👋 Dasharo User Group #10 🎉 and Developers vPub 0xF 🍻

What is this ”Empowering The Industry” about with AMD OpenSIL?

Agenda

- AMD and Intel silicon support in open-source firmware
- AMD and Intel silicon support in coreboot historically
- AMD OpenSIL introduction
- Bonus
- Q&A and Discussion

Disclaimer

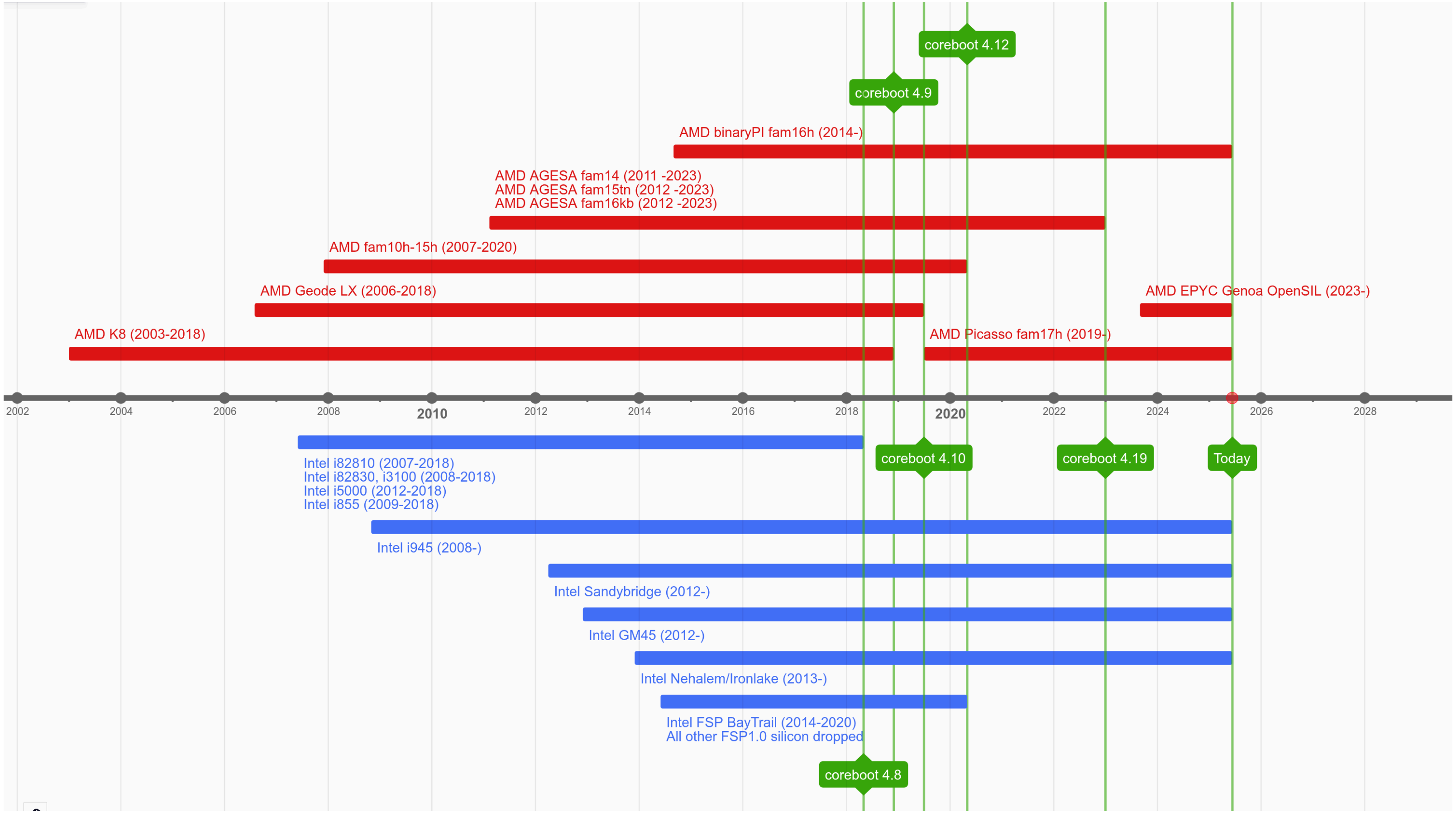
The presentation contains my own private opinions, thoughts and speculations, **not my employers**. The information contained in the presentation may not be accurate and simply aims to spark a discussion.

Historical data for coreboot x86 silicon support has been extracted with git.

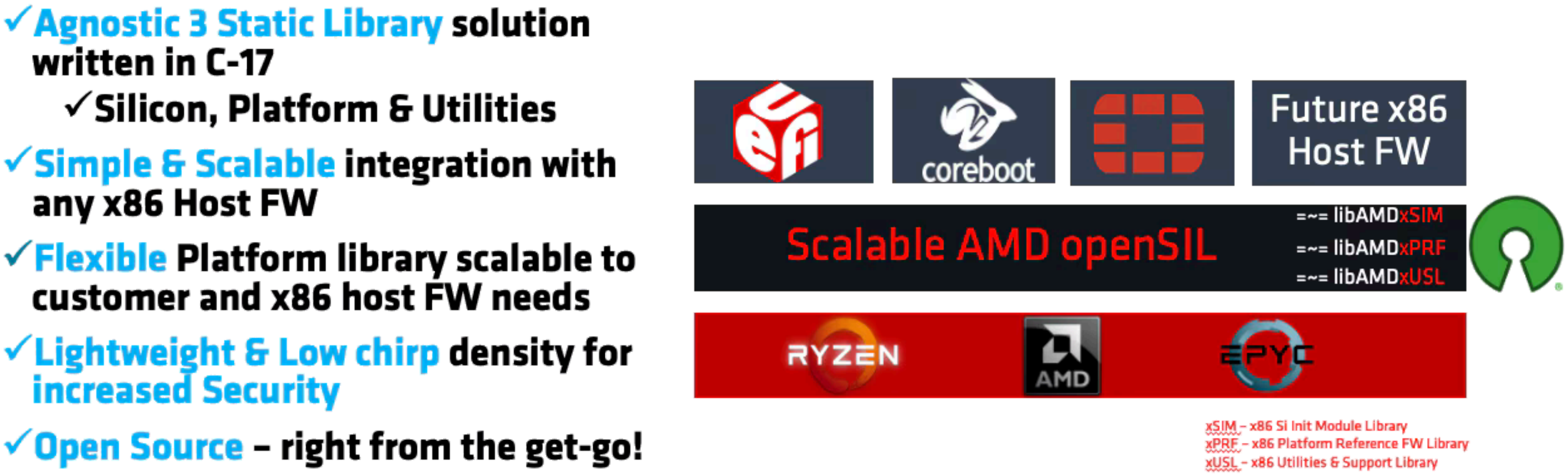
AMD and Intel silicon support in open-source firmware

- Intel:
  - Has quite strong monopoly on x86 open-source firmware (EDK2, SBL, coreboot, FSP)
  - Very stable and dominant in coreboot tree (except old FSP1.x boards)
  - Lots of (never-ending) speculative vulnerabilities
- AMD
  - Almost not present in open-source firmware frameworks besides coreboot (EDK2 contributions only recently)
  - Early silicon support was fully open-source (native, AGESA/CIMx) until mid 2014 with introduction of BinaryPI (binary AGESA) and later AMD FSP
  - Open-source firmware support for new AMD platforms nearly didn’t exist between 2015 and 2020 due to economical situation of AMD
  - Older silicon parts are not very stable in coreboot tree, often dropping from main branch (famous KGPE-D16 and others), unmaintained with poor code quality
  - AMD restores its position in open-source firmware ecosystem with OpenSIL

AMD and Intel silicon support in coreboot historically



AMD OpenSIL introduction



- ✓**Agnostic 3 Static Library solution written in C-17**
  - ✓**Silicon, Platform & Utilities**
- ✓**Simple & Scalable integration with any x86 Host FW**
- ✓**Flexible Platform library scalable to customer and x86 host FW needs**
- ✓**Lightweight & Low chirp density for increased Security**
- ✓**Open Source – right from the get-go!**

Future x86 Host FW

Scalable AMD openSIL

=~= libAMDxSIM

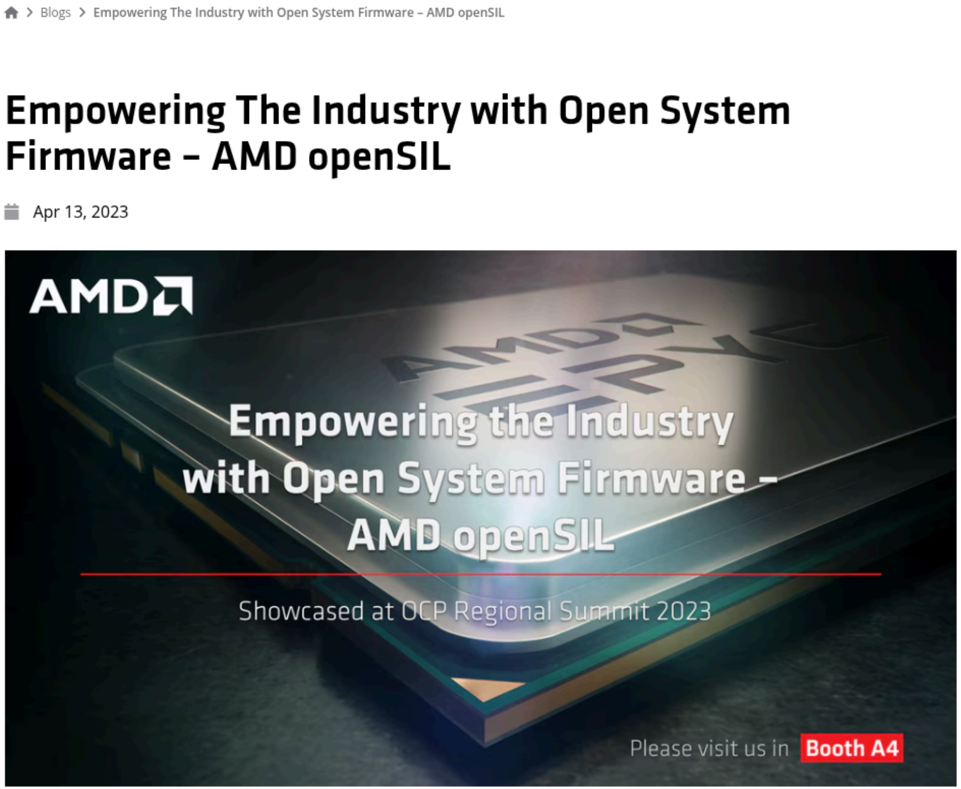
=~= libAMDxPRF

=~= libAMDxUSL

xSIM – x86 Si Init Module Library
xPRF – x86 Platform Reference FW Library
xUSL – x86 Utilities & Support Library

https://www.amd.com/en/blogs/2023/empowering-the-industry-with-open-system-firmware-.html

AMD OpenSIL - ”Empowering The Industry”



Blogs > Empowering The Industry with Open System Firmware – AMD openSIL

Empowering The Industry with Open System Firmware – AMD openSIL

Apr 13, 2023

AMD

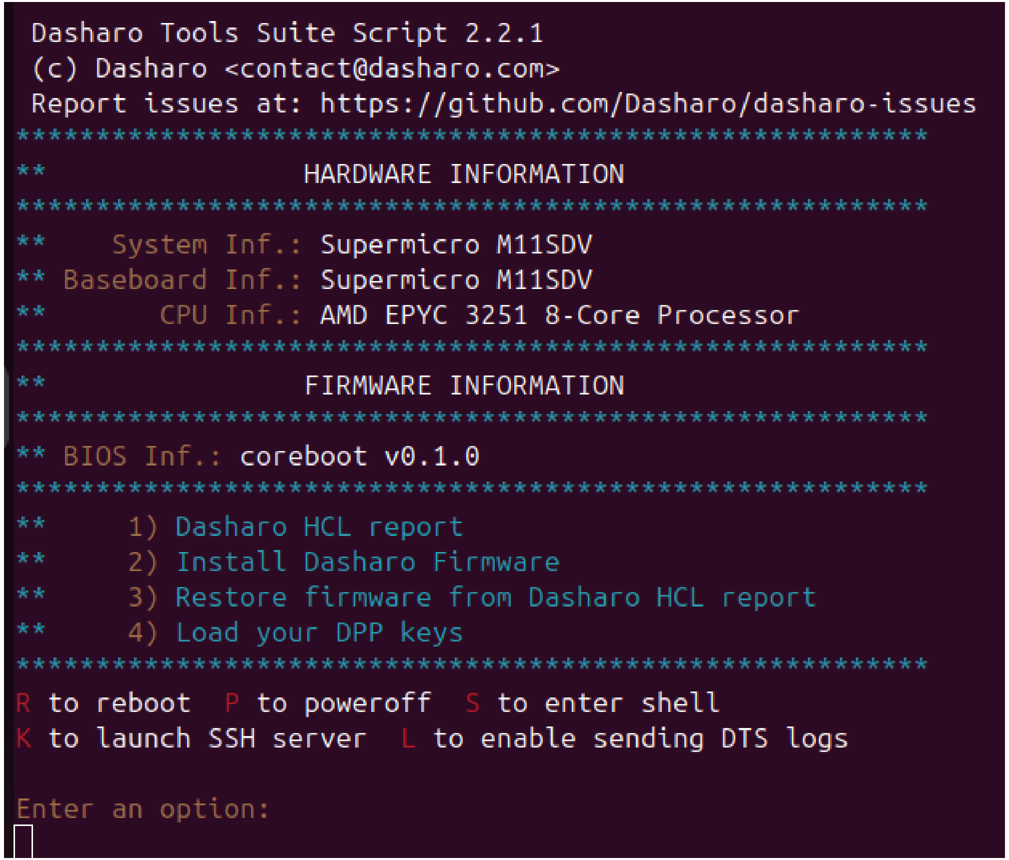
Empowering the Industry with Open System Firmware – AMD openSIL

Showcased at OCP Regional Summit 2023

Please visit us in **Booth A4**

https://www.amd.com/en/blogs/2023/empowering-the-industry-with-open-system-firmware-.html

Bonus



```
 Dasharo Tools Suite Script 2.2.1
 (c) Dasharo <contact@dasharo.com>
 Report issues at: https://github.com/Dasharo/dasharo-issues
*********************************************************
**                HARDWARE INFORMATION
*********************************************************
**    System Inf.: Supermicro M11SDV
** Baseboard Inf.: Supermicro M11SDV
**       CPU Inf.: AMD EPYC 3251 8-Core Processor
*********************************************************
**                FIRMWARE INFORMATION
*********************************************************
** BIOS Inf.: coreboot v0.1.0
*********************************************************
**     1) Dasharo HCL report
**     2) Install Dasharo Firmware
**     3) Restore firmware from Dasharo HCL report
**     4) Load your DPP keys
*********************************************************
R to reboot  P to poweroff  S to enter shell
K to launch SSH server  L to enable sending DTS logs

Enter an option:
```

Closing Thoughts

- "Empowering The Industry" ? Time will show.
  - Empowering small businesses right now? Definitely.
- AMD slowly regains its position in open-source firmware ecosystem
  - They are way ahead of Intel in terms of new features and design

Q&A