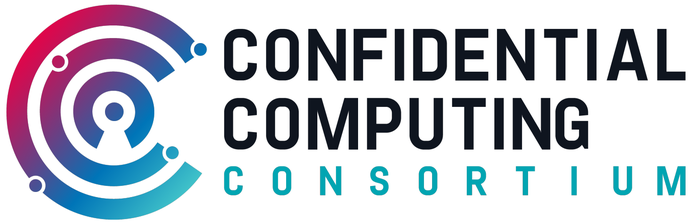
COCONUT-SVSM

2025 Annual Project Update



Introduction

Vision

COCONUT-SVSM is a platform to provide secure services to confidential virtual machines.

Introduction

Service Examples

- Virtual Trusted Platform Module
- Live Migration
- Variable Store
- Secure IRQ delivery

Introduction

History

- Launched in early 2022 with the goal of creating a secure service module for AMD SEV-SNP in Rust
- Published as Open Source software in March 2023
- Accepted as CCC project in April 2024
- Creation of a Technical Steering Committee in May 2025

Development

Statistics for the past year

- Non-merge commits: 715
- Merges: 251
- 425 files changed, 33961 insertions(+), 5952 deletions(-)
- 22 contributors in the last year
- Total of 32 contributors to date
- Company engagement: AMD, Google, HPE, IBM, Intel, Microsoft, Red Hat, SUSE, and more

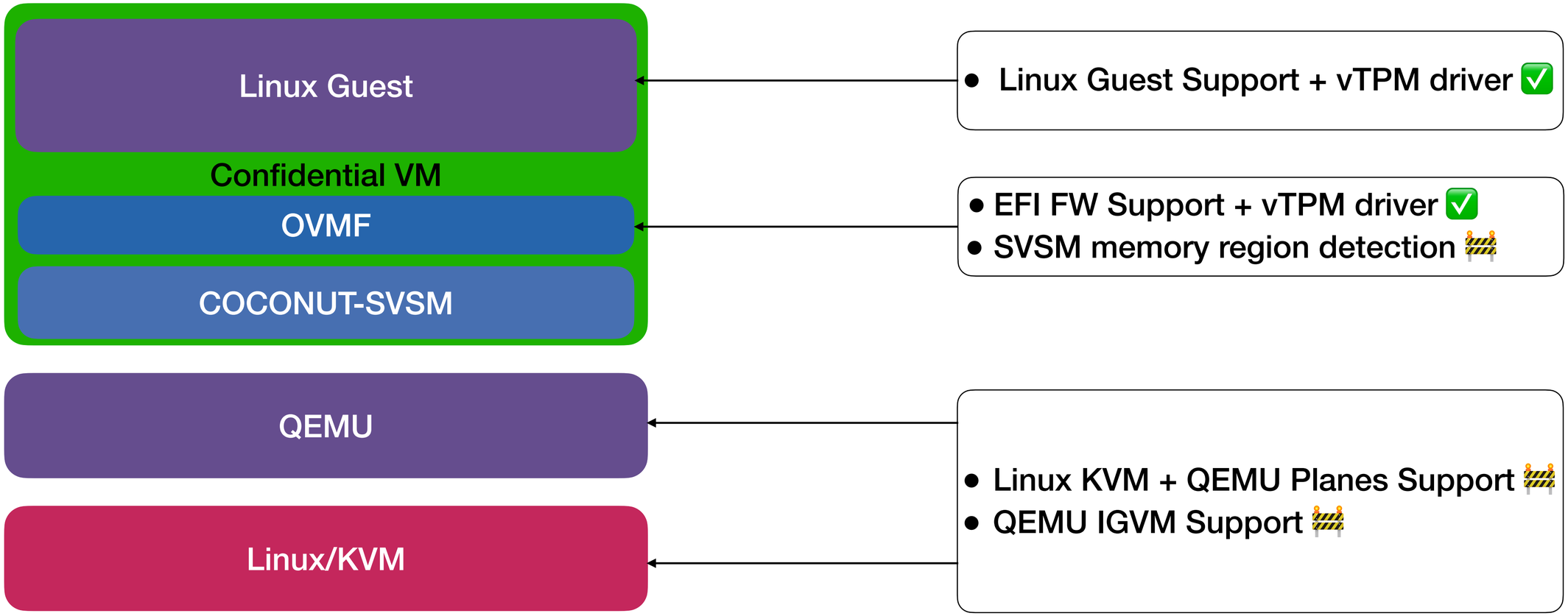
Development

Highlights

- Virtual TPM support (ephemeral) - Linux (6.16) and OVMF driver merged.
- Enhanced hypervisor support: KVM/QEMU, Hyper-V, GCE Vanadium.
- Multi-Platform support: AMD SEV-SNP, Intel TDX, Native.
- Moved to IGVM booting.
- Virtio-Block device driver.
- User-mode execution support evolving.
- Formal Verification (Experimental).

Development

Open Source Ecosystem



CONFIDENTIAL COMPUTING CONSORTIUM

COCONUT-SVSM

Development

One-Year Outlook

- Persistence support
- Platform-independent guest-management (VMM-)API
- Finish user-mode support and move services to CPL-3
- Consolidate crypto implementations
- Finish ecosystem support
- SVSM Bus
- EFI Variable Store

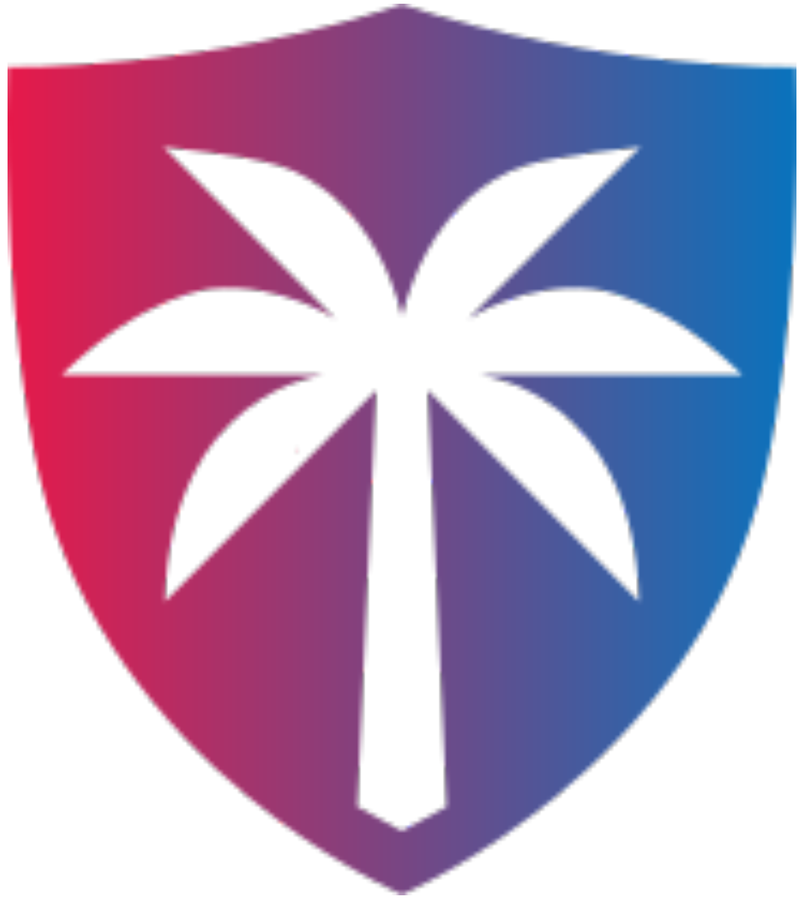
Development

Outlook Beyond

- Support running unenlightened guests.
  - Extend VMM-API for supporting paravisor-mode.
- Multi-architecture support.
- COCONUT-SVSM as a Rust target for standard library support.
- Extended Attestation Service.
- Implement more services.

Publicity

Project Logo



CONFIDENTIAL COMPUTING CONSORTIUM

COCONUT-SVSM

Publicity

Conferences

- FOSDEM
- Linux Plumbers Conference
- KVM Forum
- Linux Security Summit
- Open Confidential Computing Conference

Publicity

Conferences and Meet-ups - Outlook

- Keep presenting at open source conferences.
- Present at CCC conferences and meet-ups.
- Try to organise a COCONUT-SVSM community meet-up.

Governance

Community

- Collaboration via GitHub infrastructure.
- Public weekly development meetings.
- Project mailing list.
- Matrix chat room.

Governance

Technical Steering Committee

- Formed in May 2025.
- Closed weekly meetings for PR and Issue review, architectural discussions.
- Formal decision process
  - Voting **No** means veto.
- Decisions are published.

Governance

Technical Steering Committee

- Members:
  - Jon Lange
  - Jörg Rödel (chair)
  - Peter Fang
  - Stefano Garzarella

Thank You!

COCONUT-SVSM Community

Members of the Technical Steering Committee

Confidential Computing Consortium

CONFIDENTIAL COMPUTING CONSORTIUM

COCONUT-SVSM