Contribution ID: **405** Type: **not specified**

Enabling UEFI Secure Boot Across Modern Build Systems

Fundamental questions persist about who truly owns the machine: the user or the vendors who control the pre-enrolled keys. When UEFI firmware ships with Microsoft's keys as the sole root of trust, users must either accept vendor-dictated trust decisions or navigate complex firmware interfaces to enroll their own keys. For many in the free software community, this raises concerns about the balance between vendor control and user autonomy.

The practical consequence is that Linux distributions must obtain Microsoft signatures or remain unbootable on most commodity hardware with UEFI Secure Boot enabled. The greater ecosystem (Red Hat, Fedora, Ubuntu, Debian, openSUSE) has converged on shim—a minimal first-stage bootloader that Microsoft signs once per distribution, which then chains trust to distribution-specific keys. This creates structural dependency on Microsoft's signing process and adds complexity to build systems.

The alternative is self-signing (Gentoo, Arch, ParticleOS), where users generate and enroll their own keys directly in UEFI firmware. Manual key enrollment through inconsistent, vendor-specific firmware interfaces creates barriers that most users will not navigate. This makes self-signing viable primarily for power users, centralized enterprise environments, and embedded systems where firmware configuration is part of the deployment process—but impractical for distributions targeting general users.

Progress across build systems and distributions will take better tooling and greater cooperation. Key management remains especially challenging—securely storing private keys while making them accessible to automated CI/CD pipelines requires careful architecture that balances security with operational needs. Shared signing infrastructure that build systems could integrate with may offer a path toward reducing complexity while ensuring security. The purpose of this session is to explore what a shared approach to signing infrastructure could look like—and whether there are existing efforts we can build on or align with.

Primary author: VASQUEZ, Frank (Packt)

Presenter: VASQUEZ, Frank (Packt)

Session Classification: Build Systems MC

Track Classification: Build Systems MC