Remote Attestation of Immutable Operating Systems built on systemd

30min

ĀMUTABLE

Hi! 👋

I’m Lennart Poettering

Chief Engineer @ Amutable

OC3 2026 - Berlin, DE
March 12th, 2026

AMUTABLE

`systemd` – What was that again?

Service Manager

System Manager

Collection of Userspace Components

Verified Boot & Remote Attestation

`systemd` & Amutable: strong focus on modern security technology for the OS

Verified/measured boot & remote attestation

Use cases: general purpose OS & VMs & CoCo

Attestation managed “inside” the machine, not from VMM

Vendor neutral

Measurement in PCRs + NvPCRs

General Model

Measure both boot and runtime

Predictable wherever we can, separate PCRs/NvPCRs where we can’t

Stay close to standards, i.e. TPM + UEFI

Build OS from reasonably measurable, coarse components

Focus: image based OSes, comprised of Verity-enabled DDIs

Measurements

Currently covered:

- Boot loader configuration (`systemd-boot`)
- UKIs and their components
- Kernel parameters + system credentials + confext images + sysext images + addons
- Boot phases
- Machine identity (`/etc/machine-id`, root fs UUID, root volume key, SMBIOS product UUID)
- Used LUKS keyslot
- Every activated DDI (Verity root hash)

Measurements

More to come:

- Container activation
- Portable service attachment
- User logs in (“break glass”)
- IMDS userdata
- SMBIOS Type #11 data
- …

Your own: io.systemd.PCRExtend Varlink API

Event Log

Userspace event log extends firmware event log:

`/run/log/systemd/tpm2-measure.log`

Modelled after TPM CEL, but not quite

Covers both PCRs and NvPCRs

“`systemd-pcrlock cel`” to read it

(In fact `systemd-pcrlock` does local attestation based on it already)

NvPCRs

PCRs are scarce

NvPCRs are TPM NV Index backed pseudo PCRs

(Almost) same semantics, same security

Still scarce

systemd currently defines 3 of them, but you can add more

Reports

Added in v260:

Get metrics out of system components, pluggable

In v261:

Get “facts” out of system components, pluggable

Next:

Enrich reports with TPM quote + PCR/NvPCR log

Upload support + Varlink API

Targeted confext

Reminder: `systemd-confext` is a mechanism to overlay `/etc/` with a Verity protected DDI.

Encryption + Verity

Goal: tied to TPM chip, PCRs/NvPCRs, TPM clock

Generate targeted confext DDI from most recent node report

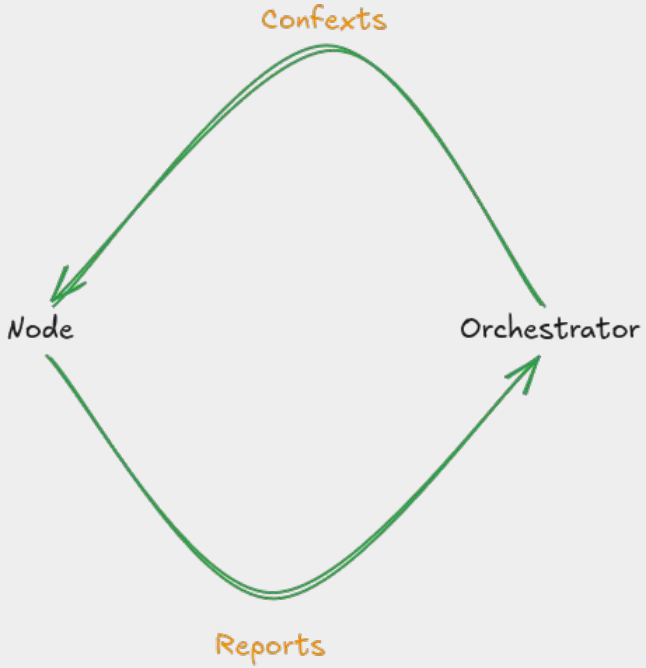
“Cryptographic Locked Loop”

CLL:

Node → orchestrator: **reports**

Orchestrator → node: **confexts**

Reports and confexts locked into each other



Summary

Let’s build Operating Systems that are measurable, from the ground up

Lot of infrastructure already

A lot more to do

In CoCo: vTPMs please

That’s it