# SEV-SNP Live Migration and VMM/KVM API Implications

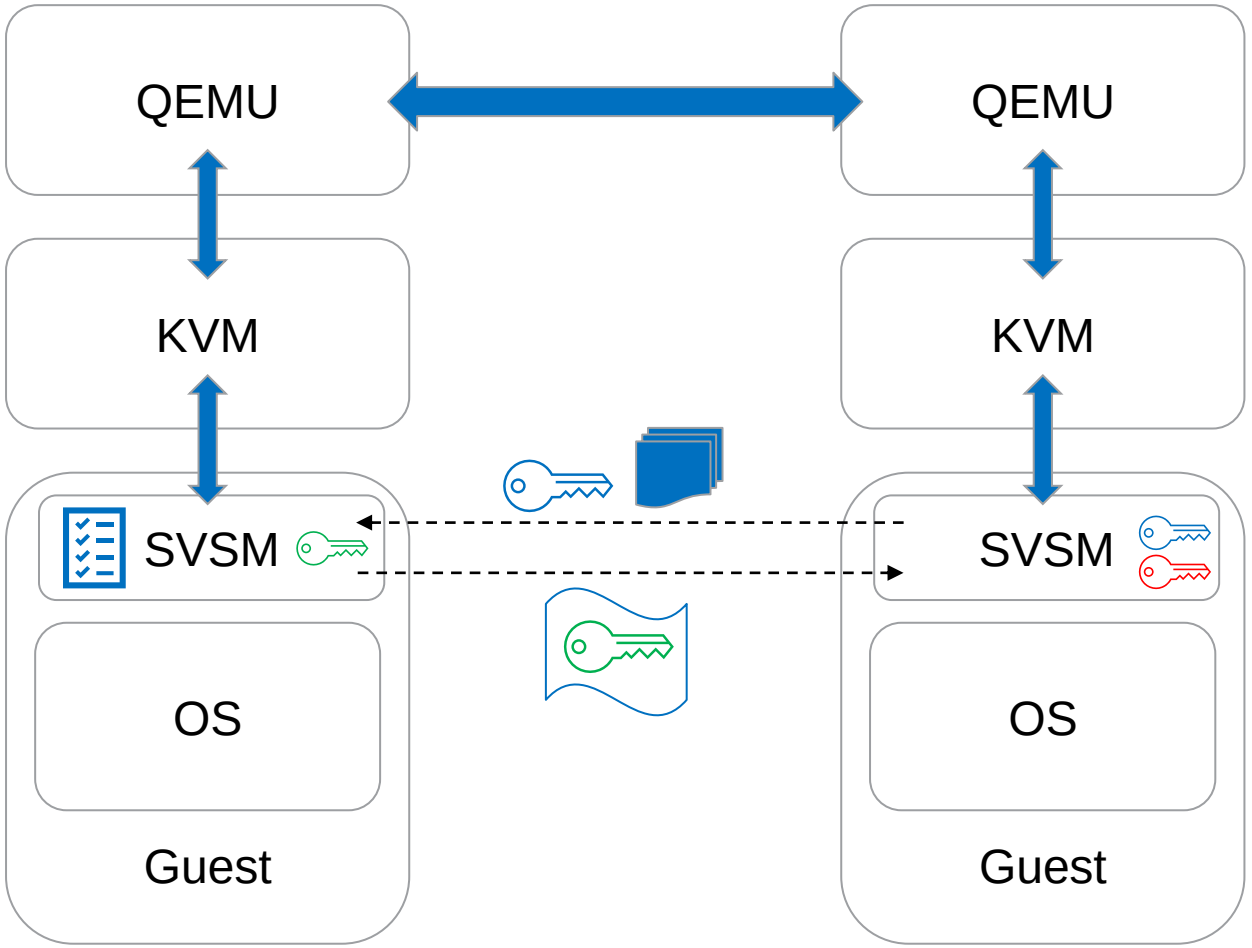
**Pankaj Gupta & Tom Lendacky**

AMD
together we advance_

# Migration Initialization

1. Dest QEMU started
   - SVSM generates public/private key pair
   - SVSM generates attestation report
     - Hash of public key as report data
   - SVSM provides attestation report, public key, and certificate data (collectively, migration data)

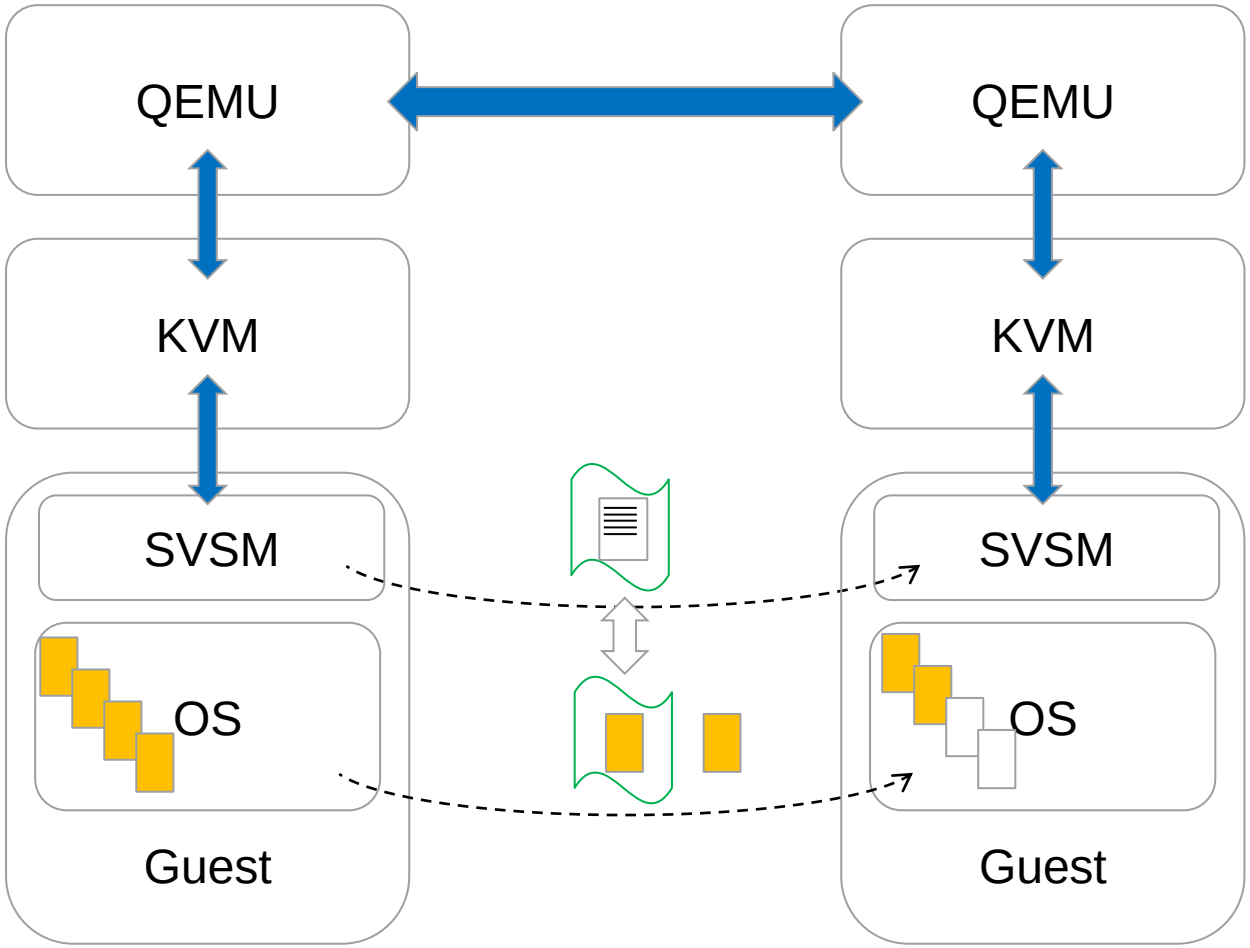
2. Src QEMU initiates migration
   - SVSM receives Dest SVSM migration data
   - SVSM validates Dest SVSM attestation report
   - SVSM initializes migration state
   - SVSM generates transport key, encrypts using Dest SVSM public key, and sends to Dest SVSM



# Migration of Pages

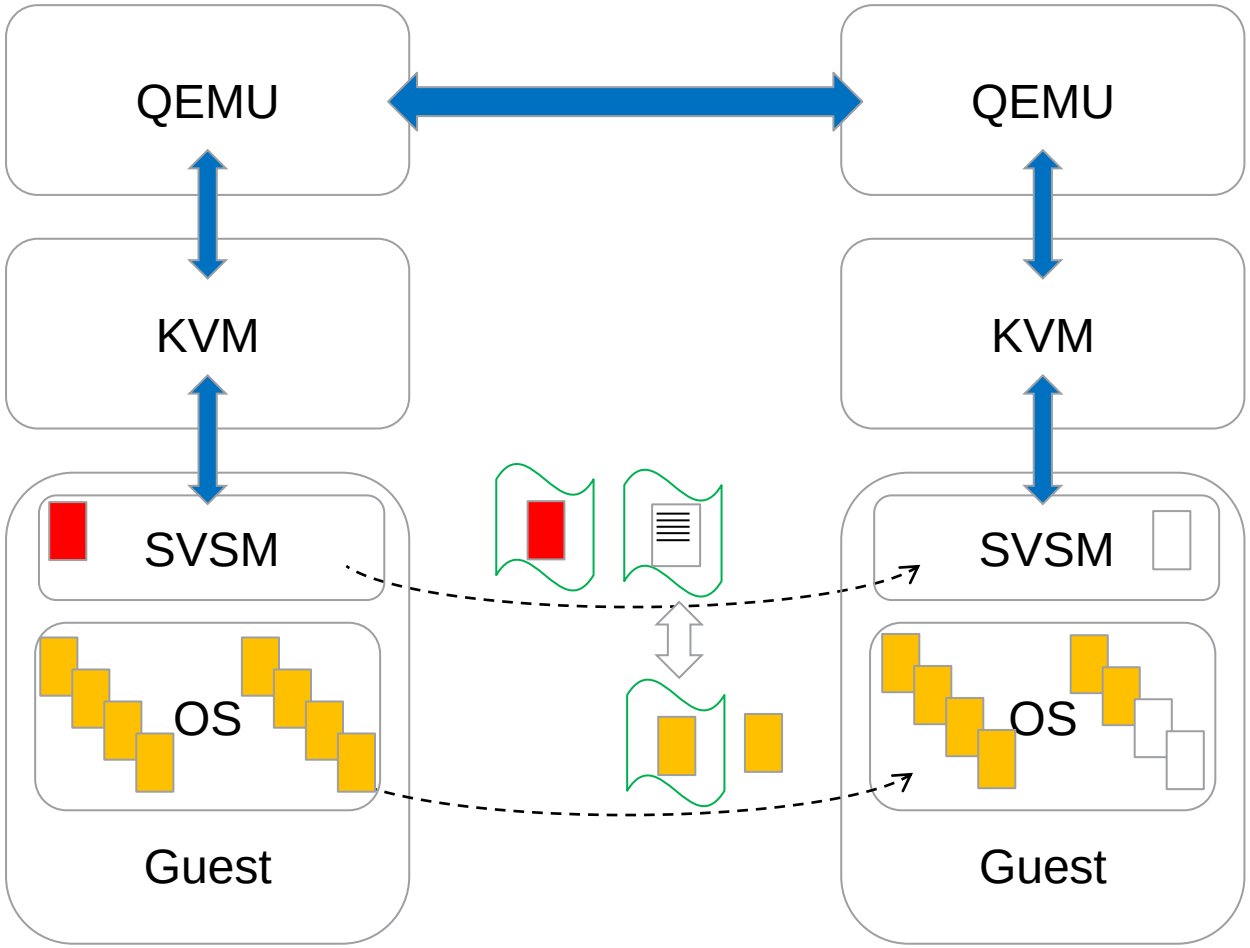
1. Src QEMU
   - Shared pages
     - Transfers in traditional manner
   - Private pages
     - SVSM encrypts page with transport key
     - SVSM returns page with metadata
     - SVSM provides encrypted page and metadata

2. Dest QEMU
   - Shared pages
     - Handles in traditional manner
   - Private pages
     - SVSM processes page based on metadata



# Migration Completion

1. Src QEMU
   - Remaining memory pages that still need to be migrated
   - Private state
     - SVSM prepares vCPU pages
     - SVSM prepares required SVSM state
     - Transfers encrypted pages and metadata
2. Dest QEMU
   - Handles remaining memory pages
   - Private state
     - SVSM processes final metadata



# New APIs

VMM

- Migration Initiation
  - Provide migration verification data
    - attestation report, etc.
  - Send migration transfer data
    - transport key, etc.
- Migration
  - Support for GMEM allows VMM to know what pages are Shared vs. Private
  - For Private pages
    - Need VMM API to send and receive the private page metadata and wrapped page(s)
- Migration Completion
  - Need VMM to receive final state

KVM

- Migration Initiation
  - Generate migration verification data
    - attestation report, etc.
  - Validate and create migration transfer data
    - transport key, etc.
- Migration
  - For Private pages
    - Need KVM API to package an encrypted page (transport encrypted with metadata)
    - Need KVM API to receive and process metadata and wrapped page(s)
- Migration Completion
  - Need KVM API to package final guest state (vCPU data, etc.) and any SVSM state (vTPM, etc.)
  - Need KVM API to process final state

# COPYRIGHT AND 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