tianocore

UEFI & EDK II Training

UEFI AND PLATFORM INITIALIZATION (PI) BOOT FLOW & OVERVIEW

tianocore.org

LESSON OBJECTIVE

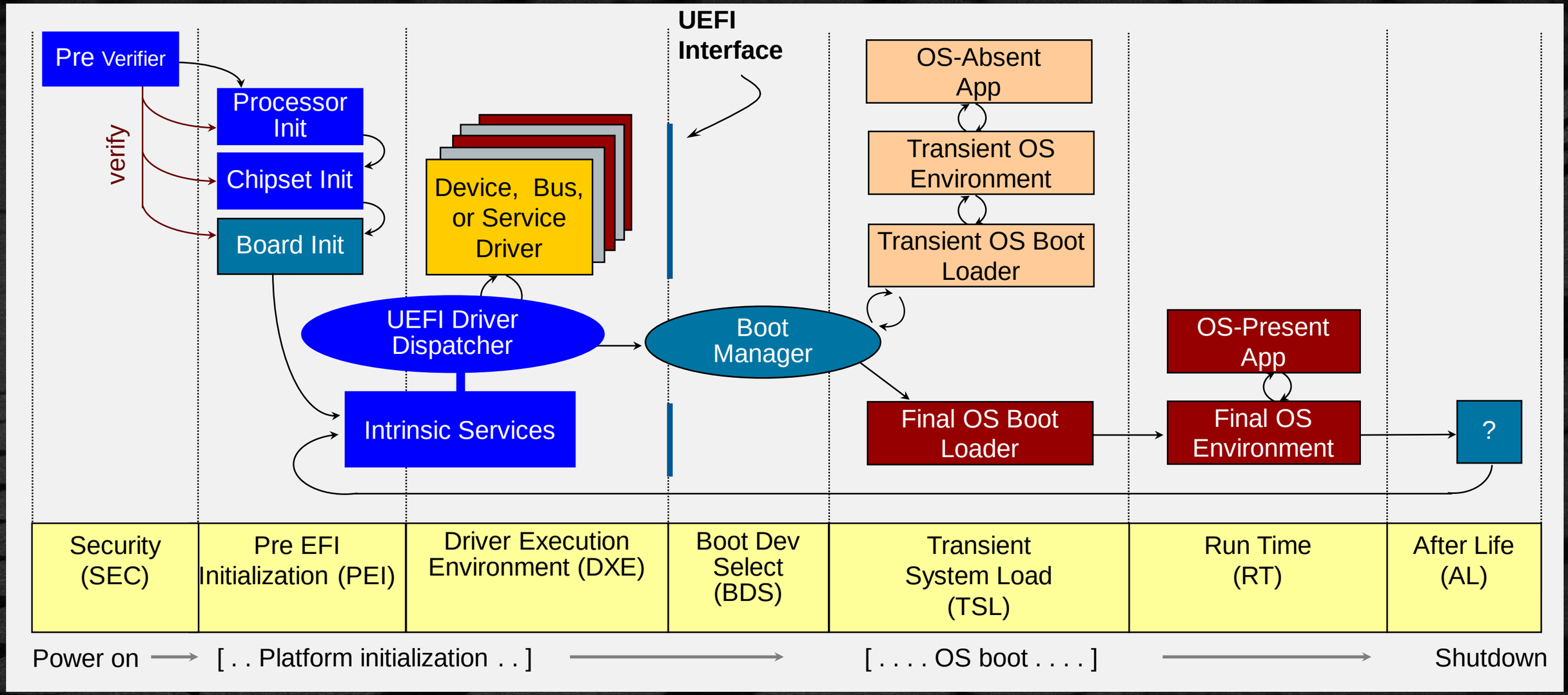
- Review PI and UEFI Boot Process
- Answer web-based training related questions
- Answer: Where does Intel® FSP Fit?
- What's new in UEFI.org

tianocore

UEFI BOOT EXECUTION FLOW

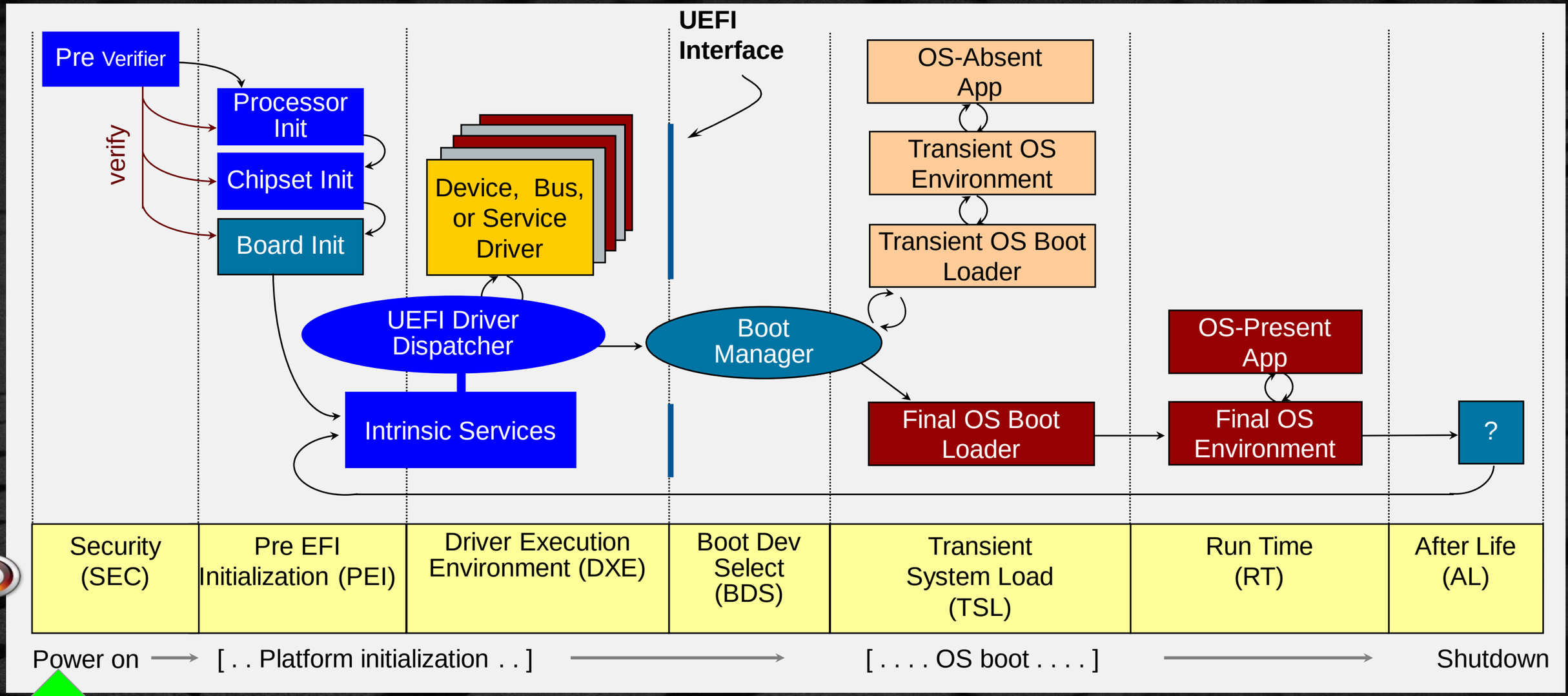
Starting at the processor reset vector

UEFI – PI & EDK II BOOT FLOW

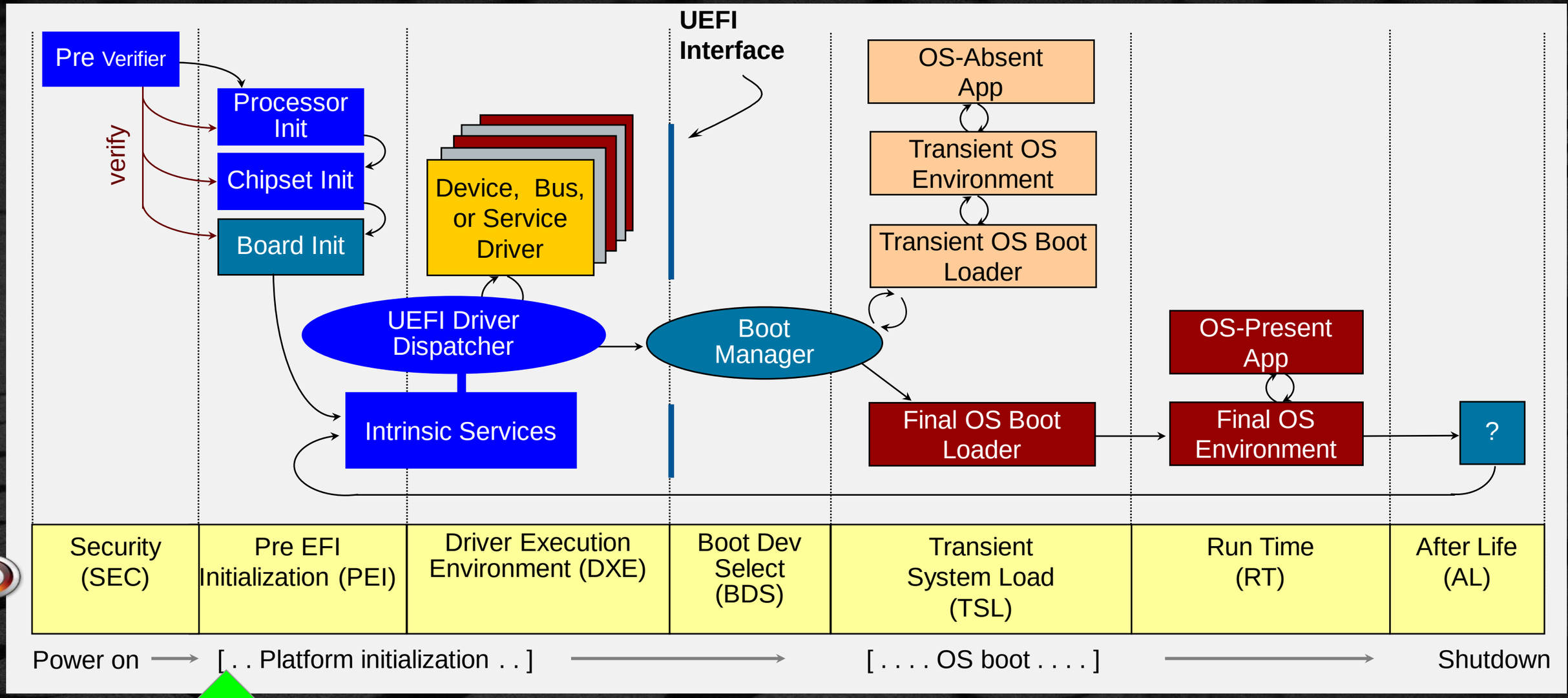


The folloiwng Slides show UEFI and Platform Initialziation (PI) Boot Execution Flow

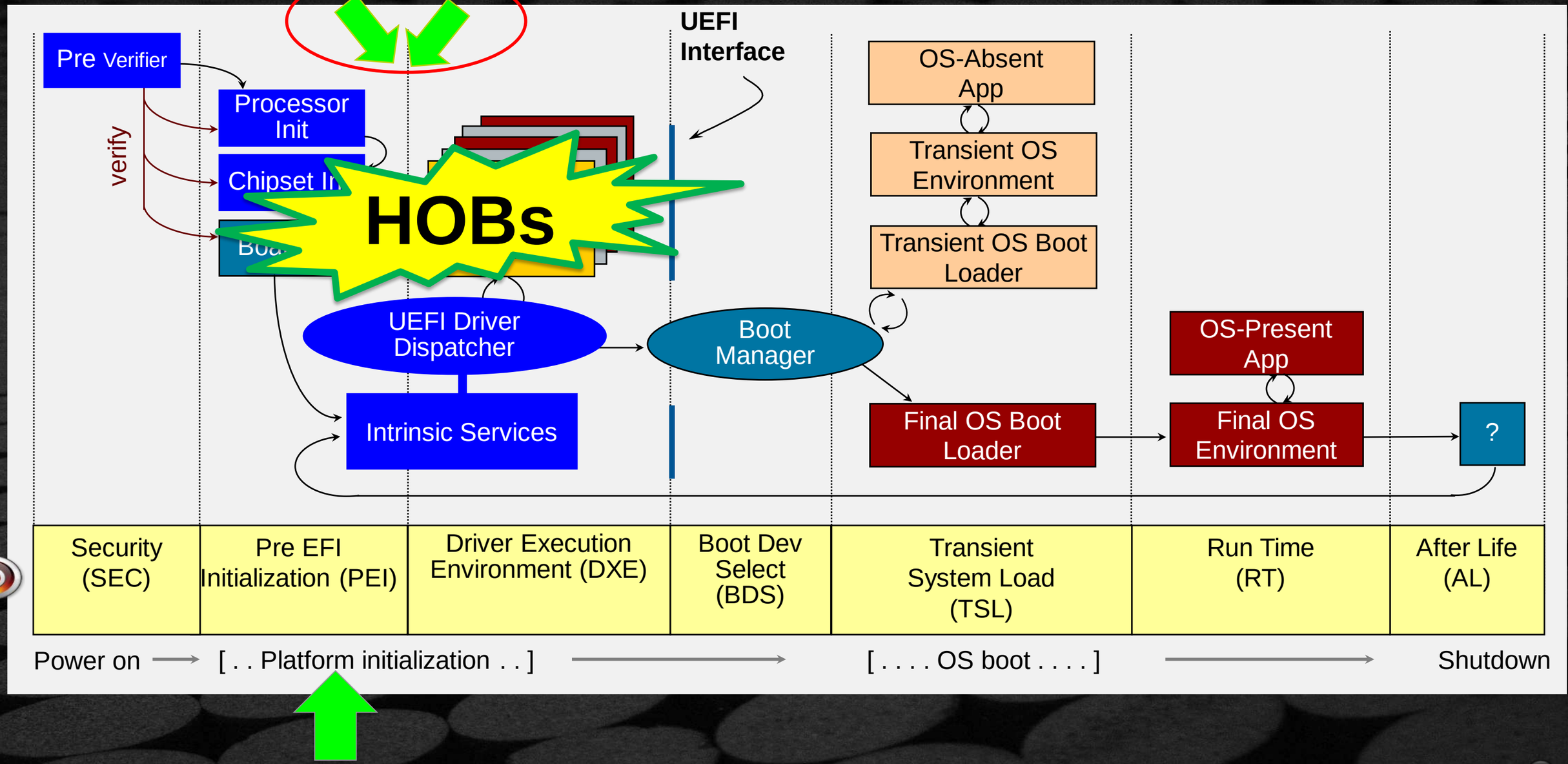
UEFI – PI & EDK II BOOT FLOW - SEC



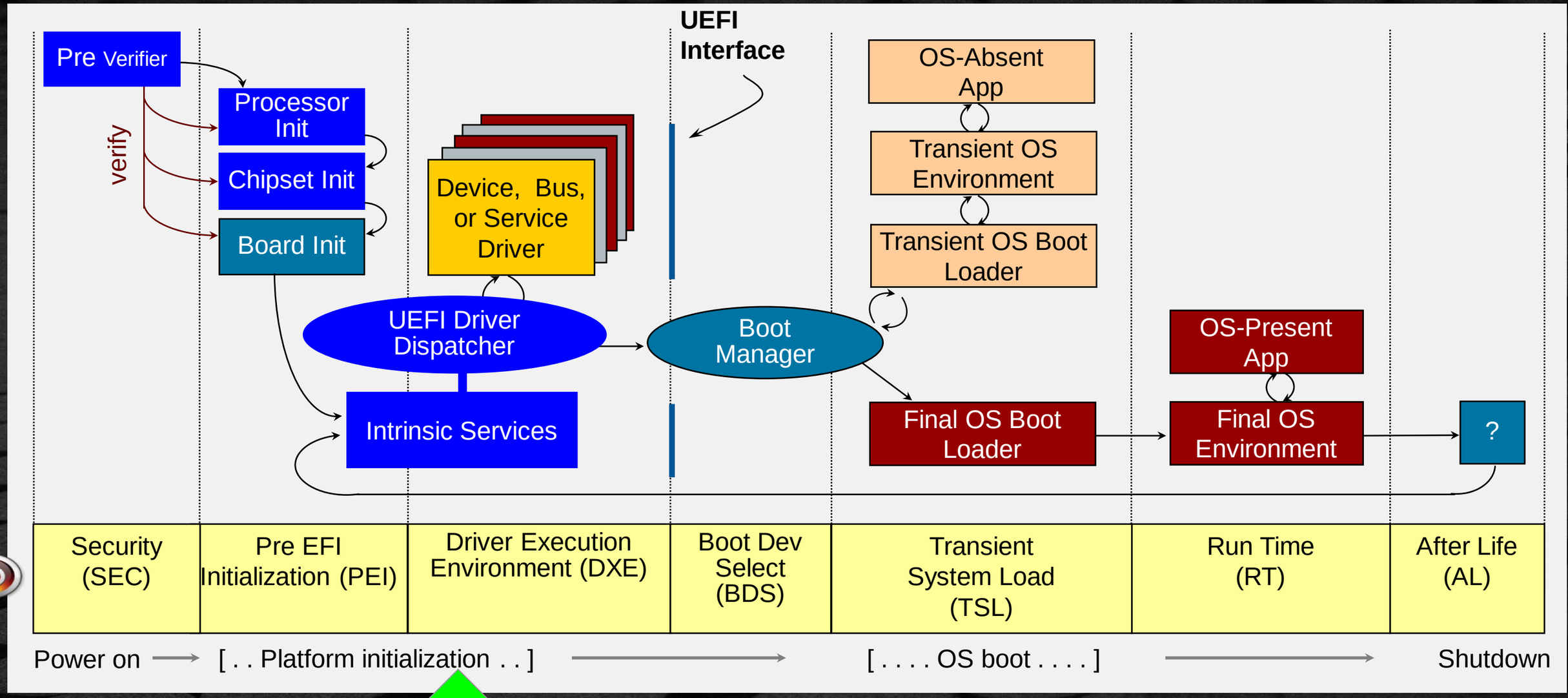
UEFI – PI & EDK II BOOT FLOW - PEI



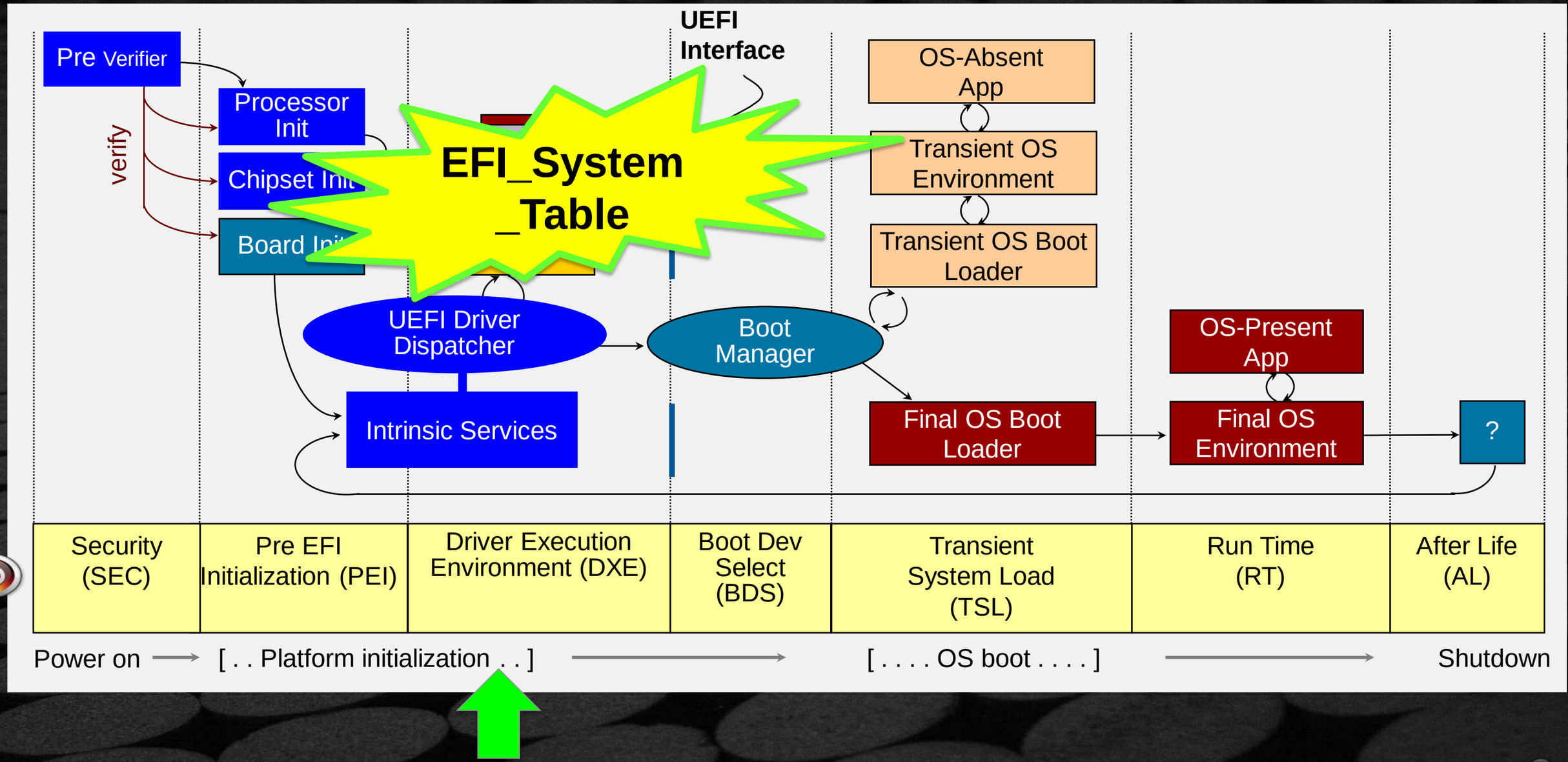
UEFI – PI & EDK II BOOT FLOW - DXEIPL



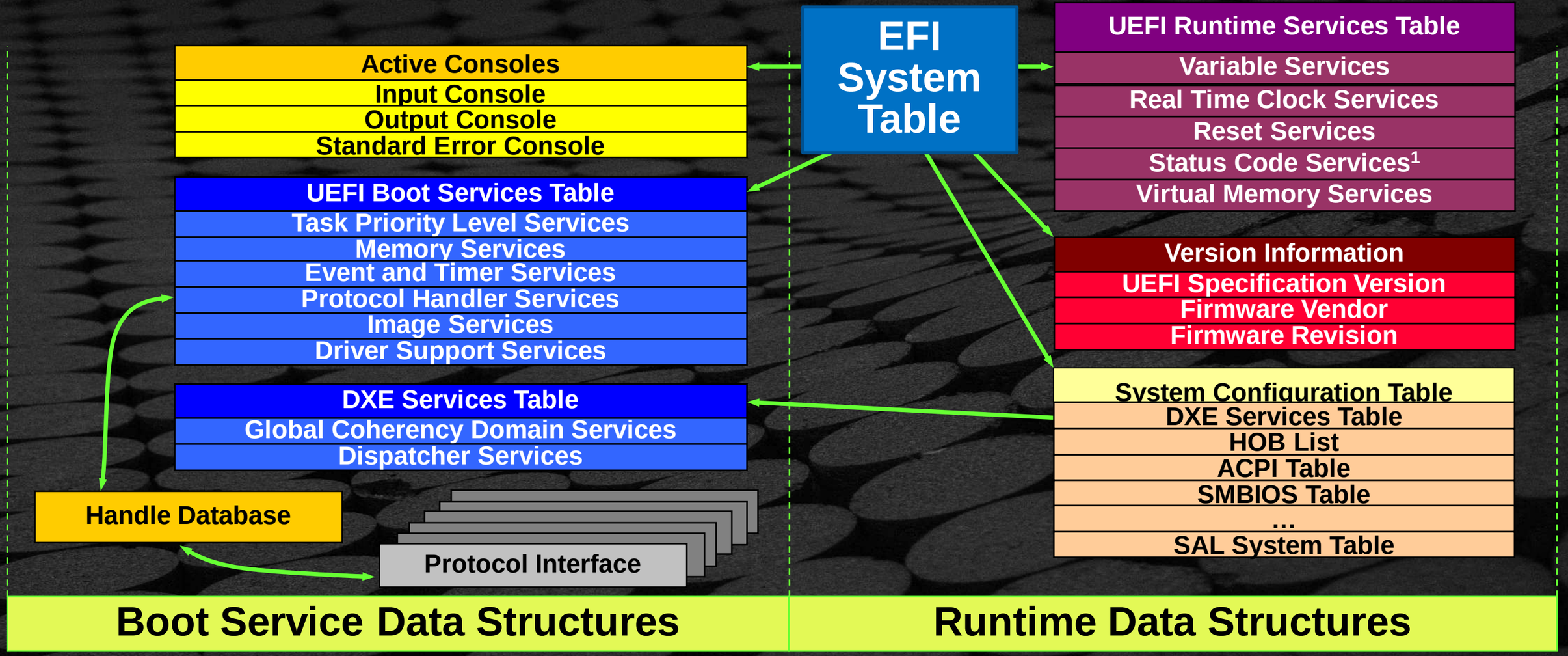
UEFI – PI & EDK II BOOT FLOW – DXE



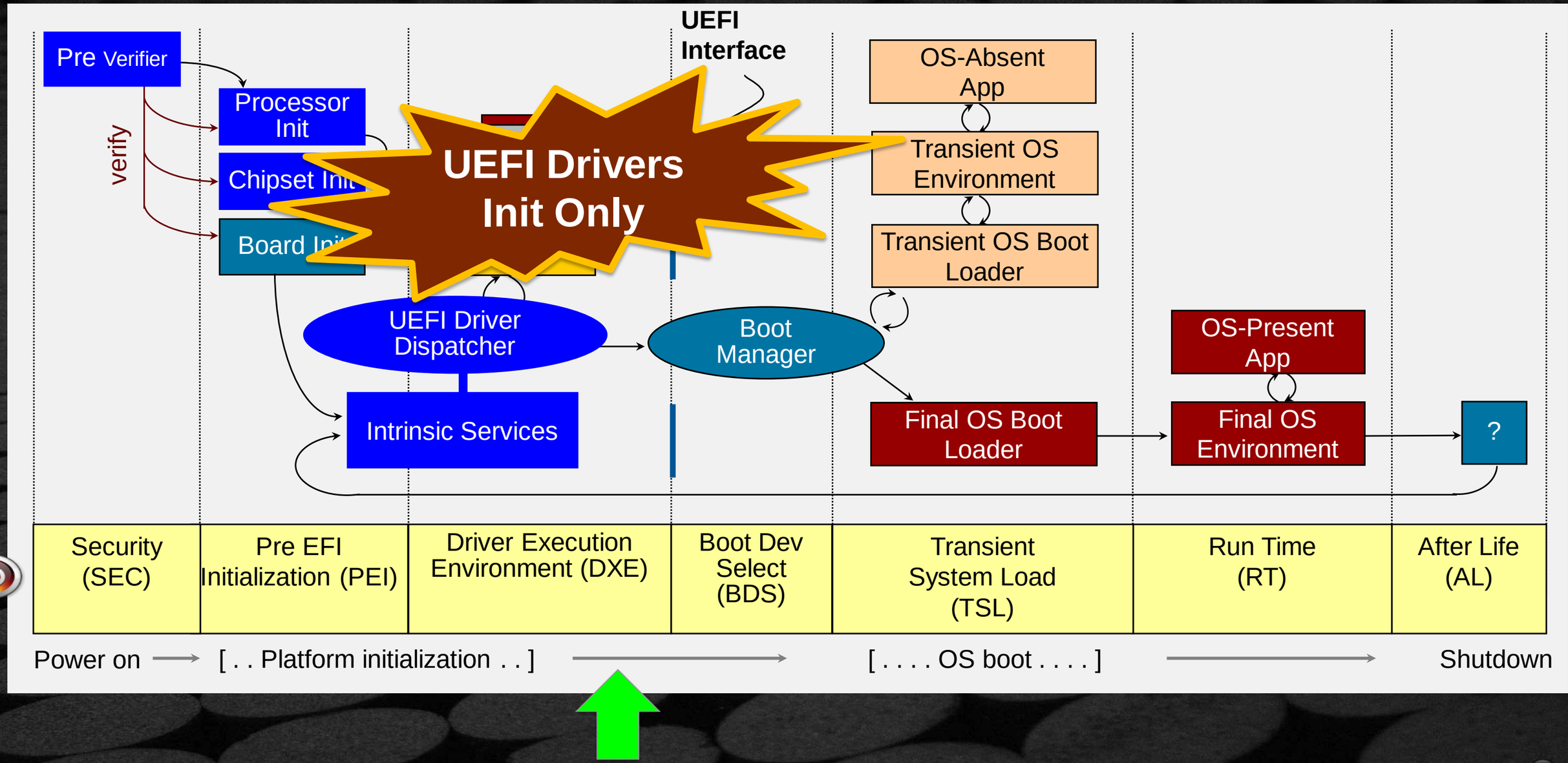
UEFI – PI & EDK II BOOT FLOW – DXE



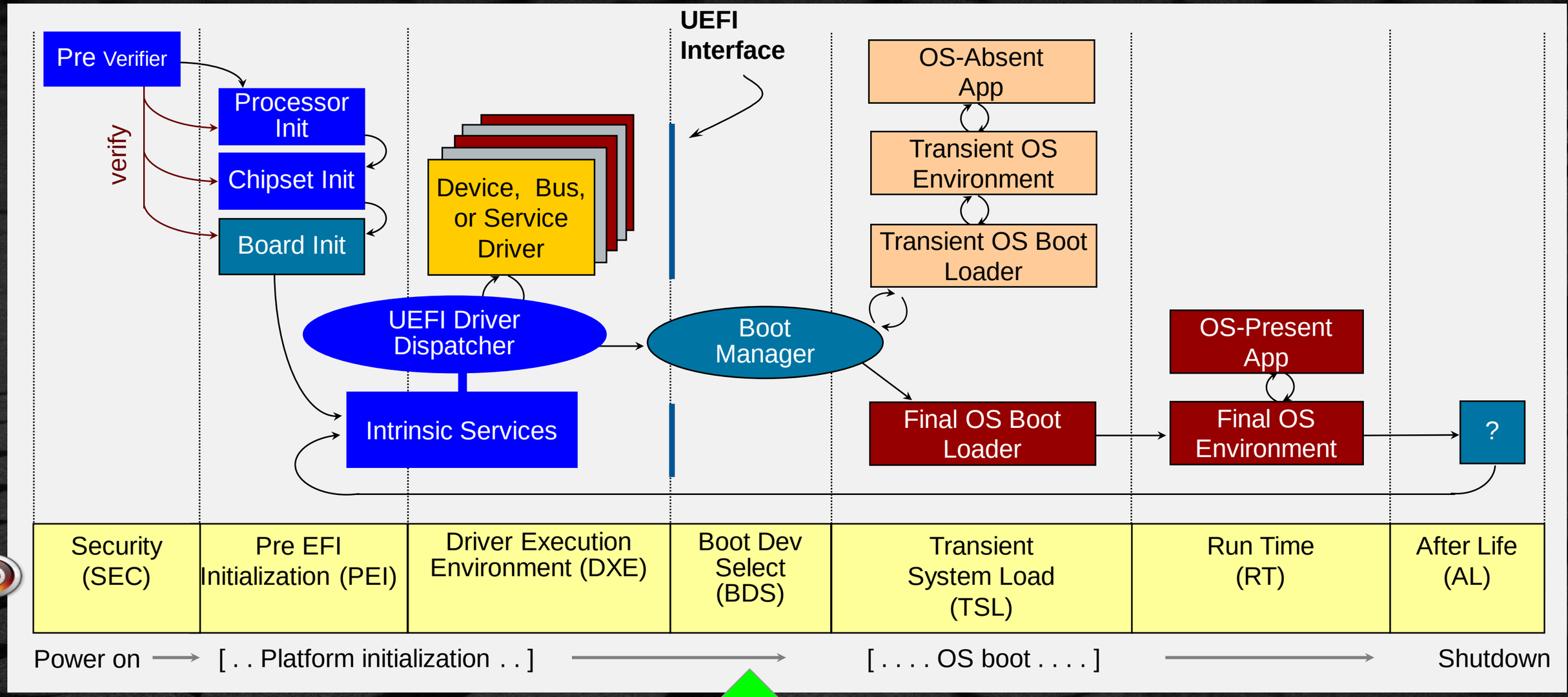
UEFI SYSTEM TABLE



UEFI – PI & EDK II BOOT FLOW – DXE UEFI



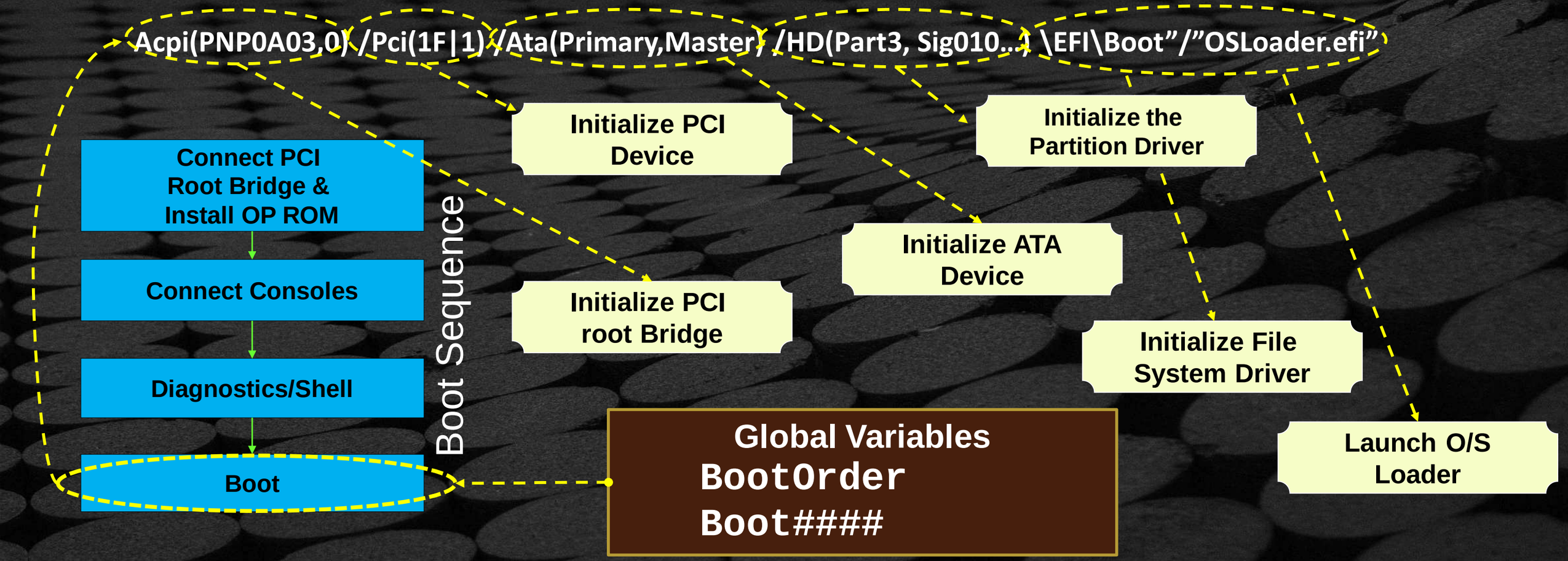
UEFI – PI & EDK II BOOT FLOW – BDS



UEFI DEVICE PATH AND GLOBAL VARIABLES

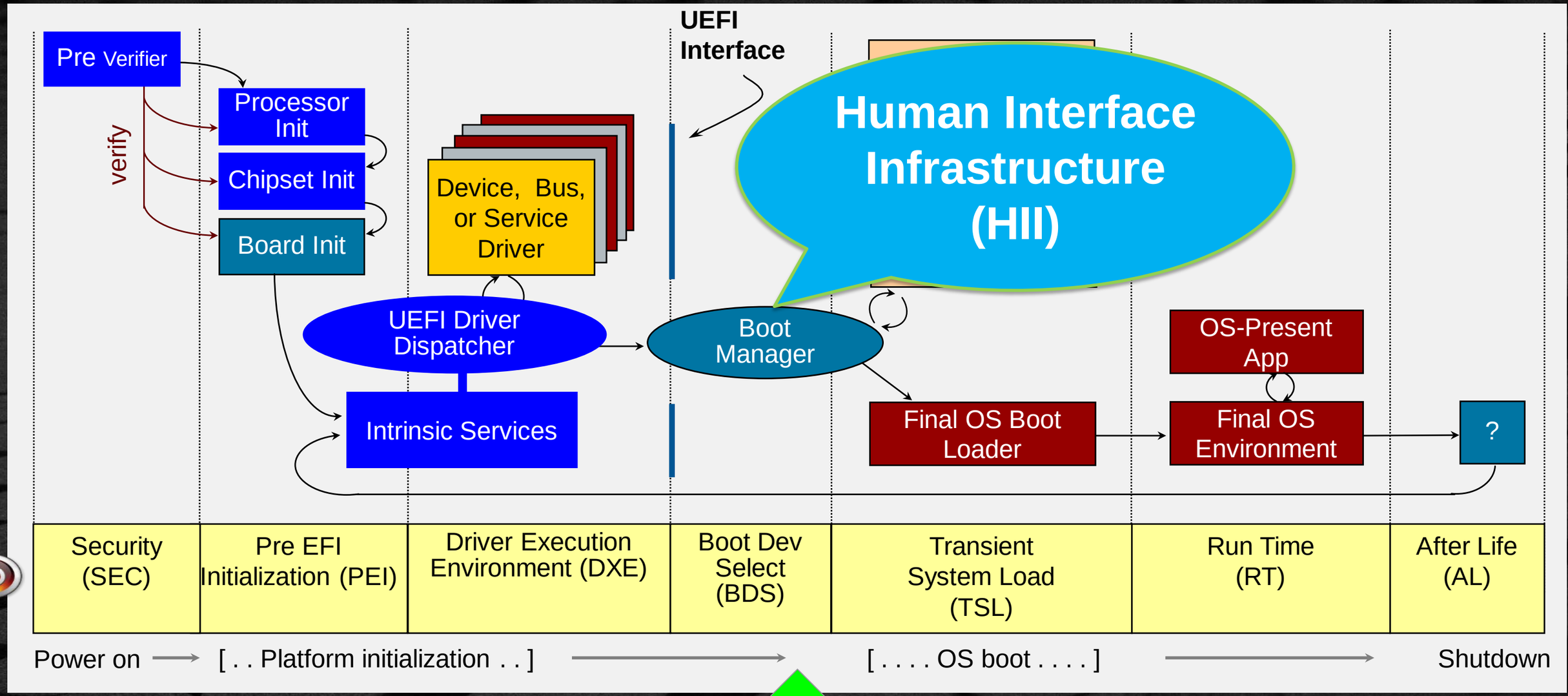
The UEFI Device Path describes a boot target

- Binary description of the physical location of a specific target

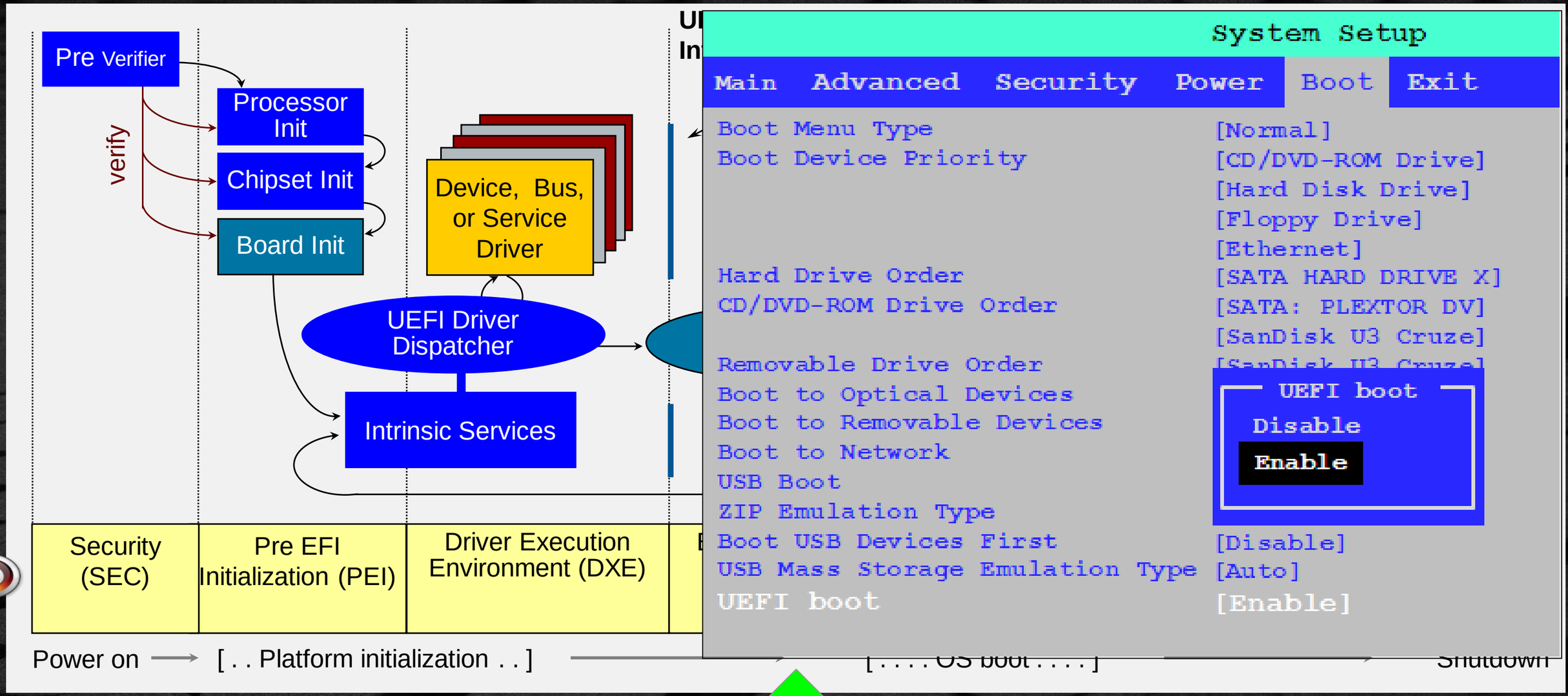


DEMO Dmpstore -

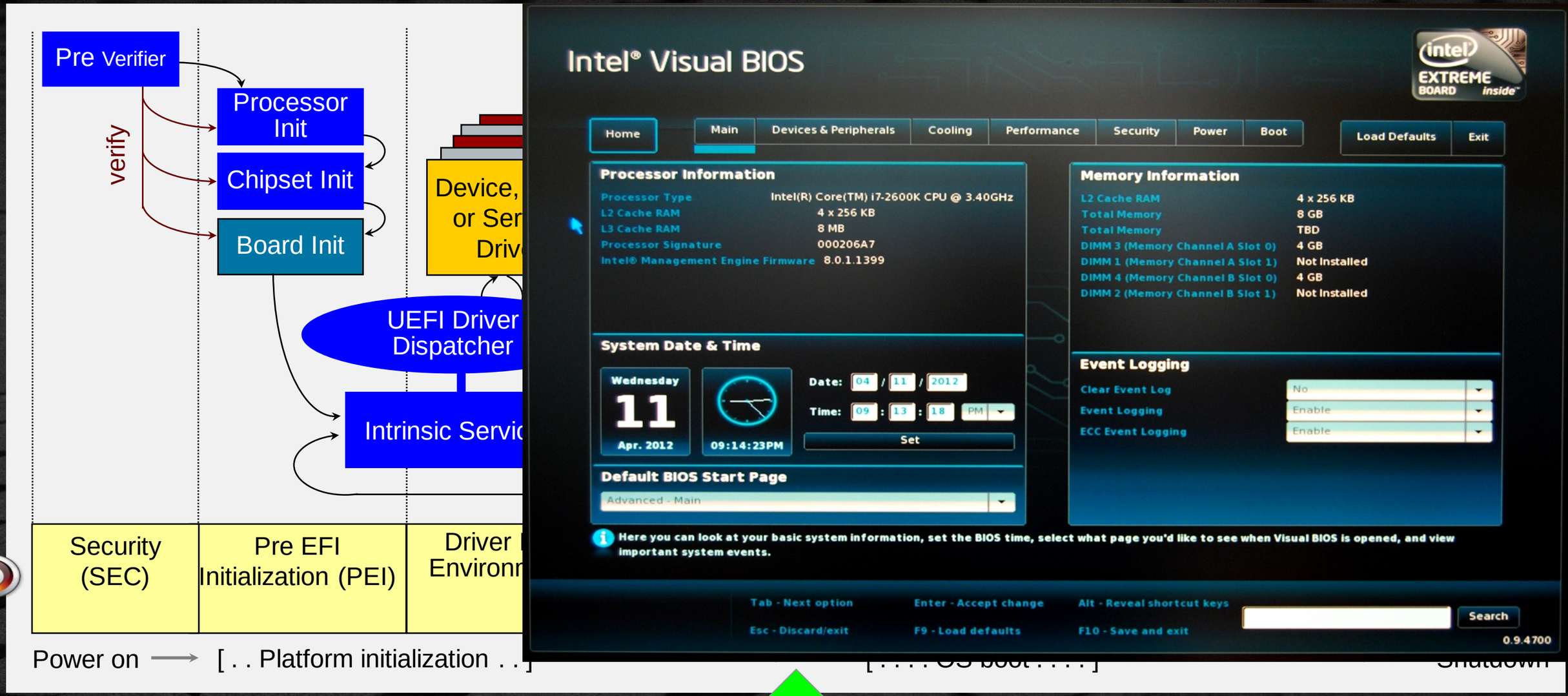
UEFI – PI & EDK II BOOT FLOW – HII



UEFI – PI & EDK II BOOT FLOW – HII

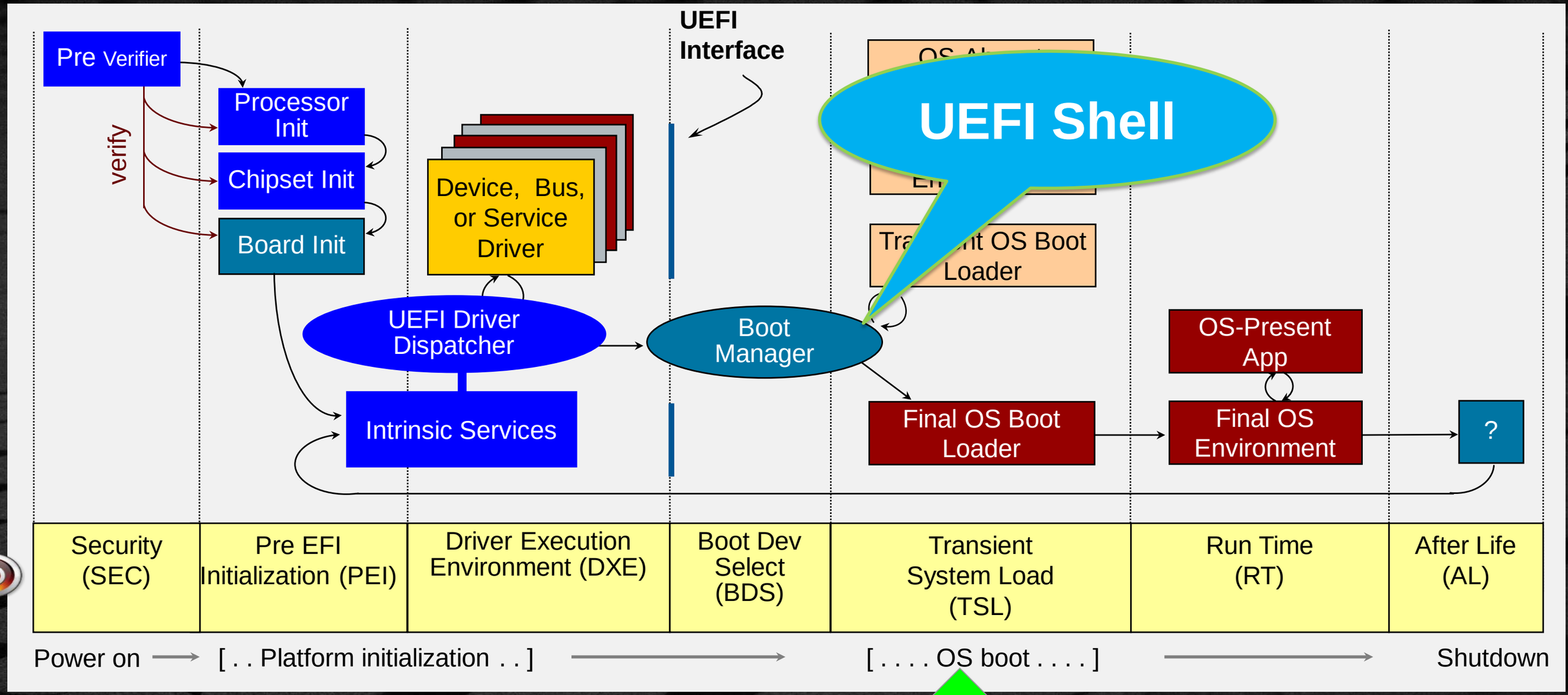


UEFI – PI & EDK II BOOT FLOW – HII

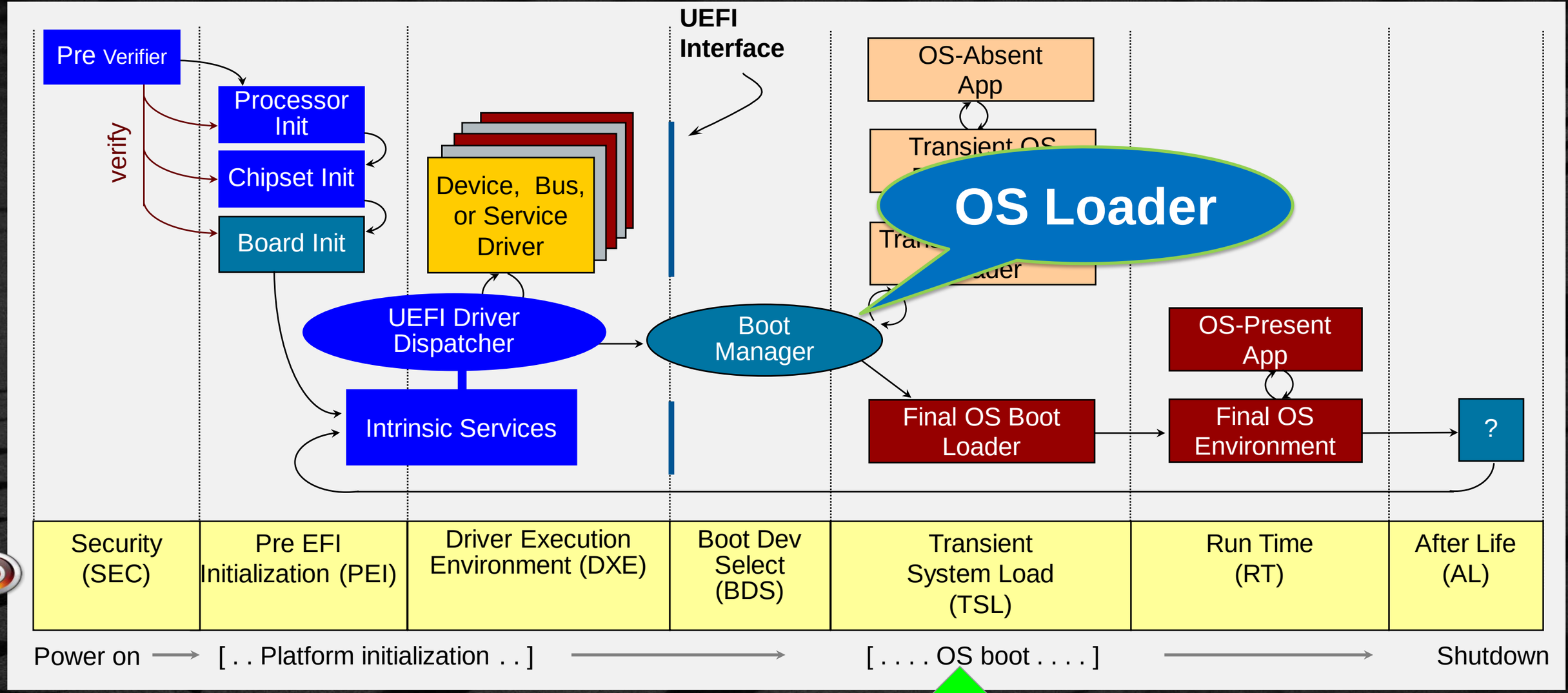


DEMO BlankDrv

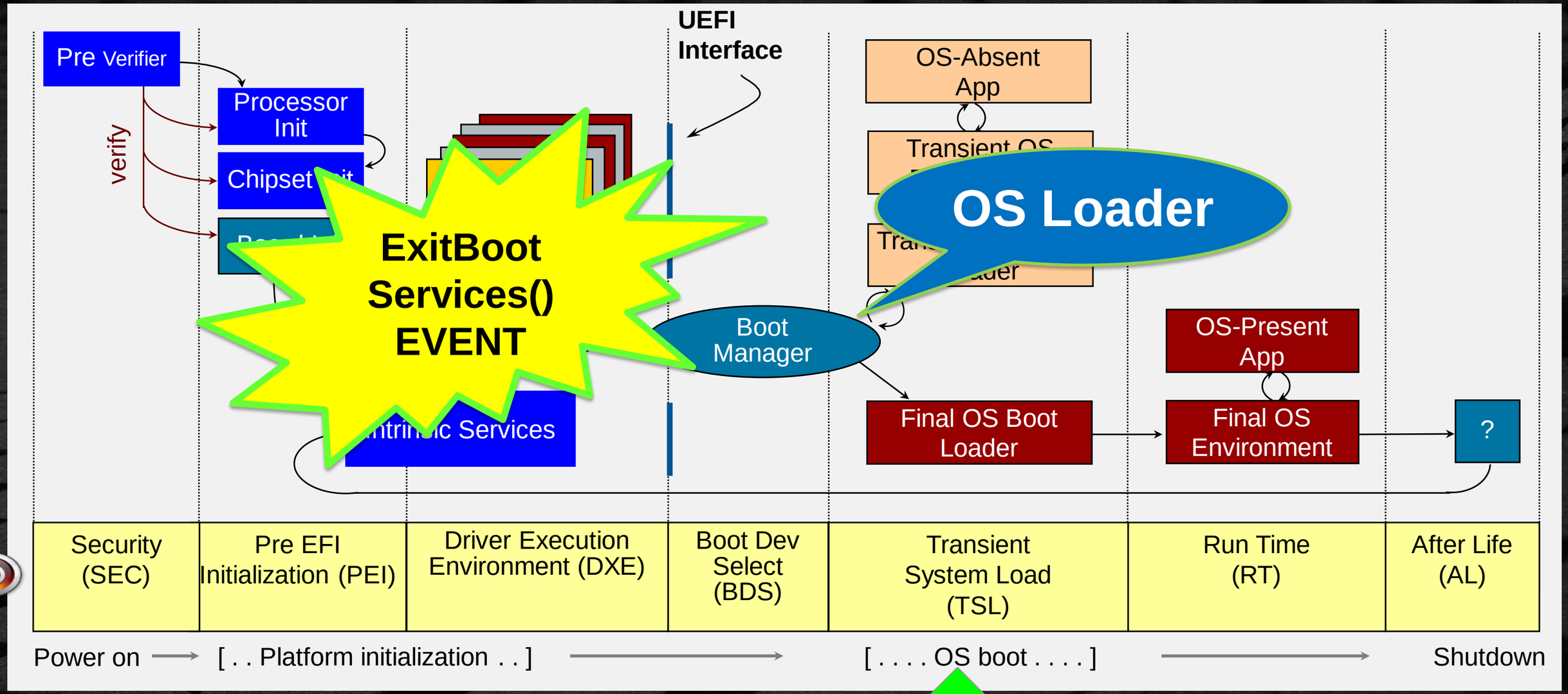
UEFI – PI & EDK II BOOT FLOW – TSL



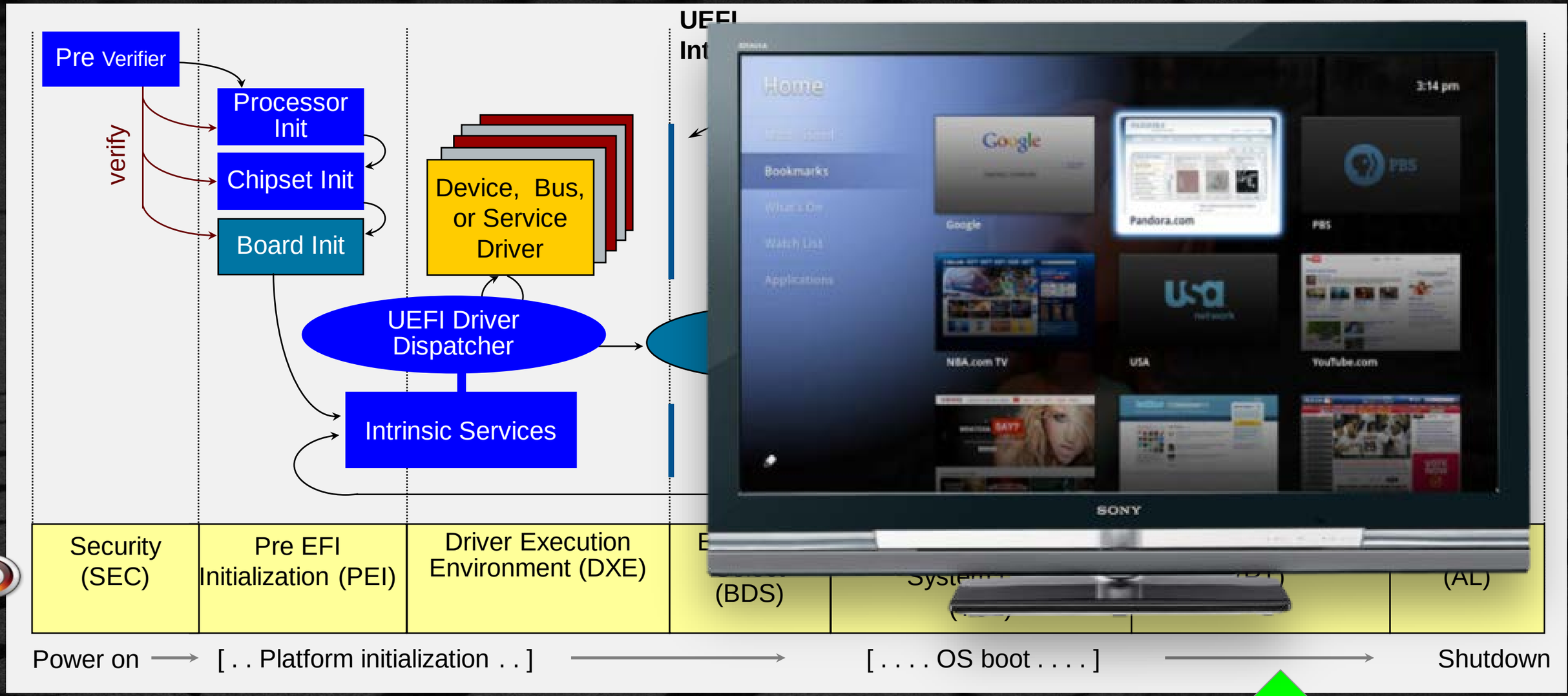
UEFI – PI & EDK II BOOT FLOW – BOOT LOADER



UEFI - PI & EDK II BOOT FLOW - EVENT

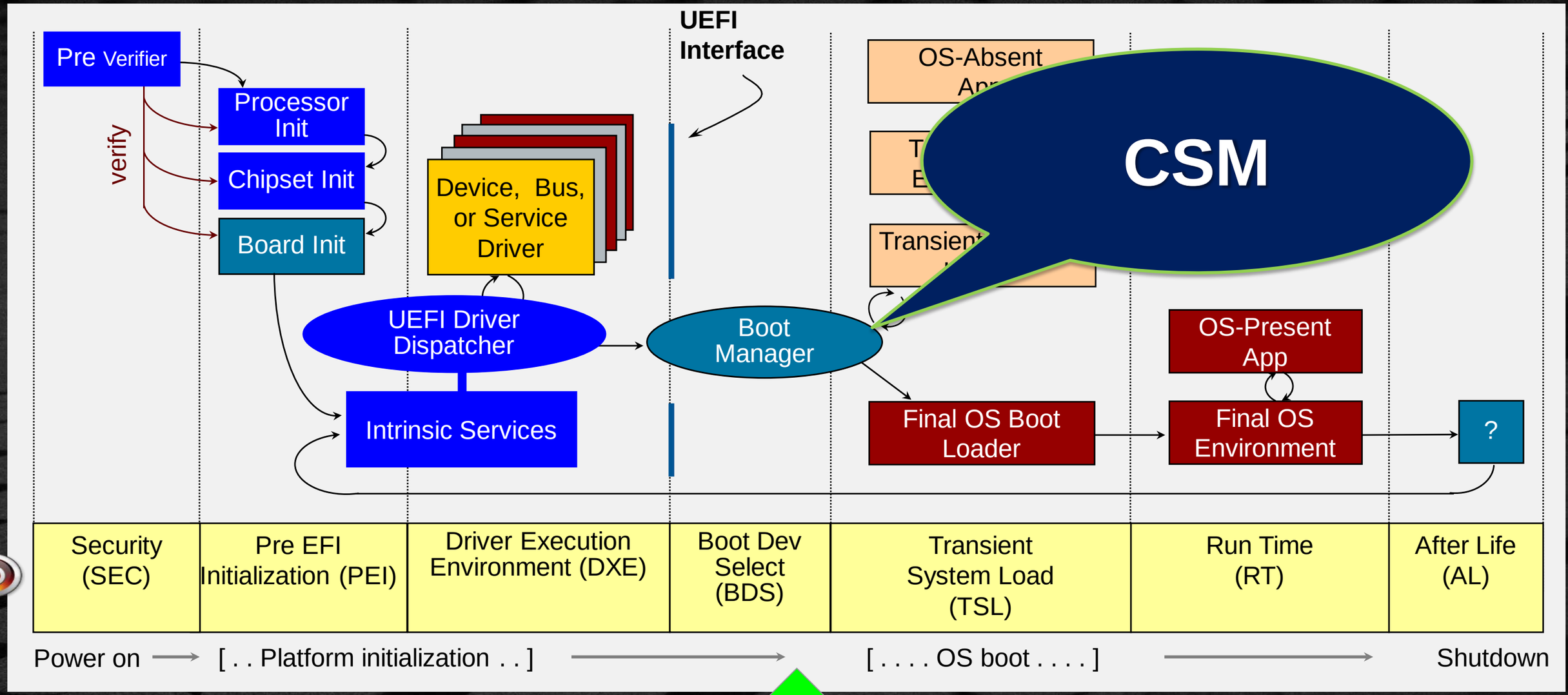


UEFI - PI & EDK II BOOT FLOW - BOOT UEFI OS



tianocore

UEFI - PI & EDK II BOOT FLOW - BOOT LEGACY



UEFI - PI & EDK II BOOT FLOW - BOOT LEGACY

THE INTEL® FIRMWARE SUPPORT PACKAGE (INTEL® FSP)

INTEL® FSP - COMPONENTS

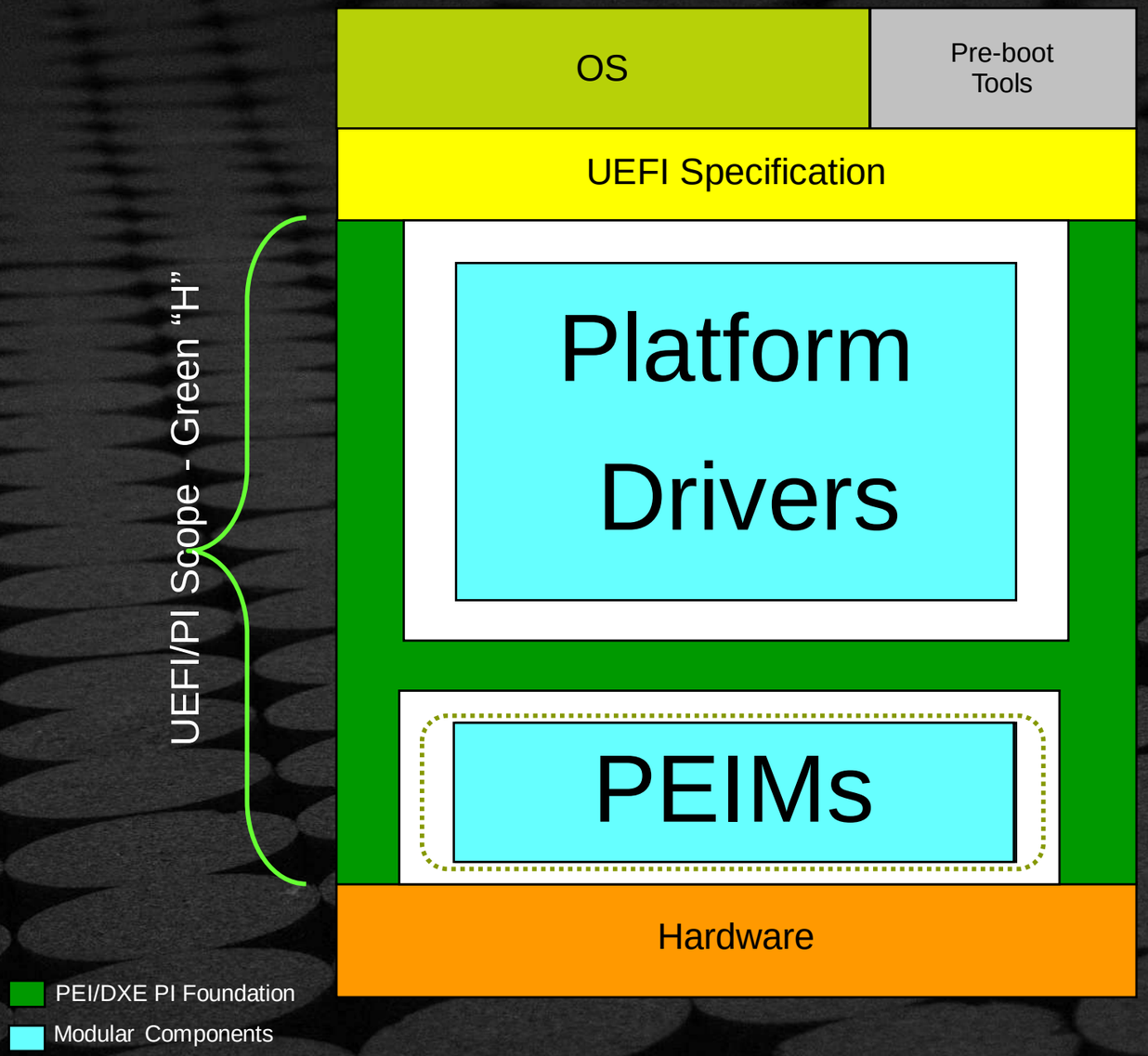
- CPU, memory controller, and chipset initialization functions as a binary package
- Provides silicon initialization ingredients
- Plugs into existing firmware frameworks
- Integration guide, includes API documentation

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

See: About Intel FSP

White Paper Example: Open Braswell - Design and Porting Guide

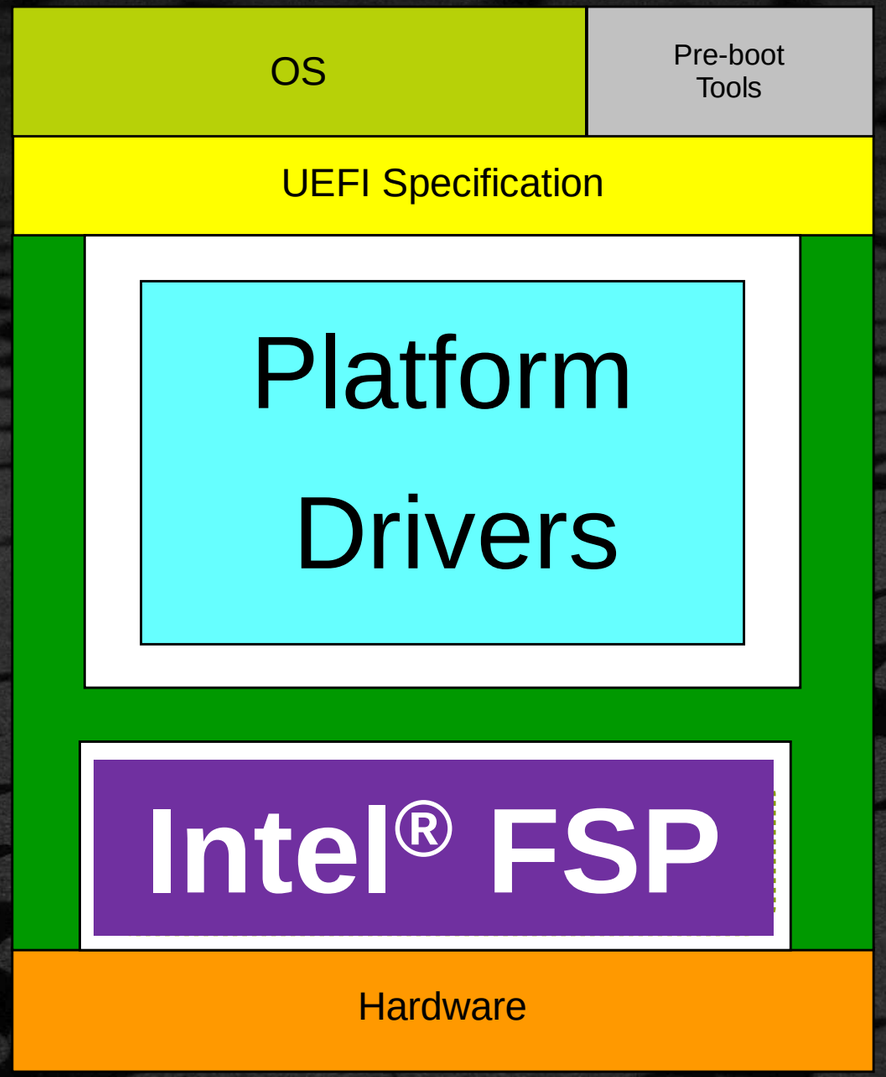
INTEL® FSP TO OPEN SOURCE EDK II



EDK II provides the framework ("Green H")

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

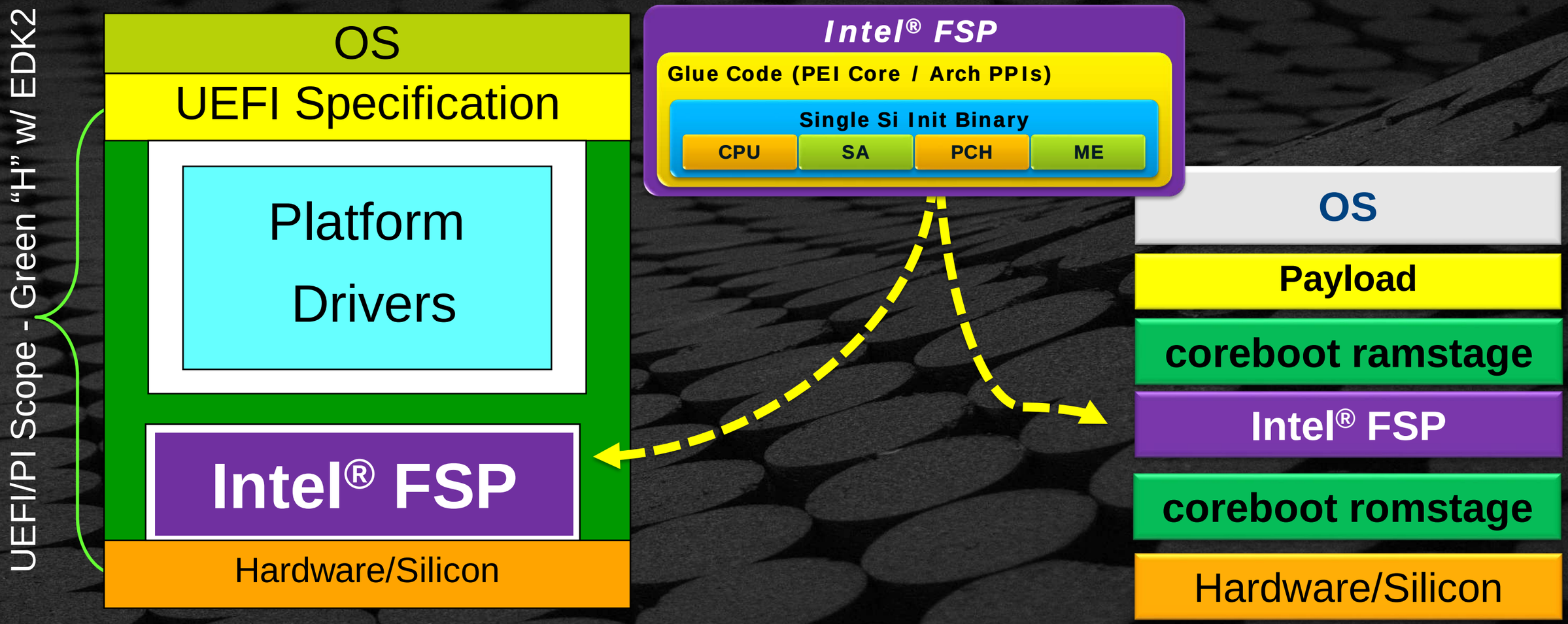
INTEL® FSP TO OPEN SOURCE EDK II



EDK II provides the framework ("Green H")

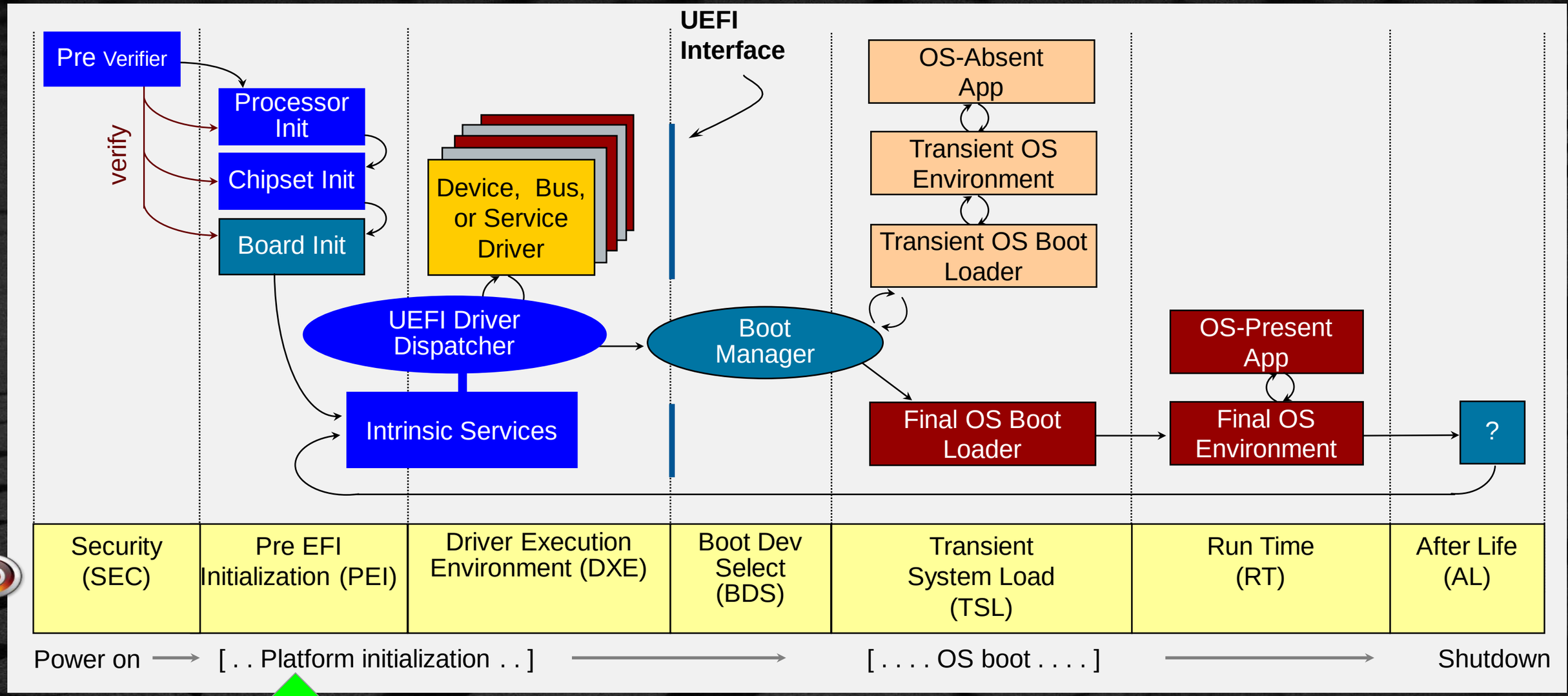
Intel® Firmware Support Package (Intel® FSP) provides low level of silicon initialization

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

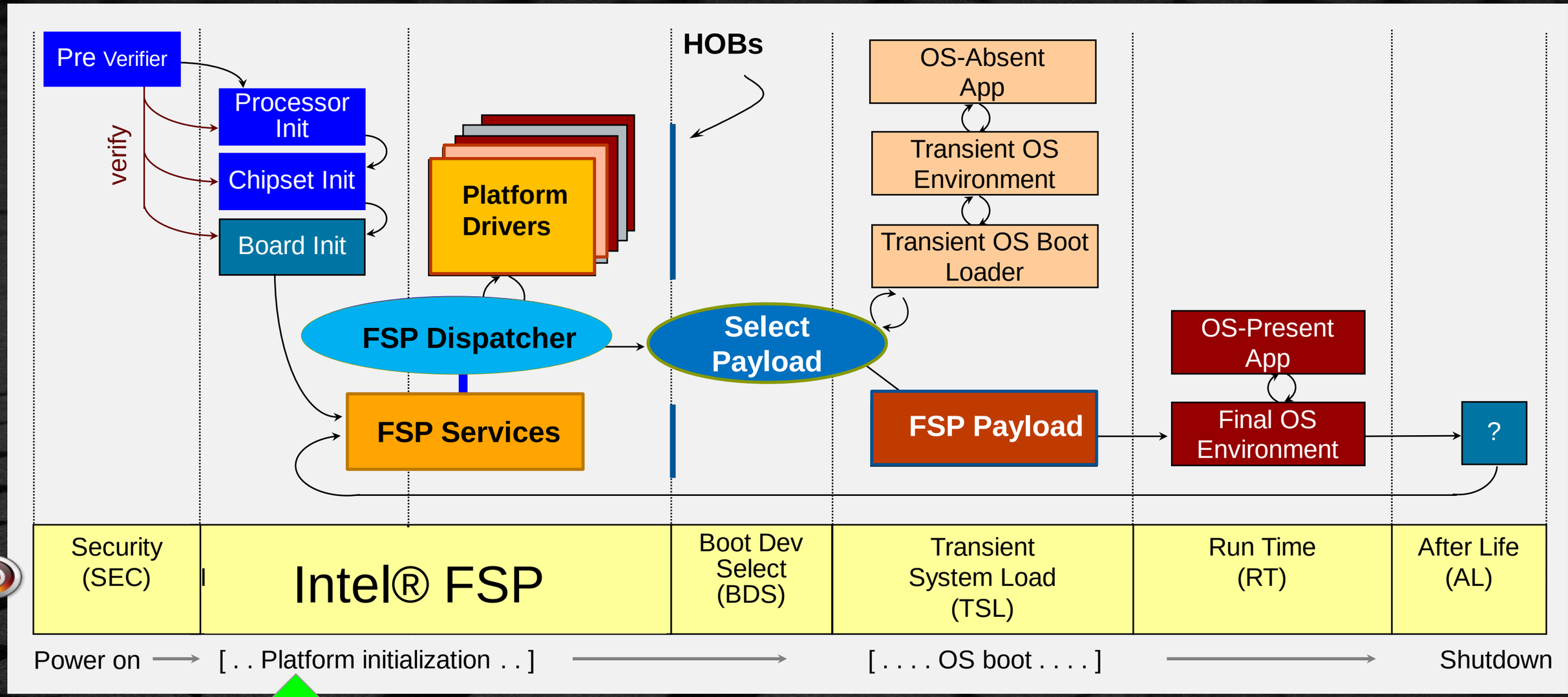


Intel FSP is independent of the bootloader solutions

UEFI – PI & EDK II BOOT FLOW – FSP



UEFI – PI & EDK II BOOT FLOW – FSP



INTEL® FSP PRODUCER

- Examples of binary instances on http://www.intel.com/fsp with 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) v2.0

Resource: https://firmware.intel.com/blog/open-source-platforms-edkii-using-intel-fsp

SOURCE FOR INTEL® FSP PRODUCER CODE

- CPU and chipset-specific code for PEIM's inside of the Intel FSP can be open or closed, added to…
- PEI core and infrastructure code at tianocore.org/edk2
  - /MdePkg
  - /MdeModulePkg
- And the code to create the Intel FSP interfaces can be found at
  - /IntelFsp2Pkg

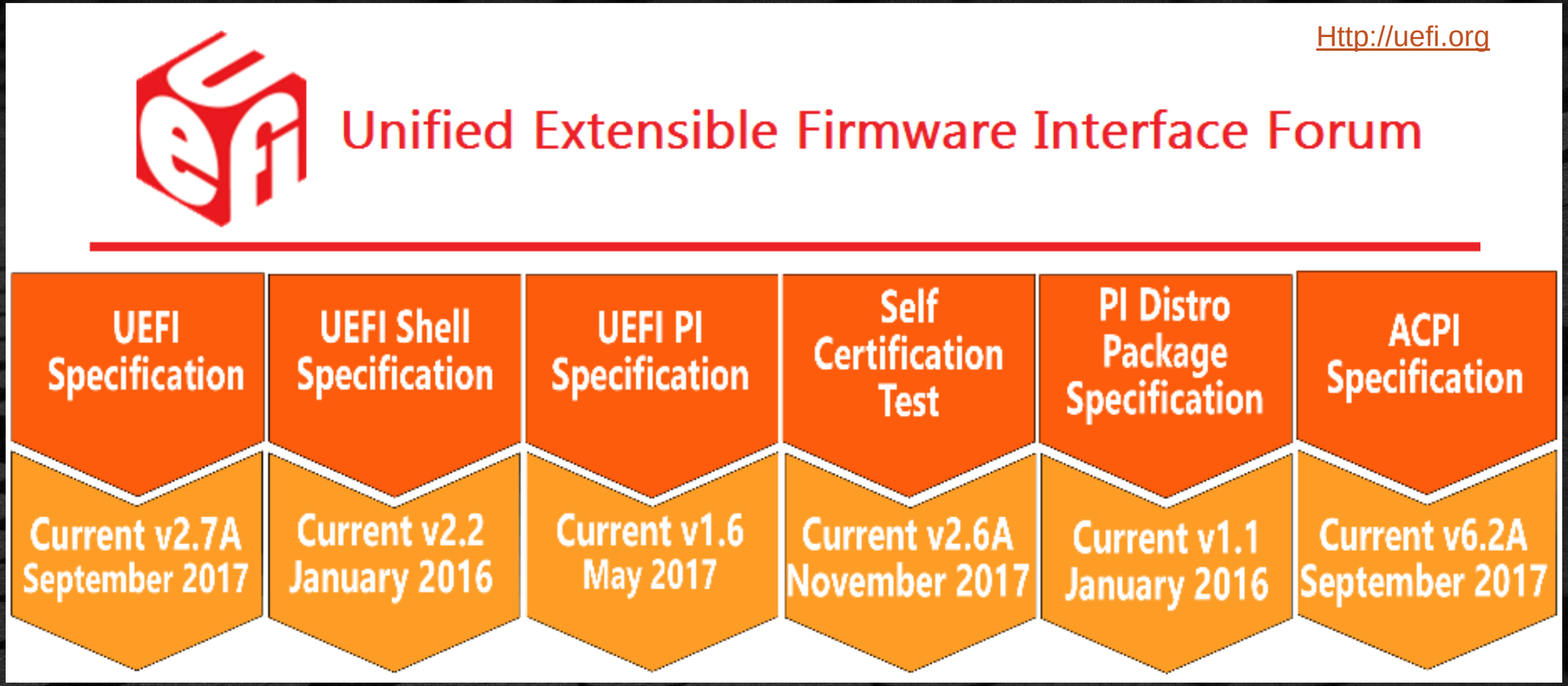
Intel FSP can encapsulate IP protected initialization code PRODUCED by Intel business units

tianocore

WHAT'S NEW IN THE UEFI SPECIFICATIONS?

LATEST UEFI SPECIFICATIONS

Http://uefi.org



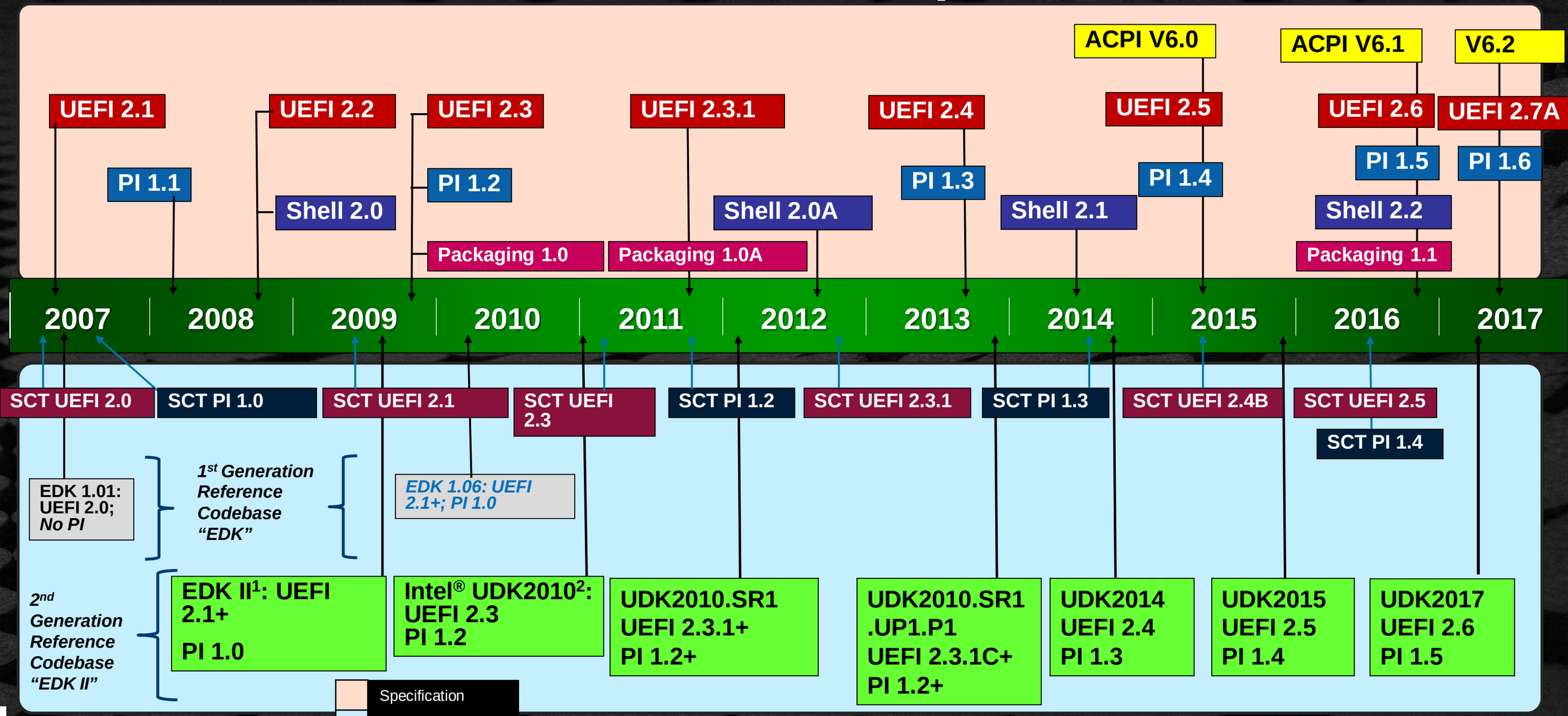
http://www.uefi.org/specsandtesttools

What's New in the UEFI Specifications

Resources Presented at Events from UEFI Forum Education Link

UEFI Specification & EDK II Reference Implementation Timeline

UEFI Specification -top & EDK II Open Source -bottom



UDK2018: Key Features - Q2 2018

UEFI Development Kit (UDK) releases are stable, validated snapshots of EDK II

- Industry Standards & Public Specifications
  - UEFI 2.7
  - UEFI PI 1.6
  - ACPI 6.2
- Centralized Config Management
- IOMMU-based DMA Protection
- Stack Guard, Heap Guard and NULL Pointer Detection
- Compilers / Tools
- Microsoft Visual Studio 2017 tool chain
- Hash-based incremental build
- Build time improvement using multi-threading in GenFds to generate FFS files
- More Info: TianoCore Wiki UDK2018

tianocore

SUMMARY

- Review PI and UEFI Boot Process
- Answer web-based training related questions
- Answer: Where does Intel® FSP Fit?
- What's new in UEFI.org

tianocore

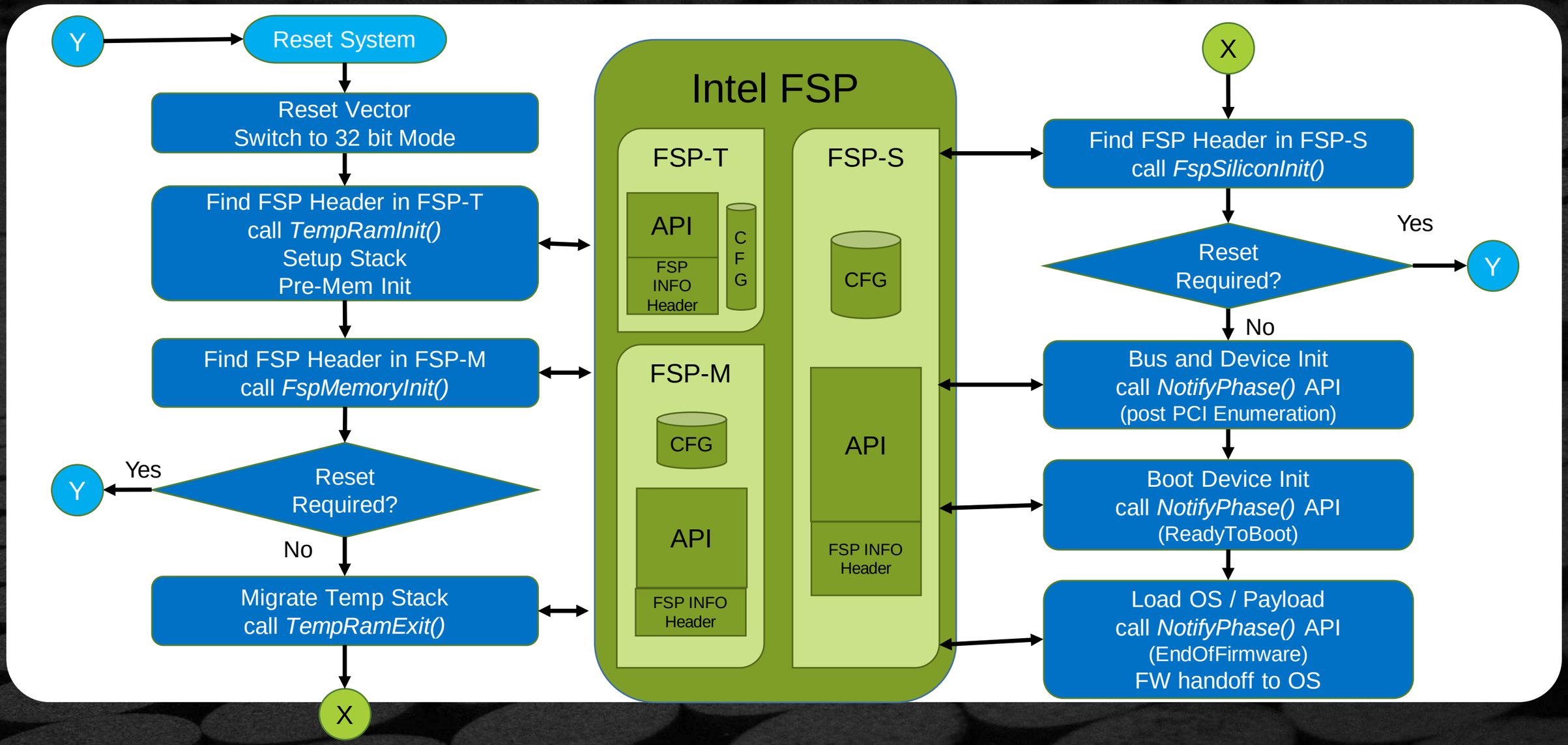
Questions?

tianocore

tianocore

BACKUP

Intel® FSP V2.0 Boot Flow



Whitpaper:Using Intel® FSP with EDK II: PDF
Intel® Firmware Support Package (Intel® FSP)

Diagram illustrates the high level boot flow

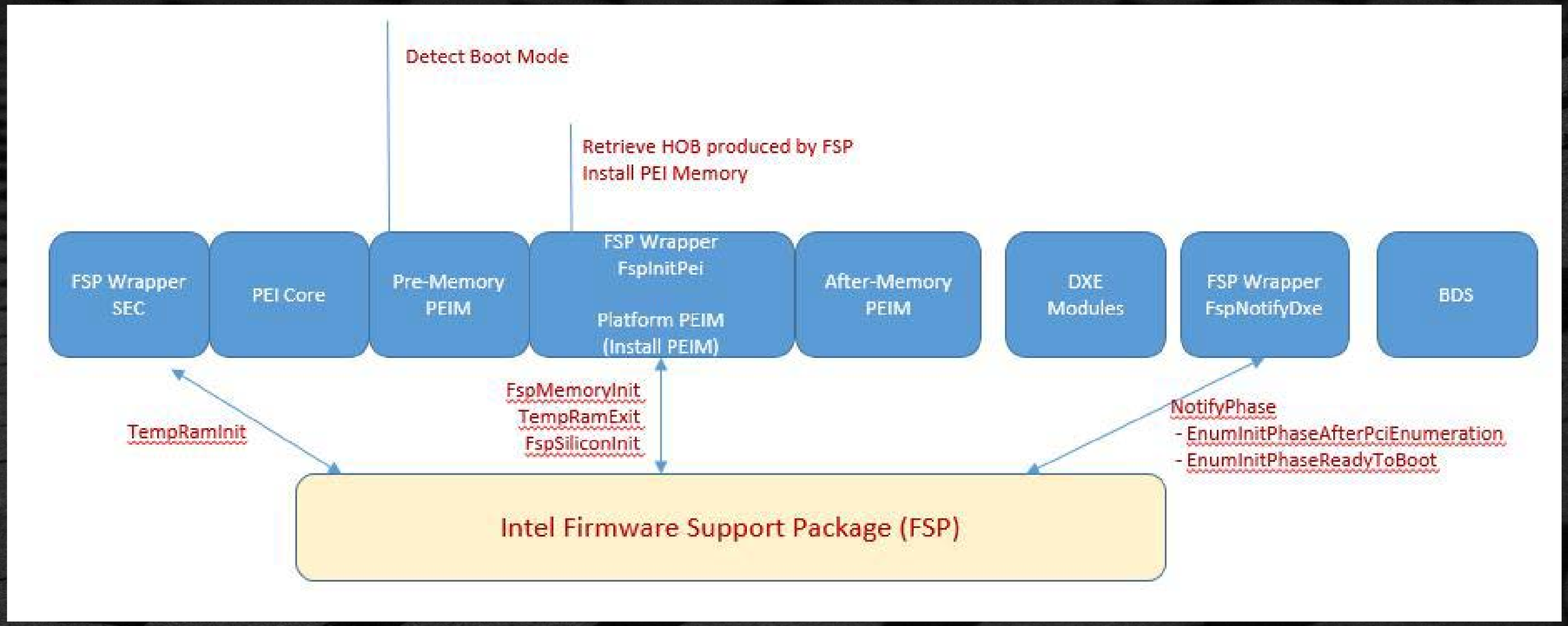


Image Source: Open Braswell Platform Desiging Porting Guide PDF

tianocore

tianocore

WAY – WAY - BACK - BACKUP

UPDATES FOR UEFI SPECIFICATION V2.5 (2.5)

Network Enhancements

- Boot from HTTP
  - HTTP API
  - HTTP Helper API
  - DNS v4/6
  - RAM Disk Device Path
- WiFi
  - Extensible Authentication Protocol (EAP) Support – point to point RFC 3748
- Transport Layer Security (TLS)
- Bluetooth
- Representational State Transfer (REST) Protocol – Web services

UPDATES FOR UEFI SPECIFICATION V2.6 (2016)

- Network Enhancements
  - Wireless MAC Connection II Protocol
  - RAM Disk Protocol
- Reliability, Availability and Serviceability (RAS)
  - Common Platform Error Record (CPER) Extension for ARM* Architecture
- User Interface
  - HII Font Ex, Glyph Generator, Image Ex and Image Generator Protocols
- IO
  - SD/eMMC Pass Thru Protocol
  - Non-identity Mapped Address Translations in PCI Root Bridge and IO Protocols

UPDATES FOR UEFI SPECIFICATION V2.7 (A)

- New private authenticated NVRAM variables with X.509 certs
  - Previously most AVs were in UEFI Secure Boot, which is a very specific environment. This change allows for more generalized interfaces and enhances the Set & Get variables services in UEFI runtime table.
- EFI HII Pop up protocol
  - Added protocol to provide services for pop windows (i.e. in setup)
- External management capability for UEFI Secure Boot
  - Allows for out-of-band management of UEFI Secure Boot keys, including service processors and hypervisors for guest firmware
- EFI HTTP Boot Callback Protocol (added)
  - Can be used for HTTP boot debugging and packet inspection.
    - This allows for printing status updates to the console during a long download during handoff to network boot file over HTTP
- Added ABI calling convention for RISC-V UEFI images
- New Reset Notification Protocol
  - Registers a function to be called before **`gRT->ResetSystem()`** is executed
  - Allows for a common warm reset (i.e. TPM, NVME storage device etc.)

UEFI FORUM ADOPTS ACPI V6.0 – 6.15

ACPI v6.1 Specification Update (2016)

- Persistent Memory – NVRAM improvements
  - NFIT Updates
  - NFIT Root Device _DSM
- Reliability, Availability and Serviceability (RAS)
  - ACPI platform error interface (APEI) Extension for ARM
  - Error Record Serialization Table (ERST) & Error Injection Table (EINJ) max wait time
  - White paper reference : A Tour beyond BIOS – Implementing the APEI with UEFI
- Management
  - Graceful Shutdown Clarifications
  - Wireless Power Calibration Device
- IO
  - Interrupt-signaled Events

UEFI ACPI V6.2 UPDATE (7)

- Secure Devices (SDEV) ACPI Table
  - New SDEV ACPI table, a list of devices that are allowed/denied to be hand-off by secure OS to a normal one.
- Heterogeneous Memory Attribute Table (HMAT)
  - New HMAT ACPI table, memory attributes for systems with heterogeneous memory architecture
- Platform Debug Trigger Table (PDTT)
  - New PDTT ACPI table, a standard way to notify all debuggers connected to the system of a fatal crash.
- Processor Properties Topology Table (PPTT)
  - New PPTT ACPI table, a description of CPU topology, available cache types and sizes.
- Windows SMM Security Mitigations Table
  - Reserved WSMT ACPI table, Microsoft's invention for system firmware to report its SMM security measures
  - Linux does not have a WSMT ACPI table equivalent so it does not have this SMM protection

UEFI SHELL SPECIFICATION V2.2 UPDATES

- Network updates
- Allow Execute() to not nest new shells
- Add command line parameter to auto exit
- New dh features
- Setvar command re-factor
- New command features for disconnect,
- comp, dmem, cls, reset, pci, bcfg, dmpstore

PACKAGING SPECIFICATION V1.1 UPDATE (1.36)

- Remove XSD reference
- Ability to convey settings with discrete subsettings
- Localized name to a package
- Ability to convey detailed produces information
- Ability to convey usage for PCDs from binary modules
- Ability to convey detailed consumes information
- Ability to convey PCD display information
- Ability to convey enumeration-like information for PCD
- Abstract type support
- Ability to convey detailed BY_START/TO_START interaction
- Ability to convey product limit information about Protocol/PPI/GUIDs

PLATFORM INITIALIZATION V1.5 UPDATES (1.6)

- SMM Environment to support newer architecture/platform designs
- ARM extensions to Vol 4
- Additional I2C PPIs
- Add PPI to allow DEC to pass HOBs to PEI
- Pre-DXE initialization of the SM Foundation
- Handling PEI PPI descriptor notifications from ASEC
- SM stand-alone infrastructure
- Core/platform integration enhancements
- New MP protocol
- Propagate PEI-phase FV verification status to DXE
- Add SD/MMC GUID to DiskInfo protocol
- Add EFI_FV_FILETYPE_SMM_CORE_STANDALONE file type
- A number of errata

PLATFORM INITIALIZATION V1.6 UPDATES (1 of 7)

- Added **`VOLUME_EXT_ENTRY_USED_SIZE`** structure
  - No need to store it in **`ZeroVector`** anymore
- A new bit reserved in FFS file header
  - Allows for new file alignments and supports hardware designs where the firmware storage must be at specific alignment
- MM Handler State Notification Protocol
  - New protocol that is used to register a callback for each MM handler and supports use of the MM infrastructure on Arm TrustZone
  - Formally known as SMM
- RISC-V Processor Family
  - Adds support for RISC-V architecture for PEI and grows the list of supported CPU bindings in the UEFI specification
- SPI Bus Overview
  - Allows for a standardized way to access SPI NOR attached flash for accessing SPI sensors and devices