

SNPGuard: Remote Attestation of SEV-SNP VMs Using Open Source Tools

Luca Wilke, [Gianluca Scopelliti](#)

7th Workshop on System Software for Trusted Execution (SysTEX'24)

gianluca.scopelliti@ericsson.com

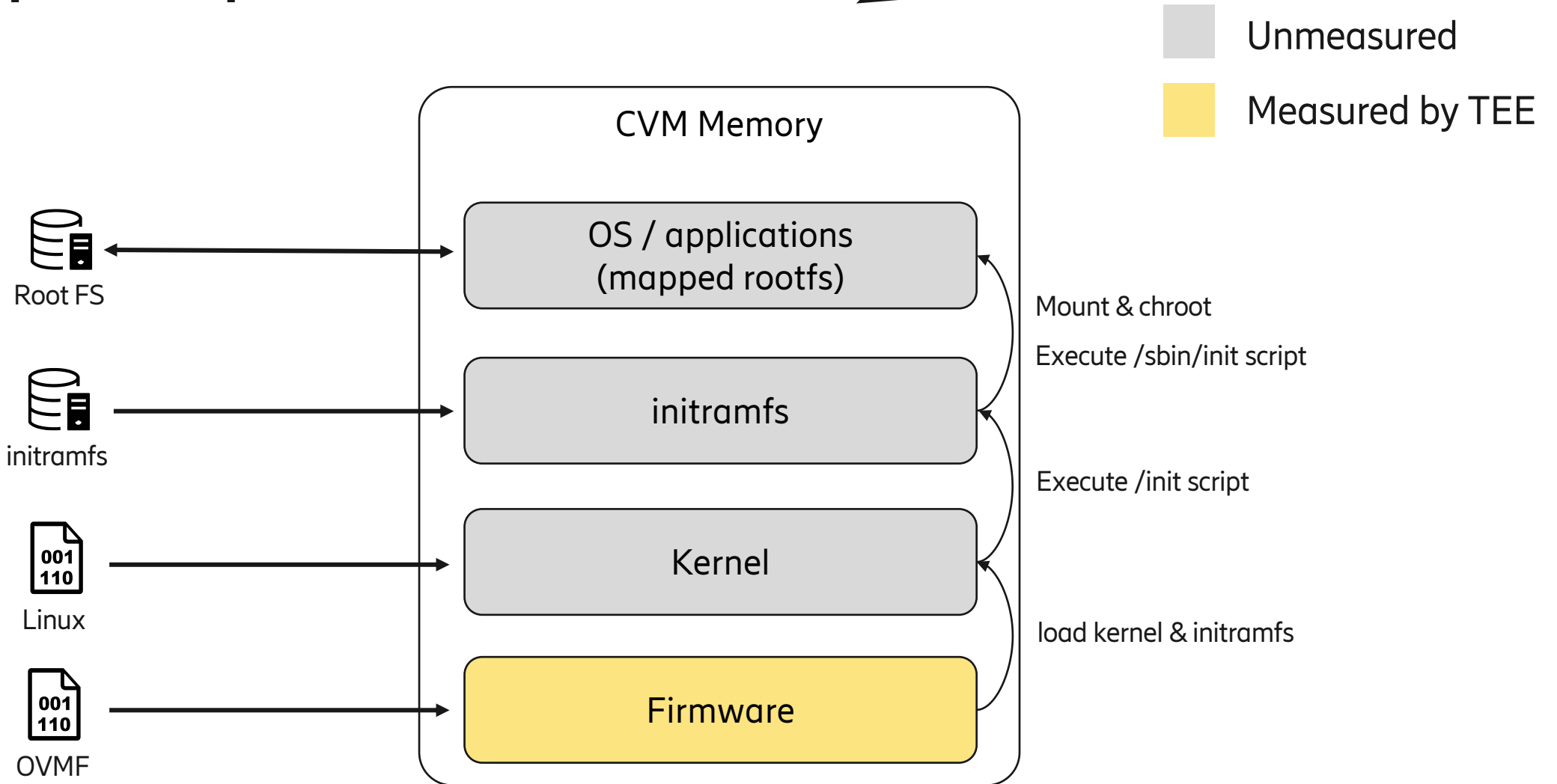


UNIVERSITÄT ZU LÜBECK

Disclaimer: This is **not** a research paper!

Recap from previous talk

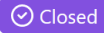
Ok.. Where do we start?



Problem: Setting up SEV-SNP workflows
is challenging!

The SEV-SNP toolchain is currently unstable

How to compute the correct launch digest of a QEMU SEV-SNP guest #30

 Closed gianlucascopelliti opened this issue on Oct 20, 2023 · 5 comments · Fixed by #32

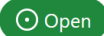


gianlucascopelliti commented on Oct 20, 2023

Hi,

Apologies for the noob question. I'm experimenting with SEV-SNP using the official scripts and tools from the repo (`snp-latest` branch). I'm at the point that I can correctly launch a SNP-enabled guest VM, and now I w

new OVMF changes break the measurement computation #194

 Open gianlucascopelliti opened this issue 2 weeks ago · 0 comments

stable-commits are not stable #194

 Open dreemkiller opened this issue on Oct 17, 2023 · 2 comments



dreemkiller commented on Oct 17, 2023

This repo works with a number of other repos (<https://github.com/AMDESE/qemu/> , <https://github.com/AMDESE/linux> , <https://github.com/AMDESE/sev-guest>) in order to complete a build.

You seem to have set up a system using the `stable-commits` file to mark the commits to use for a consistent build. However, those `stable-commits` are not commits, but branches, and those branches are changing. This is creating considerable problems for me when attempting to duplicate my work in any consistent fashion.

go

/ovmf repository made some changes to the SEV metadata section in the OVMF binary.

seems to be a new `SectionType` with ID 4 (maybe related to the SVSM?) that the library errors on the function `OvmfSevMetadataSectionDesc::try_from_bytes` called by `rs` in `src/measurement/ovmf.rs`.

but some commits made on April 17 (between [AMDESE/ovmf@ c212fec](#) and [AMDESE/](#) commits everything works fine.

ue, I can provide more details if needed.

Source: <https://github.com/AMDESE/AMDSEV/tree/snp-latest>

Official examples are incomplete or not documented

SEV-SNP Attestation Examples

repository is archived

This repository contains source, scripts, and configuration files for several open source tools that can be used together to demonstrate one way to perform remote attestation of SEV-SNP guests.

Note that these materials are intended for educational use only and come with no guarantee of fitness for any purpose.

Architectural Overviews

Architectural discussions and security considerations for each example are available in the [docs](#) directory. Currently, this repository contains the following examples:

- [SSH Key Exchange](#): Using remote attestation to securely exchange SSH public keys.
- Encrypted Disk Unlock: Using remote attestation to retrieve a disk encryption key and unlock an encrypted root filesystem.

insecure

not documented

Source: <https://github.com/AMDESE/sev-guest>

Related work either closed source or not standalone

Trustworthy confidential virtual machines for the masses

Anna Galanou*
TU Dresden
Germany
anna.galanou@tu-dresden.de

Khushboo Bindlish
DFINITY Foundation
Switzerland
khushboo.bindlish@dfinity.org

Luca Preibsch
Friedrich-Alexander-Universität
Erlangen-Nürnberg
Germany
luca.preibsch@fau.de

Yvonne-Anne Pignolet
DFINITY Foundation
Switzerland
yvonneanne@dfinity.org

Christof Fetzer
TU Dresden
Germany
christof.fetzer@tu-dresden.de

Rüdiger Kapitza
DFINITY Foundation
Switzerland
Friedrich-Alexander-Universität
Erlangen-Nürnberg
Germany
ruediger.kapitza@fau.de

code not available?

SPIRE plugin

Attesting AMD SEV-SNP Virtual Machines with SPIRE

Davi Pontes
Federal University of Campina Grande
Campina Grande, Paraíba, Brazil
davi.pontes@lsd.ufcg.edu.br

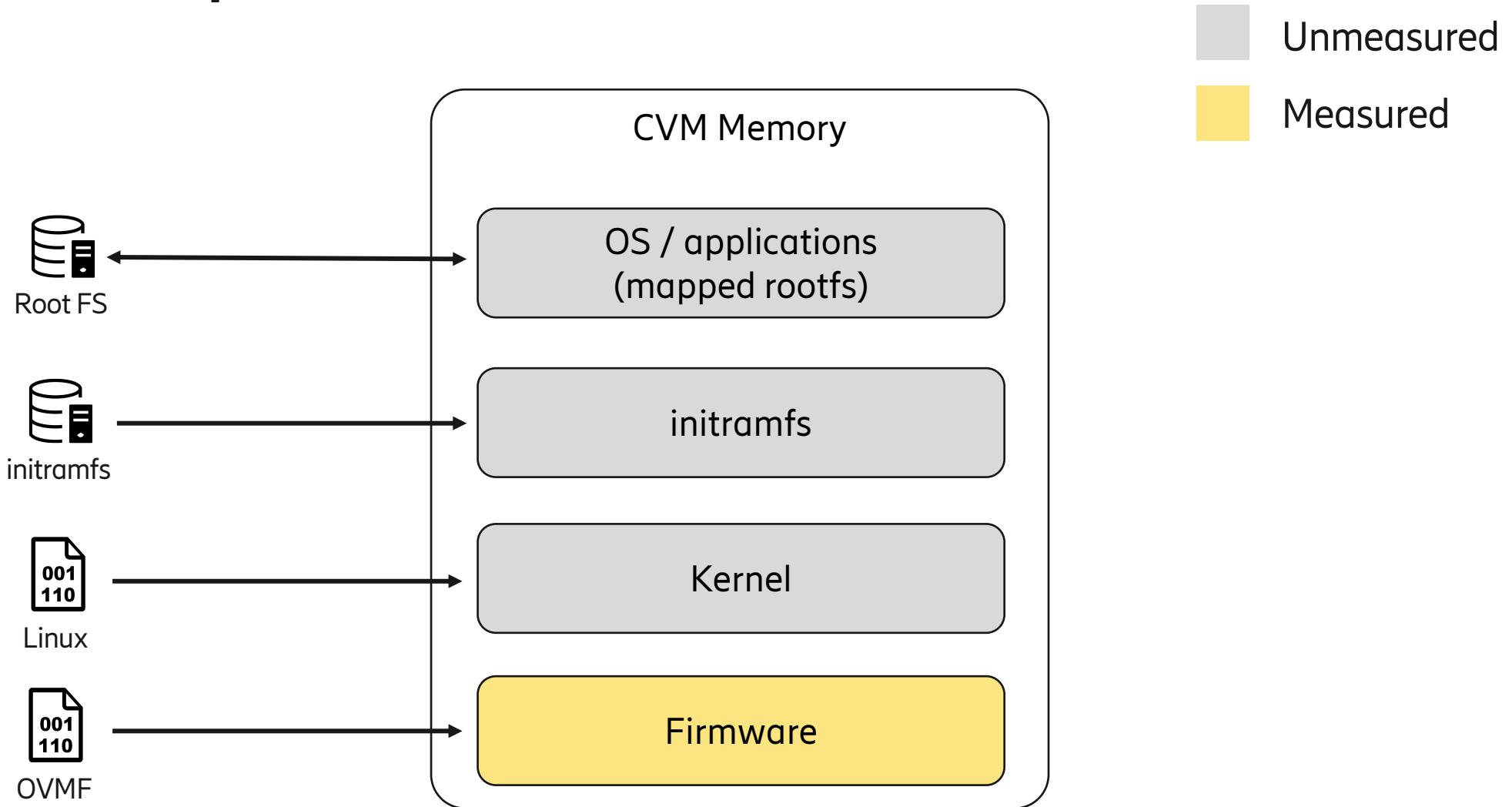
Fernando Silva
Federal University of Campina Grande
Campina Grande, Paraíba, Brazil
fernando.silva@lsd.ufcg.edu.br

Eduardo Falcão
Federal University of Rio Grande do Norte
Natal, Rio Grande do Norte, Brazil
eduardo@dca.ufrn.br

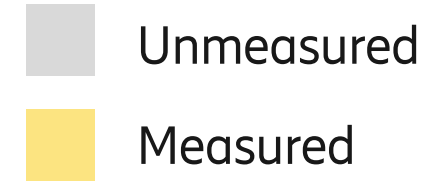
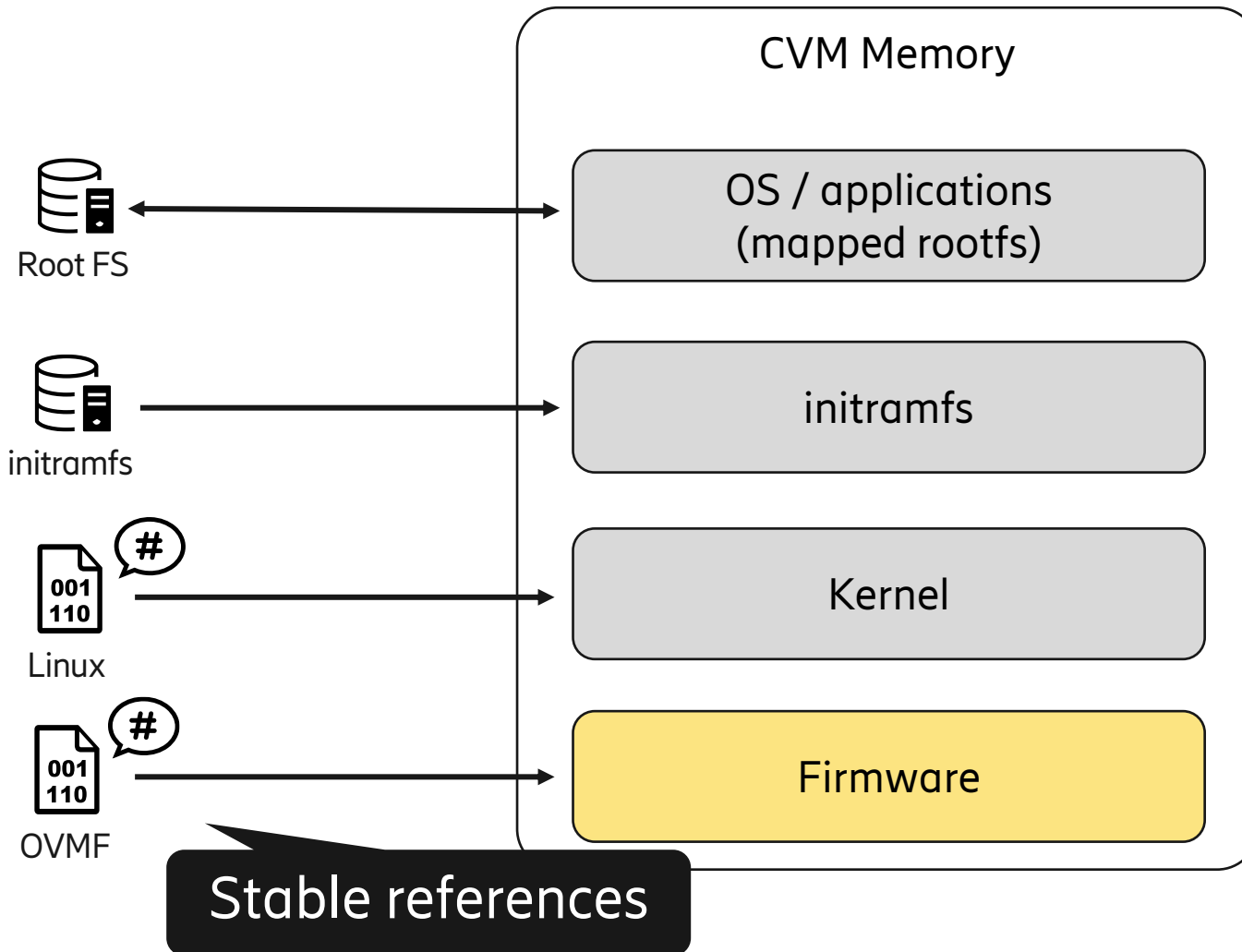
Andrey Brito
Federal University of Campina Grande
Campina Grande, Paraíba, Brazil
andrey@computacao.ufcg.edu.br

Solution: SNPGuard!

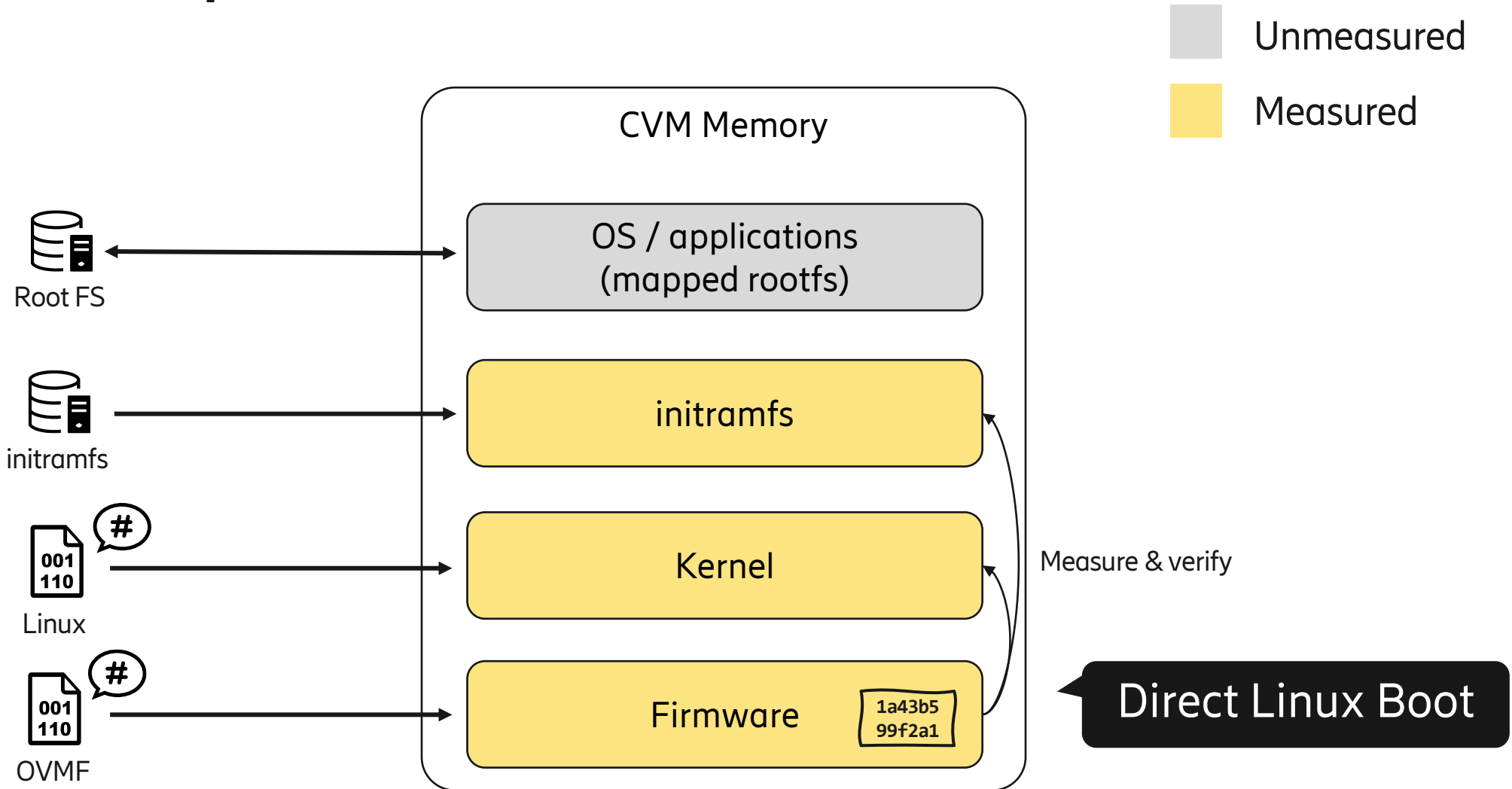
Main concepts



Main concepts

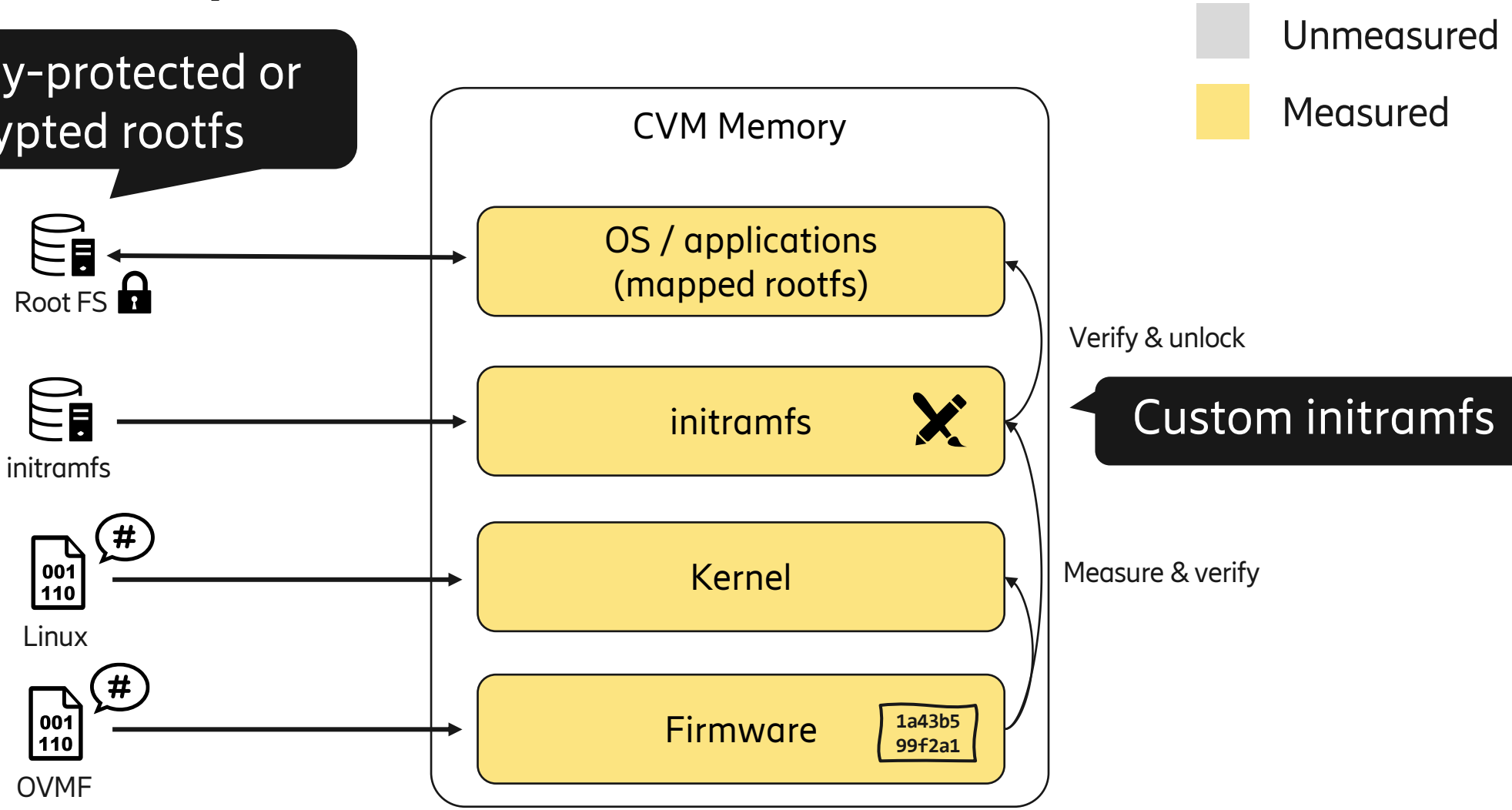


Main concepts



Main concepts

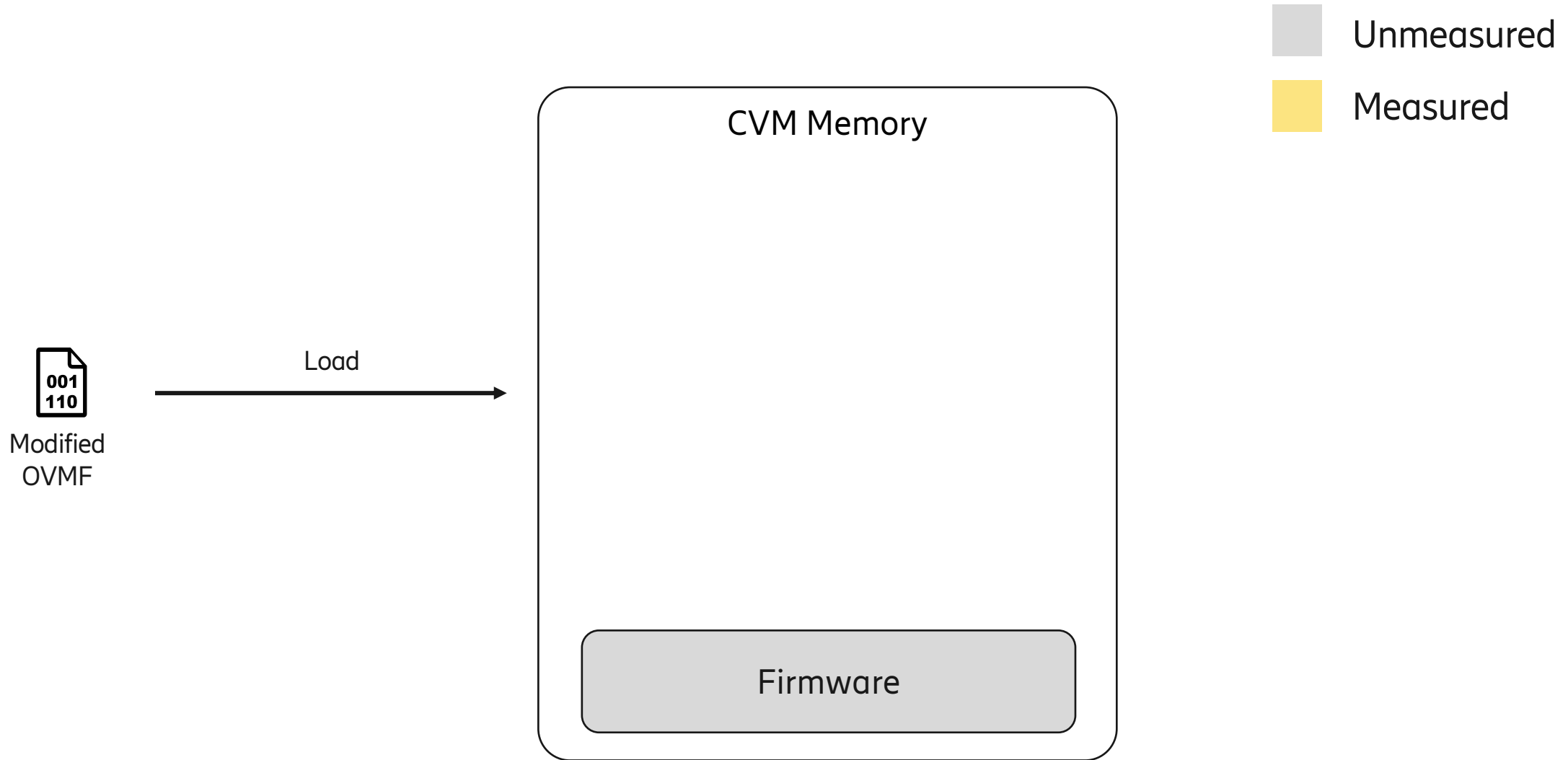
Integrity-protected or encrypted rootfs



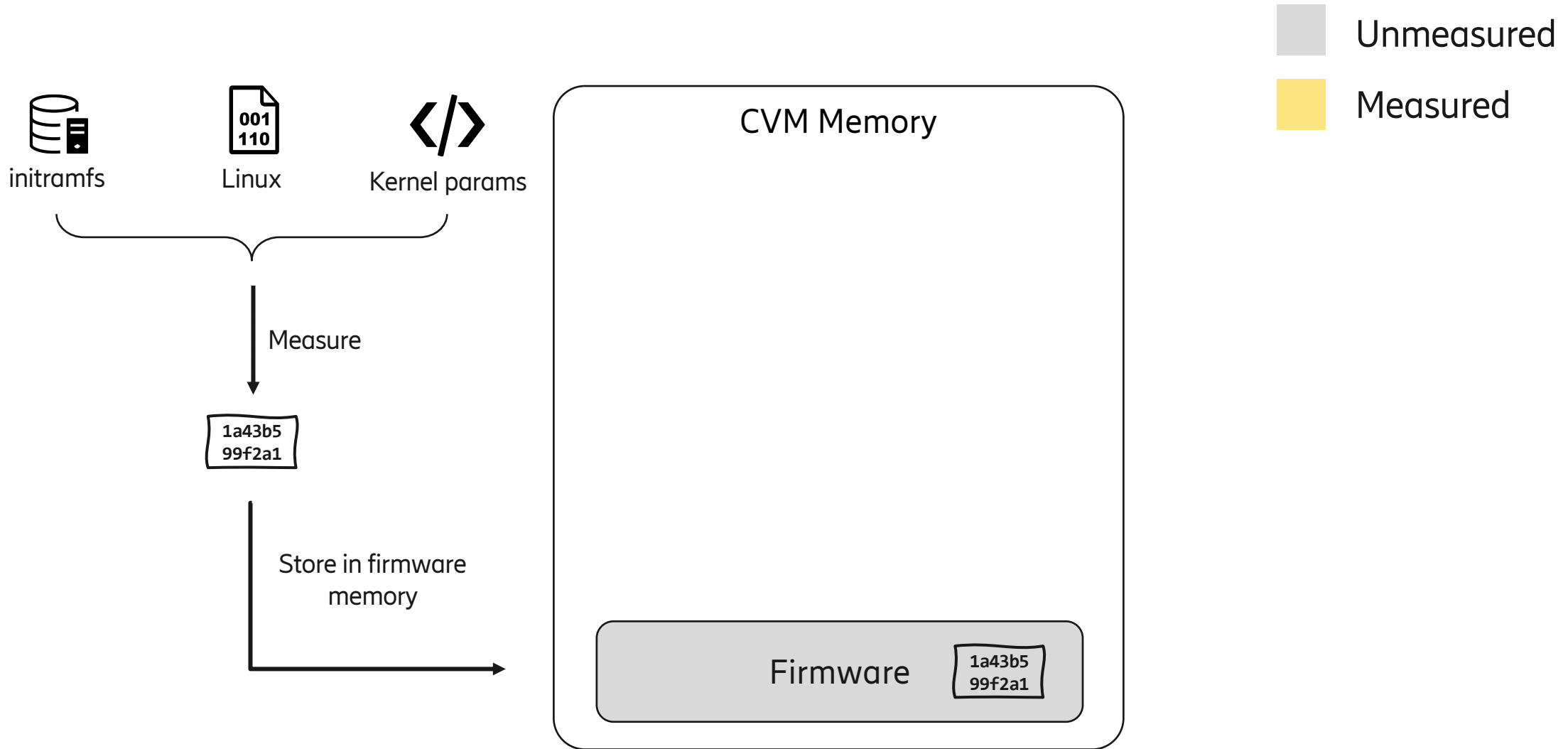
Stable references

- AMD SEV-SNP toolchain
 - public forks and “immutable” branches, e.g., “*snpguard-stable-6.9*”
 - Multiple install options:
 - Download pre-built binaries
 - Build with Docker
 - Build locally
- Attestation library
 - “virtee/sev” fixed to a specific commit

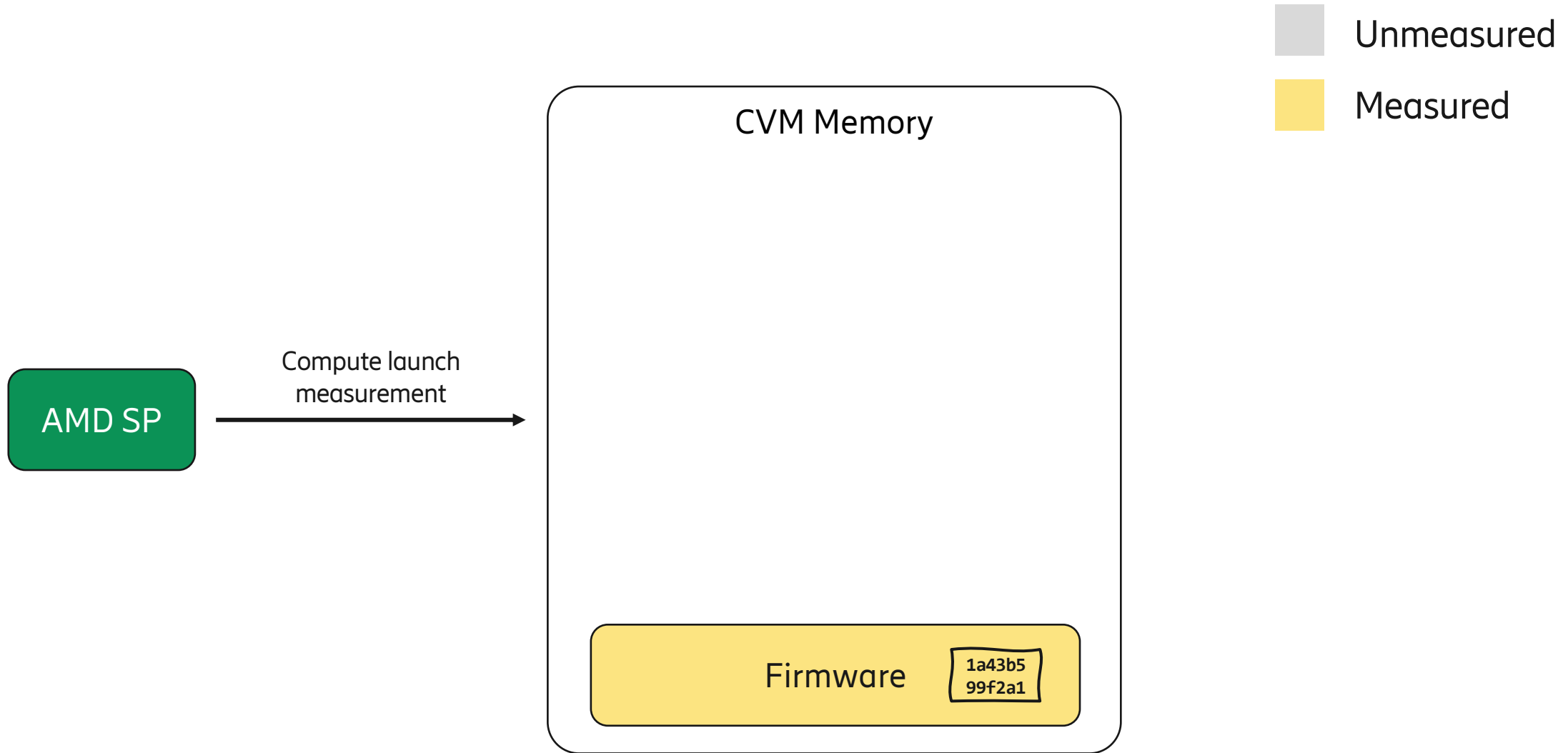
Direct Linux Boot



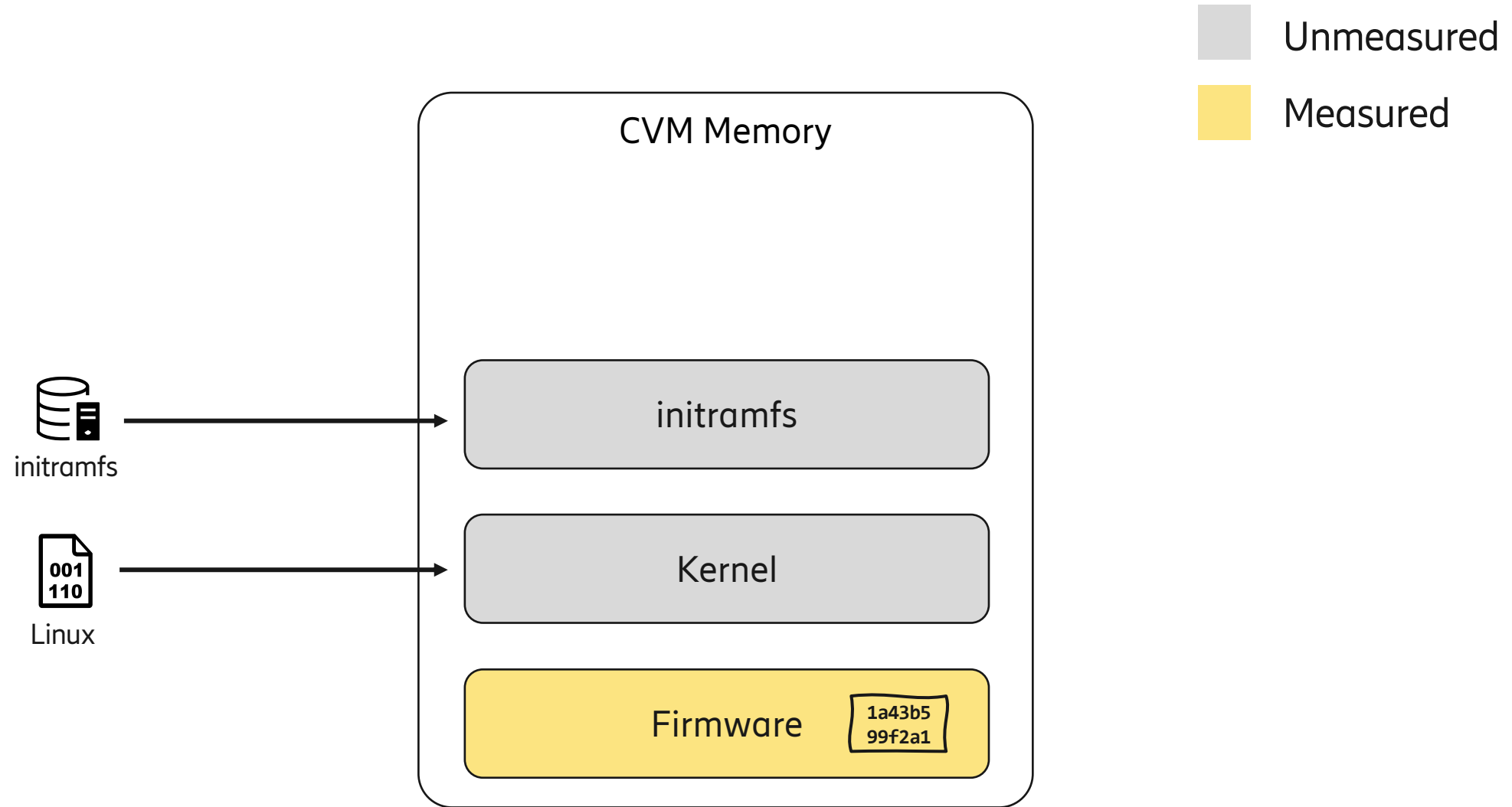
Direct Linux Boot



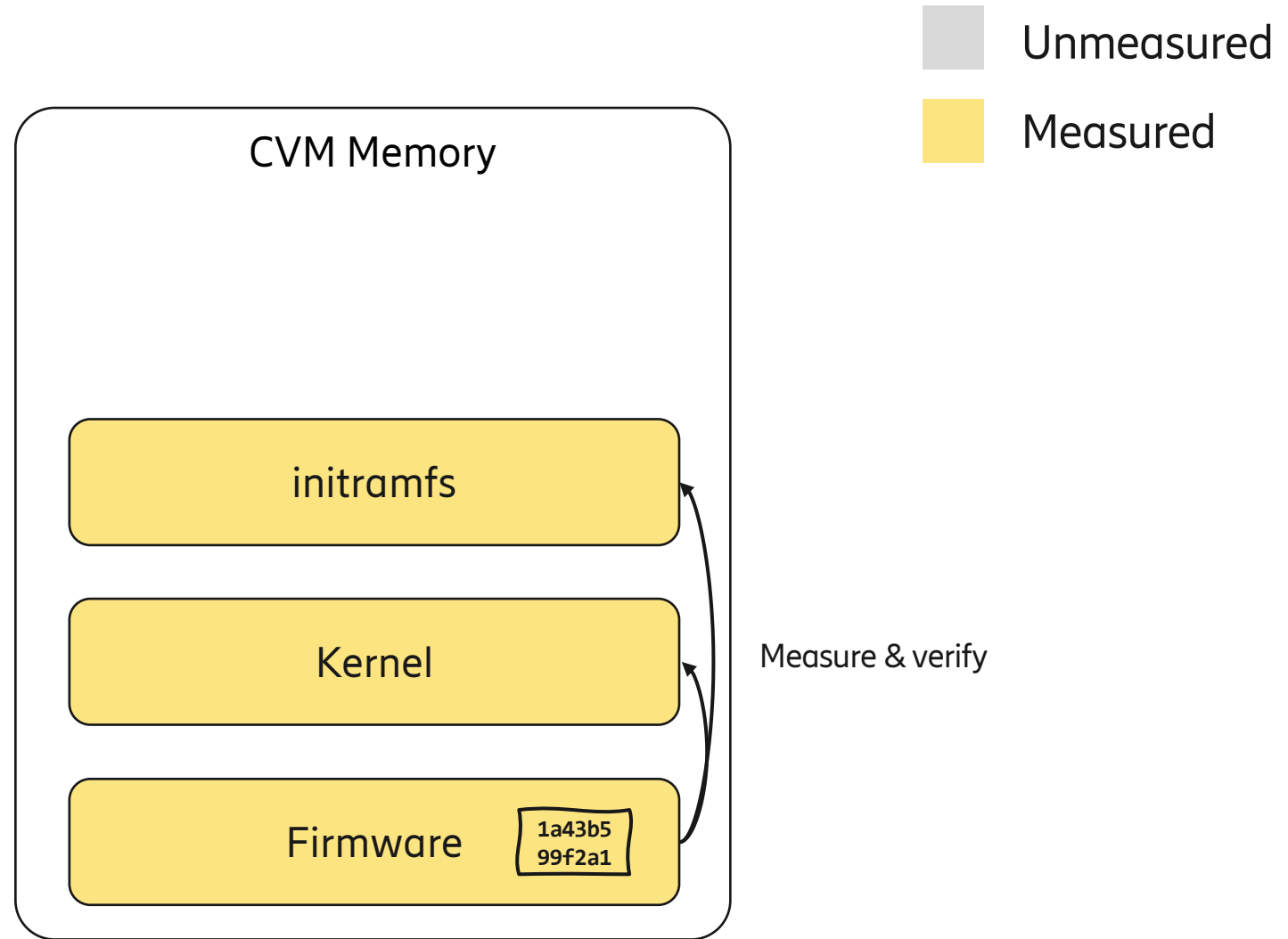
Direct Linux Boot



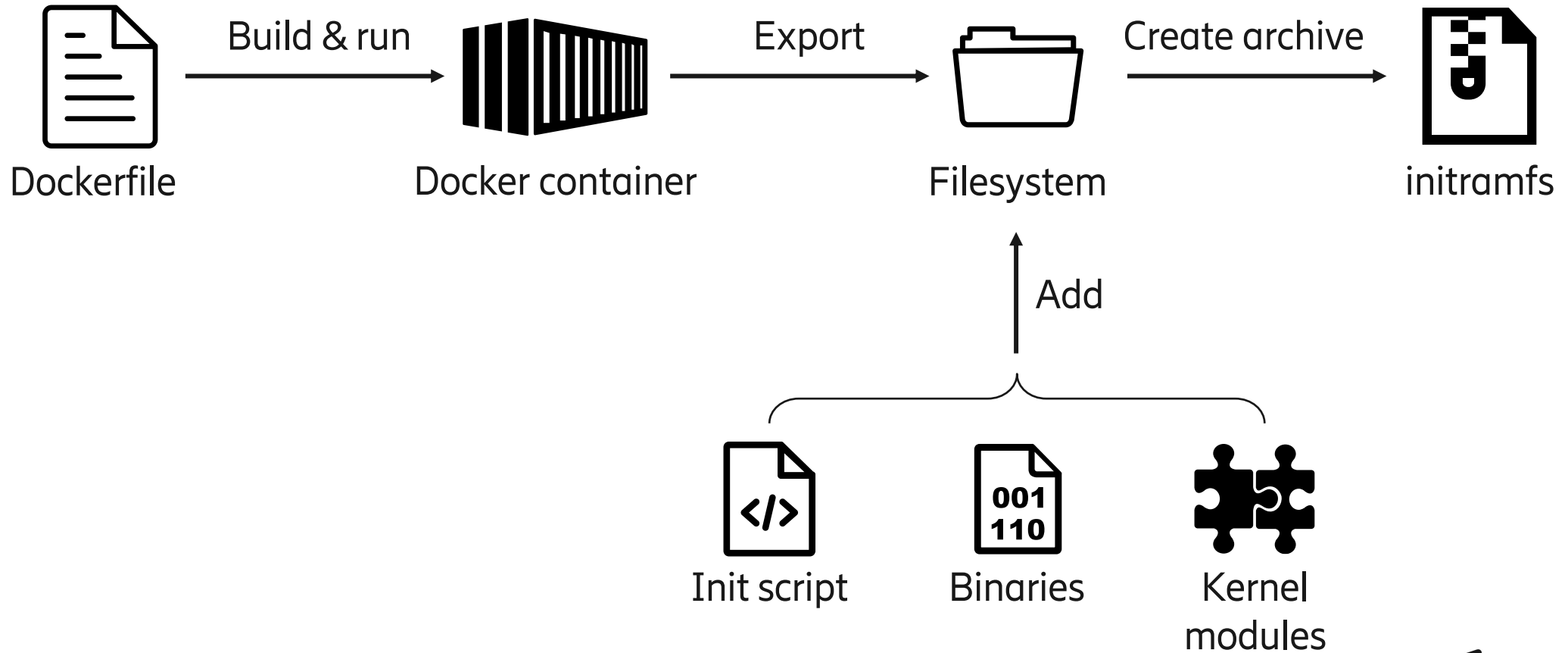
Direct Linux Boot



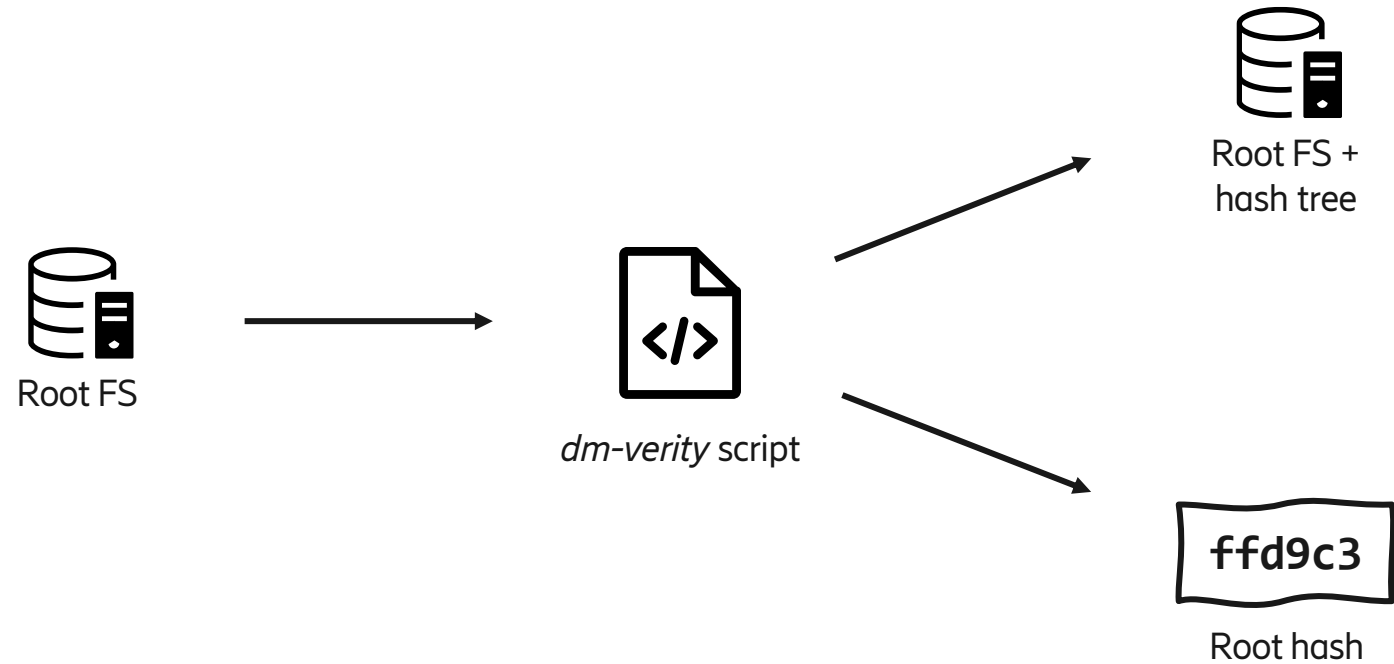
Direct Linux Boot



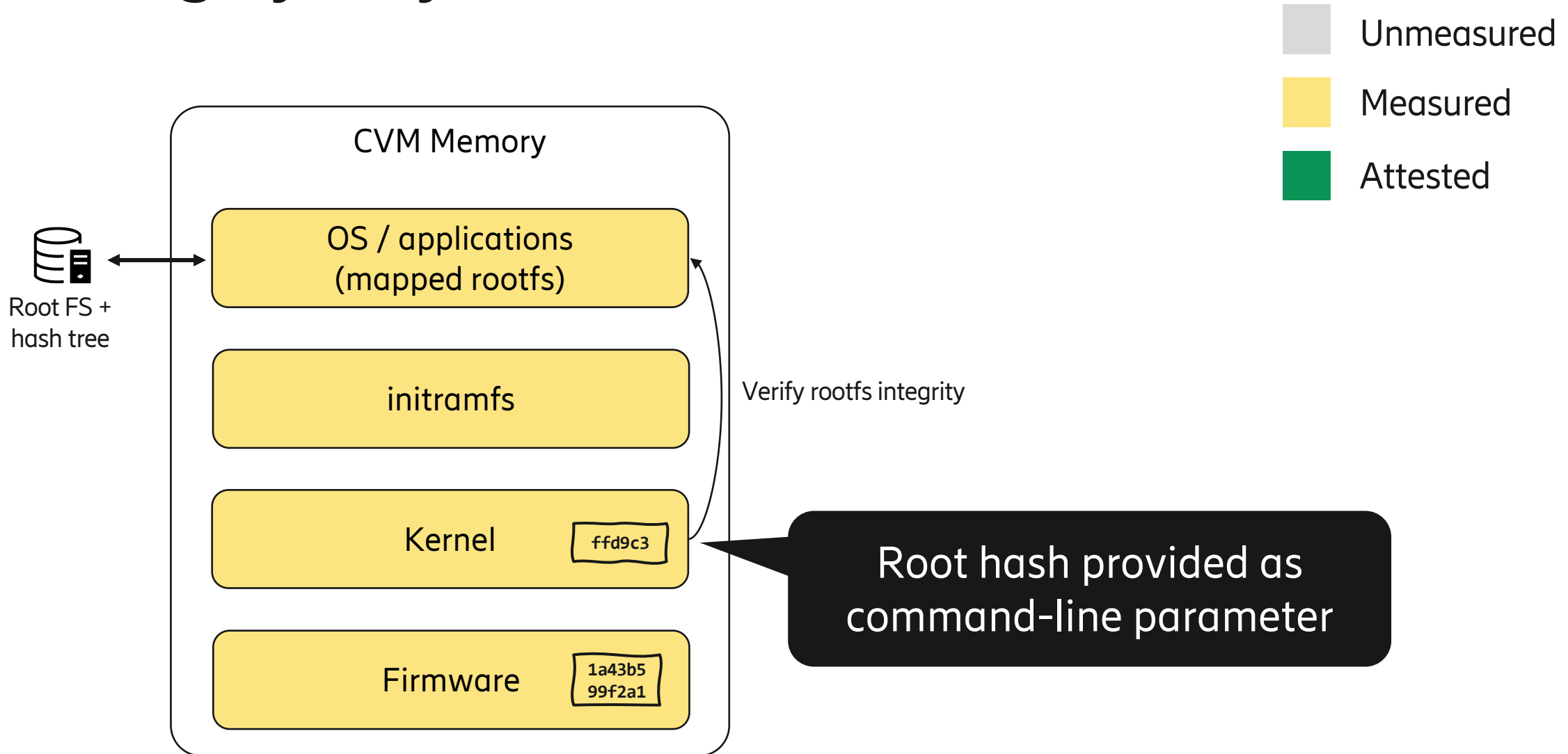
Custom initramfs



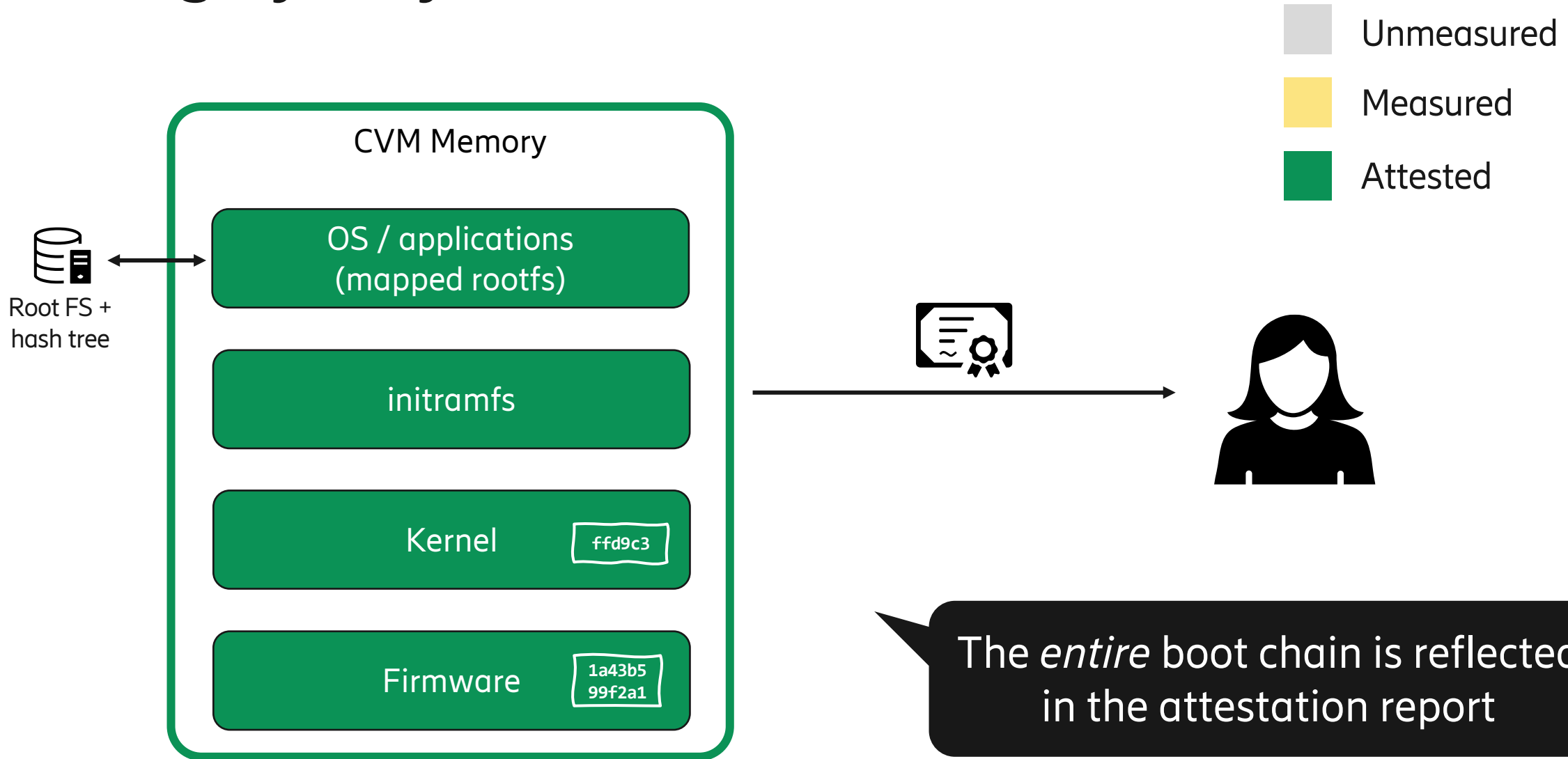
Integrity-only workflow



Integrity-only workflow



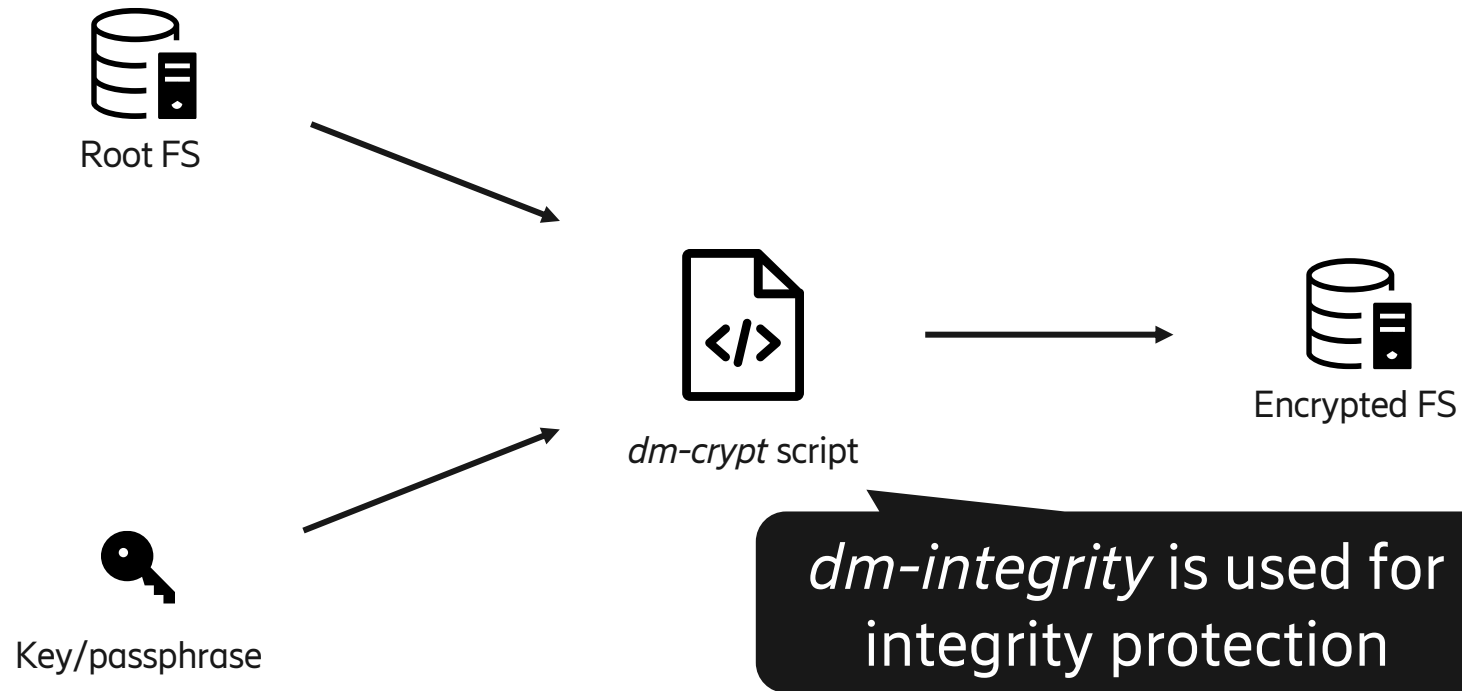
Integrity-only workflow



Integrity-only workflow

- Flexible attestation (at any time after boot)
- Root FS is read-only, but additional partitions can be mounted as r/w (*tmpfs*)
- SSH keys are regenerated in *initramfs* and stored in encrypted memory

Encrypted workflow

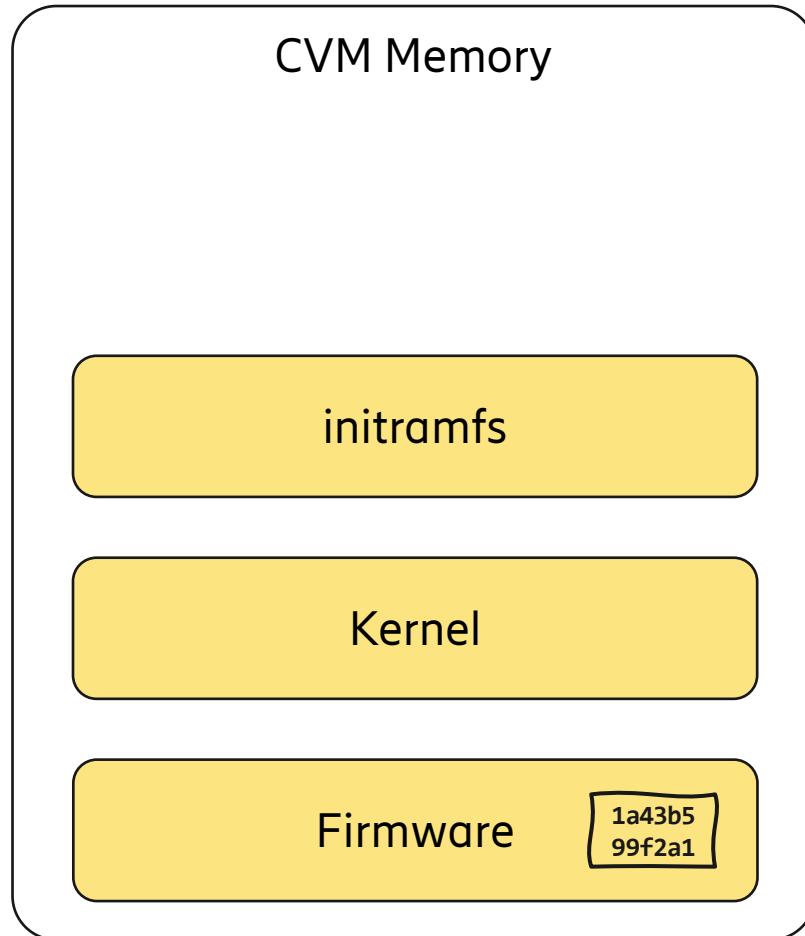


Encrypted workflow

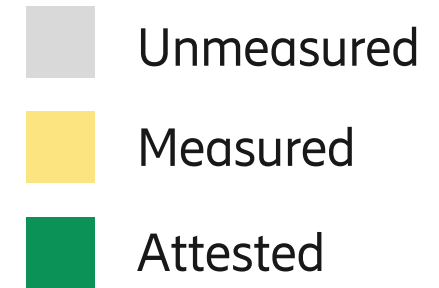
- Unmeasured
- Measured
- Attested



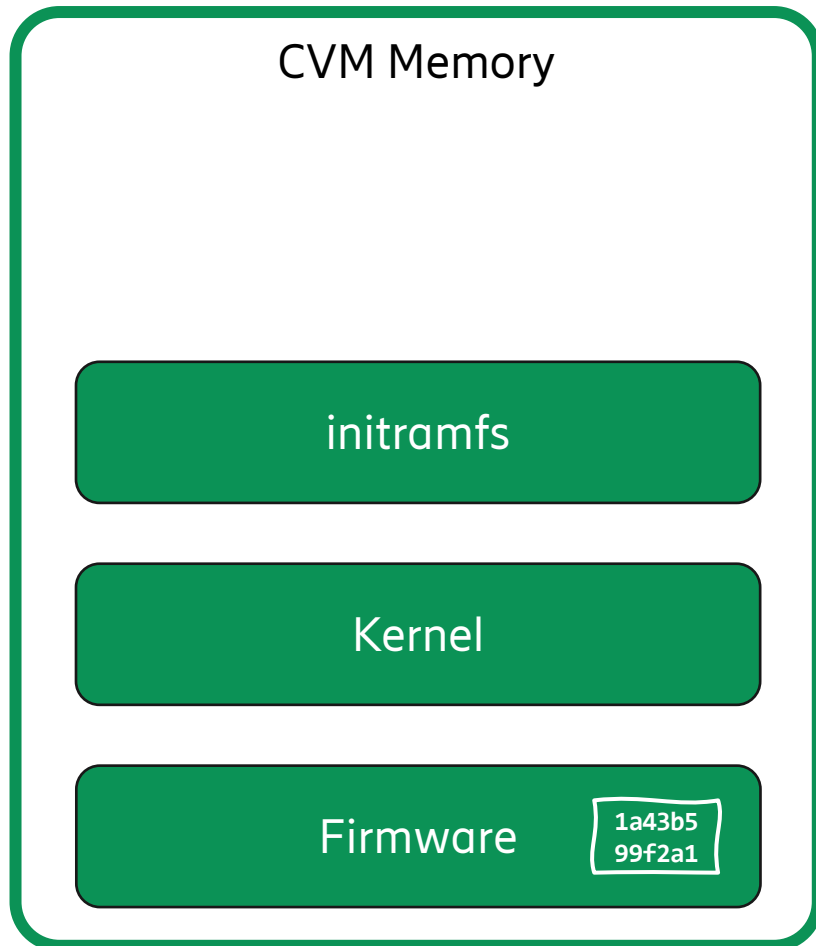
Encrypted FS



Encrypted workflow



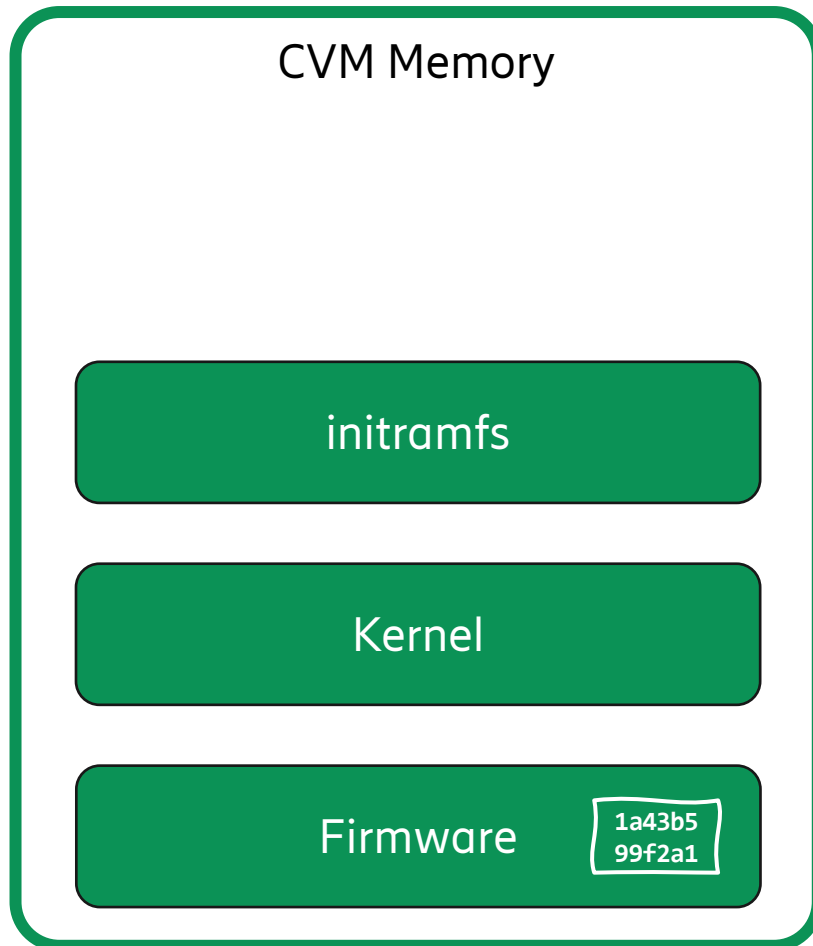

Encrypted FS



Encrypted workflow

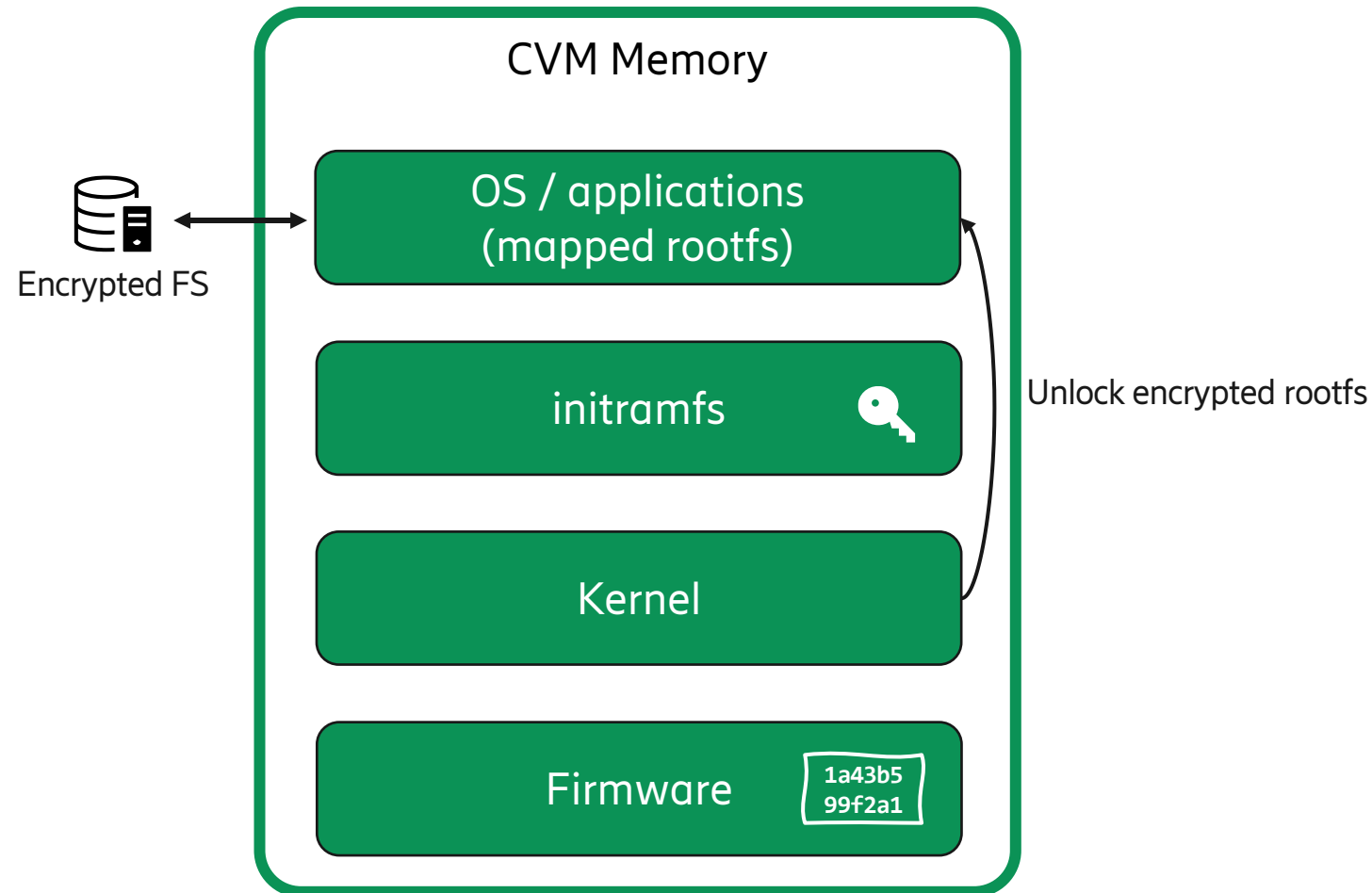
- Unmeasured
- Measured
- Attested


Encrypted FS



Encrypted workflow

- Unmeasured
- Measured
- Attested



Encrypted workflow

- Attestation **must** be done at boot time
- Rootfs is r/w
- Secrets (e.g., SSH keys) are protected

SNPGuard: Remote Attestation of SEV-SNP VMs Using Open Source Tools

- Stable reference implementation to get started with SEV-SNP
 - Building blocks can be customized or reused elsewhere
- For whom?
 - People experimenting / testing
 - TEE researchers
 - Everybody who wants to understand the CVM security model
- Future work: support vTPM and Intel TDX



Luca Wilke, [Gianluca Scopelliti](#)

7th Workshop on System Software for Trusted Execution (SysTEX'24)

gianluca.scopelliti@ericsson.com



UNIVERSITÄT ZU LÜBECK