Dasharo OSF vPub Spring 2022 (aka 3mdeb vPub vol. 5)

vPub Event

3mdeb Team

General rules

Our mission is to fill the space left by lack of direct human-to-human backstage discussion, networking and after-parties.

We are primarily dedicated to open source firmware, open source hardware, open instruction set architecture and reasonably secure operating systems.

Thank you for spending time with us! First of all have fun!

General rules

- For details (including clickable links) please visit: https://vpub.dasharo.com
- Chat is on #dasharo-osf-vpub:matrix.org
  - You can join video and audio from there
  - Presenters have to use https://meet.jit.si/dasharo-osf-vpub
  - Please note #dasharo-osf-vpub is just one of the channels in Dasharo Matrix Space, feel free to join others #dasharo:matrix.org
- Please note we using Jitsi free tier. We kindly ask to use video only when necessary (to say hello, for toast) or when the number of active participants gets small.
- Be kind to each other.
- Adult beverages allowed.
- Mute by default.
- No audio or video recording
- "Last *haker* standing party"
- Feel free to introduce yourself and tell us why you joined.
- Feel free to queue the topics, questions, problems, by adding to notes Etherpad widget.

History

- This is fifth event
  - not counting unofficial ones organized as part of virtual conferences
- Last event was called "Dasharo OSF vPub Winter 2022" and had place on 17th Feb 2022
- We were visited by 68 unique nicknames
- Event last for 7.5h (8PM UTC - 3:30AM UTC)
- Slides can be found in Dasharo OSF vPub Archive: https://vpub.dasharo.com/archive/vpub-0x4/

What's new

- We trying to make as much space for open discussion as possible
- On top of next 2 hours we have presentations topics that we will discuss today:
  - Daniel Maslowski will introduce us to RustSBI project
  - Michał Żygowski will present Qubes OS and MSI PRO Z690-A DDR4
- Please note we looking for project/topics and products suggestions for next vPub
  - On-going call for participation is on the bottom of vPub website
- After above talks if we would have enough energy we can switch to some open discussion topics we prepared for today:
  - What fun things we can do with analyze swtpm+QEMU+coreboot,
  - TrenchBoot - what's up in the project, how LKML patches, D-RTM in QEMU?
  - Seamless firmware deployment ideas/brainstorming,
  - Dasharo compatible with MSI Z690 DDR4 community test results.
  - Other stuff from notes in Etherpad widget

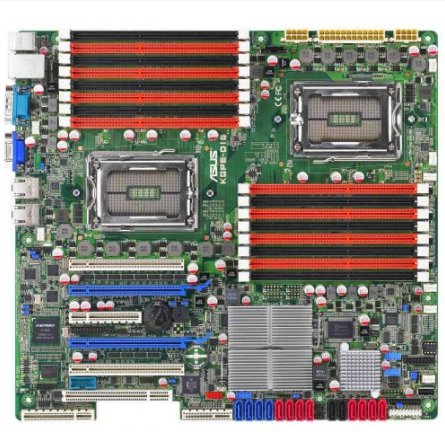
Crowdfunding

- Technology Common Trust created Open Firmware Found: https://technologycommons.org/OFF/

Intel ACM

- We didn't discussed much last time and discussion kind of died, but maybe we can get back to it today.
- Public review of the open letter draft to open the Intel ACMs code,
- Read-only version available here: https://pad.riseup.net/p/qmlVCDtO74uKOMbDaHUg

Dasharo compatible with ASUS KGPE-D16

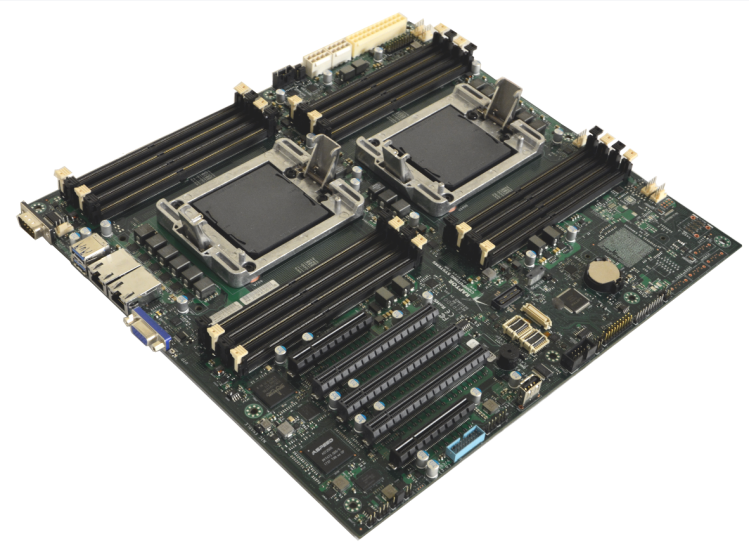


- Project sponsored by Immunefi with the purpose of building trustworthy platform for blockchain developers.
- Last release: v0.3.0 16 Dec 2021, Next release: WW22'22
- Documentation: https://docs.dasharo.com/variants/asus_kgpe_d16/releases/
- How to buy:
  - https://store.vikings.net/en/VKGS-WORK-D16
  - https://store.vikings.net/en/d16ryf

Dasharo compatible with MSI PRO Z690-A

- Funded through BTC anonymous contributions
  - KUDOS to Technology Common Trust Open Firmware Fund
- Last release: v0.4.0 13 May 2022, Next release: TBD
- Documentation: https://docs.dasharo.com/variants/msi_z690/releases/
- How to buy: TBD

Dasharo compatible with RCS Talos II

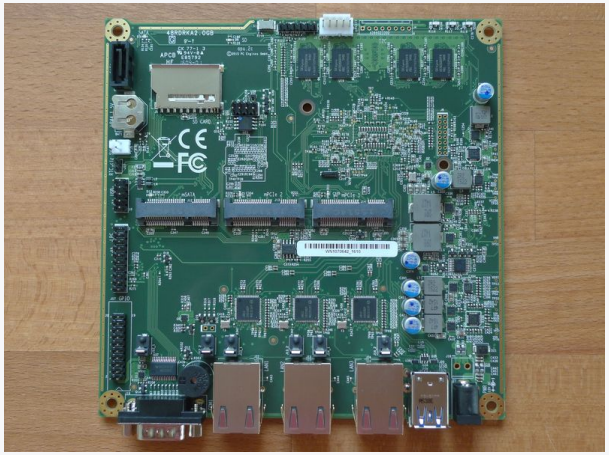


- Project sponsored by Insurgo with the purpose of building trustworthy platform for general purpose use.
- Last release: v0.5.0 12 Apr 2022
- Documentation: https://docs.dasharo.com/variants/talos_2/releases/
- How to buy: write to https://insurgo.ca/#contact

Dasharo compatible with Dell OptiPlex

- Project sponsored by 3mdeb with the purpose of creating daily driver for SME.
- Last release: v0.1.0 18 Jan 2021
- Documentation: https://docs.dasharo.com/variants/dell_optiplex/overview/
- How to buy: 3mdeb eBay https://www.ebay.pl/usr/3_mdeb

Dasharo for PC Engines



- Project sponsored by PC Engines with the purpose of providing high quality firewall hardware.
- Last release: v4.15.0.3 16 Feb 2022
- Documentation: https://pcengines.github.io
- How to buy: https://www.pcengines.ch/order.htm
- This firmware is not branded Dasharo, but based on it bake custom PC Engines firmware and provide it under Dasharo branding.

Dasharo compatible hardware

- **NovaCustom NV40 Series**
  - Project sponsored by NovaCustom with the purpose of providing open source firmware laptop.
  - Last release: v1.0.0 19 Jan 2022
  - Documentation: https://docs.dasharo.com/variants/clevo_nv41/releases
  - How to buy: https://configurelaptop.eu/nv40-series/

- Website: https://ost2.fyi/
- OpenSecurityTraining2 reward system plans and ideas,
  - Idea of Slack with access to trainers for students who finished at least one course was approved and is under implementation,
- Other ideas discussed at FOSDEM'22 after-party: NFT

Root of Trust

- Recent advancements in Root of Trust technologies (MS Pluton announcements, TrenchBoot project status)

Next vPub plans and ideas

- Dasharo open-source firmware vPub Summer 2022
  - may be replaced by hybrid Qubes OS mini-summit

Q&A