

UEFI & EDK II Training

UEFI AND PLATFORM INITIALIZATION (PI) BOOT FLOW &
OVERVIEW

tianocore.org

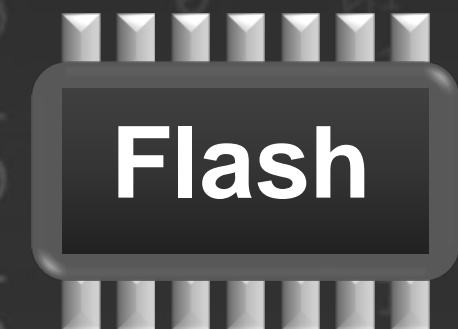


LESSON OBJECTIVE

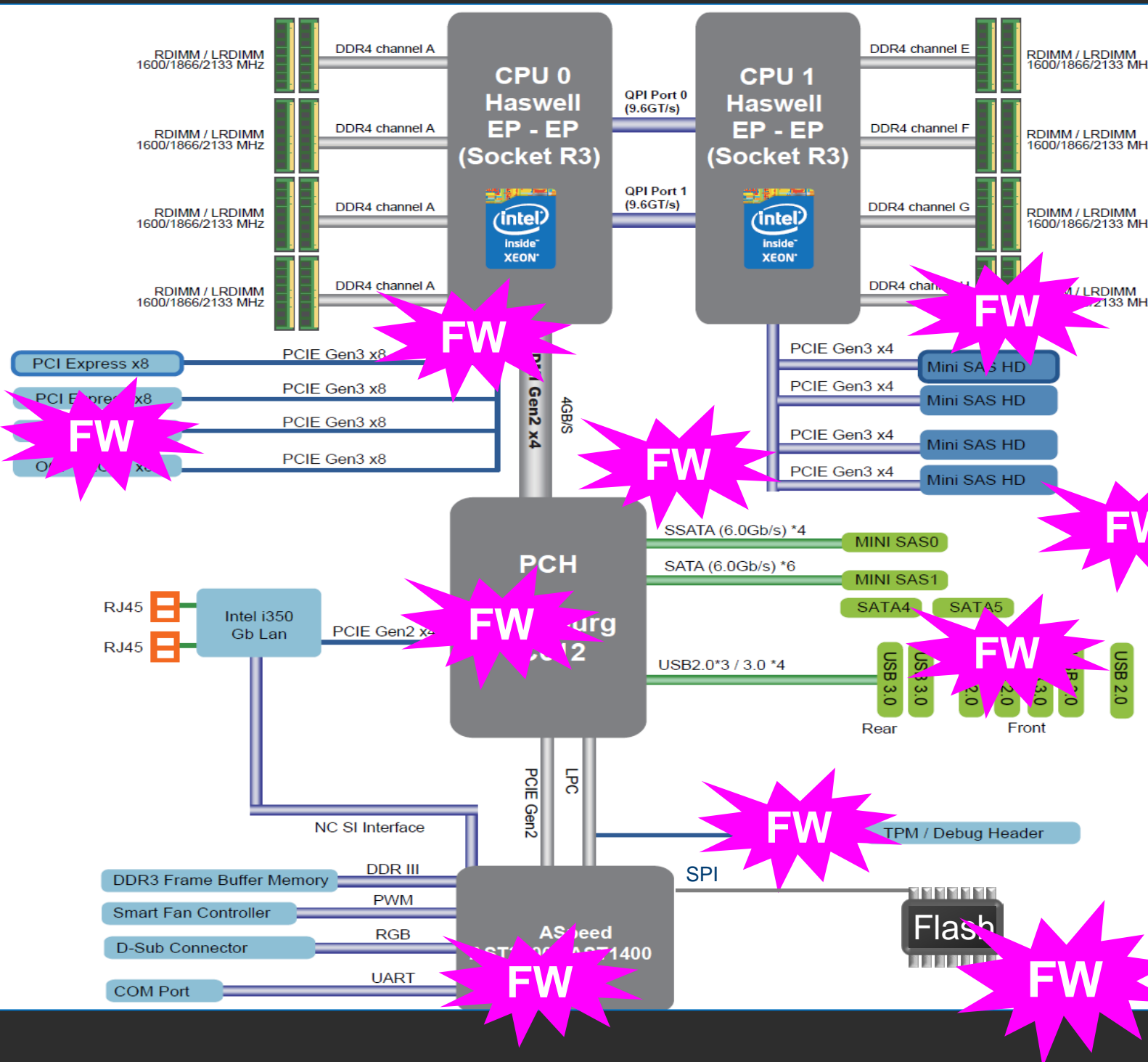
- Where is the System Firmware
- Review UEFI Platform Initialization Boot Flow Process
- What about Management Mode (Formerly Known as SMM)
- What is Intel[®] Firmware Support Package (Intel[®] FSP)
- The UEFI.org Forum & Tianocore.org

WHERE IS THE FIRMWARE

Where is the UEFI Firmware on a platform

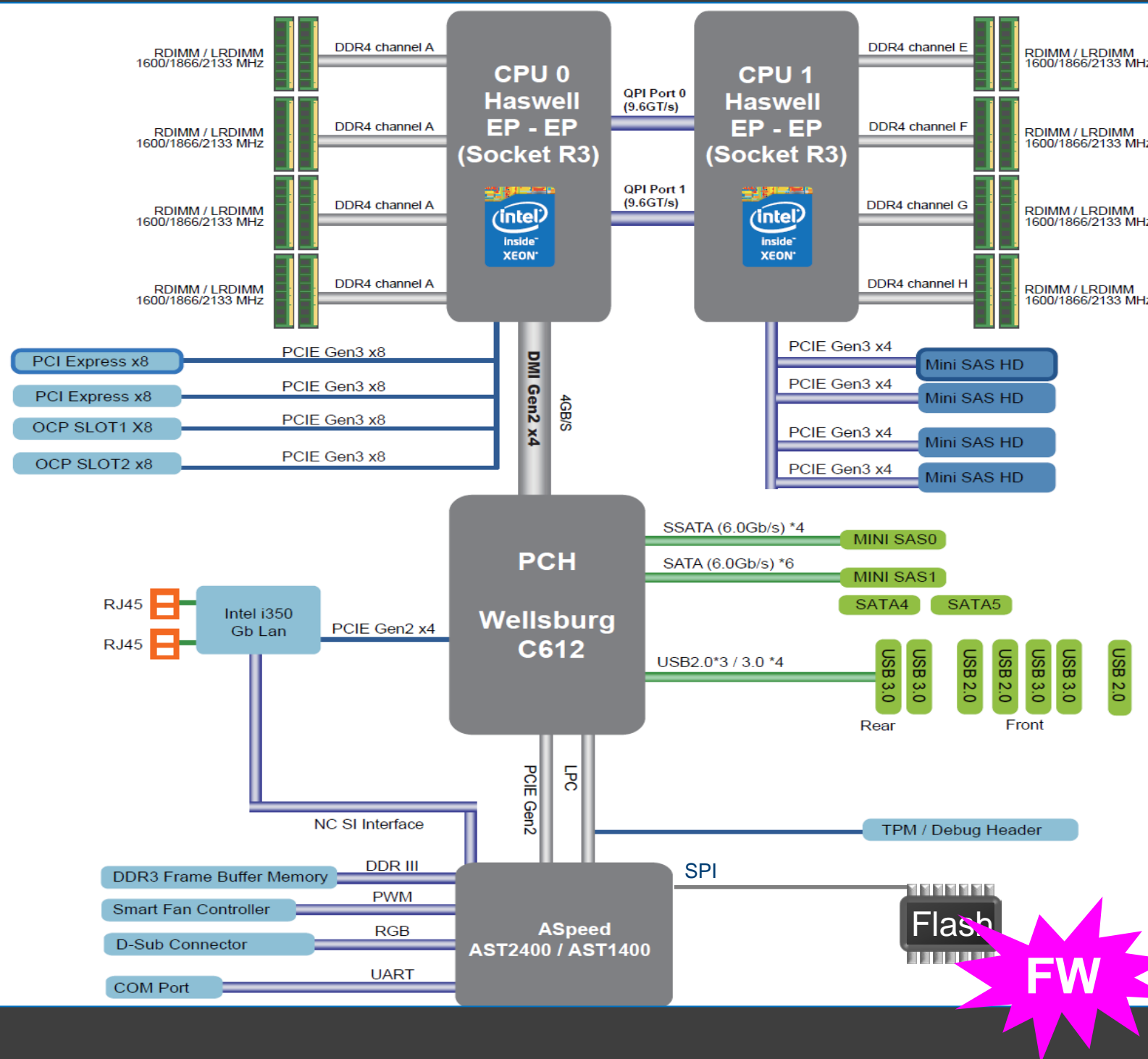


Firmware is Everywhere



- GBe NIC, WiFi, Bluetooth, WiGig
- Baseband (3G, LTE) Modems
- Sensor Hubs
- NFC, GPS Controllers
- HDD/SSD
- Keyboard and Embedded Controllers
- Battery Gauge
- Baseboard Management Controllers (BMC)
- Graphics/Video
- USB Thumb Drives, keyboards/mice
- Chargers, adapters
- TPM, security coprocessors
- Routers, network appliances

Main system firmware (BIOS, UEFI firmware, coreboot)

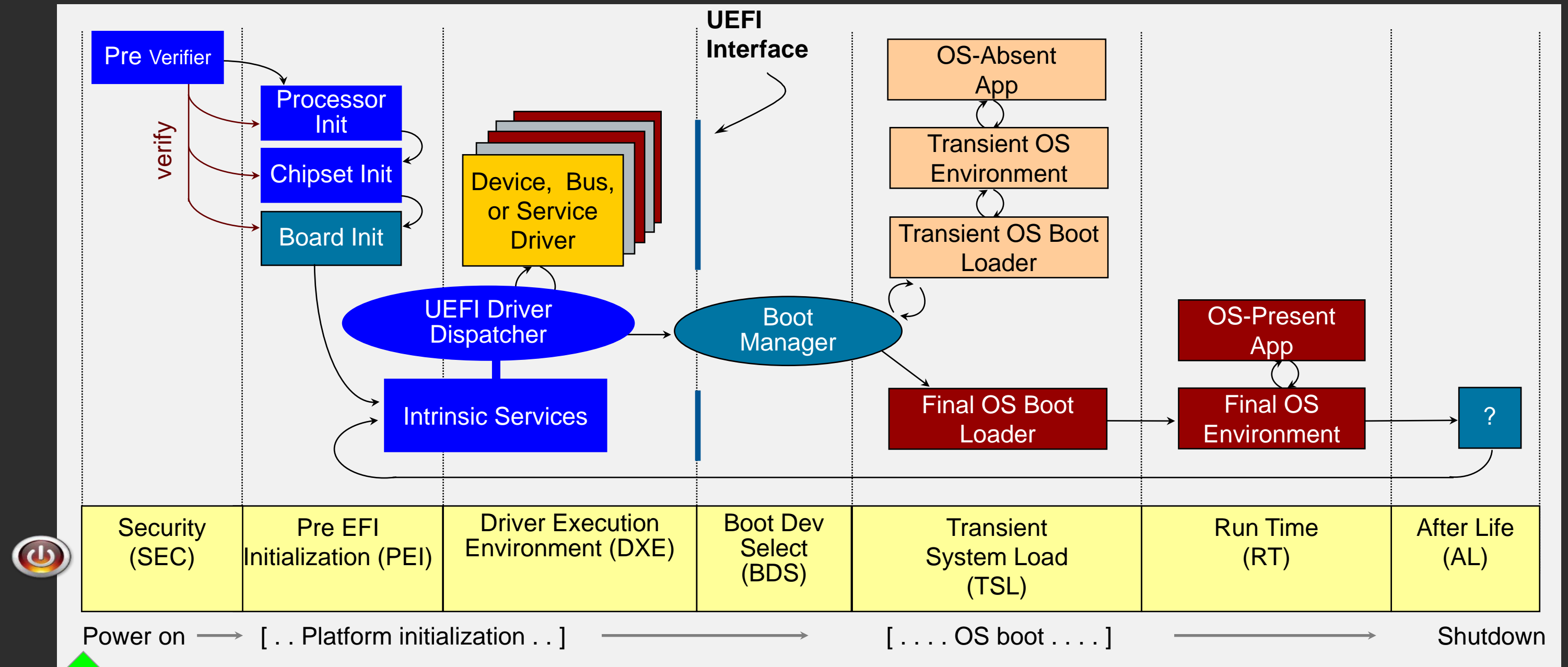


Main system firmware (BIOS, UEFI firmware, coreboot)

UEFI BOOT EXECUTION FLOW

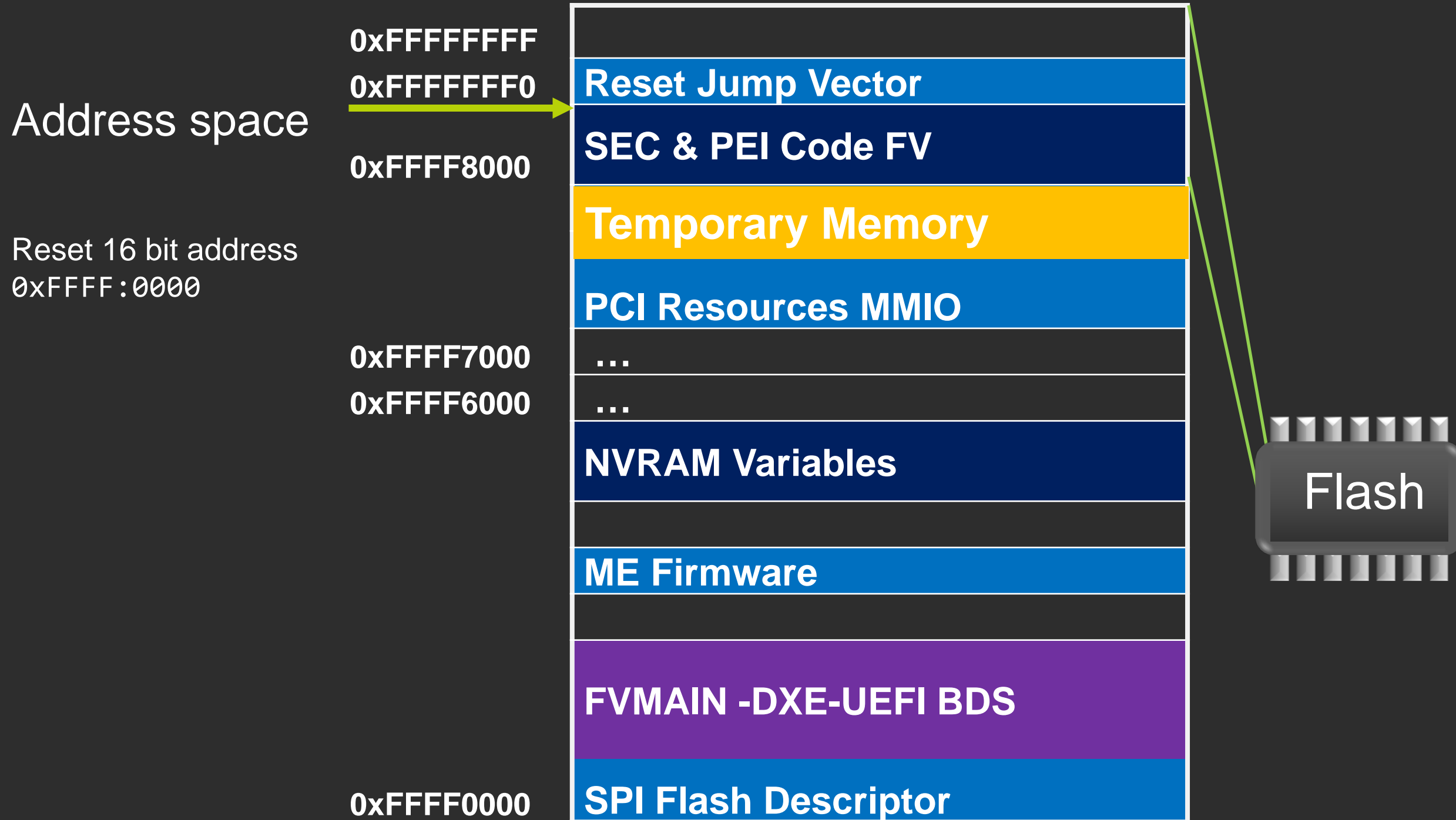
Starting at the processor reset vector

UEFI – PI & EDK II BOOT FLOW - SEC

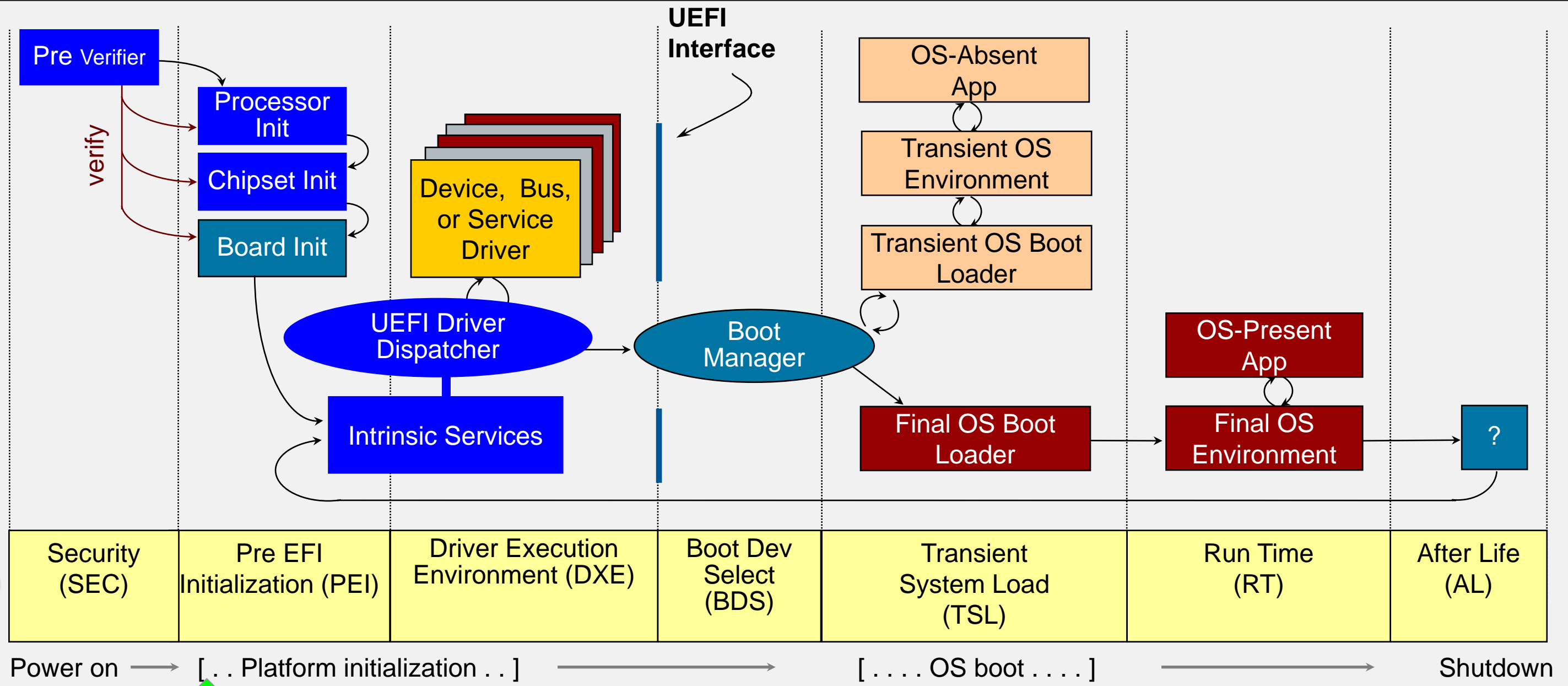


System Reset Vector
Stage 7 on IA

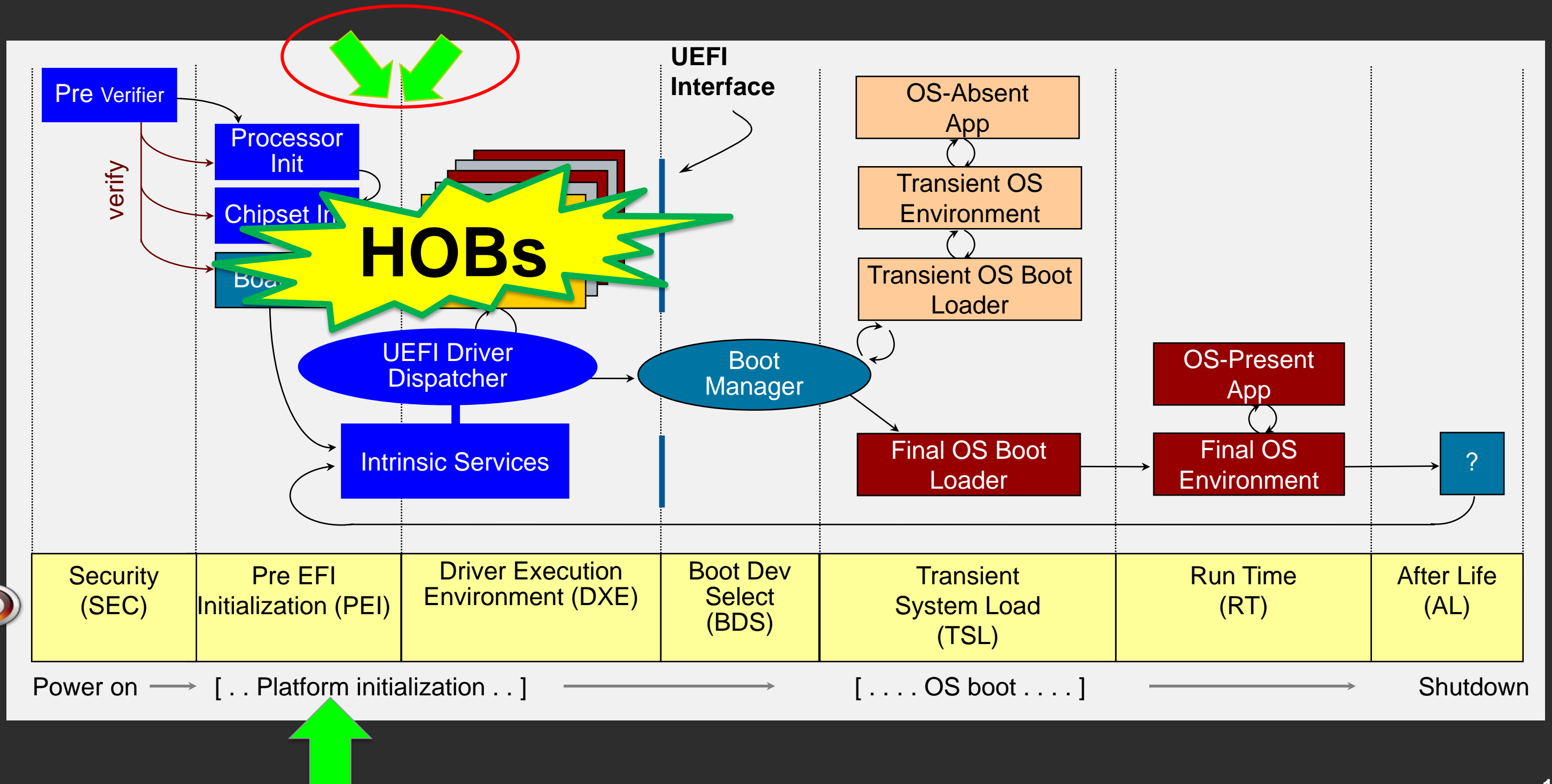
PRE-MEMORY INIT



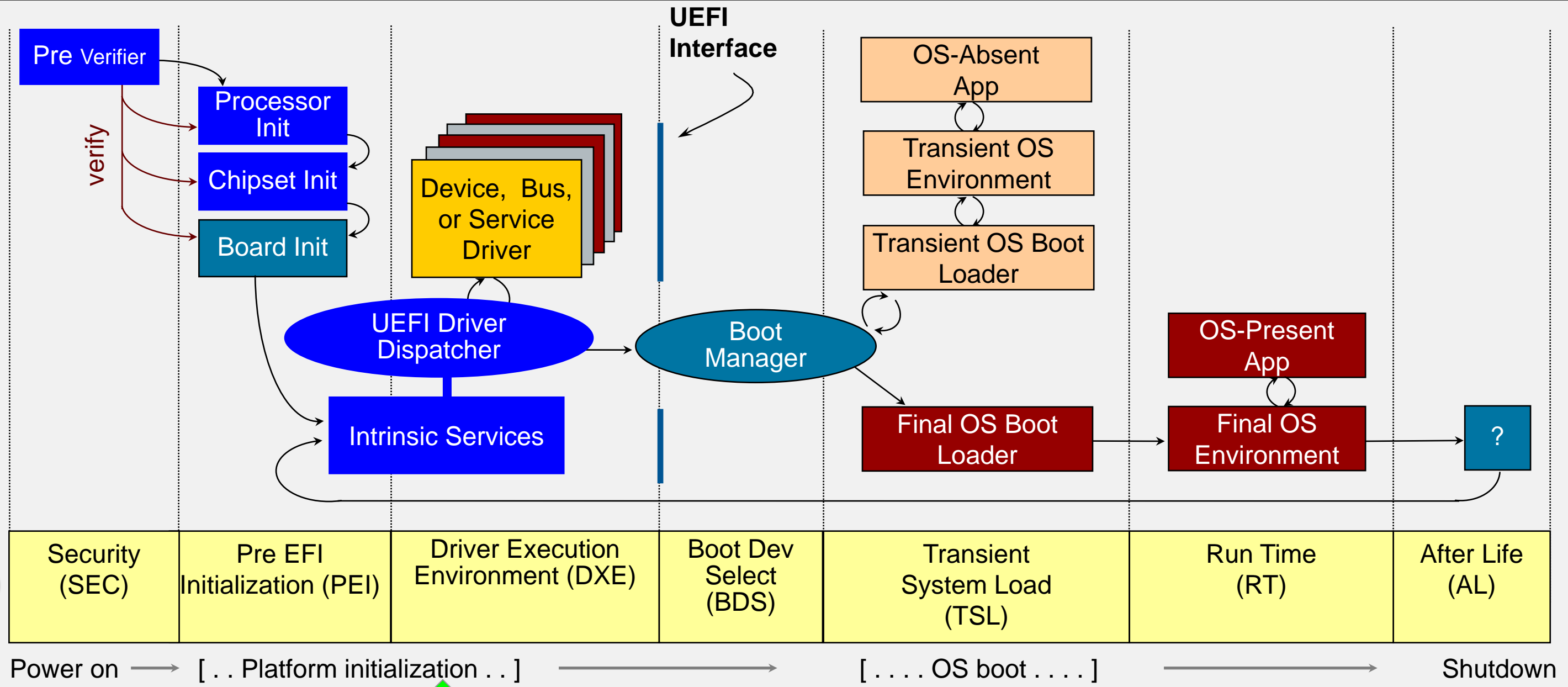
UEFI – PI & EDK II BOOT FLOW - PEI



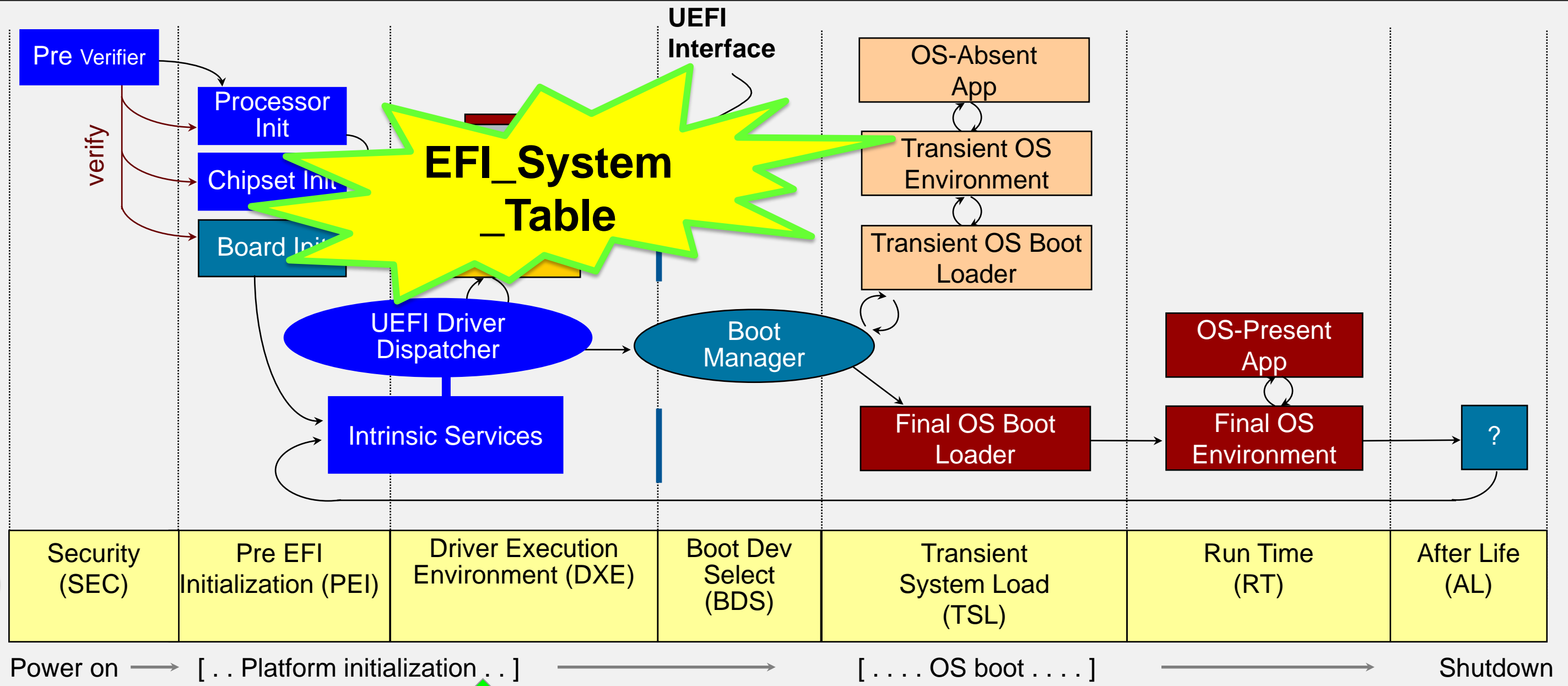
UEFI – PI & EDK II BOOT FLOW - DXEIMPL



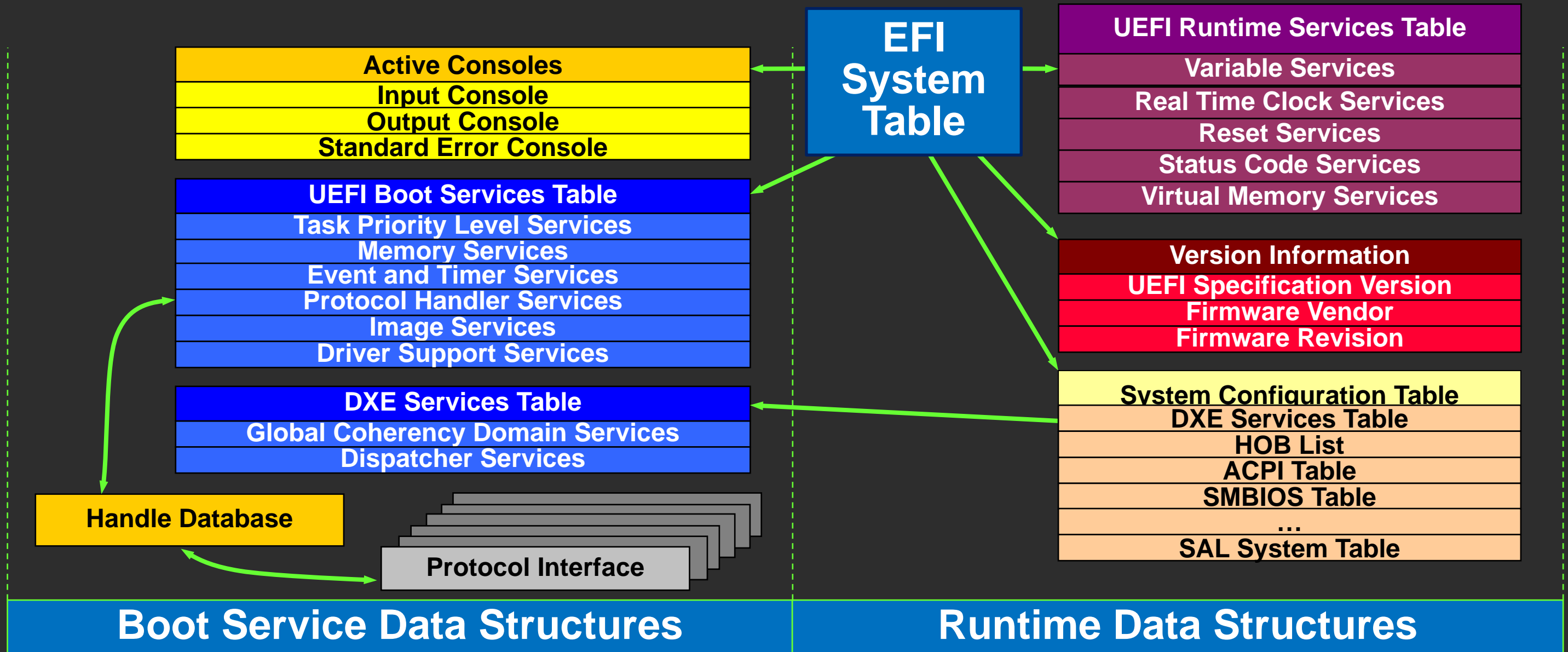
UEFI – PI & EDK II BOOT FLOW – DXE



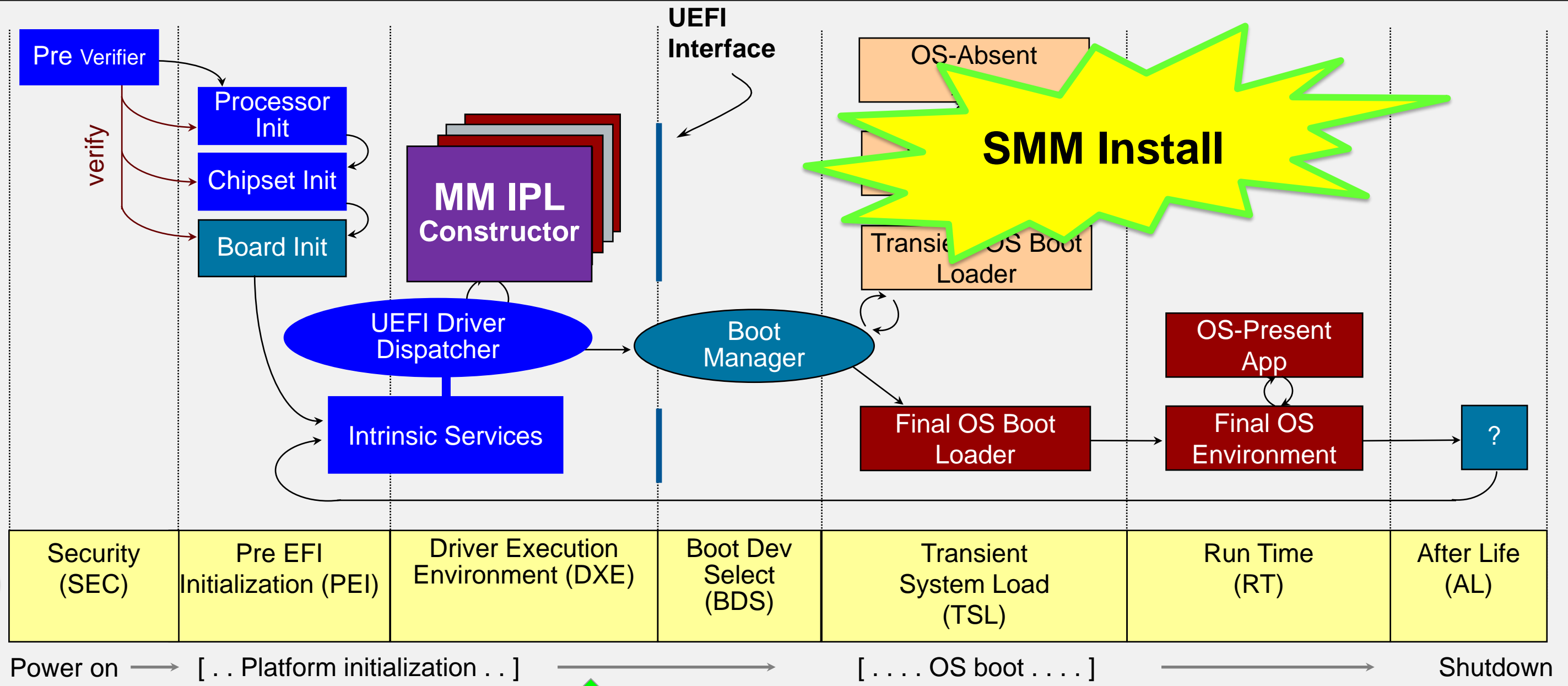
UEFI – PI & EDK II BOOT FLOW – DXE



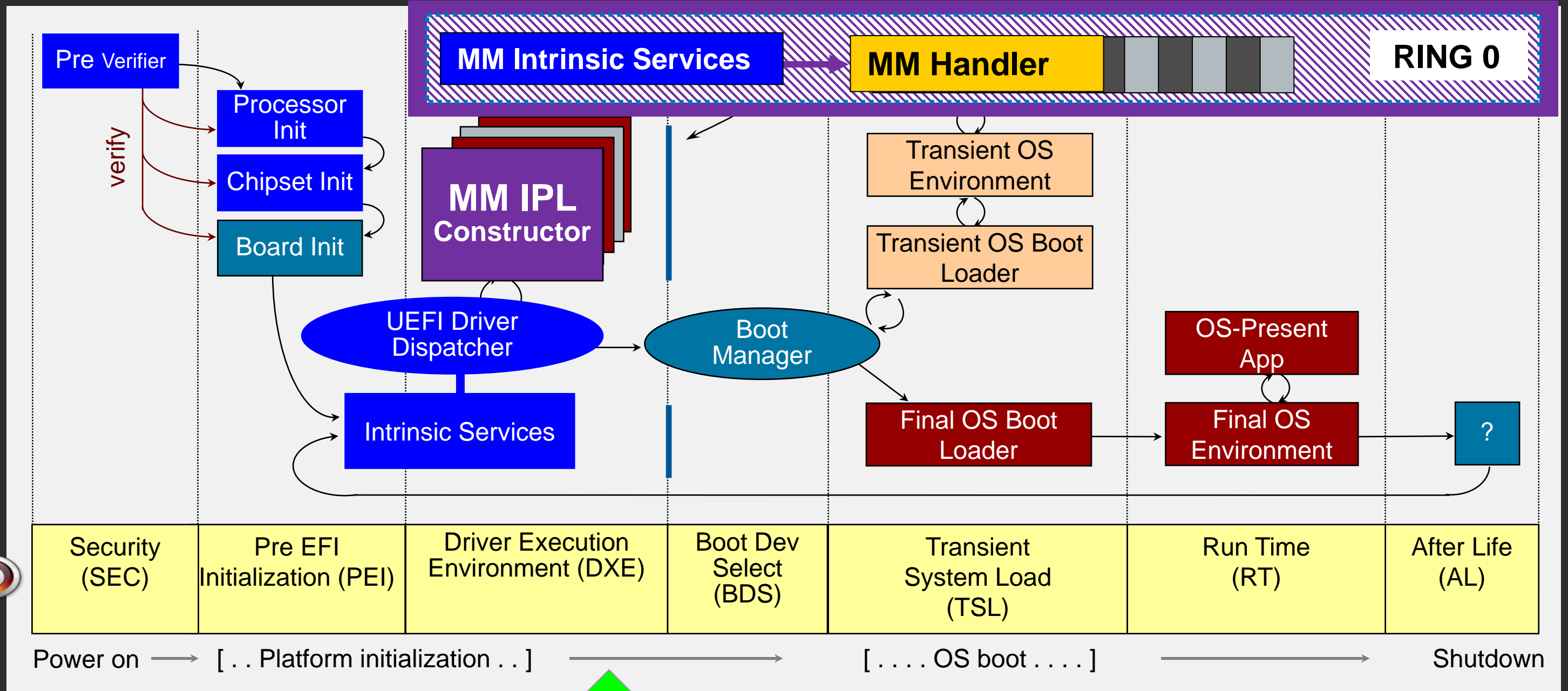
UEFI SYSTEM TABLE



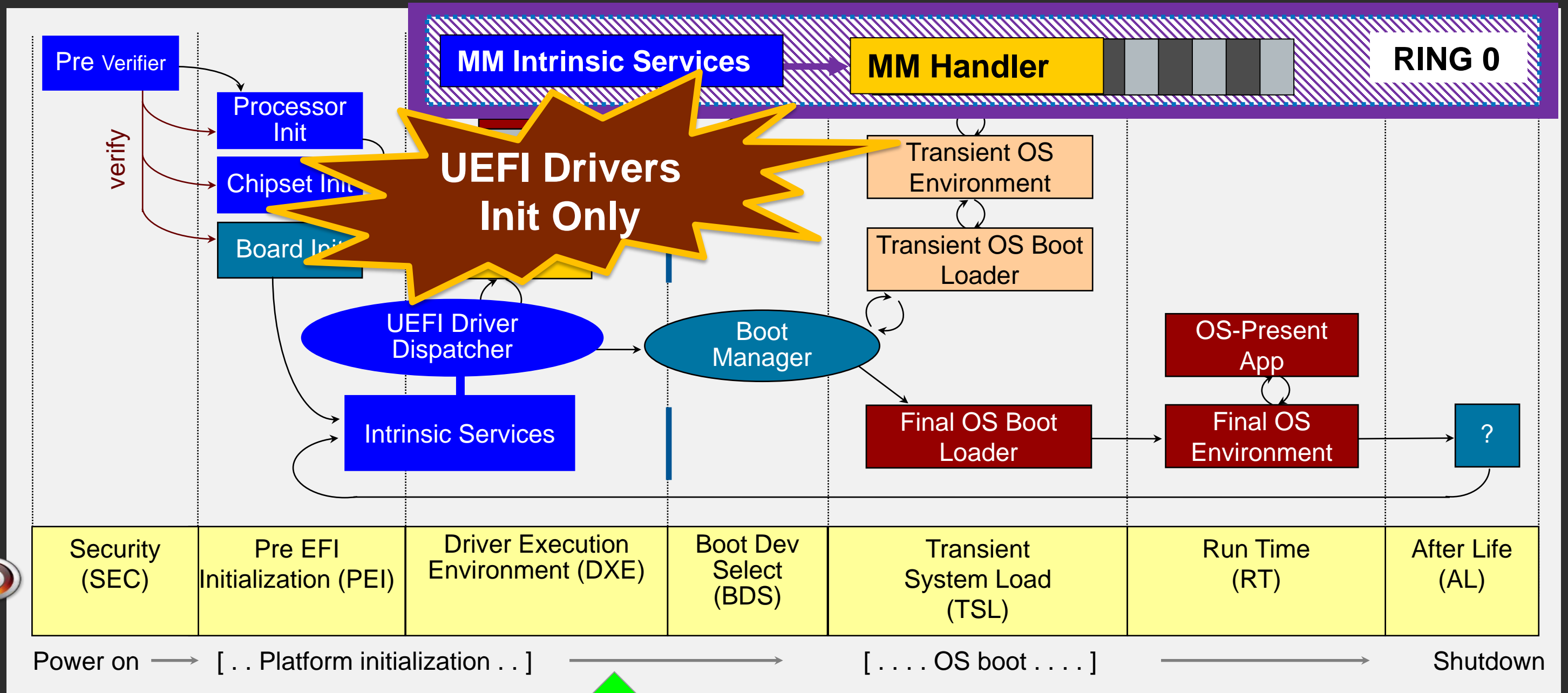
UEFI - PI & EDK II BOOT FLOW - SMM



UEFI - PI & EDK II BOOT FLOW - SMM



UEFI – PI & EDK II BOOT FLOW – DXE UEFI



Protocols

- Interfaces consisting of functions and data structures named by a GUID and stored in the Handle Database

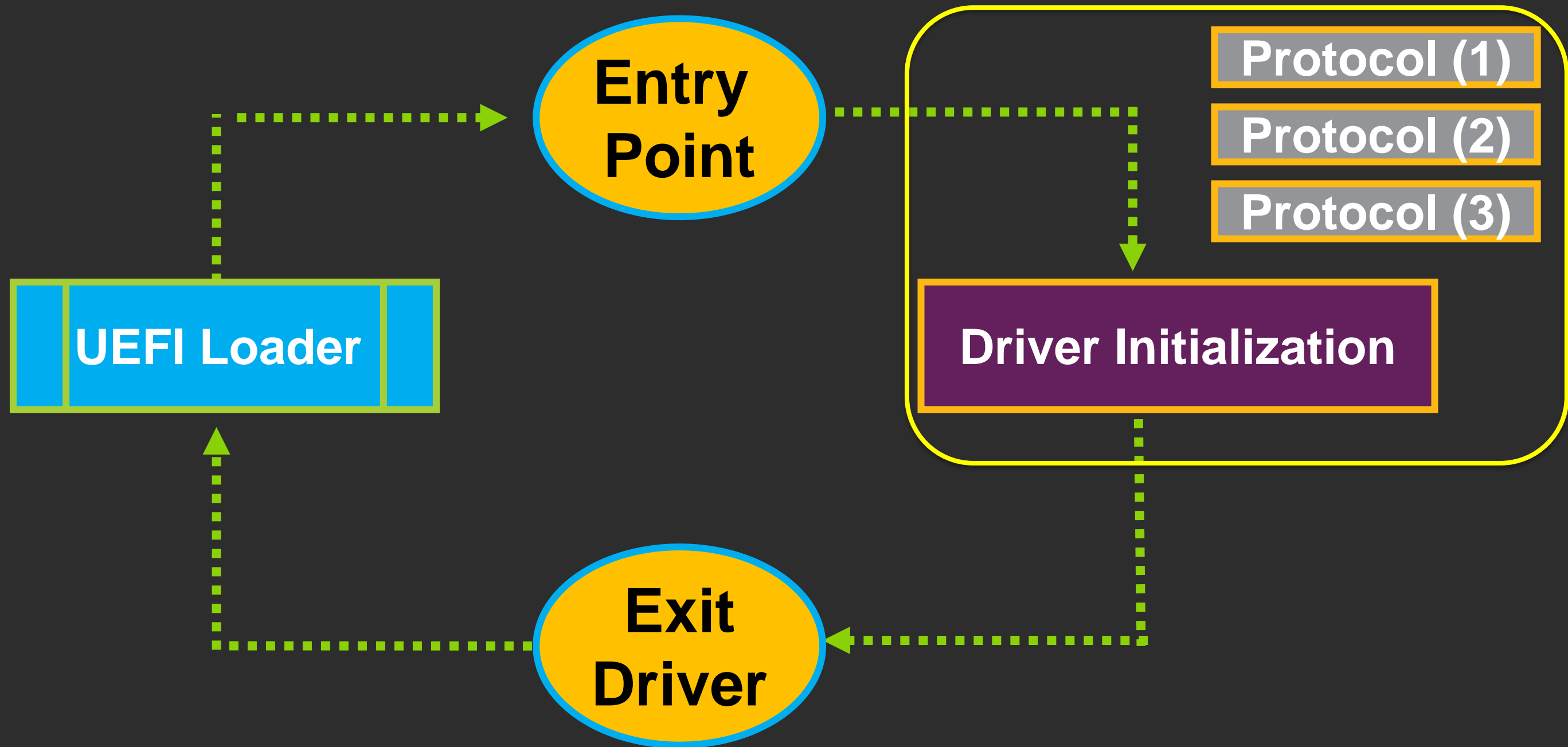
Handle Database

- Everything in the platform system gets a handle, drivers, devices, Images, etc.

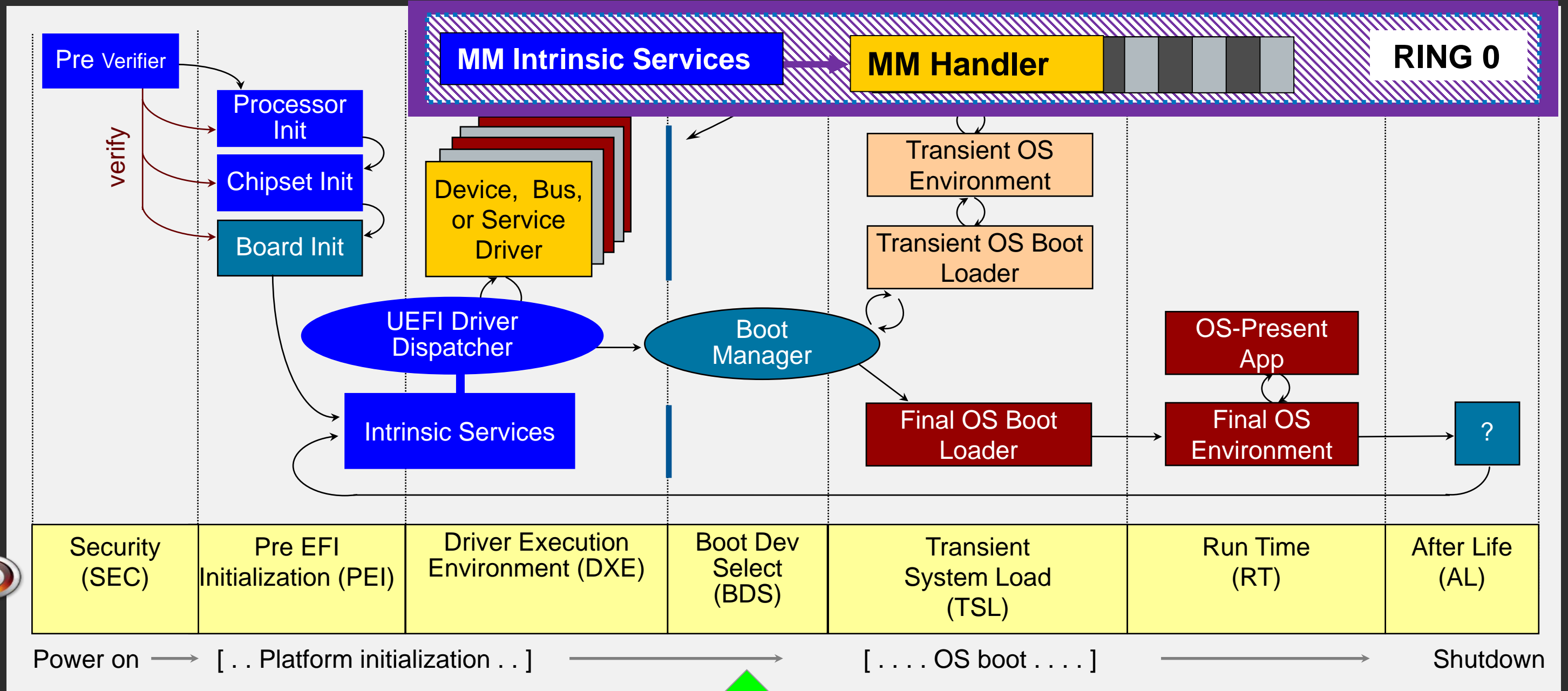
GUIDs

- The UEFI Platform only knows items in the Handle Database by its GUID

DXE Dispatcher Installs Drivers



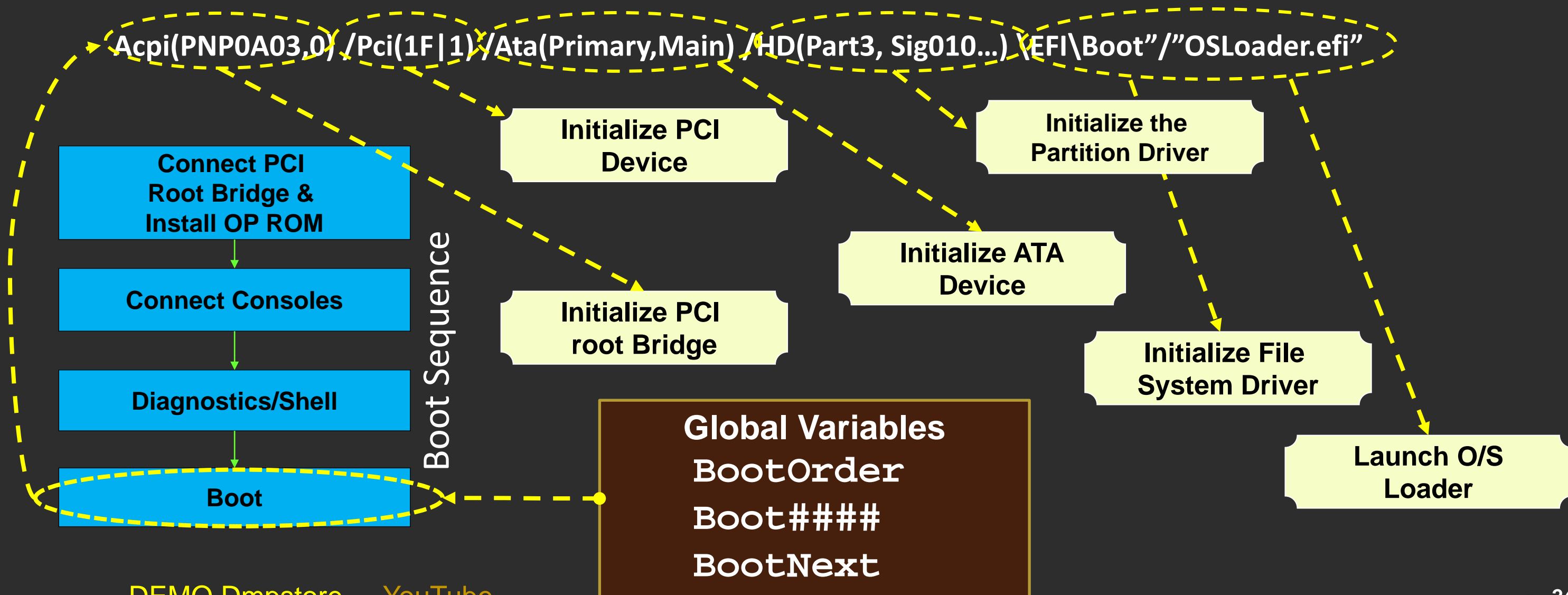
UEFI – PI & EDK II BOOT FLOW – BDS



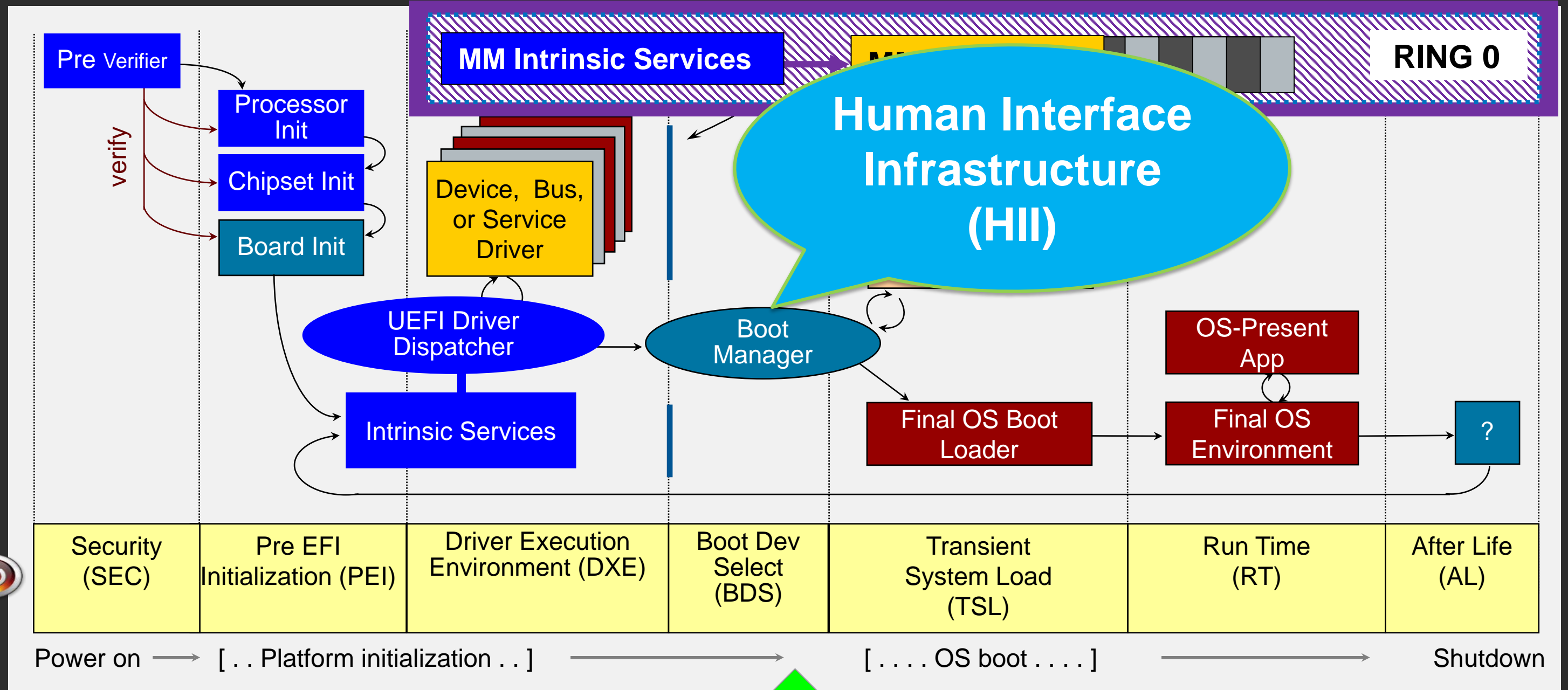
UEFI DEVICE PATH AND GLOBAL VARIABLES

The UEFI Device Path describes a boot target

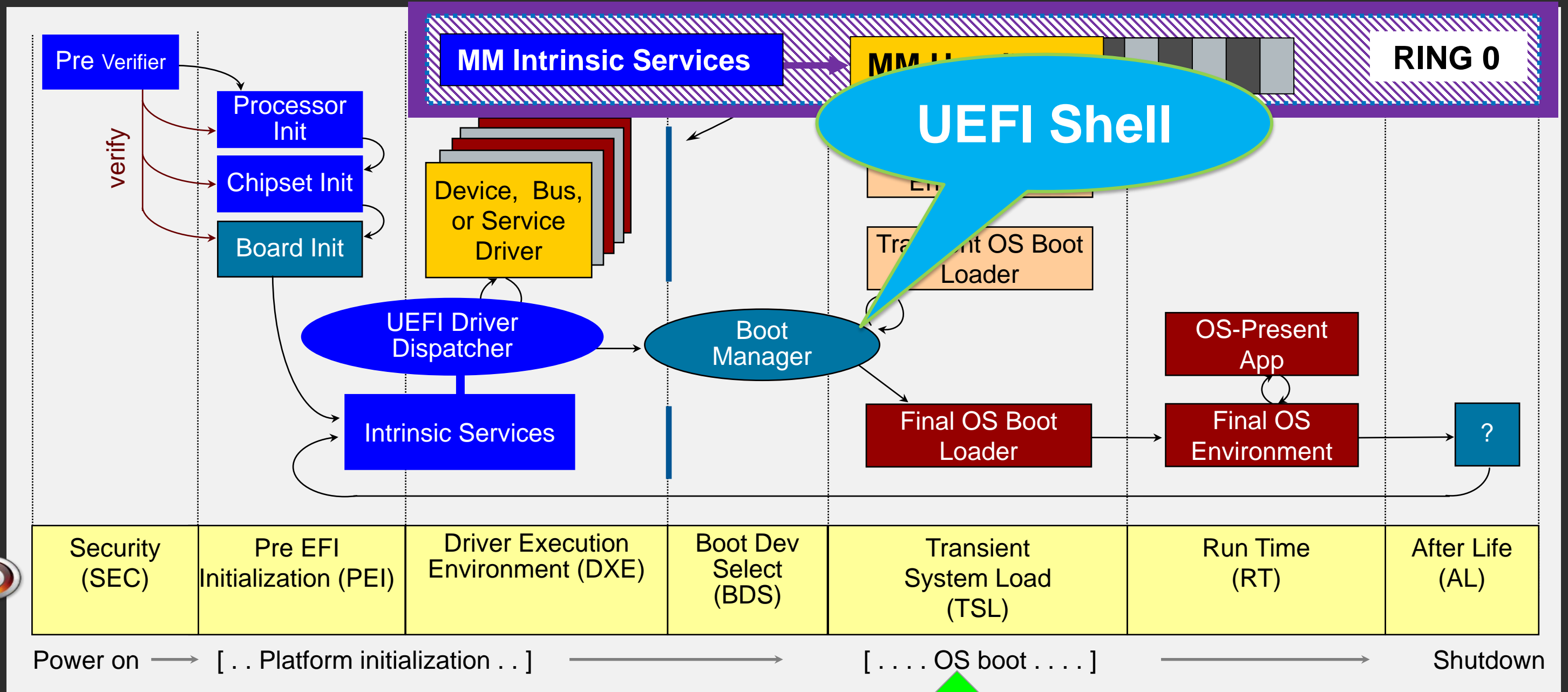
- Binary description of the physical location of a specific target



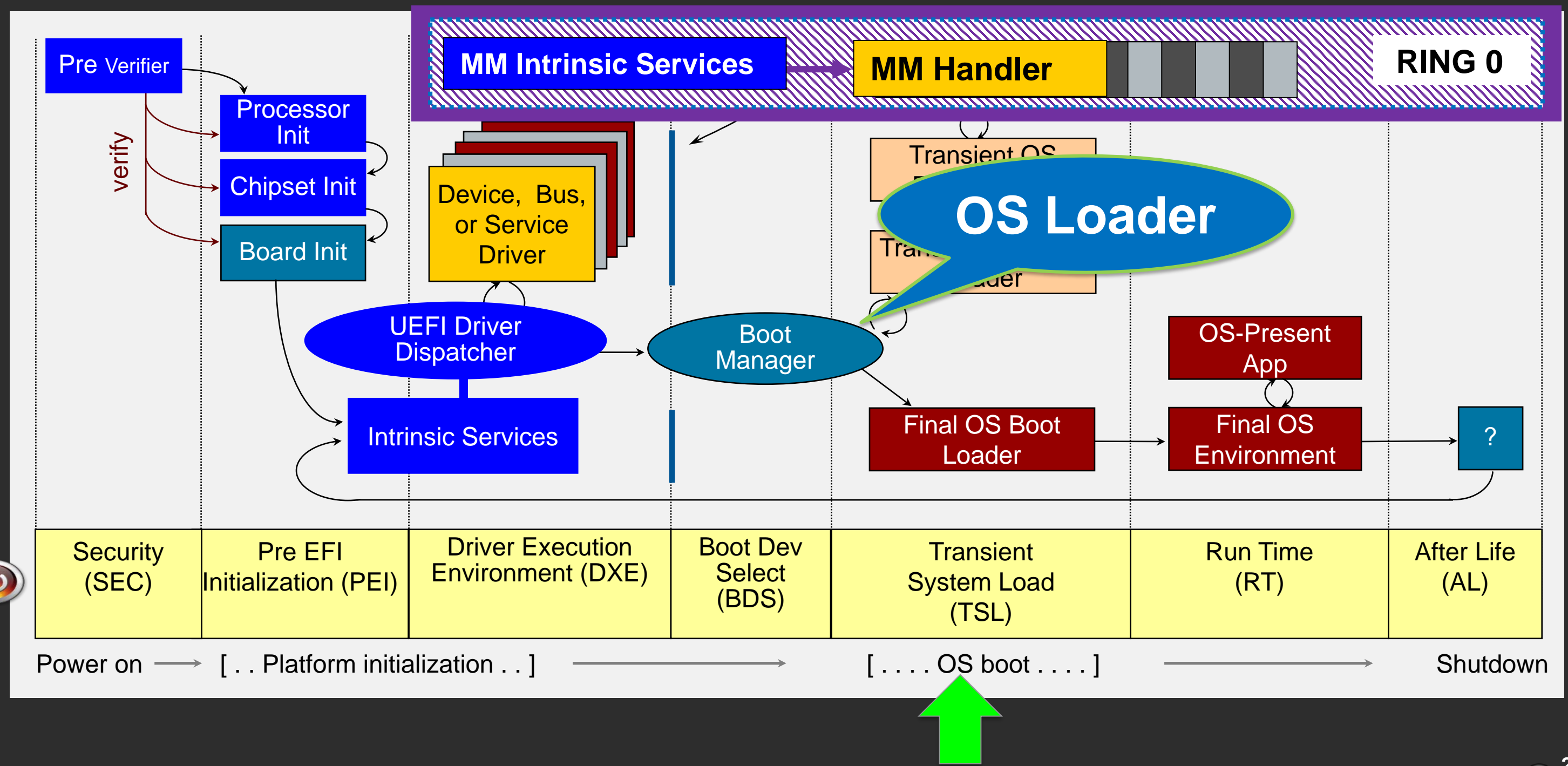
UEFI – PI & EDK II BOOT FLOW – HII



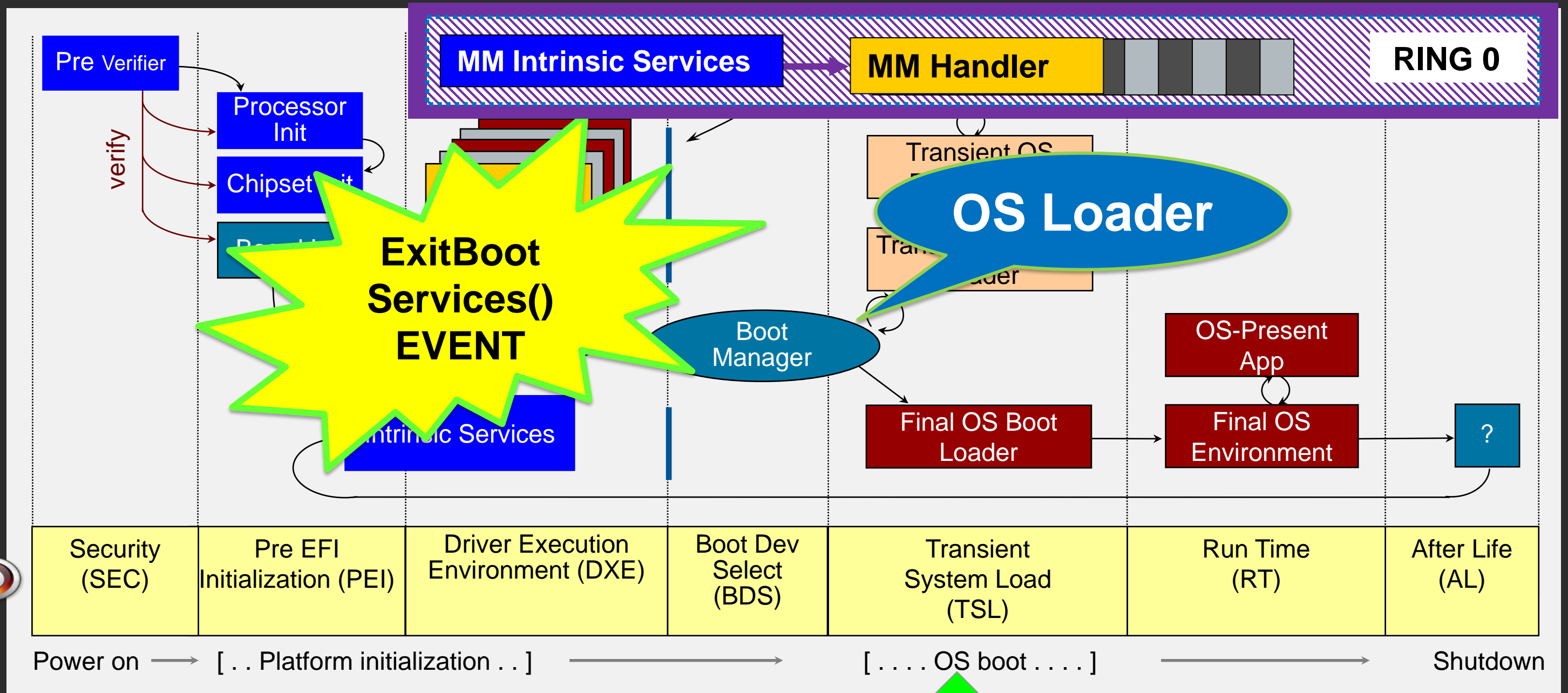
UEFI – PI & EDK II BOOT FLOW – TSL



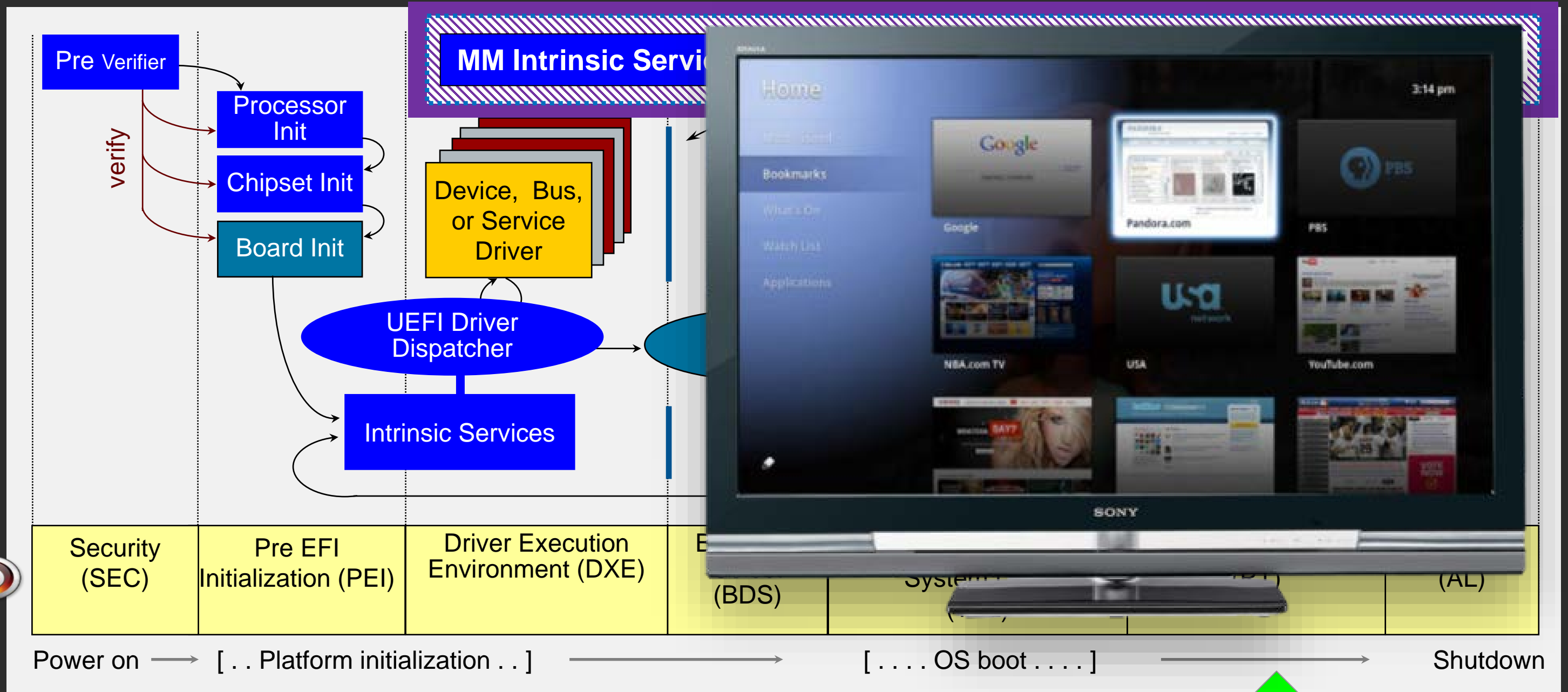
tianocore **UEFI – PI & EDK II BOOT FLOW – BOOT LOADER**



UEFI - PI & EDK II BOOT FLOW - EVENT



UEFI - PI & EDK II BOOT FLOW - BOOT UEFI OS



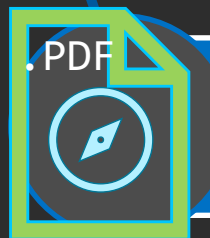
THE INTEL[®] FIRMWARE SUPPORT PACKAGE (INTEL[®] FSP)

What is Intel® Firmware Support Package?

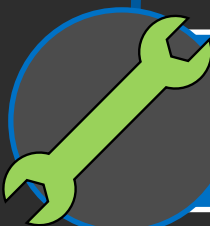
Includes:



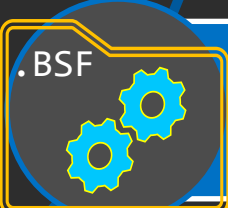
A binary firmware device (FD) file - contains multiple FSP Modules



An integration guide



A rebasing tool



A Boot Setting File (BSF) or YAML file for Configuration of the Updatable Product Data (UPD)

What Does Intel® FSP Provide?

- Provides silicon initialization code:
 - Initializes processor core, chipset as explained in BIOS Writers' Guide
 - Is relocatable in ROM
 - Can be configured for platform customization
- Boot loader agnostic and can be easily integrated with many options:
 - Open source boot loaders: UEFI –EDK II, Coreboot, U-boot, etc.
 - RTOS
 - Others

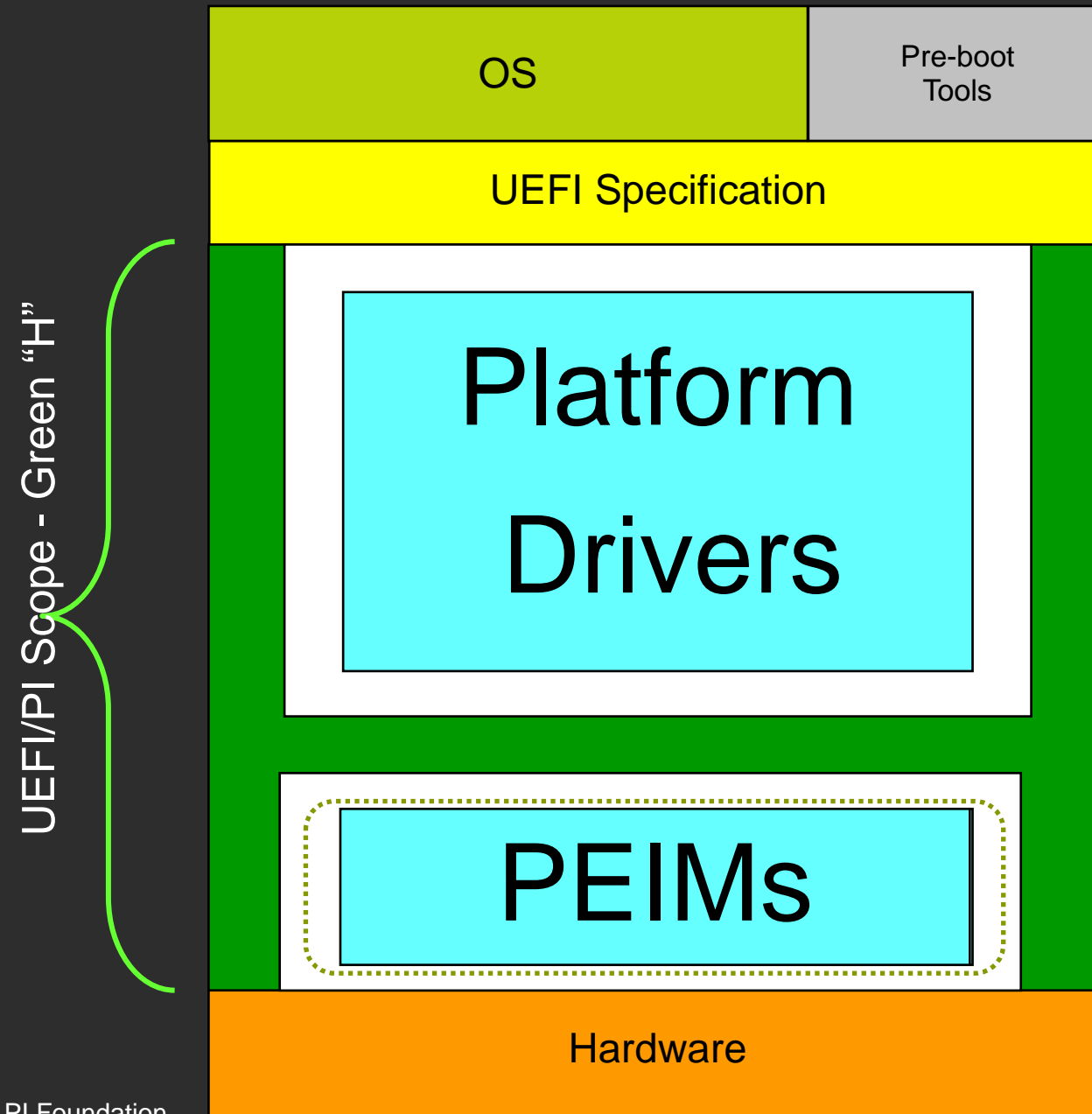
Intel FSP is currently available for the many Intel hardware-producing divisions



See: [About Intel FSP](#) (Intel® FSP 2.3 July 2021)

White Paper Example: [Open Braswell - Design and Porting Guide](#)

Intel® FSP is NOT a stand-alone boot-loader

Intel® FSP to Open Source EDK II

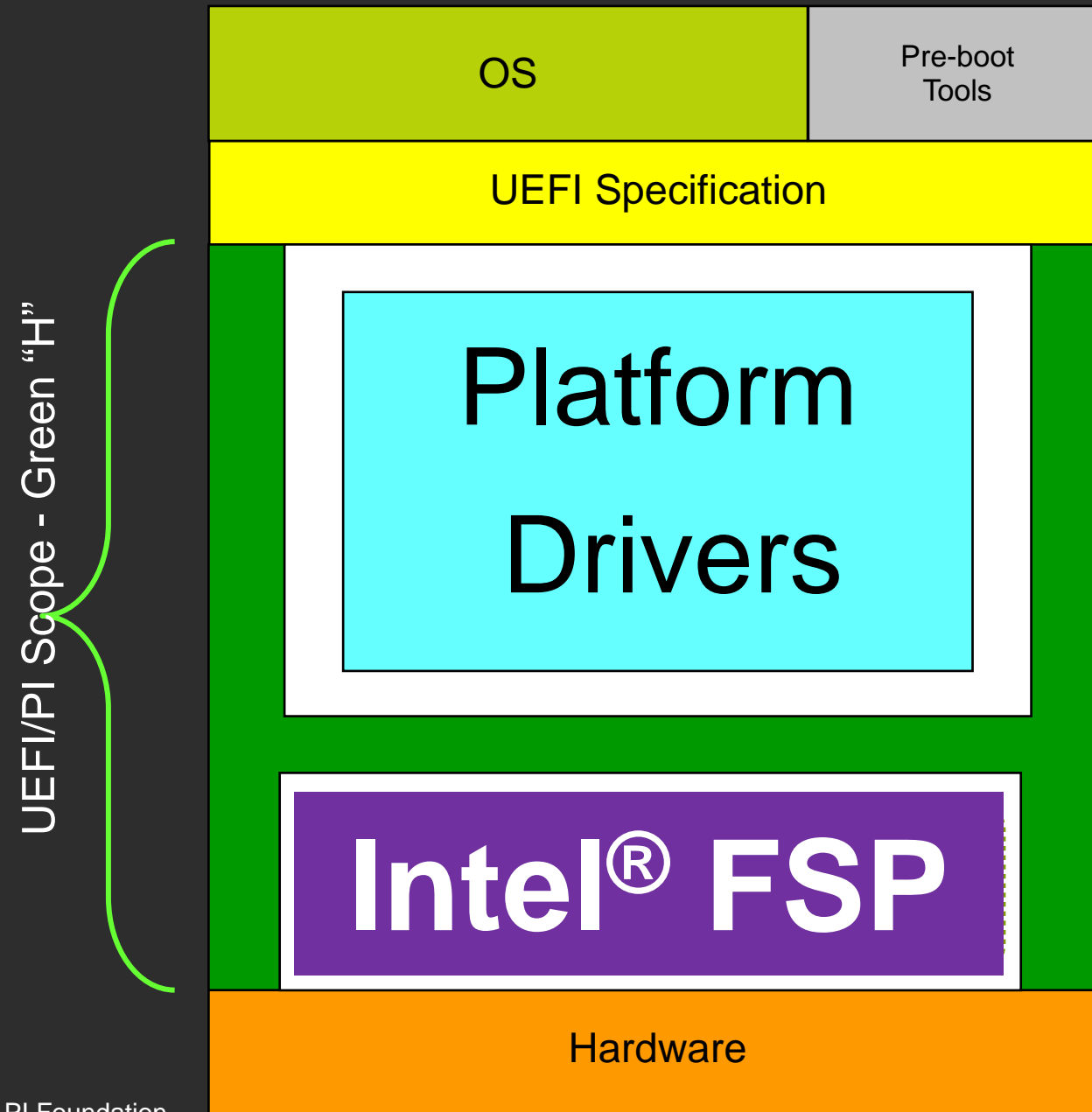


 PEI/DXE PI Foundation
 Modular Components

EDK II provides the framework ("Green H")

Intel® Firmware Support Package (Intel® FSP) provides low level of silicon initialization

Intel® FSP to Open Source EDK II

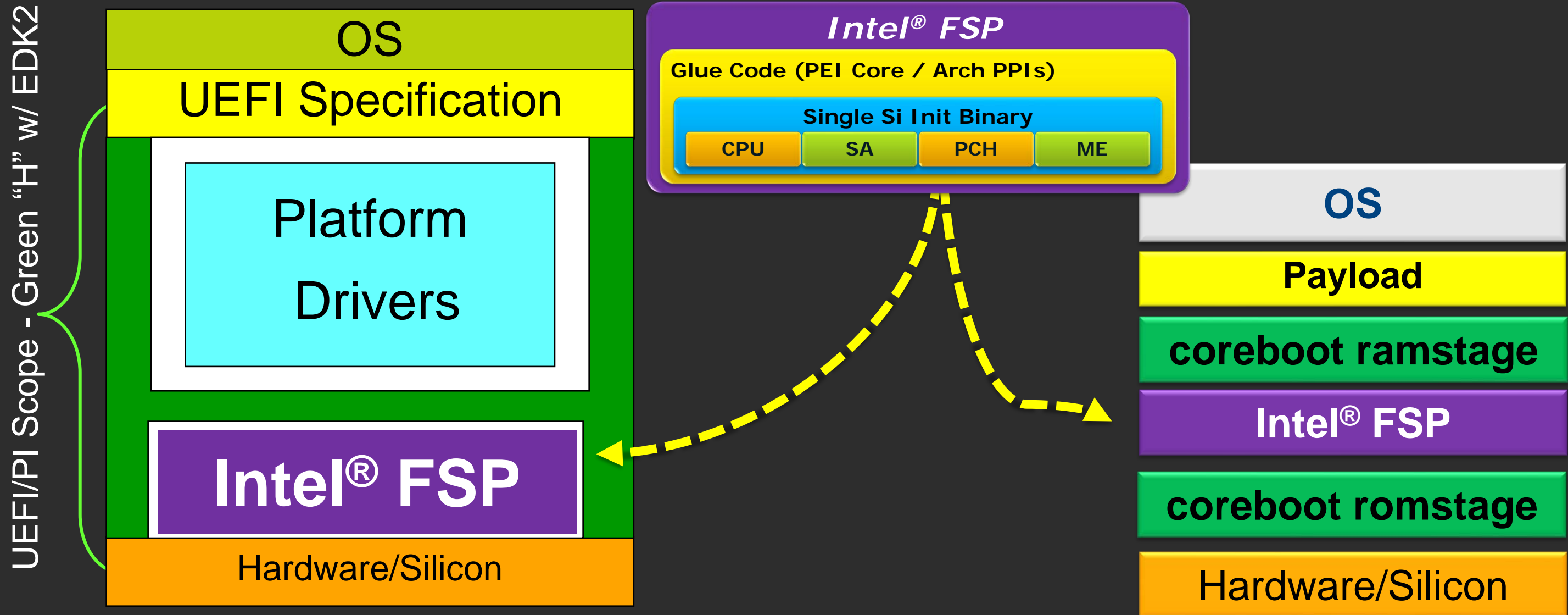


■ PEI/DXE PI Foundation
■ Modular Components

EDK II provides the framework (“Green H”)

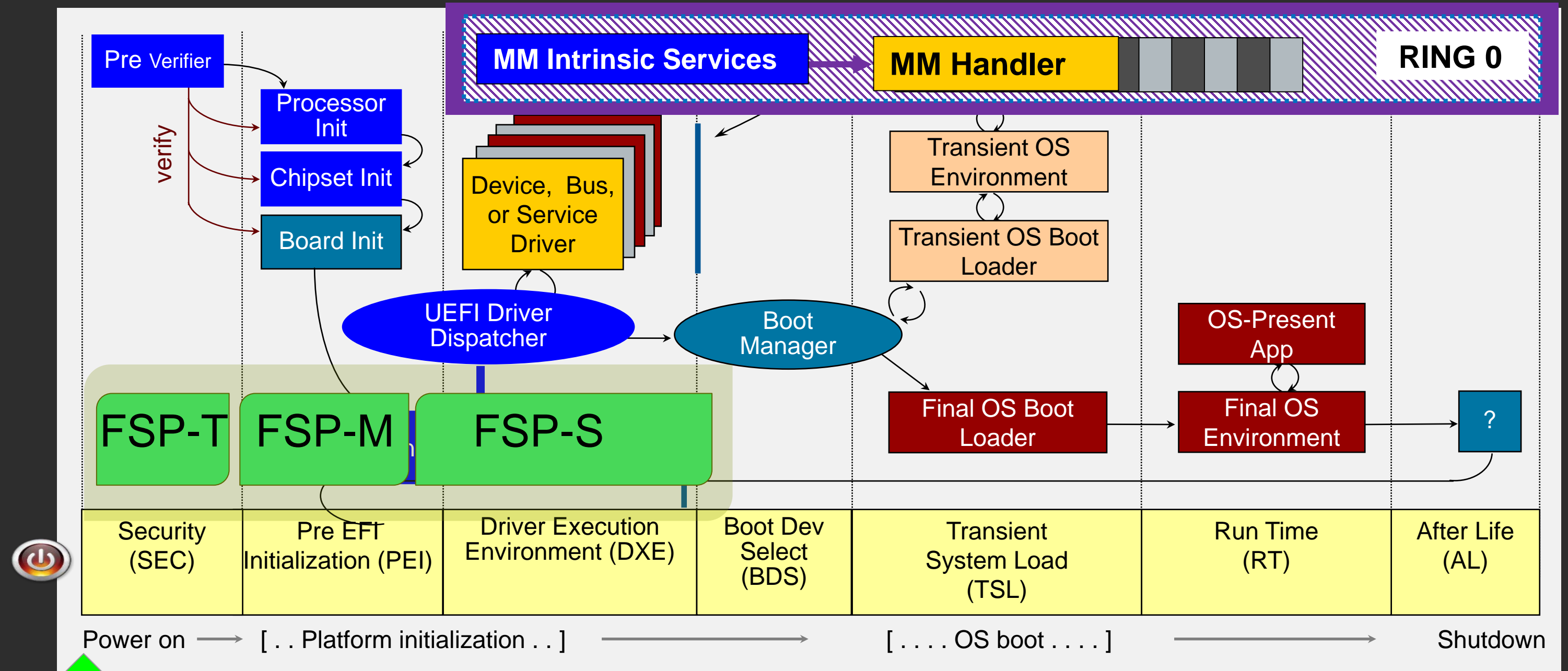
Intel® Firmware Support Package (Intel® FSP) provides low level of silicon initialization

Intel® FSP "Produced" to "Consuming" Intel® Architecture Firmware

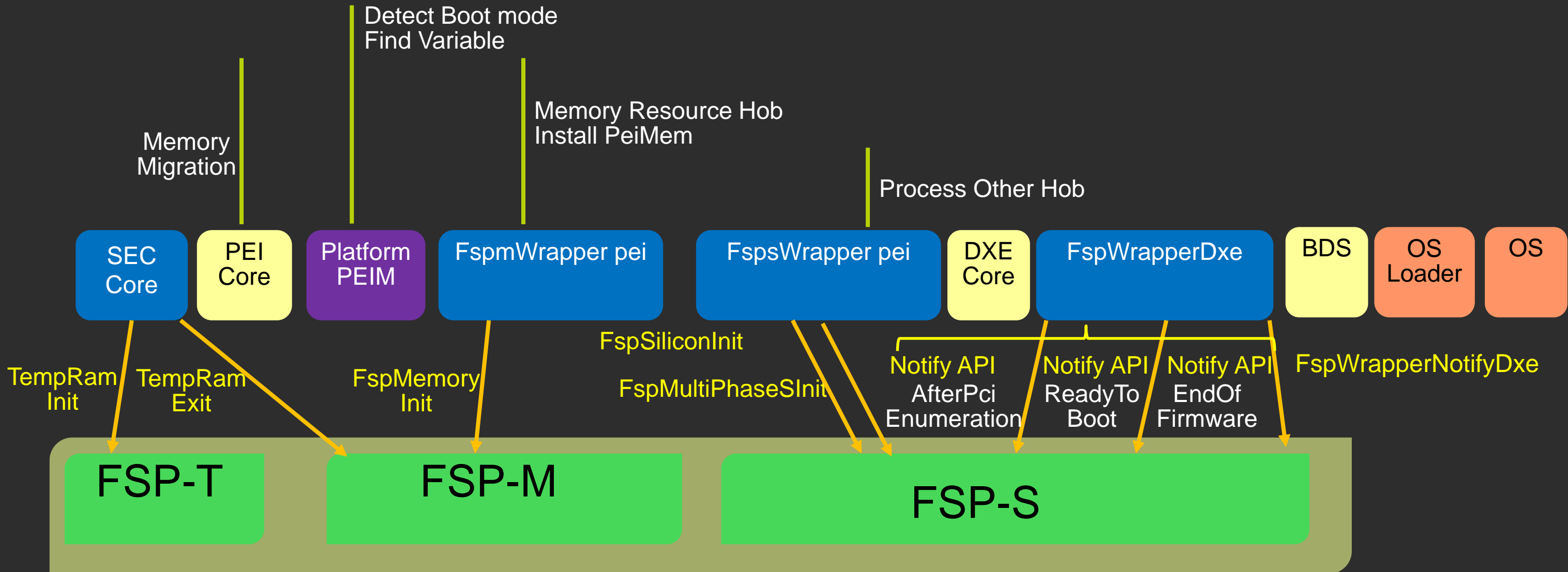


Intel FSP is independent of the bootloader solutions

UEFI – PI & EDK II BOOT FLOW – FSP

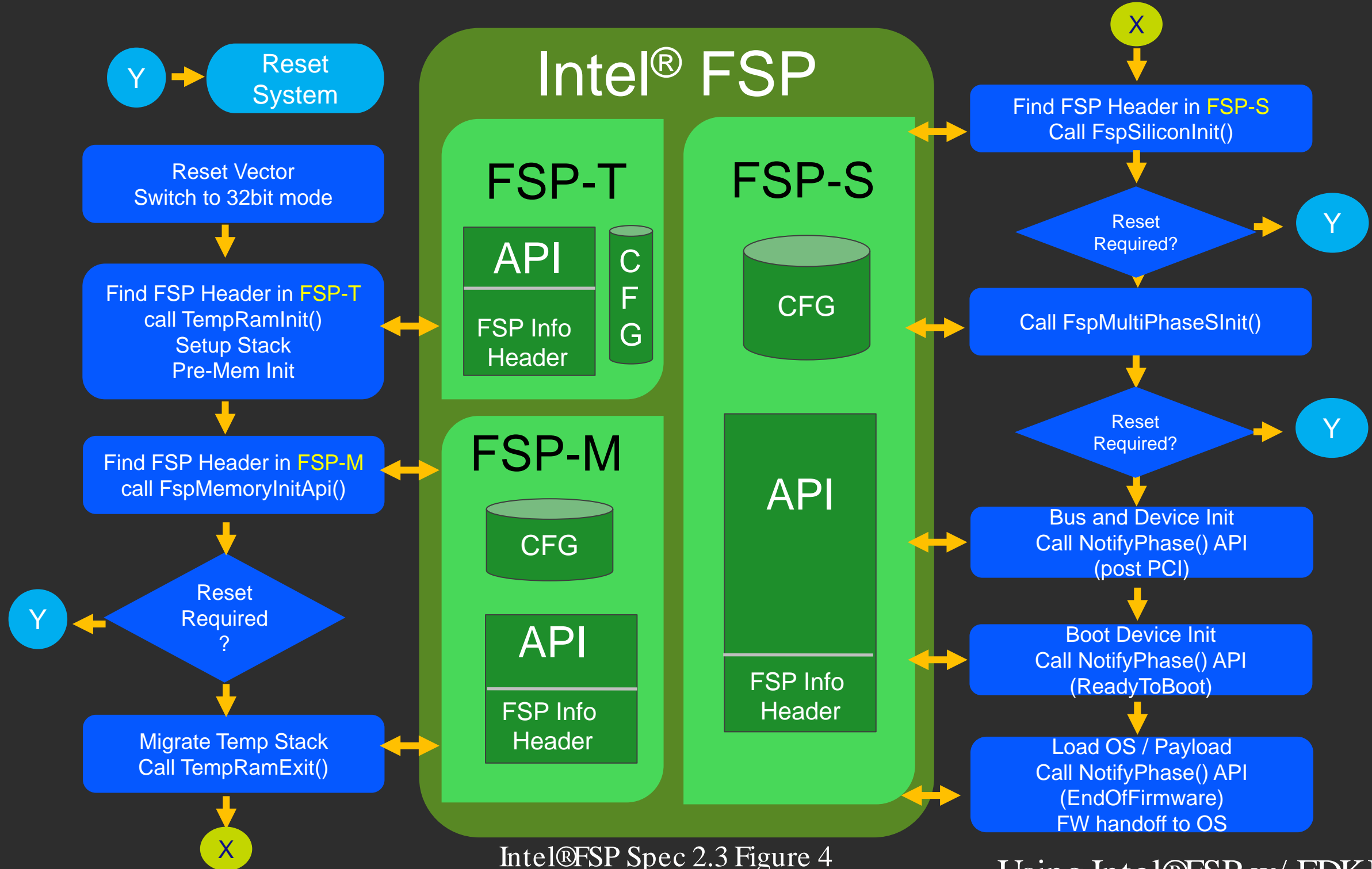


Boot Flow with UEFI & Intel® FSP



Original Source: [Using the Intel® FSP with EDK II \(2.0\)](#) Fig 4. – This now shows a 6th API added in FSP 2.2

Intel® FSP v2.3 Boot Flow



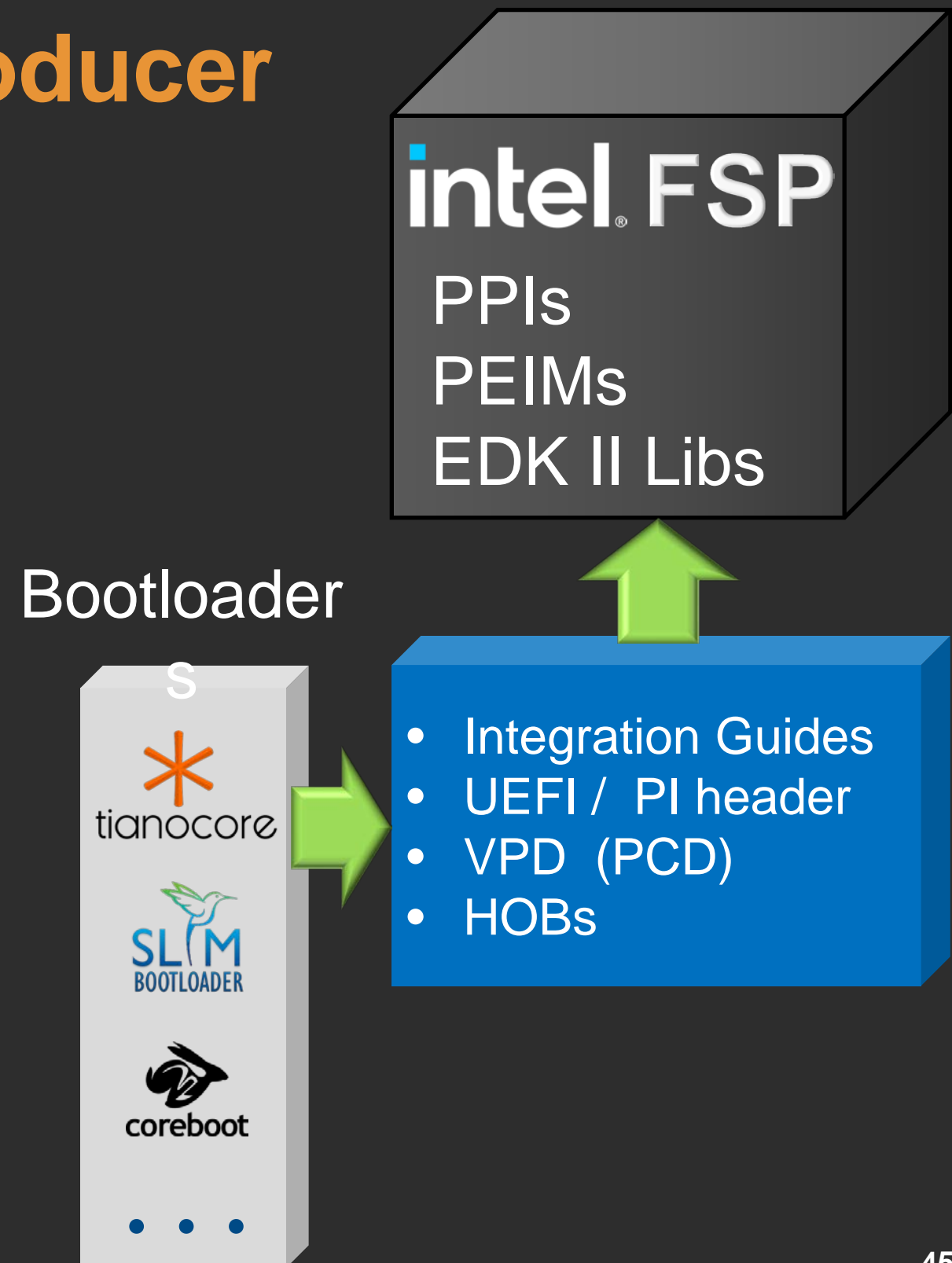
Intel® FSP Producer

- Examples of binary instances on <http://www.intel.com/fsp> w/integration guides
 - This includes hardware initialization code that is EDK II based PEI Modules (PEIM's)
- Modules are encapsulated as a UEFI PI firmware volume w/ extra header
- Configure w/Vital Product Data (VPD)-style Platform Configuration Data (PCD) externalized from the modules
- Resultant output state reported via UEFI Platform Initialization (PI) Hand Off Block (HOB)

[Intel® Firmware Support Package \(Intel® FSP\) External Architecture Specification \(EAS\) v2.3](#) [Link v2.0](#)

Resource:

<https://software.intel.com/content/www/us/en/develop/articles/intel-firmware-support-package.html>



WHAT'S NEW IN THE UEFI SPECIFICATIONS?

LATEST UEFI SPECIFICATIONS



Unified Extensible Firmware Interface Forum

[Http://uefi.org](http://uefi.org)

UEFI Specification	UEFI Shell Specification	UEFI PI Specification	Self Certification Test	PI Distro Package Specification	ACPI Specification
Current v2.9 March 2021	Current v2.2 January 2016	Current v1.7A April 2020	Current v2.7B April 2015	Current v1.1 January 2016	Current v6.4 January 2021



Added definitions for Compute Express Link (CXL)* Spec version 2.0

New ACPI entry: CXL Early Discovery Table (CEDT)

ACPI – PRM Spec

<https://uefi.org/specsandtesttools>



<https://www.computeexpresslink.org/>



Each Table must be the same version FW Test Suite For ACPI Testing

wiki.ubuntu.com/FirmwareTestSuite/

EDK II - Open Source

Community Development

- Stable Tag Releases- cycle of releasing stable versions of EDK II Firmware
- Adding UEFI Spec updates and new key features and bug fixes
- Three phases of development
 - Development phase
 - Soft Feature Freeze
 - Hard Feature Freeze

More Information on Stable Tag Releases:
[TianoCore Wiki](https://www.tianocore.org/wiki/)



Tag: edk2-stable202202 Features:
[edk2 releases Stable tag](#)

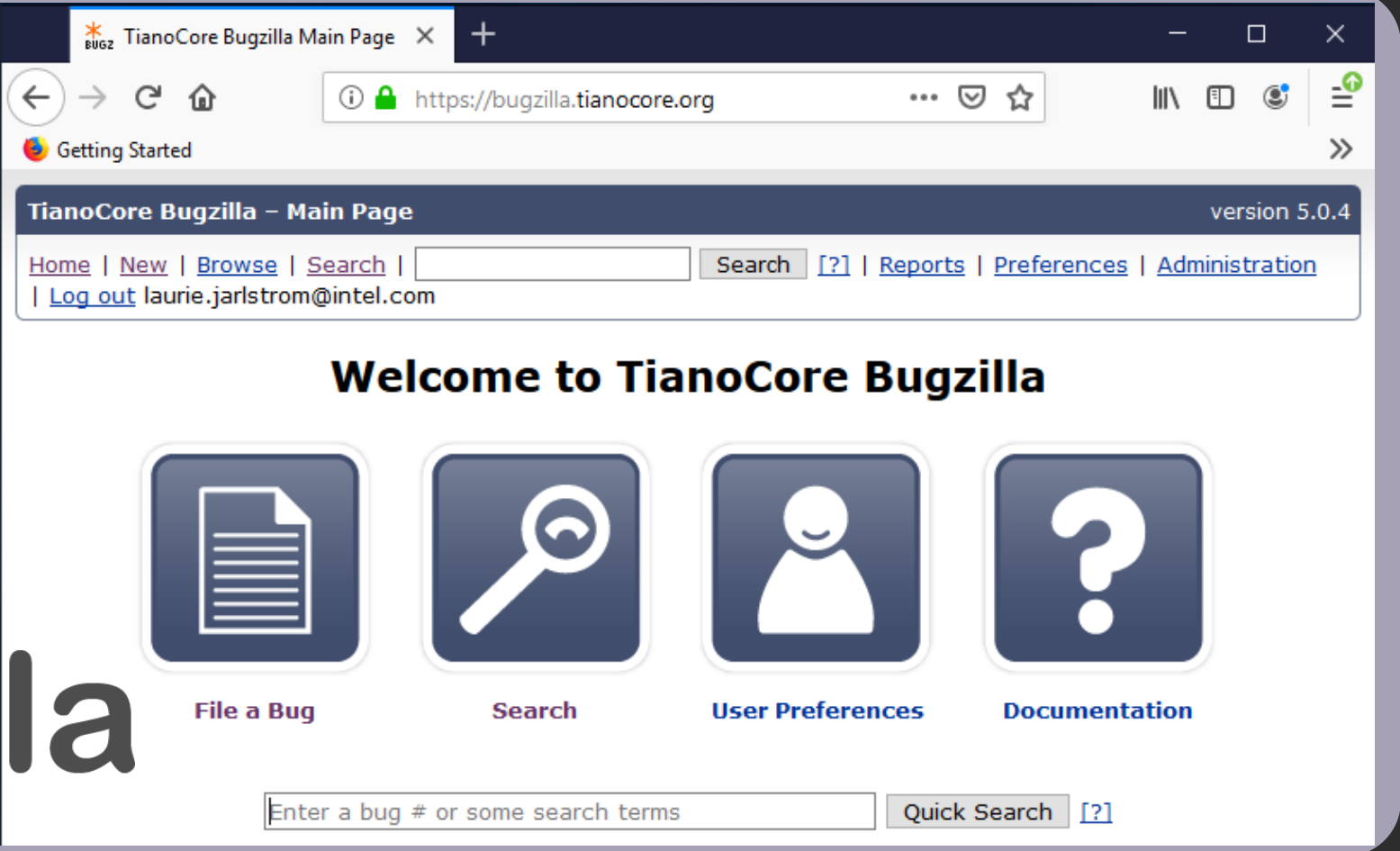
Report a bug on Bugzilla



Create a user account <https://bugzilla.tianocore.org/>

Search if bug “already” reported

File New Report – Pick a product – fill out form for the bug



The screenshot shows the Tianocore Bugzilla Main Page in a web browser. The browser's address bar displays <https://bugzilla.tianocore.org>. The page title is "TianoCore Bugzilla - Main Page" with a version number of 5.0.4. The navigation bar includes links for Home, New, Browse, Search, Reports, Preferences, Administration, and a Log out button for the user laurie.jarlstrom@intel.com. The main content area features a "Welcome to TianoCore Bugzilla" message and four large icons: "File a Bug" (document icon), "Search" (magnifying glass icon), "User Preferences" (person icon), and "Documentation" (question mark icon). At the bottom, there is a search bar with the placeholder text "Enter a bug # or some search terms" and a "Quick Search" button.



Bugzilla

Summary

- ★ The System Firmware is a binary image that starts execution as the reset vector & is typically a SPI device
- ★ UEFI & PI Boot Flow Process, SEC, PEI, DXE, BDS, TSL, OS
- ★ System Management Mode is in Ring 0 in the System FW
- ★ Intel® FSP will initialize the processor, chipset and memory
- ★ The UEFI.org & Tianocore.org for Specs and Open source

Questions?



Return to Main Training Page



Return to Training Table of contents for next presentation [link](#)



ACKNOWLEDGEMENTS

Redistribution and use in source (original document form) and 'compiled' forms (converted to PDF, epub, HTML and other formats) with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code (original document form) must retain the above copyright notice, this list of conditions and the following disclaimer as the first lines of this file unmodified.

Redistributions in compiled form (transformed to other DTDs, converted to PDF, epub, HTML and other formats) must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS DOCUMENTATION IS PROVIDED BY TIANOCORE PROJECT "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL TIANOCORE PROJECT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS DOCUMENTATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2021-2022, Intel Corporation. All rights reserved.