**# Title:**

Mandate the UEFI implementation to allocate pages from the 48-bit address range first.

**# Status:**

Draft

**# Document:**

UEFI Specification 2.10 Errata

**# License:**

SPDX-License-Identifier: CC-BY-4.0

**# Submitter:**

* Arm (Jose Marinho, Samer El-Haj-Mahmoud)
* Google (Ard Biesheuvel)
* TianoCore Community (<https://www.tianocore.org>)

**# Summary of the change**

The Arm architecture supports up-to 52 bits of physical address (FEAT\_LPA, FEAT\_LPA2), though the baseline is 48 bits.  
Some OSs only support 48 bit addressing by default.

In order to support these OSs, this ECR mandates the UEFI implementation to allocate pages from the 48-bit address range first. Once the 48-bit range is depleted, the UEFI implementation is permitted to allocate pages at higher addresses.

**# Benefits of the change**  
The compliant firmware can correctly interoperate with OSs that only support 48-bit physical address space.

**# Impact of the change**Changes to the EDK2 allocation for AArch64 are required to ensure mappings are below the 2^48 limit.

**# Detailed description of the change [normative updates]**

* Insertions highlighted
* Removals in ~~red~~

**2. Overview  
…**

**2.3 Calling Conventions**

**…**

**2.3.6. AArch64 Platforms**

**…**

**Note**: The state of other system control register bits is not dictated by this specification.

* All floating point traps and exceptions will be disabled at the relevant exception levels (FPCR=0, CPACR\_EL1.FPEN=11, CPTR\_EL2.TFP=0). This implies that the FP unit will be enabled by default.
* Implementations of boot services will enable architecturally manageable caches and TLBs i.e., those that can be managed directly using implementation independent registers using mechanisms and procedures defined in the ARM Architecture Reference Manual. They should not enable caches requiring platform information to manage or invoke non-architectural cache/TLB lockdown mechanisms.
* MMU configuration: Implementations must use only 4k pages and a single translation base register. On devices supporting multiple translation base registers, TTBR0 must be used solely. The binding does not mandate whether page tables are cached or un-cached.
* Interrupts are enabled, though no interrupt services are supported other than the UEFI boot services timer functions (All loaded device drivers are serviced synchronously by “polling”). All UEFI interrupts must be routed to the IRQ vector only.
* The architecture generic timer must be initialized and enabled. The Counter Frequency register (CNTFRQ) must be programmed with the timer frequency. Timer access must be provided to non-secure EL1 and EL0 by setting bits EL1PCTEN and EL1PCEN in register CNTHCTL\_EL2.
* The system firmware is not expected to initialize EL2 registers that do not have an architectural reset value, except in cases where firmware itself is running at EL2 and needs to do so.
* 128 KiB or more of available stack space
* The ARM architecture allows mapping pages at a variety of granularities, including 4KiB and 64KiB. If a 64KiB physical page contains any 4KiB page with any of the following types listed below, then all 4KiB pages in the 64KiB page must use identical ARM Memory Page Attributes (as described in [Map EFI Cacheability Attributes to AArch64 Memory Types](https://uefi.org/specs/UEFI/2.10/02_Overview.html#map-efi-cacheability-attributes-to-aarch64-memory-types) ):

– EfiRuntimeServicesCode

– EfiRuntimeServicesData

– EfiReserved

– EfiACPIMemoryNVS

Mixed attribute mappings within a larger page are not allowed.

**Note**: This constraint allows a 64K paged based Operating System to safely map runtime services memory.

Platform firmware must not return allocations outside of the 48-bit addressable range of memory unless:  
 1. that range is completely exhausted, or  
 2. that was explicitly requested via the AllocateAddress allocation type.  
If any of the above conditions occurs, an OS that lacks support for addresses wider than 48-bit may malfunction.  
  
Note: Platform firmware may need to allocate memory at a specific address in order to satisfy a platform-specific requirement. That behaviour is allowed by the constraints above.  
  
Note: the exception 1) above accommodates systems that have fewer memory, in the 48-bit addressable range, than what is required for proper system operation. The exception allows firmware to remain compliant when only memory above the 48-bit addressable range is available for allocation.

Note: Systems that support FEAT\_LPA/FEAT\_LVA, but not FEAT\_LPA2, are unable to map memory outside the 48-bit addressable range when using 4K pages. Thus, the platform firmware cannot map memory outside the 48-bit addressable range while remaining UEFI compliant.  
On those systems, any allocation outside the 48-bit addressable range is forbidden, even in the 2 scenarios listed above.