

# Qubes OS on modern Alder Lake desktop

Qubes OS Summit 2022





Michał Żygowski



- Introduction
- Qubes OS on desktop. Why?
- Desktop and open-source firmware?
- Dasharo
- Qubes OS certification requirements
- Present and future of desktop support in OSF
- Demo
- Q&A



Michał Żygowski  
*Firmware Engineer*

-  [@\\_miczyg\\_](https://twitter.com/_miczyg_)
-  [michal.zygowski@3mdeb.com](mailto:michal.zygowski@3mdeb.com)
-  [linkedin.com/in/miczyg](https://linkedin.com/in/miczyg)
-  [facebook.com/miczyg1395](https://facebook.com/miczyg1395)
- Braswell SoC, PC Engines and Protectli maintainer in coreboot
- OpenPOWER System Software Technical Workgroup chair
- 5 years in Open Source Firmware
- interested in advanced hardware and firmware security features
- OST2 instructor
- TrenchBoot developer



- 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

- Qubes OS is magnificent in terms of security
- Sometimes with security come sacrifices
- Qubes OS heavily depends on virtualization which has a non-zero performance penalty
  - This can be noticeable on laptops (especially the older ones like Lenovo x230)
- Keeping the old machines well supported by fully open-source firmware, like coreboot for Lenovo Thinkpad x230 is great, but at some point we have to move forward

- The main disadvantage of desktops is almost zero mobility, while laptops are all-in-one devices ready to use, but...
- Desktops outperform mobile devices
- Are they less secure?
  - Not necessarily ;)



- Answer is: **YES**
- For a long time coreboot had no port of a modern desktop (except some single node mini-servers which could serve as workstation)
- Latest supported machine is 9th Gen Intel Core device
- Big elaboration about the state on [reddit](#)
- The time has come to break this status quo

- An opportunity to support most recent 12th Generation Intel Core Alder Lake based desktop with open-source firmware appeared
- MSI PRO Z690-A has been selected as a new port target to Dasharo
- Now what is Dasharo you may ask?

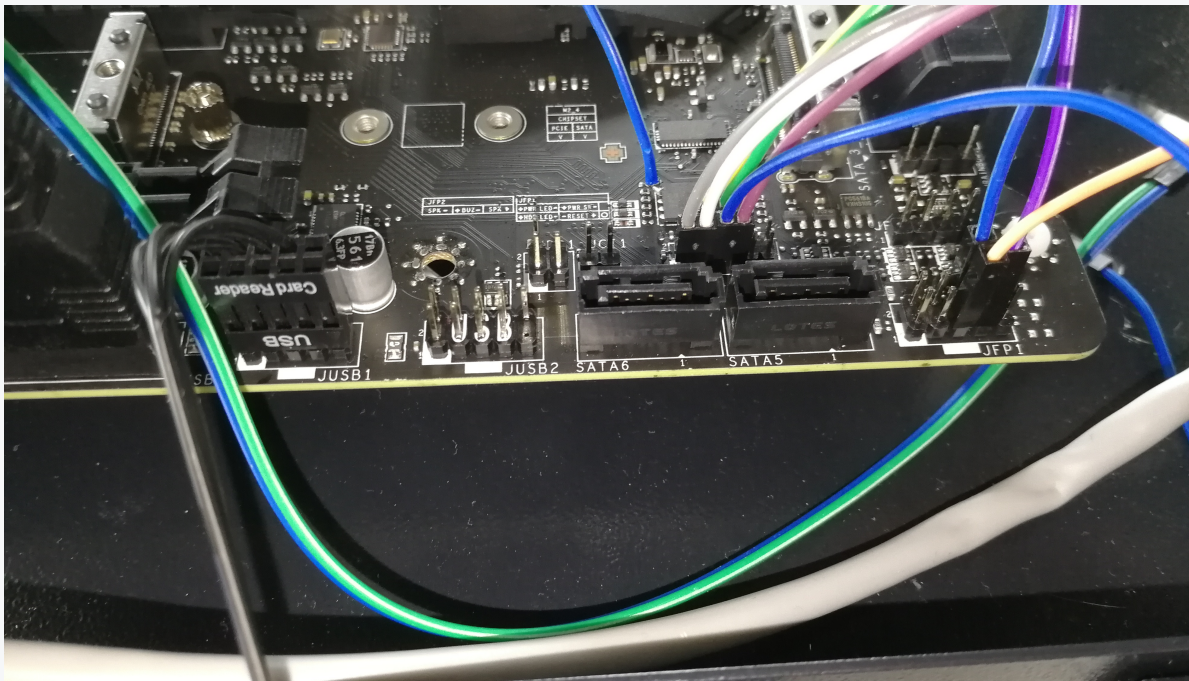






Dasharo is open source firmware distribution, we prefer clean and simple code, long term maintenance, privacy-respecting implementation, liberty for the owners, and trustworthiness for all.

- Dasharo compatible with MSI PRO Z690-A (WIFI) DDR4
- Most recent release v1.0.0 with basic support completed
- More on [docs.dasharo.com](https://docs.dasharo.com) (including binaries and documentation)
- How you make it possible? Just like this:



What we currently support:

- Booting Linux distros and Windows 10/11
- Booting Qubes OS :) (apparently MSI firmware has some issues)
- UEFI compliant boot mode
- iPXE
- Boot from USB, NVMe, SATA
- PS/2 keyboard/mouse support
- UEFI Secure Boot
- TPM and measured boot



What we WANT to support:

- Overclocking
- Firmware setup password
- ME disabling
- Firmware flashing with USB with FLASHBIOS button
- Power state after power fail
- And many many more...

But what we would really like  
is to meet Qubes certification  
requirements.

- In June this year Demi Marie Obenour started a new thread on [qubes-devel](#) mailing list called "Future certification requirements"
- The thread describes 7 security aspects of the hardware and firmware that must be met to be eligible for certification
- These mostly touch the following:
  - PCI devices state
  - DMA
  - USB and Network controllers
  - and PCI Option ROMs

- We plan a new release of Dasharo v1.1.0 compatible with MSI PRO Z690-A DDR4 WIFI
- One of the new features addresses one of the future certification requirements:

3. The firmware's network stack (if any) must be disabled **by default**.

Rationale: This is a large attack surface **that** is almost never useful for desktops or laptops, except in corporate environments.

- Other features included:
  - Codebase rebased on recent coreboot tree with various Alder Lake support improvements and fixes
  - [Bugfix for Ventoy delay bug](#)
  - Bugfix for incorrectly parsed PCI aperture above 4G
  - Implement network boot enable/disable option

# 3MDEB Present and future of desktop support in OSF

- In the new release we also planned to cover the performance differences compared to MSI firmware
- However these settings are SKU dependent and their change may be dangerous on different CPU:
  - Custom AC/DC loadline for voltage regulator
  - Custom power limits
  - Custom lccMax (current limit)
- Dasharo provides Intel recommended defaults for these
- In the future it will be possible to tune these parameters when overclocking setup options become available

Cinebench R23 results after applying same settings for i5-12600K CPU:

Firmware	Multi Thread	Single Thread
MSI 1.70	17020	1852
Dasharo v1.1.0, Intel defaults	15438	1731
Dasharo v1.1.0, AC/DC loadline 0.8 mOhm	16760	1634
Dasharo v1.1.0, AC/DC loadline 0.8 mOhm, IccMax 250A	16722	1714
Dasharo v1.1.0, AC/DC loadline 0.8 mOhm, IccMax 250A, Power Limits 241W	16712	1621
Dasharo v1.1.0, all modifications	16702	1640

- All modifications mean: AC/DC loadline 0.8 mOhm, IccMax 250A, Power Limits 288W, Energy Efficient Turbo Disabled, Cache frequency Limit equal 49
- Abnormal Single Thread score are caused by irregular CPU affinity (sometimes the load is generated on Efficient core)



# 3MDEB Present and future of desktop support in OSF

- We would like to continue efforts with supporting the desktops with open-source firmware
- Raptor Lake 13th Gen Intel Core CPU can be supported on the ported MSI PRO Z690-A (WIFI) DDR4
- Z690 chipset allows full overclocking capabilities of Intel system, so can generate the most performance
- We see much interest in the desktop segment, hopefully Qubes OS project also has some demand on such machines :)

# DEMO time!

- Securing the desktop from firmware side is possible thanks to open-source firmware
- Securing the desktop from software side is possible thanks to Qubes OS project
- What do you need more?
- More Hz on the CPU cores? Sure go ahead.
  - But this machine already boots Qubes OS insanely fast!
  - Actually typing disk password takes longer than loading whole system :)

# Q&A



Thank you!