

TrenchBoot AEM - Project Status

FOSDEM 2024

Open Source Firmware, BMC and Bootloader devroom

Maciej Pijanowski





Maciej Pijanowski
Engineering Manager

-  [@macpijan](https://twitter.com/macpijan)
-  maciej.pijanowski@3mdeb.com
-  linkedin.com/in/maciej-pijanowski-9868ab120
- over 7 years in 3mdeb
- Open-source contributor
- Interested in:
 - build systems (e.g., Yocto)
 - embedded, OSS, OSF
 - firmware/OS security



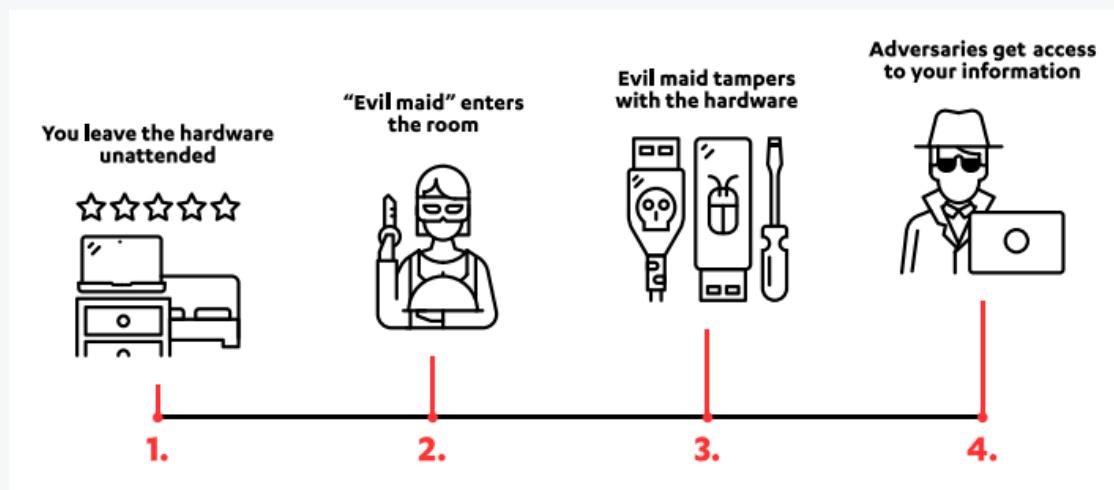
- coreboot licensed service providers since 2016 and leadership participants
- UEFI Adopters since 2018
- Yocto Participants and Embedded Linux experts since 2019
- Official consultants for Linux Foundation fwupd/LVFS project since 2020
- IBM OpenPOWER Foundation members since 2020

- Intro
- Qubes OS AEM
- Current state
- Further plans
- Q&A

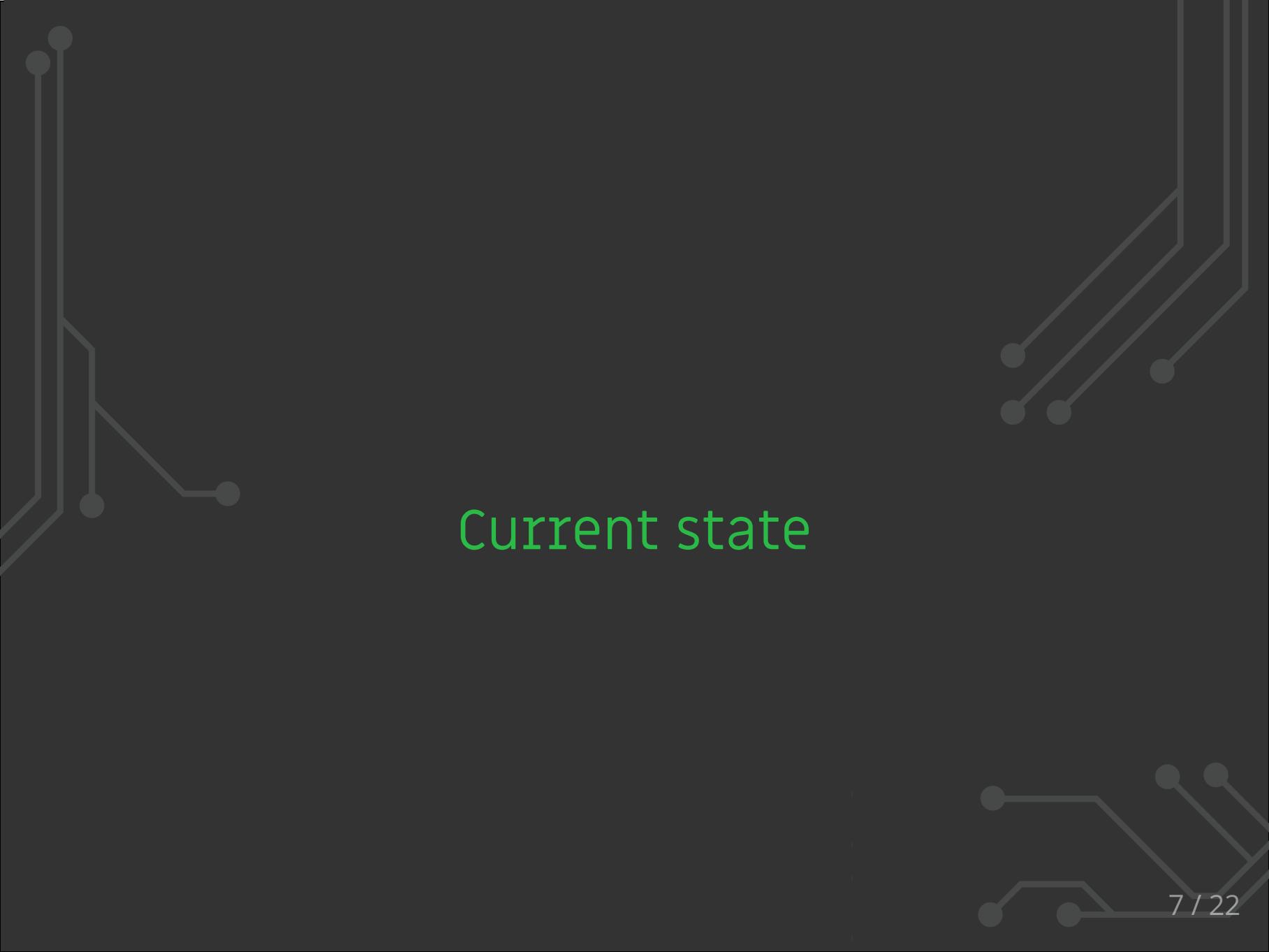
- Today we will cover current state since Oct 2023 and further plans
- Project has been already discussed during past Qubes OS summits
 - <https://www.youtube.com/watch?v=A9GrIQsQc7Q&t=17441s>
 - <https://www.youtube.com/live/xo2BVTn7ohs?si=BVUnKccSe-saRf2b&t=5441>



- A set of software packages and utilities
 - <https://github.com/QubesOS/qubes-antievilmайд>
- The goal to protect against Evil Maid attacks
- Requires TPM
- Requires **Dynamic Root of Trust for Measurement (DRTM)**
 - technology from silicon vendor
 - needs to be present in hardware and supported by the firmware

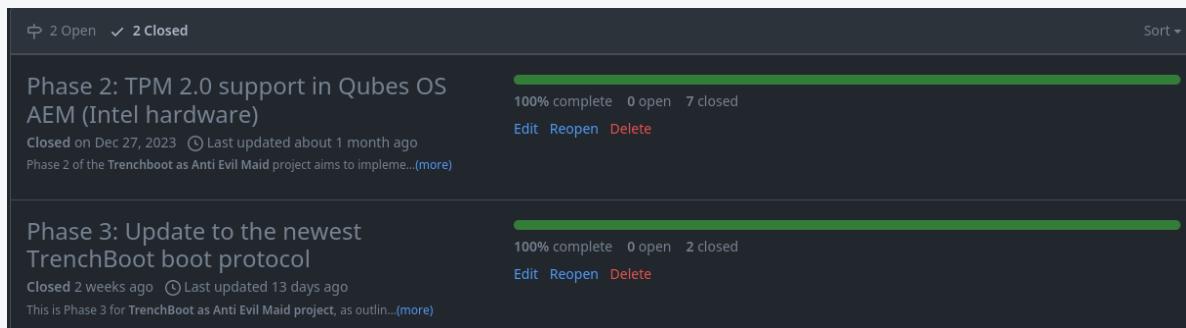


<https://blog.f-secure.com/de/evil-maid-attacken-wenn-die-putzfrau-den-pc-hackt/>



Current state

- Phase 2 released
 - <https://github.com/TrenchBoot/trenchboot-issues/milestone/2>
- Phase 3 released
 - <https://github.com/TrenchBoot/trenchboot-issues/milestone/3>
- Phase 4 started
 - <https://github.com/TrenchBoot/trenchboot-issues/milestone/4>

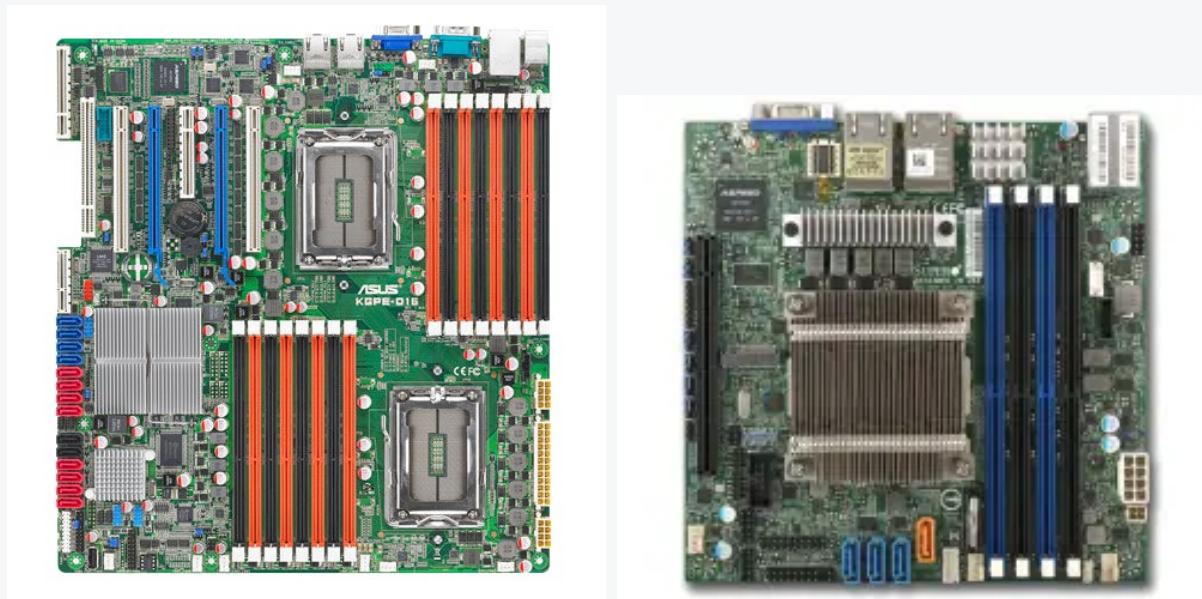


- Qubes OS AEM on Intel boards with TPM 2.0
- GH release
 - GRUB: https://github.com/TrenchBoot/grub/releases/tag/aem_v0.2
 - Xen: https://github.com/TrenchBoot/xen/releases/tag/aem_v0.2
 - Qubes OS AEM: https://github.com/TrenchBoot/qubes-antievilmaid/releases/tag/aem_v0.2
- Blog post
 - https://blog.3mdeb.com/2023/2023-09-27-aem_phase2/



- Update to recent TrenchBoot boot protocol
- GH release
 - GRUB: https://github.com/TrenchBoot/grub/releases/tag/aem_v0.3
 - Xen: https://github.com/TrenchBoot/xen/releases/tag/aem_v0.3
 - Qubes OS AEM: https://github.com/TrenchBoot/qubes-antievilmaid/releases/tag/aem_v0.3
- Upstreaming into Qubes OS still in progress
 - Xen: <https://github.com/QubesOS/qubes-vmm-xen/pull/160>
 - GRUB: <https://github.com/QubesOS/qubes-grub2/pull/13>
- Blog post
 - https://blog.3mdeb.com/2024/2024-01-12-aem_phase3/

- Qubes OS AEM on AMD boards with TPM 1.2 and TPM 2.0
- HW selection
 - Asus KGPE-D16
 - Supermicro M11SDV-4C-LN4F (QubesOS 4.2 install issue)
 - subject to change



QubesOS installation issue: <https://github.com/QubesOS/qubes-issues/issues/8322#issuecomment-1904423204>

Further plans

- Phase 5
 - UEFI support
 - so far we focused on legacy boot
 - both Intel and AMD
 - both TPM 1.2 and TPM 2.0
 - Finalizing scope
 - To be presented as another GH milestone
 - Opens up wider hardware variety

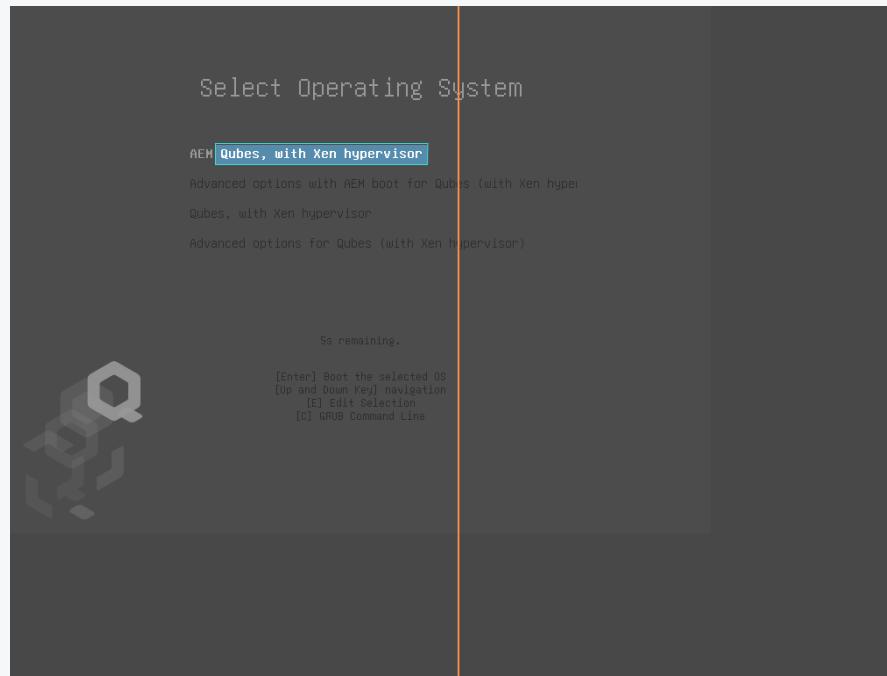


- Project consists of multiple moving parts
- Installation of custom packages under QubesOS can be challenging
- A lot of manual work was required
- We have started some automation effort as shown in the last status



```
[qubesos@dom0 ~]$ sudo anti-evil-maid-install -m /dev/sdal
trousers_changer_migrate: already migrated
trousers_changer_identify: identifying TPM
WARN: Reading full size of the NV index
trousers_changer_identify: TPM identity: 220479728a7546379fafb02dcc3c15b2ca87146c
anti-evil-maid-install: WARNING: Installing MFA AEM on the same disk
anti-evil-maid-install: as Qubes OS will NOT provide any resistance
anti-evil-maid-install: against keyboard observation during boot!
anti-evil-maid-install: Additionally, compromise recovery using
anti-evil-maid-install: freshness token revocation will be a lot
anti-evil-maid-install: less feasible.
Press <ENTER> to continue...
anti-evil-maid-install: Labeling filesystem aem
anti-evil-maid-install: Assigned slot 0 to this AEM media
anti-evil-maid-install: Generating new 160-bit TOTP seed
```

- The goal is to move that forward
 - Run tests on hardware, not only QEMU
 - Automatically install artifacts from Github Actions

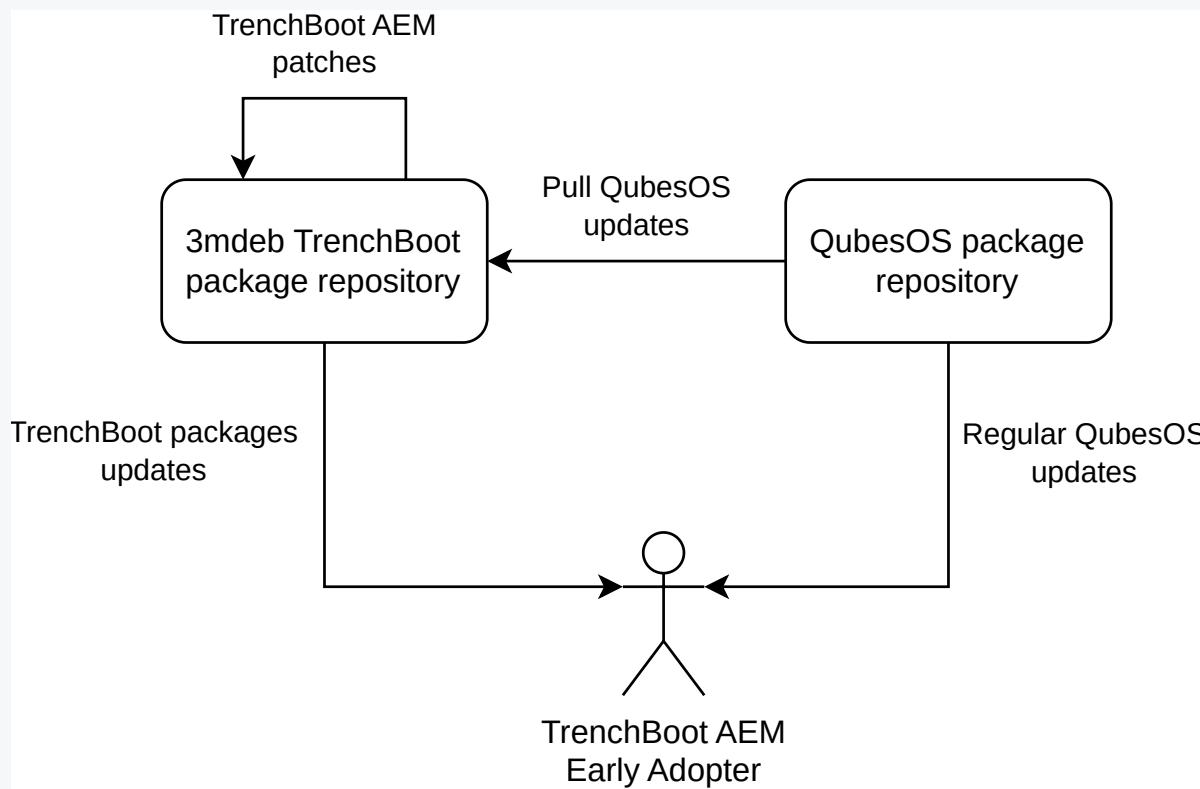


- Intel series in progress
 - v7 and counting
 - <https://lore.kernel.org/lkml/2023110222751.219836-1-ross.philipson@oracle.com/>
- nlnet grant for AMD equivalent
 - <https://nlnet.nl/project/TrenchBoot-AMD/>
- Sync with Oracle's latest work
- Will need some more time to start this effort
 - ideally if some Intel part is already merged





DASHARO



- Interested? Join [Matrix channel](#).

- TrenchBoot Matrix channel
 - <https://matrix.to/#/#OSFW-Trenchboot:matrix.org>



We are open to cooperate and discuss

-  contact@3mdeb.com
-  facebook.com/3mdeb
-  [@3mdeb_com](https://twitter.com/3mdeb_com)
-  linkedin.com/company/3mdeb
- <https://3mdeb.com>
- [Book a call](#)
- [Sign up for the newsletter](#)

Feel free to contact us if you believe we can help you in any way. We are always open to cooperate and discuss.



Q&A



The poster features a dark background with a large, faint circular gear pattern in the center. In the top left corner is the 3MDEB logo, which includes a stylized shield with a crown and a gear-like shape. To its right is the text "3MDEB". Below these, the main title "FOSDEM 2024 UNOFFICIAL AFTERPARTY WITH 3MDEB TEAM!" is displayed in large, white, outlined font. To the right of the title is a small illustration of two beer mugs clinking. At the bottom left, there's a small icon of a location pin next to the venue details: "THE FUNKY MONKEY RUE ARCHIMÈDE 65 11000 BRUXELLES BELGIUM". On the bottom right is a small photograph of the interior of "The Funky Monkey" bar, showing tables and chairs. The bottom of the poster has a decorative border of blue hexagonal patterns.

**FOSDEM 2024
UNOFFICIAL
AFTERPARTY WITH
3MDEB TEAM!**

**Sunday, 04th February
Start at 19:00 (7:00 PM)**

 THE FUNKY MONKEY
RUE ARCHIMÈDE 65
11000 BRUXELLES
BELGIUM



 **FOR MORE INFORMATION :**
<https://matrix.to/#/#dasharo-osf-vpub:matrix.org>