



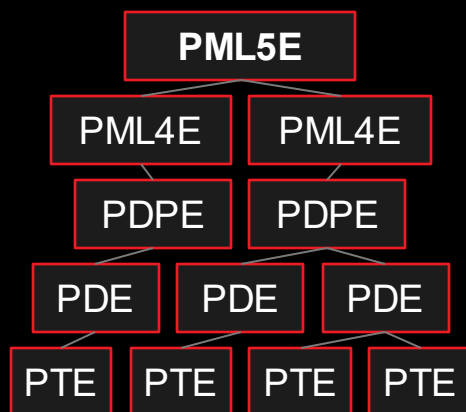
AMD SEV-TIO: Implementation Challenges

Trusted device assignment for confidential VMs

Three page tables must agree on every access

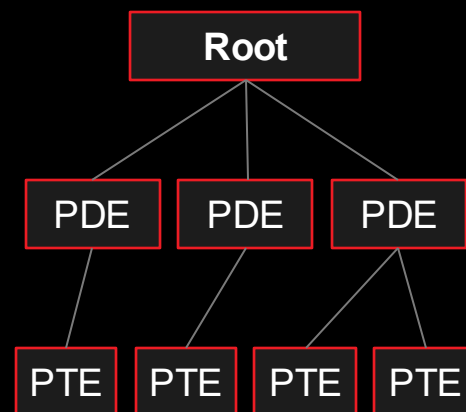
NPT

- GPA to SPA
- Untrusted



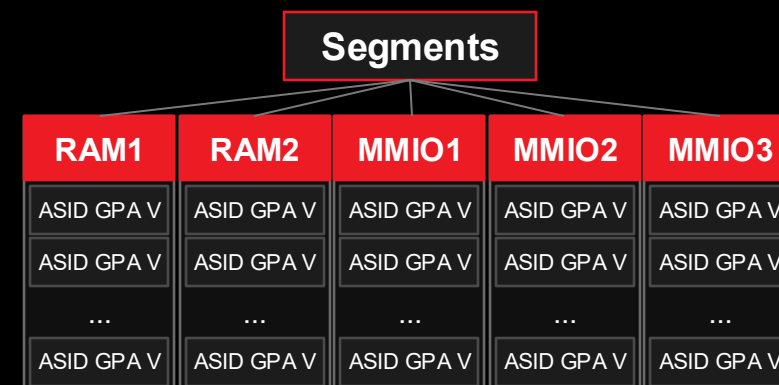
IOMMU

- No faults
- Page sizes - ANY



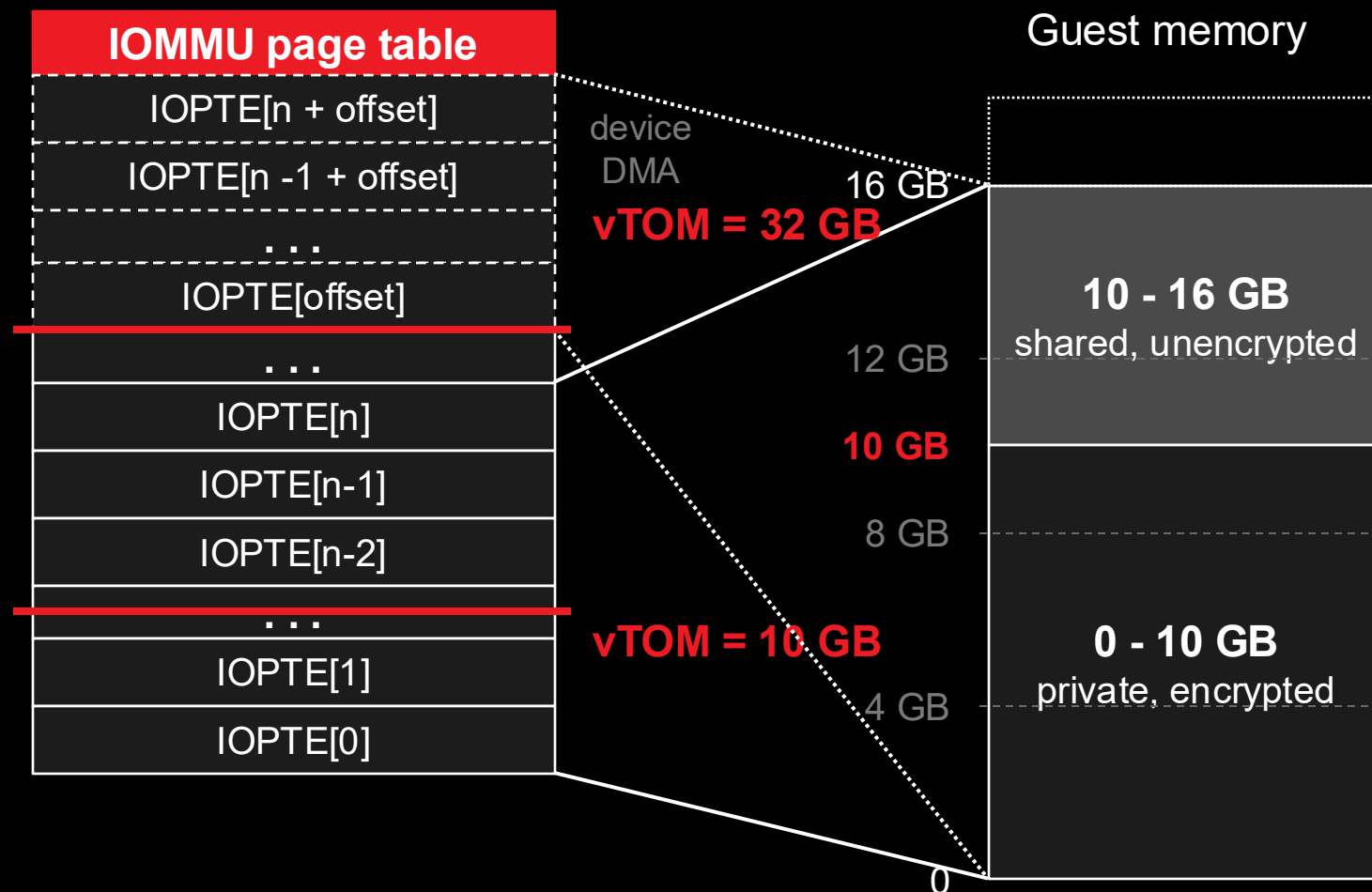
RMP

- HW write protected
- 2MB is first of 512 4K entries
- RMPUPDATE
- PSMASH



VTOM ("virtual top of memory") (private AND shared DMA)

Host memory



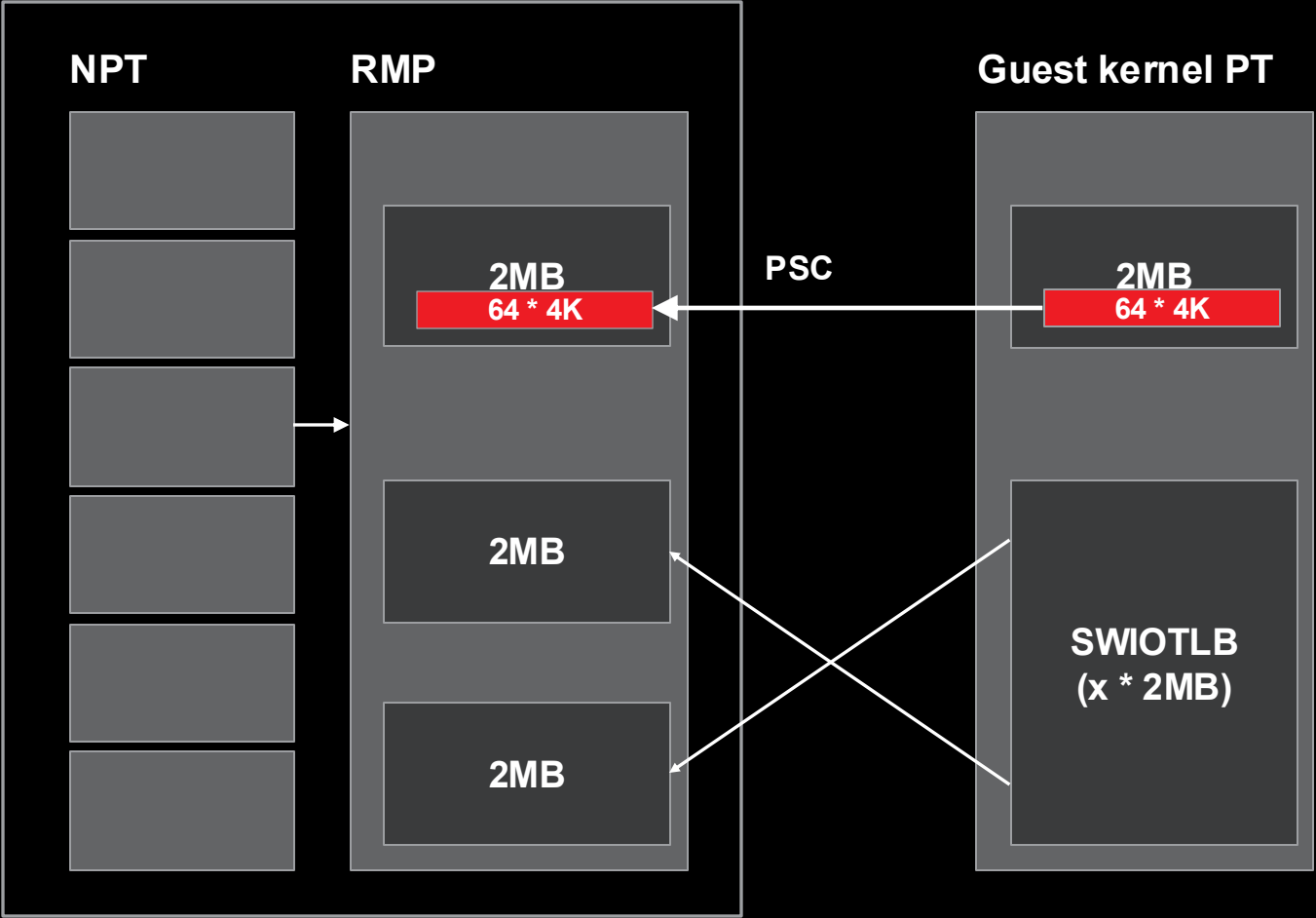
Cbit?
hwIOMMU?
VTOM!

TODO:

- Add ARCH_HAS_PHYS_TO_DMA
- Add arch-specific device.h

Sharing temporary pages => PSMASH

HV / QEMU



/dev/sev-guest

GHCB interface
uses SWIOTLB

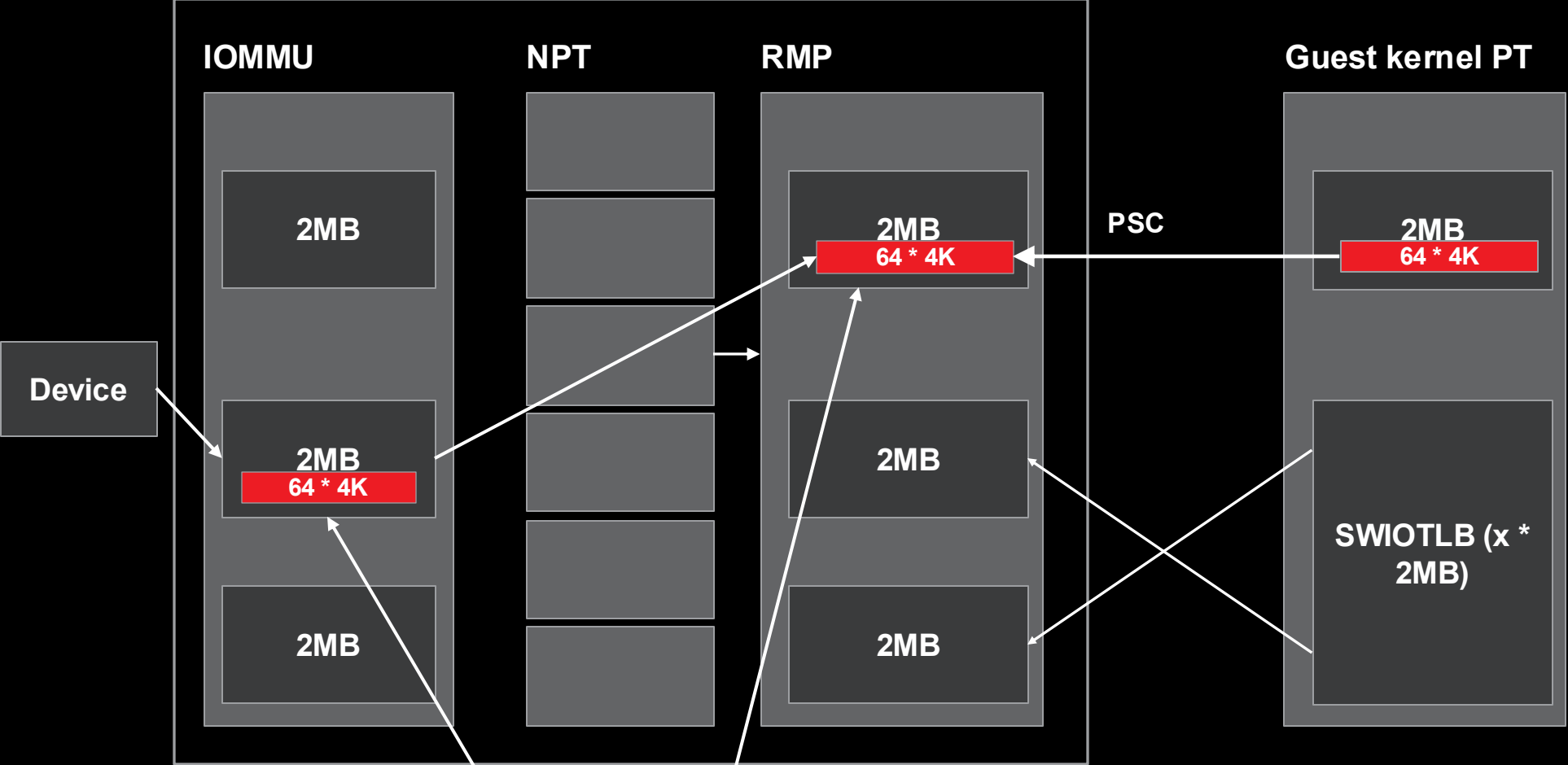
**NO support for
UNSMASH**

TODO:
force DMA alloc
2 MB min
(huge granule)

SWIOTLB
4 KB pages,
2 MB aligned

Sharing temporary pages => PSMASH_IO

HV / QEMU



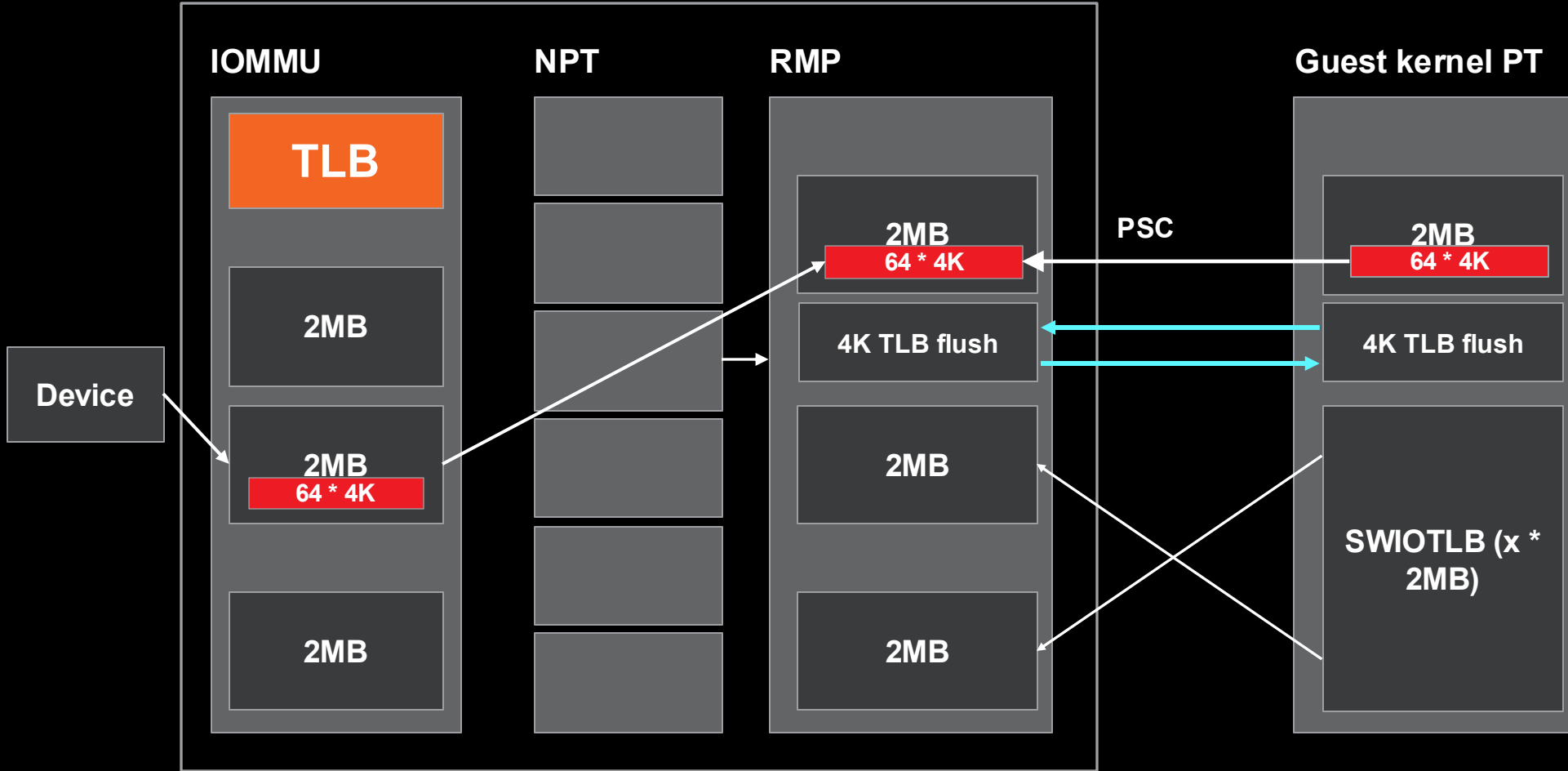
initial IOMMU
smashing
("cut_mapping")
done without
TMPM

TMPM
(memory mover)

IOMMU TLB flushing

```
private <-> shared | rw -> ro | vmpl#N -> vmpl#N-1
```

HV / QEMU



```
G: copy A and B into Page
    (alloc'd at boot?)
G: call HV via GHCB
```

```
H: share Page (rmpupdate)
H: clear A
H: make Page private
  (rmpupdate)
H: return from GHCB
```

```
G: if !(changed(A) &&
      !changed(B))
    panic()
```

Links

<https://github.com/AMDESE/AMDSEV/tree/tsm>

Copyright and disclaimer

©2026 Advanced Micro Devices, Inc. All rights reserved.

AMD, the AMD Arrow logo and combinations thereof are trademarks of Advanced Micro Devices, Inc. Other product names used in this publication are for identification purposes only and may be trademarks of their respective companies.

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

