F-UKI - links to talks, upstream PRs, specs and documentations

References:

- *UKI spec*: https://github.com/uapi-group/specifications/blob/main/specs/unified_kernel_image.md
- Emanuele's FOSDEM 2024 talk on UKI/secure boot work Red Hat is doing https://archive.fosdem.org/2024/events/attachments/fosdem-2024-2024-uki-addons-and-extensions-safely-extending-ukis-kernel-command-line-and-initrd/slides/22125/Uki_addons_O97iYns.pdf
- Lennart's FOSDEM 2024 talk on systemd-boot and UKI https://archive.fosdem.org/2024/events/attachments/fosdem-2024-1987-systemd-boot-systemd-stub-ukis/slides/22834/systemd-boot_systemd-stub_UKIs_mNuvmv0.pdf
- SHIM source: https://github.com/rhboot/shim/
- SBAT details: https://github.com/rhboot/shim/blob/main/SBAT.md

- Computer hardware IDS (CHID): https://learn.microsoft.com/en-us/windows-hardware/drivers/dashboard/using-chids
- Secure boot and measured boot Microsoft page: https://learn.microsoft.com/en-us/windows/security/operating-system-security/system-security/secure-the-windows-10-boot-process
- Controlling secure boot https://www.rodsbooks.com/efi-bootloaders/controlling-sb.html
- Measured boot design https://trustedfirmware-a.readthedocs.io/en/v2.11/design_documents/measured_boot.html
- Remote attestation using ephemeral TPM https://dl.acm.org/doi/pdf/10.1145/3627106.3627112
- *Intel TDX whitepaper* https://cdrdv2.intel.com/v1/dl/getContent/690419
- *AMD Secure Encrypted Virtualization* https://www.amd.com/en/developer/sev.html

Links to activities

- KVM Forum 2024 talk page: https://pretalx.com/kvm-forum-2024/talk/HJSKRQ/
- Hypervisor interface design doc:
  - https://docs.google.com/document/d/14P5L2mwaGcfsKKnDkQL5dxi7j1Mc1rzXtbuvilA5xfU/edit?usp=sharing
- QEMU hypervisor interface:
  - https://mail.gnu.org/archive/html/qemu-devel/2025-01/msg05693.html
- Systemd PRs:
  - https://github.com/systemd/systemd/pull/35091
  - Doc update: https://github.com/uapi-group/specifications/pull/131
  - https://github.com/systemd/systemd/pull/35747