AMD SEV-SNP Attestation: Establishing Trust in Guests

Jeremy Powell
Linux Security Summit Europe
September 2022

AMD
together we advance_

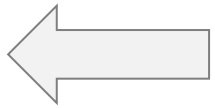
Threat Model – Untrusted Cloud Provider

- Cloud Provider not trusted with **confidentiality** or **integrity**
  - Can run malicious hypervisors (memory replay, memory aliasing, event injects, …)
  - Can run malicious guests (masquerade as other guests, unauthorized memory access…)
  - Can run malicious host applications (unauthorized memory access, …)
  - Can install malicious devices (unauthorized DMA to guest, …)
  - Can misconfigure the platform (insecure platform configuration, …)
  - Can launch guest incorrectly (maliciously altered initial guest image, enable of insecure configuration, …)

- Cloud Provider is trusted for **availability** of the guest.
  - Pushes the run button for the guest repeatedly

Threat Model – Untrusted Cloud Provider

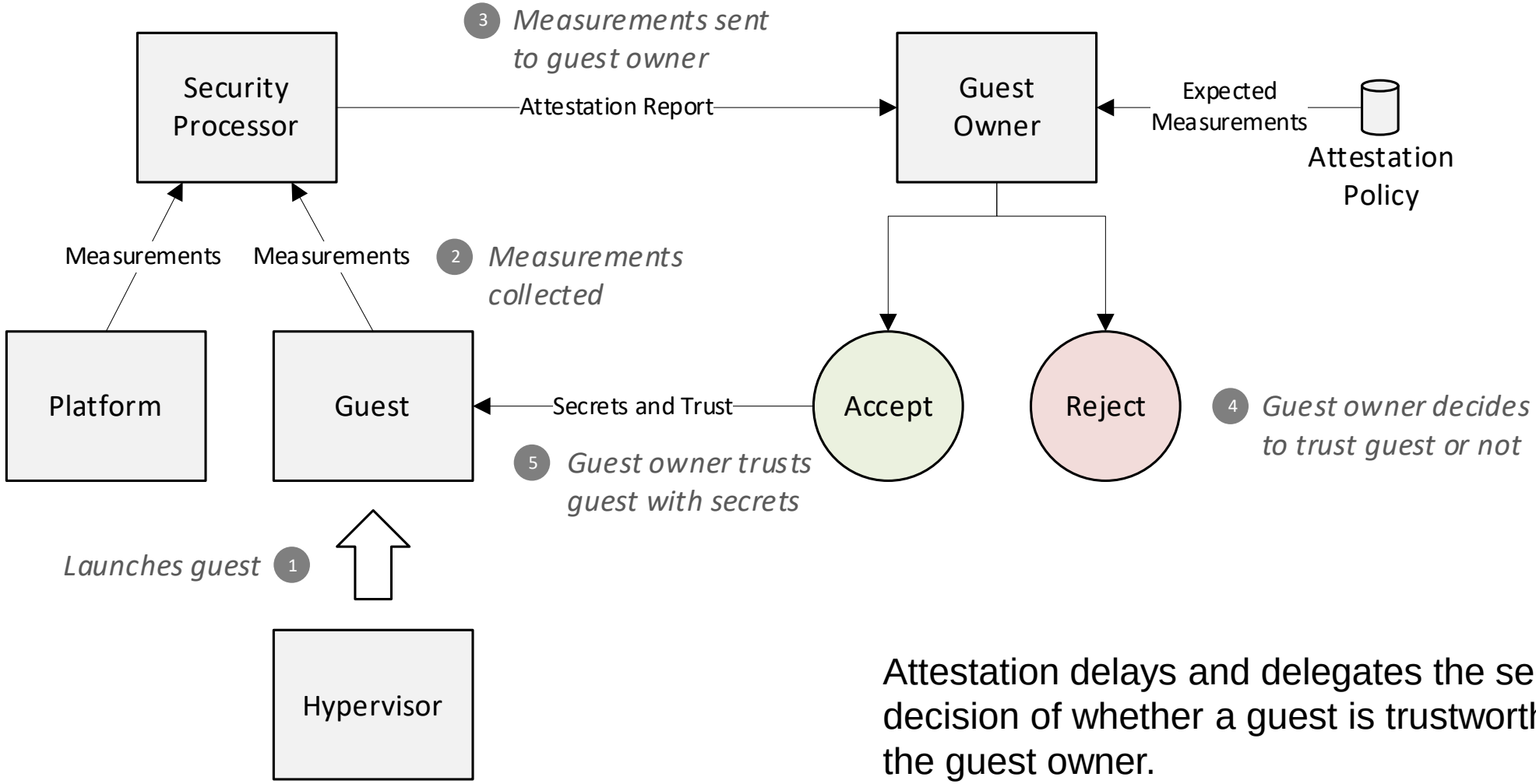
- Cloud Provider not trusted with **confidentiality** or **integrity**
  - Can run malicious hypervisors
  - Can run malicious guests
  - Can run malicious host applications
  - Can install malicious devices
  - Can misconfigure the platform
  - Can launch guest incorrectly



Let's talk about this a little more…

- Cloud Provide is trusted for **availability** of the guest.
  - Pushes the run button for the guest repeatedly

Overview of Attestation



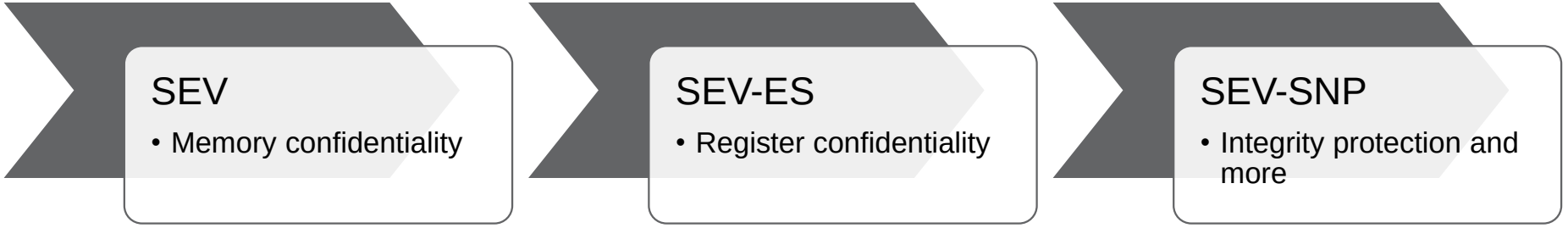
Attestation delays and delegates the security decision of whether a guest is trustworthy to the guest owner.

AMD SEV-SNP Overview

- ***Secure Nested Paging*** (SEV-SNP) is the latest generation of AMD Secure Encrypted Virtualization (SEV) technology designed for Confidential Computing

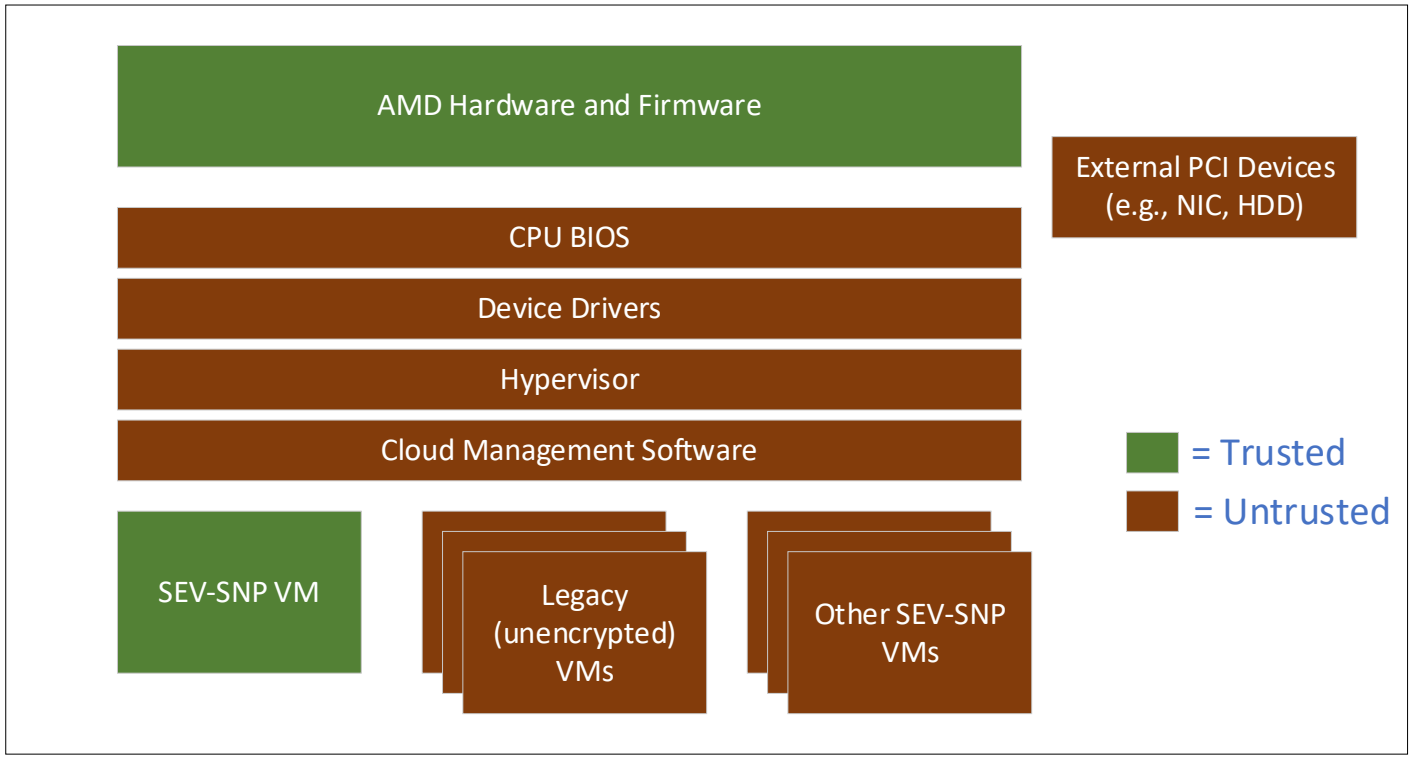
- SEV-SNP builds on existing AMD SEV and AMD SEV-ES (Encrypted State) features to provide ***stronger security, additional use models, and more*** to protected VMs
  - SEV and SEV-ES supported in 1st and 2nd Generation AMD EPYC™ Processors (2017)
  - SEV-SNP supported starting in 3rd Generation AMD EPYC™ Processors (2021)

- SEV-SNP is designed to protect a VM from a malicious hypervisor in specific ways
  - Useful in public cloud and any scenario where the hosting environment cannot be trusted

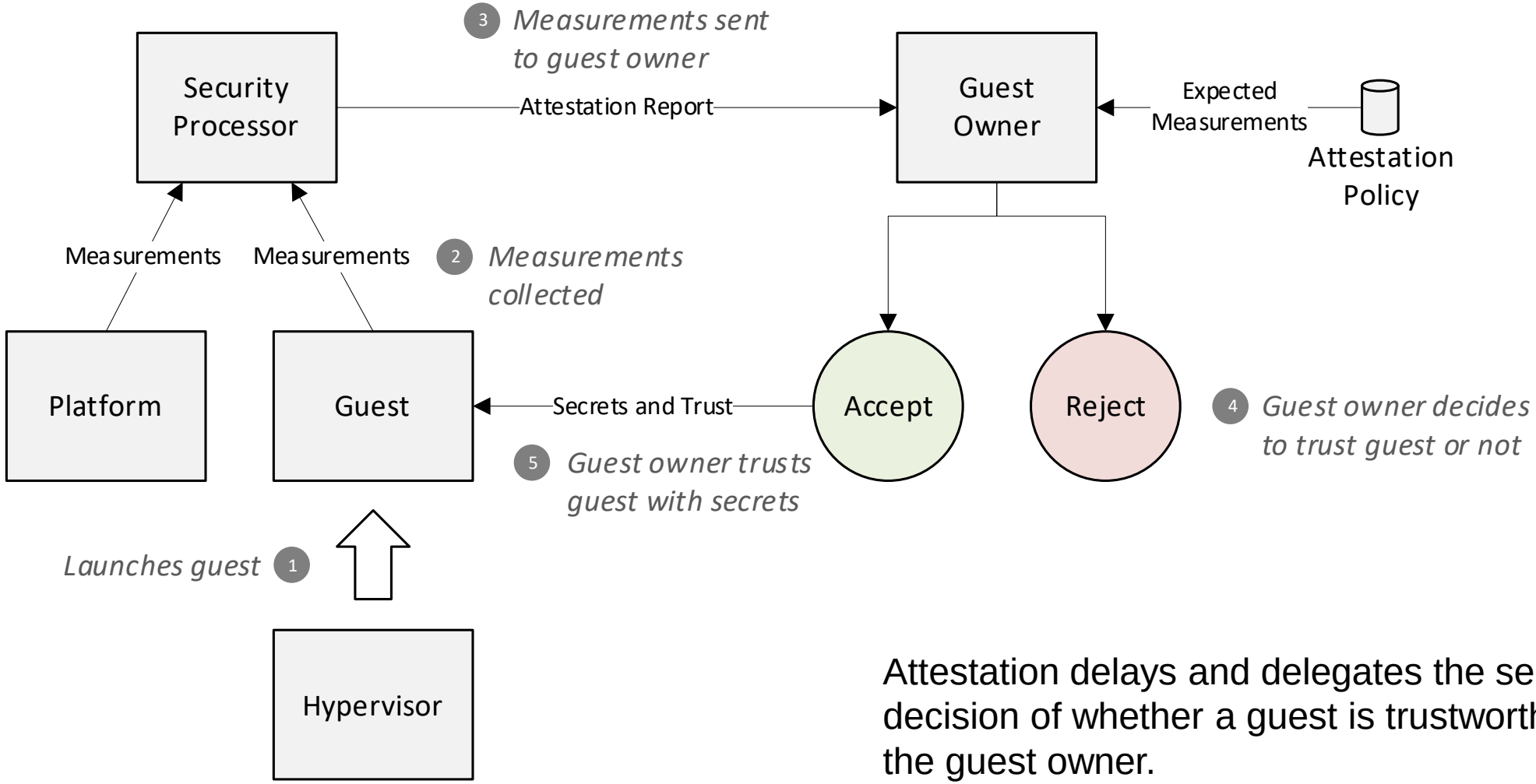


Measurements of Trusted Computing Base (TCB)

- AMD firmware and microcode
  - Security processor boot loader
  - Security processor operating system
  - SEV-SNP firmware
  - x86 Microcode
- SEV-SNP Guest
  - Launch metadata and measurements
  - Guest configuration
  - x86 runtime configuration

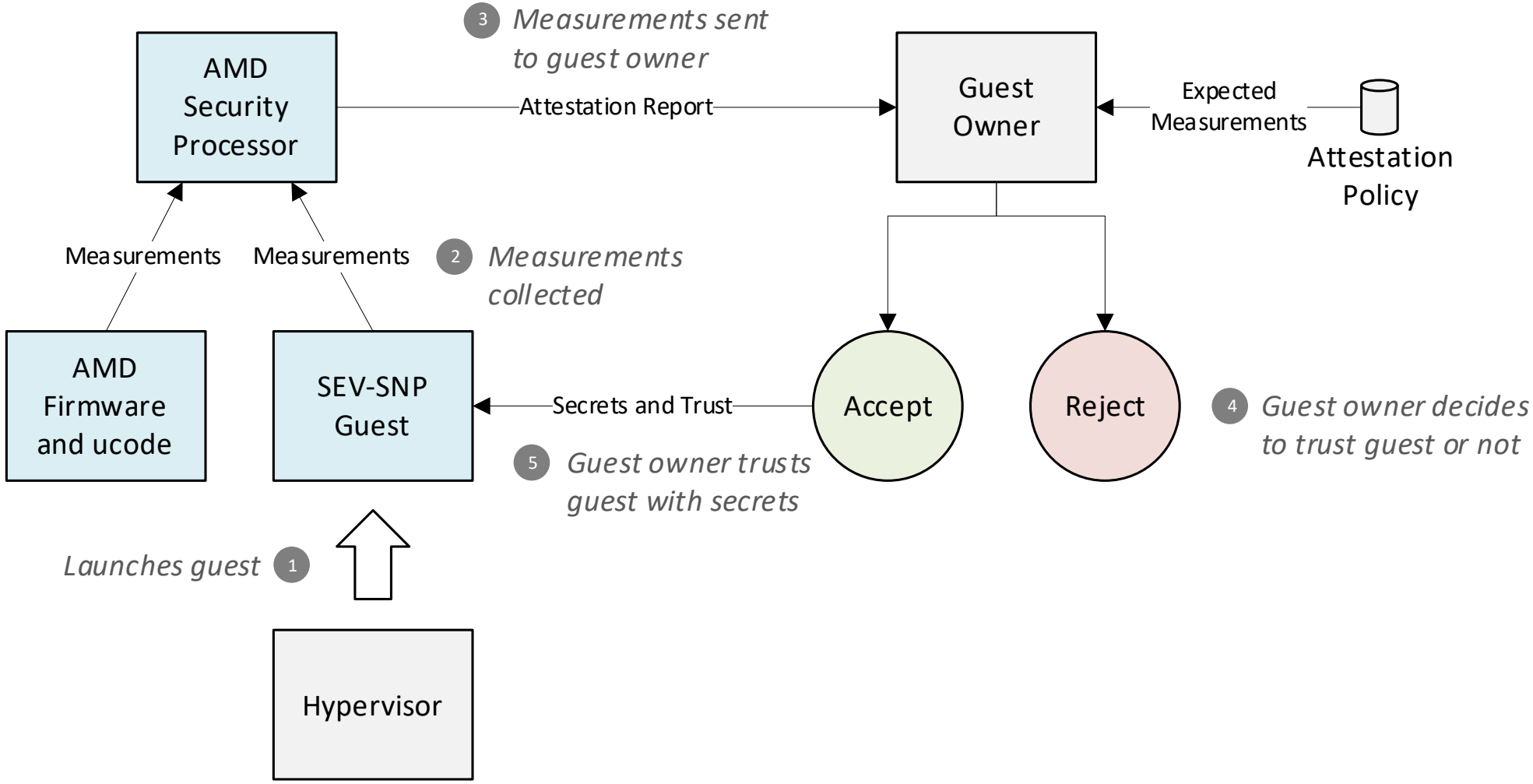


Overview of Attestation



Attestation delays and delegates the security decision of whether a guest is trustworthy to the guest owner.

Overview of Attestation in AMD SEV-SNP

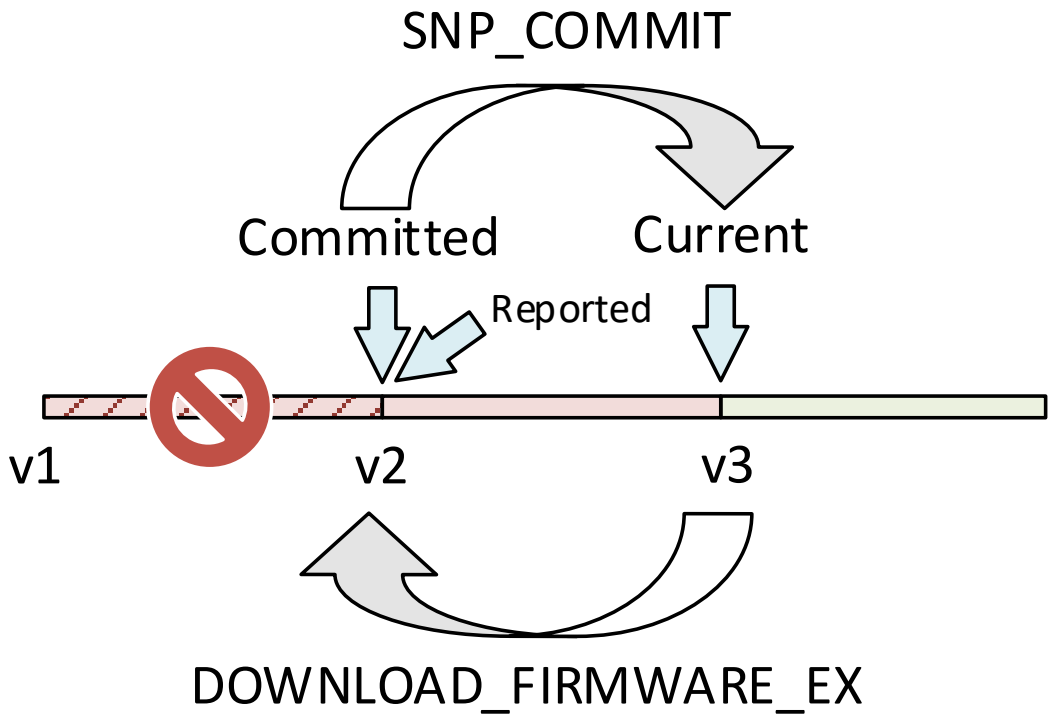


AMD SEV-SNP Attestation Components

- Platform Measurements
  - Platform versioning
  - Platform runtime configuration
  - Chip identification
- Guest Measurements
  - Owner identification
  - Guest image identification
  - Initialize image measurement
  - SEV-SNP guest policy
  - Migration agents
- Authenticity of Report
- Attestation Report Retrieval
- Binding Guest Credentials to Report

TCB Version Tracking

- TCB components
  - Security processor boot loader
  - Security processor operating system
  - SEV-SNP firmware
  - x86 Microcode
- Multiple TCB versions tracked
  - Committed: Anti-rollback limit
  - Current: Currently executing firmware version
  - Reported: Version reported to guest
- Committed and Current
  - Provisional firmware: Committed < Current
  - Committed firmware: Committed = Current
- Reported
  - Can hide provisional updates from guests
  - Guest may not be ready to see newer versions
    (e.g., versioned attestations discussed in a bit..)

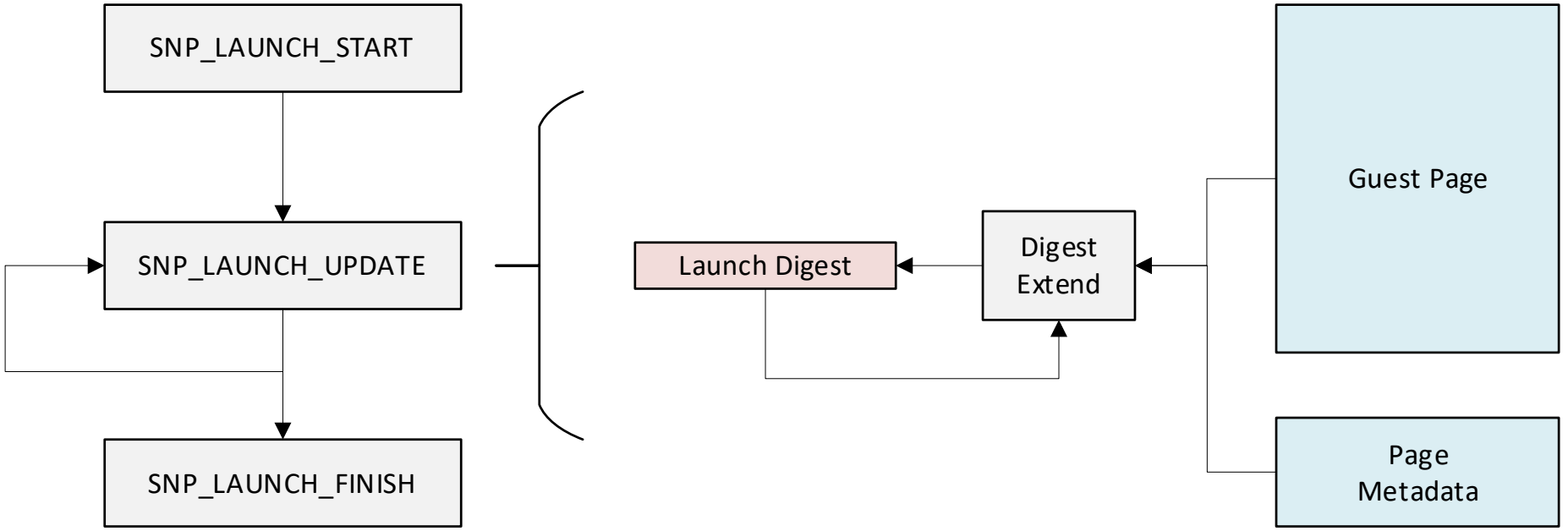


Invariant:
Reported <= Committed <= Current

Attestation Report: Platform Measurements

Report Field	Description	Usage and Verification
CHIP_ID	Unique chip identifier	Connects the report to the certificate of the attestation key that signed this report
PLATFORM_INFO	Indicates properties of the platform configuration, such as whether whole system memory encryption or Simultaneous Multithreading (SMT) is enabled	Do you require whole system memory encryption to be on? Do you require SMT to be off?
CURRENT_TCB	Security Version Numbers (SVNs) of the currently executing platform firmware and microcode	Informational
COMMITTED_TCB	SVNs of the anti-rollback minimum of the platform firmware and microcode	Does this TCB address all the vulnerabilities you care about?
REPORTED_TCB	Hypervisor has option to report a lower version to ease continuity on TCB update	Connects the report to the certificate of the attestation key that signed this report
LAUNCH_TCB	SVNs of the version of the platform firmware and microcode at time of launch of this guest	Do you care if the guest *once* executed with a particular TCB version?

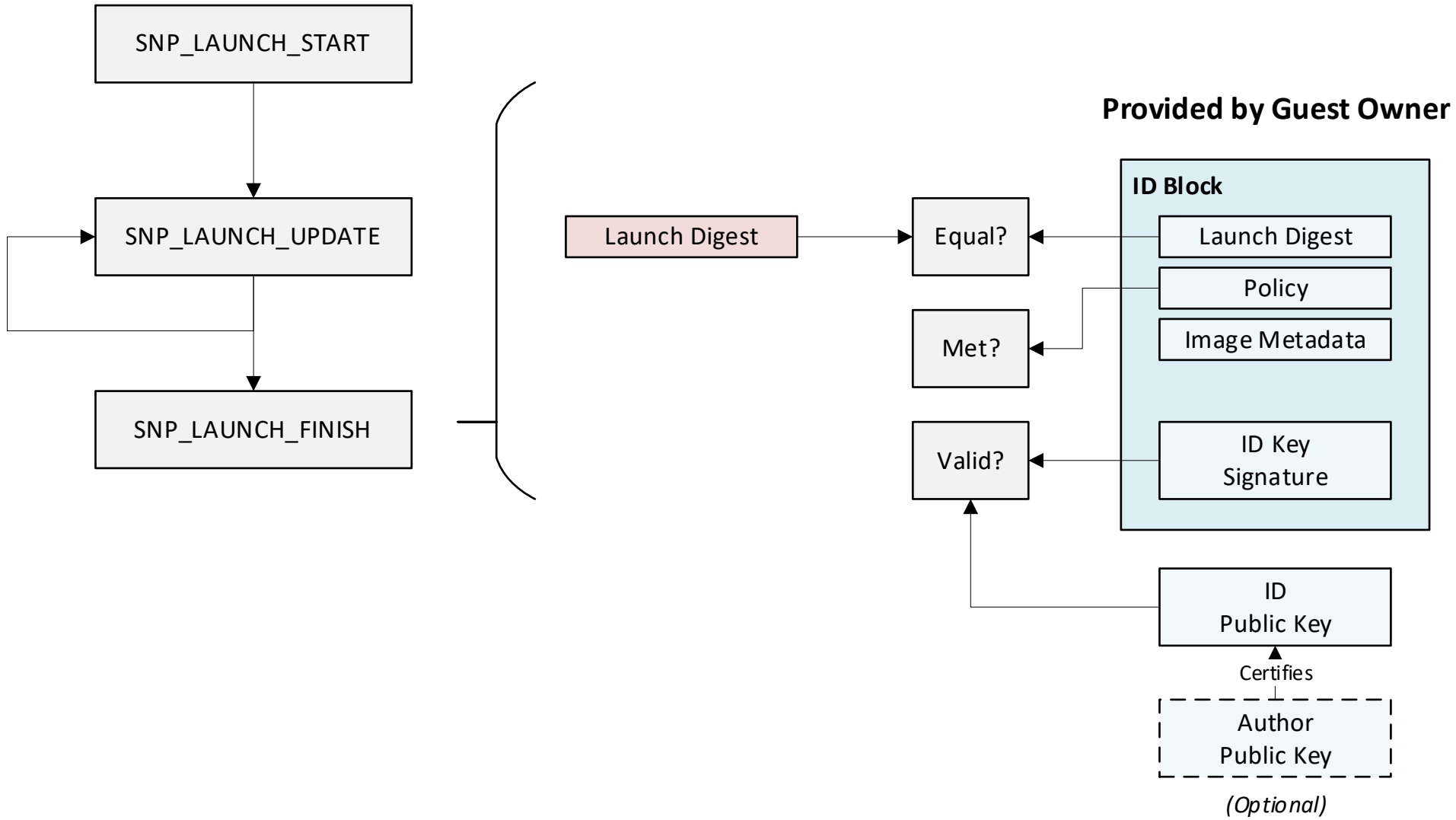
Attestation Report: Guest Measurements



LD := Hash(LD || Page || Metadata)

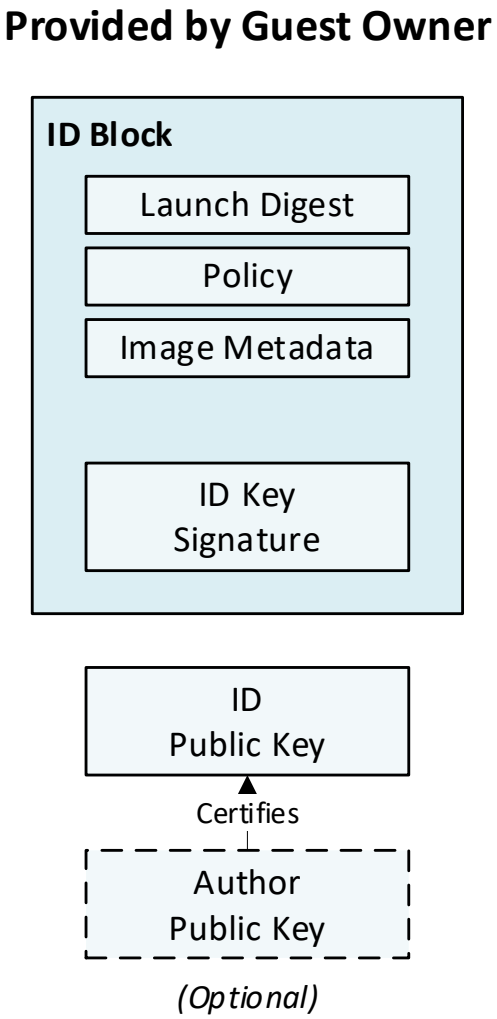
(slight simplification)

Attestation Report: Guest Measurements



Attestation Report: Guest Measurements

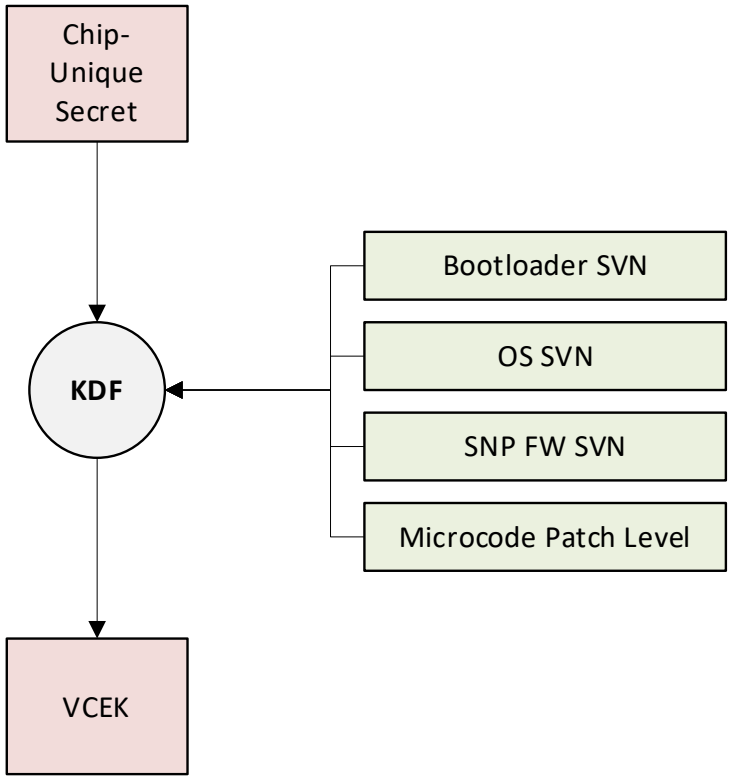
- Identity block
  - Expected measurement
  - Guest policy that restricts configuration
  - Image metadata like image identifiers
  - Signature by the ID key
- Identity Key
  - Guest owner's key
  - Signs ID block
  - Firmware receives public key
  - Optionally signed by an Author Key to ease key management
- Conceptually
  - Firmware fails launch if signature isn't valid
  - Firmware fails launch if policy or measurement are incorrect
  - Firmware puts image metadata in attestation reports
  - Firmware puts public key digest in attestation reports
  - Guest owner checks that ID key digest in attestation report matches their ID key



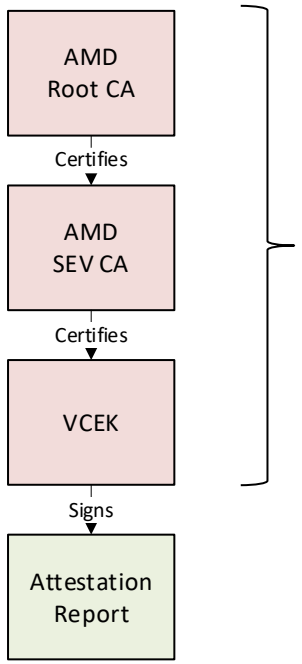
Attestation Report: Guest Measurements

Report Field	Description	Usage and Verification
FAMILY_ID IMAGE_ID GUEST_SVN	Guest image identification information	Is this the image you expected?
MEASUREMENT	Measurement of the guest's address space, including page types as defined in SNP_LAUNCH_UPDATE	Did the hypervisor set the guest up as you expected?
ID_KEY_DIGEST AUTHOR_KEY_DIGEST	Owner's ID and Author key digests, identifying the owner	Is this you?
POLICY	SEV-SNP guest policy restricting various things like SEV-SNP debug commands	Is the policy what you expected?
REPORT_ID MA_REPORT_ID	Connects this attestation report to its migration agent's report, if one is present.	Did you expect a migration agent to be bound to this guest? Does the migration agent's attestation report check out?

Authenticity of Attestation Report



REPORTED_TCB is mixed into the chip unique secret to derive the Versioned Chip-Endorsement Key (VCEK), which is used as the attestation key



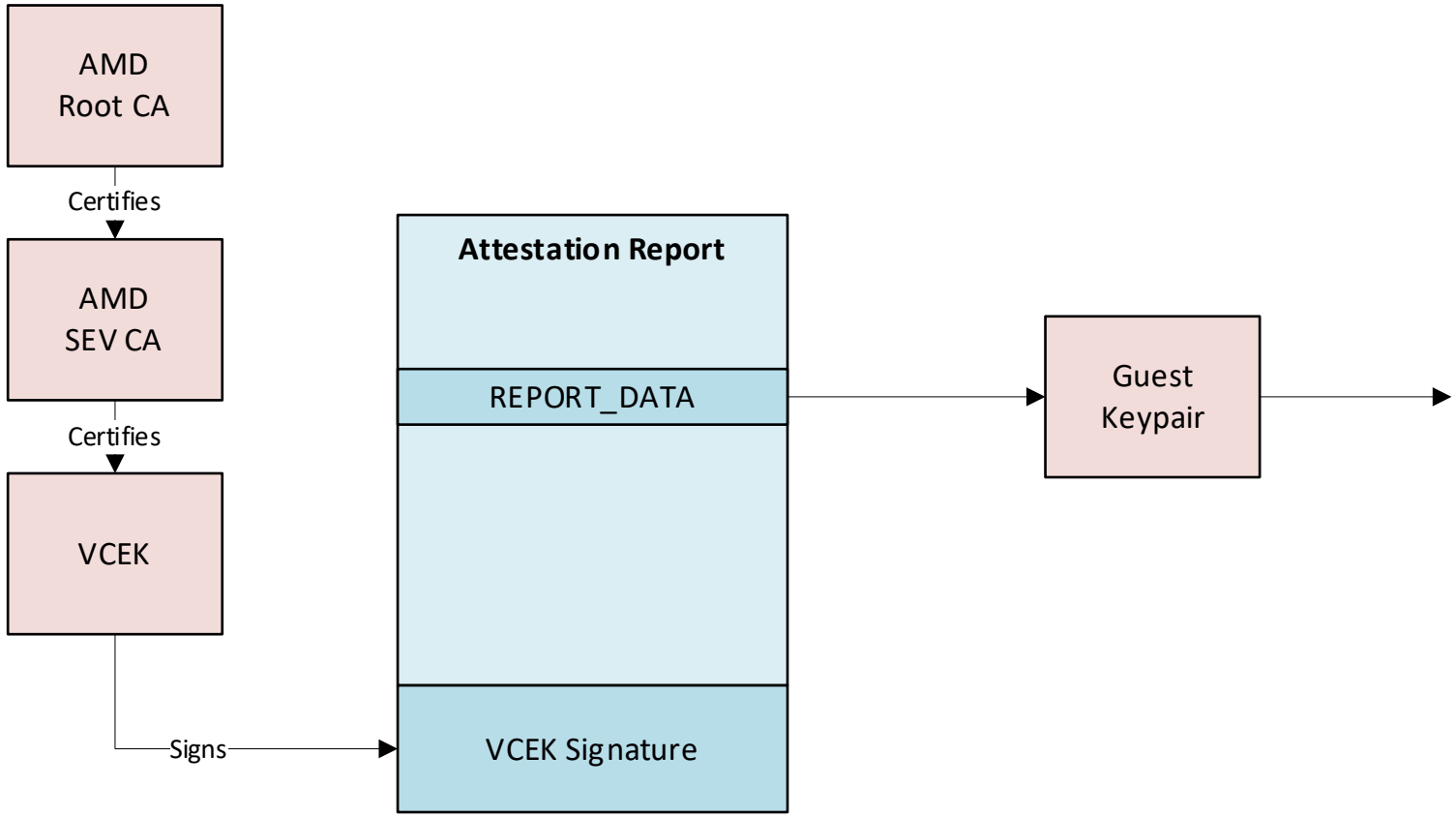
Certificates retrieved from AMD Key Distribution Service (KDS)

AMD Certificate Authority certifies the VCEK

VCEK signs the attestation report

Binding Guest Credentials to Attestation Report

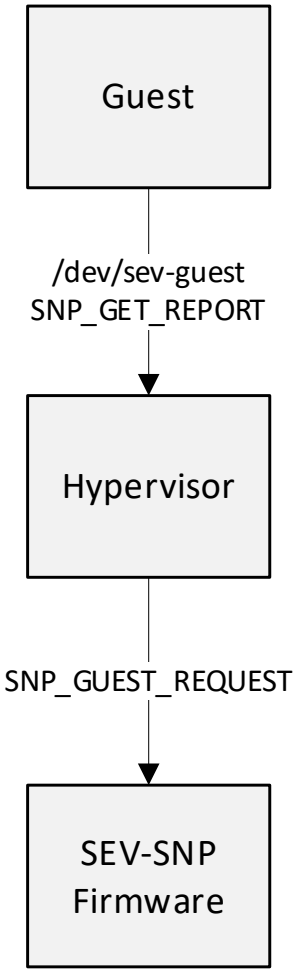
- REPORT_DATA provided by guest
  - 64 btyte field
  - Not interpreted by firmware
  - Placed into the attestation report
- Guest can…
  - Generate a key pair
  - Calculate digest of public key
  - Place digest in REPORT_DATA
  - Send report and public key to relying party to use
  - Key could establish trusted channel
  - Key could chain trust to a virtual TPM in guest



Retrieving Attestation Reports

- Reports retrieved via guest message
  - Guest construct MSG_REPORT_REQ message
  - Guest encrypts and integrity protects message with key shared at guest launch
  - Guest sends wrapped request to hypervisor
  - Hypervisor invokes SNP_GUEST_REQUEST on wrapped request
  - SEV-SNP firmware returns attestation report through same channel
- Linux guest retrieves reports via IOCTLs on /dev/sev-guest
  - SNP_GET_REPORT – retrieves report
  - SNP_GET_EXT_REPORT – retrieves report and certificates (see below)
- Linux host can provide attestation key certificates via IOCTLs on /dev/sev
  - SNP_SET_EXT_CONFIG – stores attestation key certificates for retrieval by /dev/sev-guest

  E.g., VCEK certificate chain is retrieved from AMD Key Distribution Service (KDS) and stored in the host via SNP_SET_EXT_CONFIG. The guest retrieves the report and certificate chain via SNP_GET_EXT_REPORT.



Conclusion and Future Work

- SNP attestation
  - Provides confidence in the platform configuration
  - Provides confidence in the guest configuration and launch
  - Can bootstrap deeper chains of trust into the guest
- See Tom Lendacky's KVM Forum talk on SVSM (and vTPM)
- https://github.com/AMDESE/sev-tool
  - Multitool for various AMD SEV (legacy) and SEV-SNP tasks
  - Validates VCEK signatures on attestation report
  - Validates VCEK certificate chain
- https://github.com/virtee/sev and https://github.com/virtee/sevctl
  - Rust library and Multitool for AMD SEV (legacy)
  - Pull request for adding SNP features https://github.com/virtee/sev/pull/20

Disclaimer

The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. The information contained herein is subject to change and may be rendered inaccurate releases, for many reasons, including but not limited to product and roadmap changes, component and motherboard version changes, new model and/or product differences between differing manufacturers, software changes, BIOS flashes, firmware upgrades, or the like. Any computer system has risks of security vulnerabilities that cannot be completely prevented or mitigated. AMD assumes no obligation to update or otherwise correct or revise this information. However, AMD reserves the right to revise this information and to make changes from time to time to the content hereof without obligation of AMD to notify any person of such revisions or changes.

THIS INFORMATION IS PROVIDED 'AS IS." AMD MAKES NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE CONTENTS HEREOF AND ASSUMES NO RESPONSIBILITY FOR ANY INACCURACIES, ERRORS, OR OMISSIONS THAT MAY APPEAR IN THIS INFORMATION. AMD SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. IN NO EVENT WILL AMD BE LIABLE TO ANY PERSON FOR ANY RELIANCE, DIRECT, INDIRECT, SPECIAL, OR OTHER CONSEQUENTIAL DAMAGES ARISING FROM THE USE OF ANY INFORMATION CONTAINED HEREIN, EVEN IF AMD IS EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.


AMD