecture, Ryzen 7000-series Mobile CPUs with RDNA2 graphics, formerly **Sabrina**, AMD Family 17h, Model A0h
- **Phoenix** - Zen4 core architecture, Ryzen 7000-series Mobile CPUs with RDNA3 graphics, formerly **Morgana**, AMD Family 19h, Models 70h-7Fh?
- **Glinda** - very new and very little information about it, also probably a temporary codename
- **Genoa** - Zen4 core architecture, EPYC 9004 server processors

AMD coreboot status

- family14, Trinity and Kabini removed from the master branch and moved to 4.18 branch (January 2023)
- boards affected:
  - PC Engines apu1
  - MSI MS-7721 (FM2-A75MA-E35)
  - Lenovo AMD G505s
  - HP Pavilion m6 1035dx
  - ASUS F2A85-M (LE, PRO), A88XM-E and AM1I-A
  - ASRock E350M1 and IMB-A180
  - and others...
- **Since then there were no AMD board removals yet**

AMD coreboot status

- Starlabs could build coreboot firmware for their AMD laptops thanks to the publication of Cezanne FSP to amd_blobs repository in September 2022
  - mb/starlabs/cezanne: Add Cezanne Byte Mk I
  - mb/starlabs/cezanne: Add Cezanne StarBook Mk VI variant
  - **NEW: There is no update to the patches unfortunately**
- AMD Mendocino and Phoenix still in development with the former being in more advanced state, FSP not published yet
  - **NEW: FSP published for Mendocino, but not for Phoenix**
- The FSP publication interval is quite long (1.5 a year between Picasso FSP and Cezanne FSP release to public, and 1.25 a year after Cezanne APU release FSP has been published)
  - **NEW: Interval between Cezanne and Mendocino is only 5 months**
  - **NEW: Mendocino is Zen2 while Cezanne is Zen3, so maybe not so big update**
  - **NEW: Mendocino has been released to the market at the end of 2022**

AMD coreboot status

- patches covering KGPE-D16 bootblock support are out there
  - they have been abandoned because of lack of activity
  - KGPE-D16 needs some love and attention, which, unfortunately, 3mdeb can't humbly provide right now without any support from community
- Marty Plummer ("hanetzer") is working on adapting Picasso/Cezanne AMD FSP for on a non-Chromebook device ASRock x370 Killer SLI
  - Dasharo vPub 0x8 recording
  - Dasharo vPub 0x9 recording
  - Join Dasharo Matrix Space or Dasharo vPubs to know more

Ryzen photo by Fritzchens Fritz, CC0 1.0 Universal Public Domain Dedication

AMD server status

- PoC for Genoa-based (AMD EPYC 9004) reference board Onyx on GitHub
- coreboot source also available and merged to upstream repository
- UEFI EDKII-based PoC code also available on GitHub:
  - opensil-uefi-interface
  - EDKII Platform

- In the beginning of 2023 no news on official OSF support on servers from AMD
- Porting AGESA to AMD FSP and maintaining it was too costly
- New approach to open-source firmware on AMD server - OpenSIL
- OpenSIL announced on OCP Regional Summit 2023 Prague (April 2023)
- OpenSIL - open-source Silicon Initialization Library
  - Scalable with any host firmware interface/framework
- More about OpenSIL:
  - OCP Global Summit 2023
  - OSFC 2023

AMD EPYC photo by Raysonho @ Open Grid Scheduler / Grid Engine, CC0, via Wikimedia Commons

AMD OpenSIL coreboot

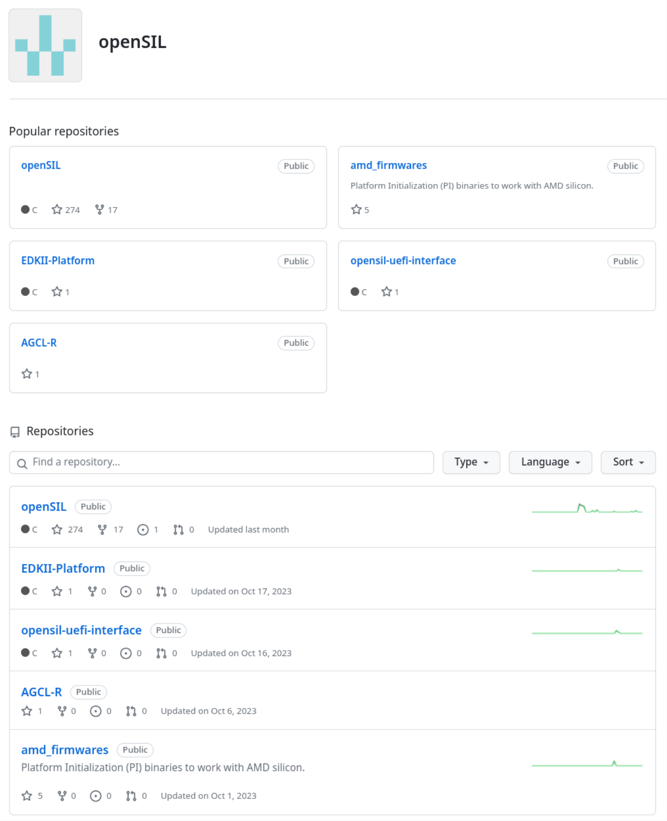
- Building is quite trivial
  - Build toolchain: **`make crossgcc-i386 && make crossgcc-x64`**
  - Select mainboard **`AMD/Onyx_poc`** with **`make menuconfig`**
  - Run **`make`** to build
- coreboot takes around 1MB in total (decompressed)
  - Although blobs' size is notable:

```
Name                                Offset      Type            Size    Comp
...
apu/amdfw                           0x1ffc0     amdfw        4317184  none
```

- Not all blobs are present though:

```
   ** WARNING **
coreboot has been built without an APCB.
This image will not boot.
```

AMD OpenSIL future



openSIL

Popular repositories

openSIL Public
● C ☆ 274 17

amd_firmwares Public
Platform Initialization (PI) binaries to work with AMD silicon.
☆ 5

EDKII-Platform Public
● C ☆ 1

opensil-uefi-interface Public
● C ☆ 1

AGCL-R Public
☆ 1

Repositories

Find a repository... | Type | Language | Sort

openSIL Public
● C ☆ 274 17 1 0 Updated last month

EDKII-Platform Public
● C ☆ 1 0 0 0 Updated on Oct 17, 2023

opensil-uefi-interface Public
● C ☆ 1 0 0 0 Updated on Oct 16, 2023

AGCL-R Public
☆ 1 0 0 0 Updated on Oct 6, 2023

amd_firmwares Public
Platform Initialization (PI) binaries to work with AMD silicon.
☆ 5 0 0 0 Updated on Oct 1, 2023

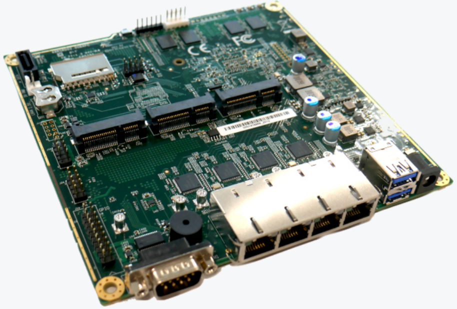
- coreboot uses an OpenSIL fork which is 4 commits behind upstream repository and has 1 additional commit fixing clang build
- The OpenSIL is constantly developed and improved by AMD and partners on a private repository
- Planned to go **production in 2026** with the 6th generation of AMD EPYC processors
- AMD plans to cover the **client segment with OpenSIL support** too (Ryzen desktop and mobile processors)
- The Genoa POC will also be available as AGESA+EDKII based UEFI firmware with the help of AGESA Compatibility Layer - Reduced (AGCL-R)

3MDEB

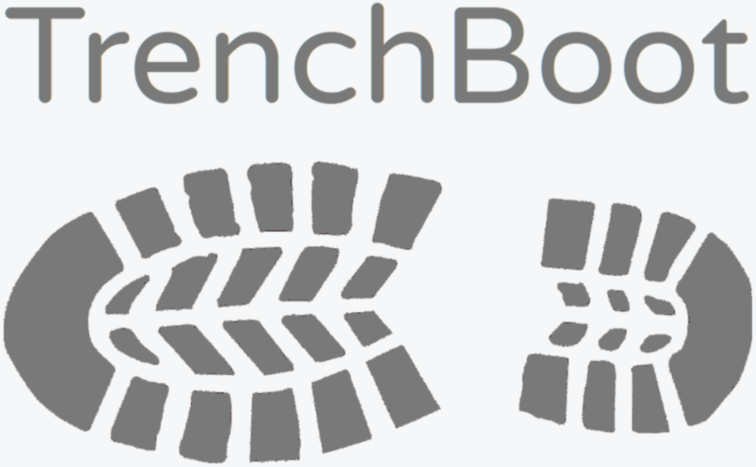
PC Engines platforms - yet another chance?

- Last year we announced the end of PC Engines' sponsorship of open-source firmware
- We tried to gather community interested in the open-source firmware for apu2 board and launch a subscription model, however the response was very little and we didn't succeed
- This year we see another chance to revive the project with [Dasharo]
- Starting with backorder of the TPMs for [APU2] and [APU3/4/6] as well as [Dasharo Entry Subscription] to support the project

PC Engines™



TrenchBoot DRTM on AMD platforms



- Early attempts on SuperMicro M11SDV in 2020 on Qubes OS Summit
  - Only legacy boot mode, no UEFI support for booting Xen
- This years the effort will be continued to cover UEFI boot mode for both Linux and Xen
- More details on the **TrenchBoot status presentation at 16:20 CET (UTC+1)** in this room
  - Make sure you do not miss it!

DASHARO ENTRY SUBSCRIPTION

Special Updates

Early access to updates enhancing privacy, security, performance, and compatibility. More frequently than community releases with transparency of reproducible binaries, clear signature chains, and an open source code supply chain.

Exclusive Newsletter

Comprehensive and meaningful release notes, in-depth feature documentation, and Software Bill of Materials (SBOM) details. Clear initial deployment and update procedures with full access to test results and logs.

Premiere Support

Personalized, priority assistance directly from the Dasharo Team. Technical queries resolved promptly and precisely.

Roadmap influence

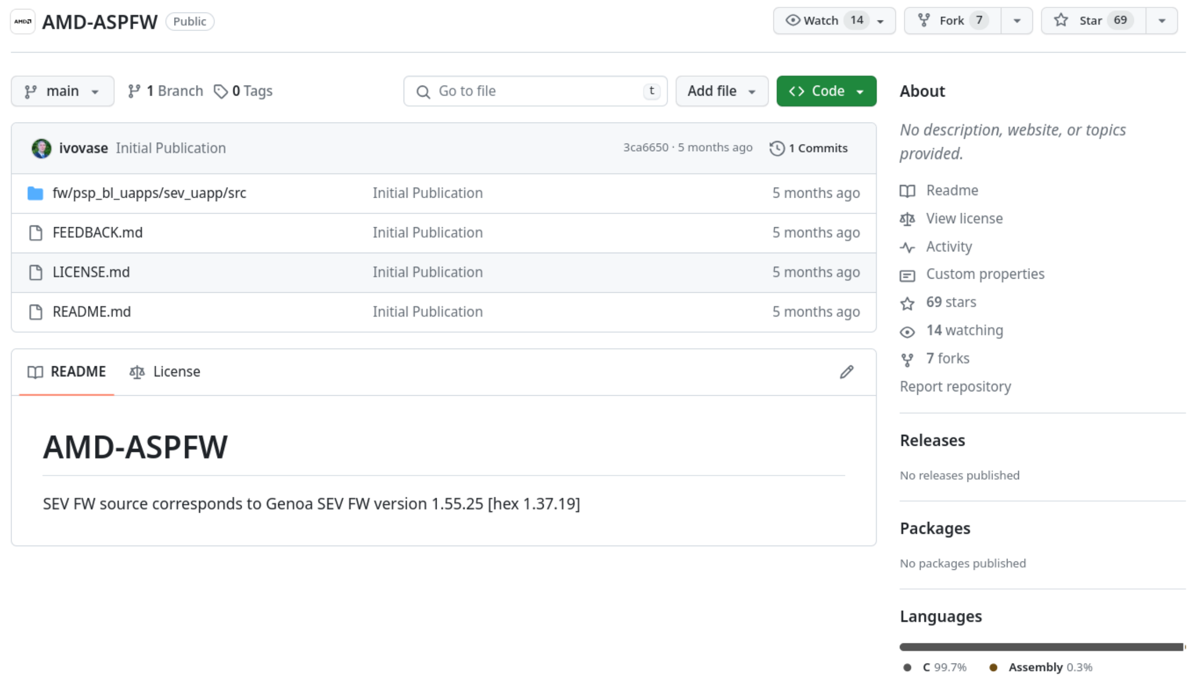
Influence the direction and development of new features, ensuring our firmware evolves to meet your specific needs and industry trends.

Sign up to Dasharo newsletter to get up to date information about supported platforms and the their status.

Bonus

AMD open-sourced the AMD PSP code for Secure Encrypted Virtualization (SEV)

[AMD PSP SEV FW on GitHub]



AMD-ASPFW Public

Watch 14 | Fork 7 | Star 69

main | 1 Branch | 0 Tags | Go to file | Add file | Code

ivovase Initial Publication 3ca6650 · 5 months ago 1 Commits

fw/psp_bl_uapps/sev_uapp/src	Initial Publication	5 months ago
FEEDBACK.md	Initial Publication	5 months ago
LICENSE.md	Initial Publication	5 months ago
README.md	Initial Publication	5 months ago

README | License

AMD-ASPFW

SEV FW source corresponds to Genoa SEV FW version 1.55.25 [hex 1.37.19]

About

No description, website, or topics provided.

Readme
View license
Activity
Custom properties
69 stars
14 watching
7 forks
Report repository

Releases

No releases published

Packages

No packages published

Languages

● C 99.7% ● Assembly 0.3%

Special thanks to:

- Paul Grimes (AMD)
- Felix Held (AMD)

For insights, review and suggestions to the presentation.

Q&A

Thank you