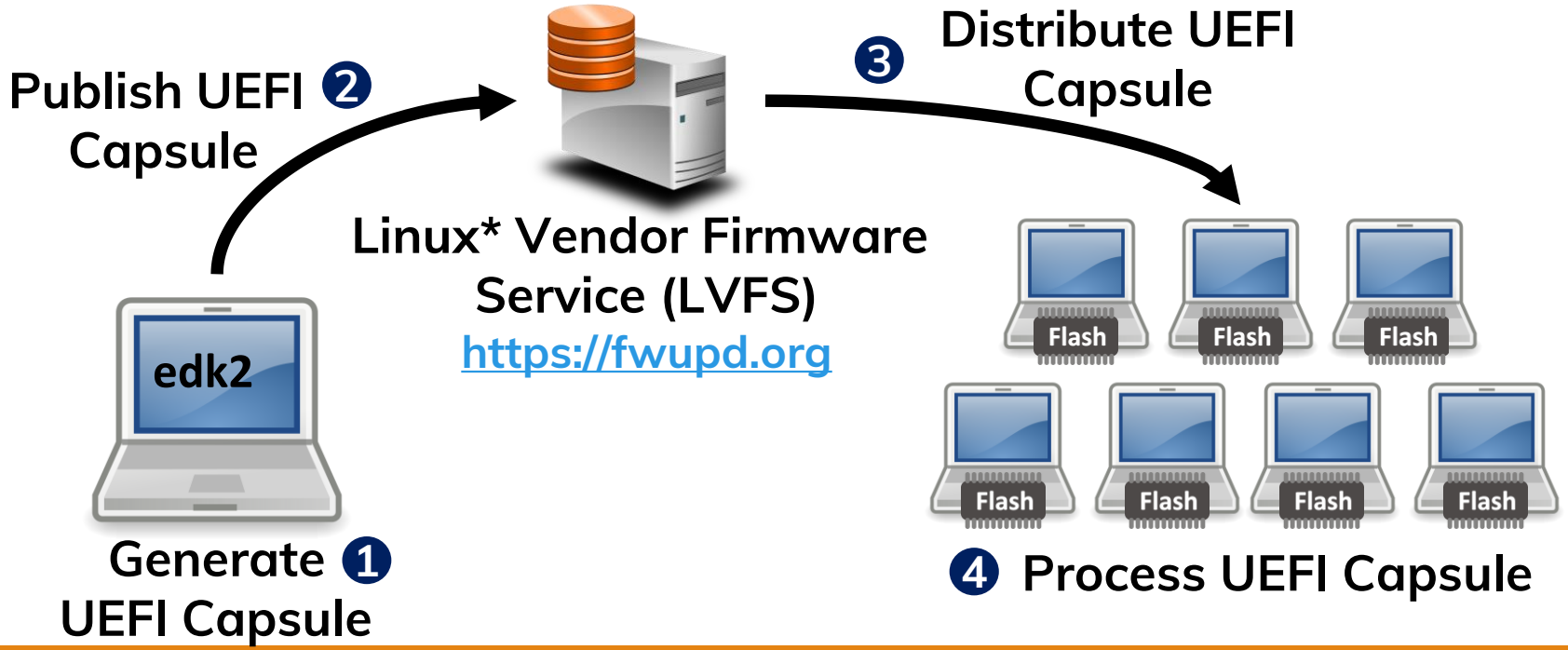
System Firmware and Device Firmware Updates using Unified Extensible Firmware Interface (UEFI) Capsules

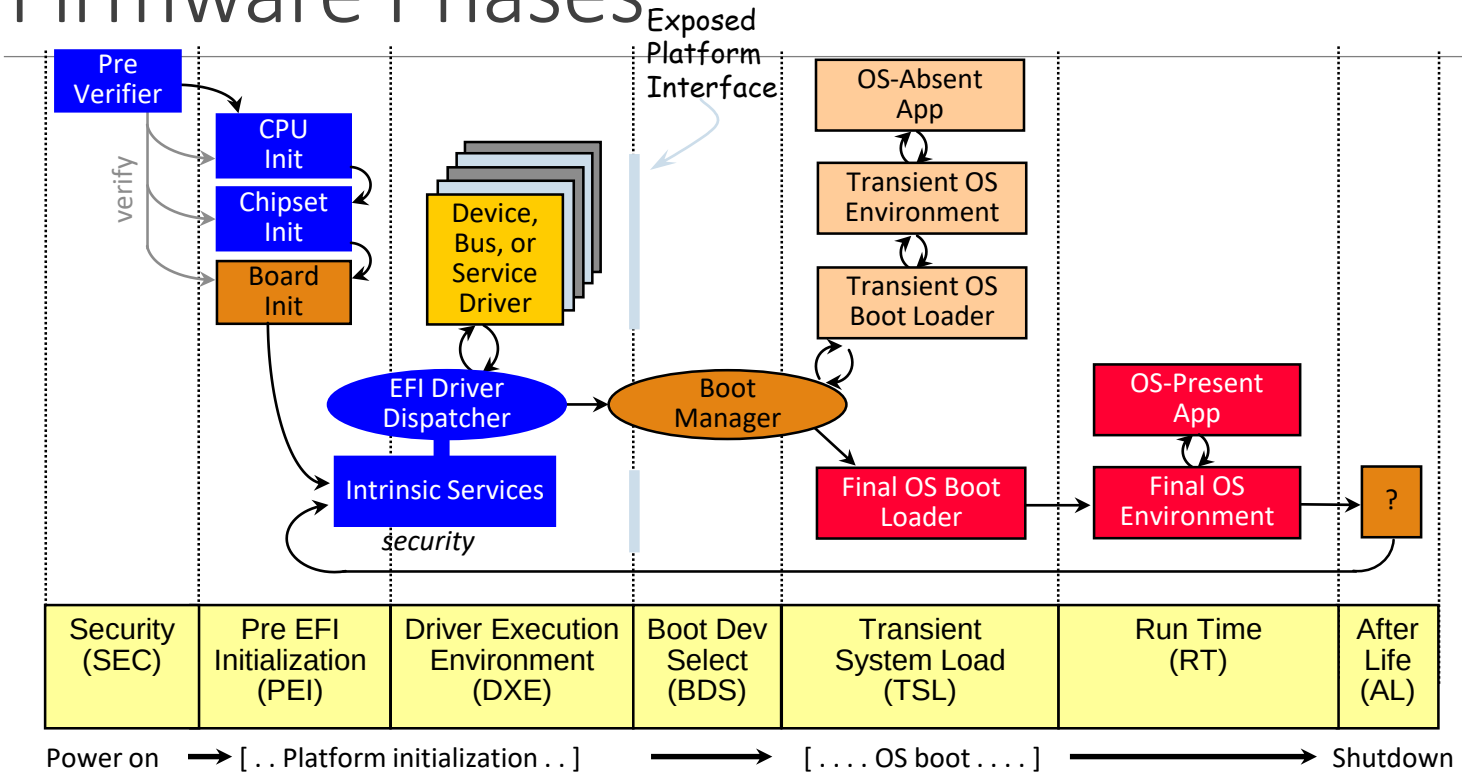
HARRY HSIUNG, INTEL CORPORATION

LINUX PLUMBERS CONFERENCE - AUGUST 2020

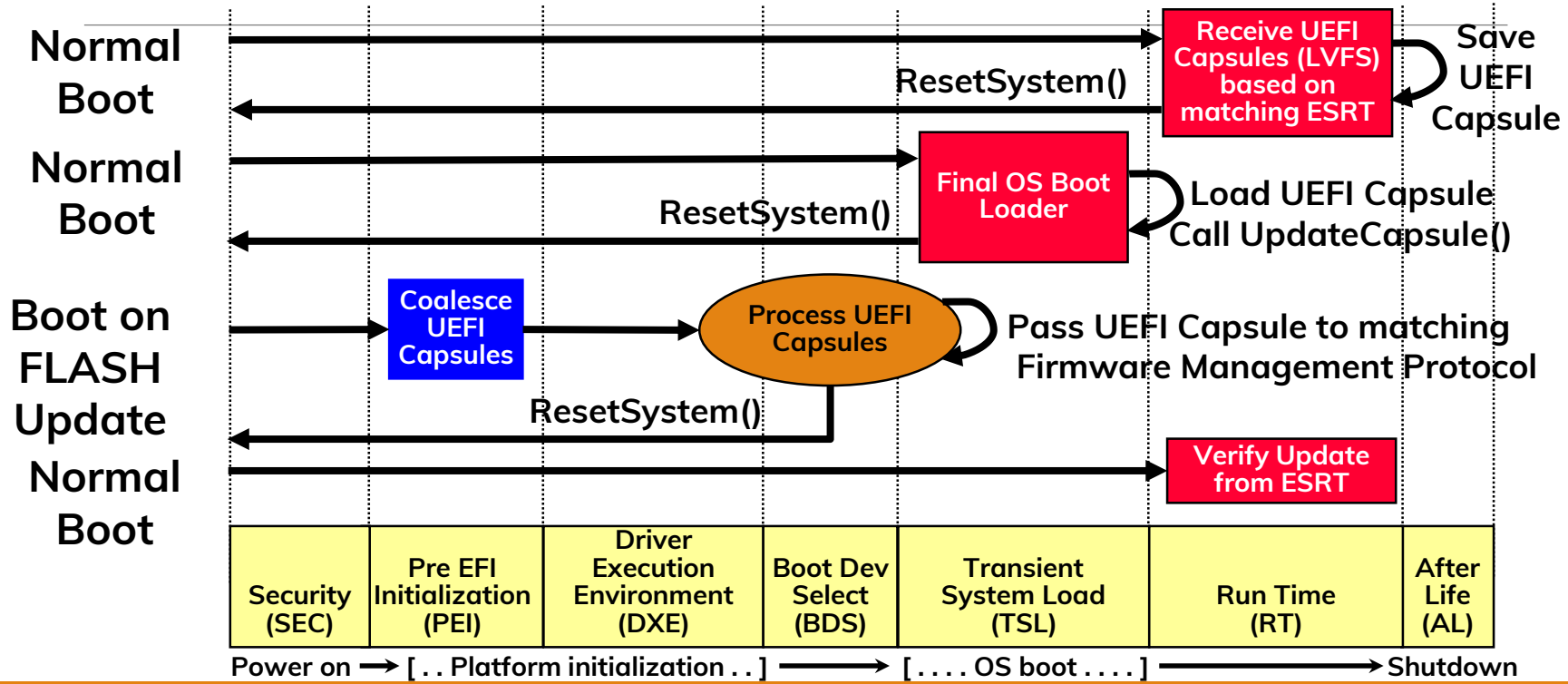
Building and Distributing UEFI Capsules for Firmware Update



Platform Initialization (PI) Architecture Firmware Phases

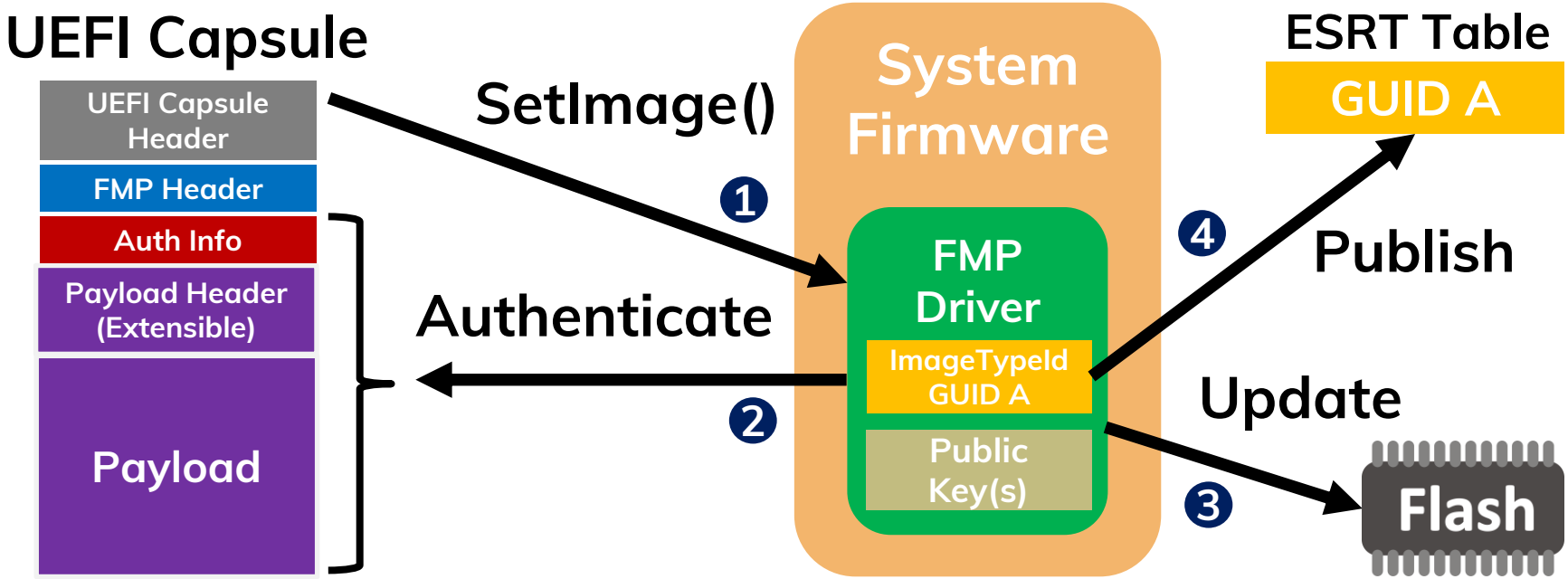


PI Architecture Firmware Phases
Example UEFI Capsule Processing



ESRT= EFI System Resource Table

Process UEFI Capsule



FMP = UEFI Firmware Management Protocol
GUID = Globally Unique Identifier

EDK II UEFI Capsule Features

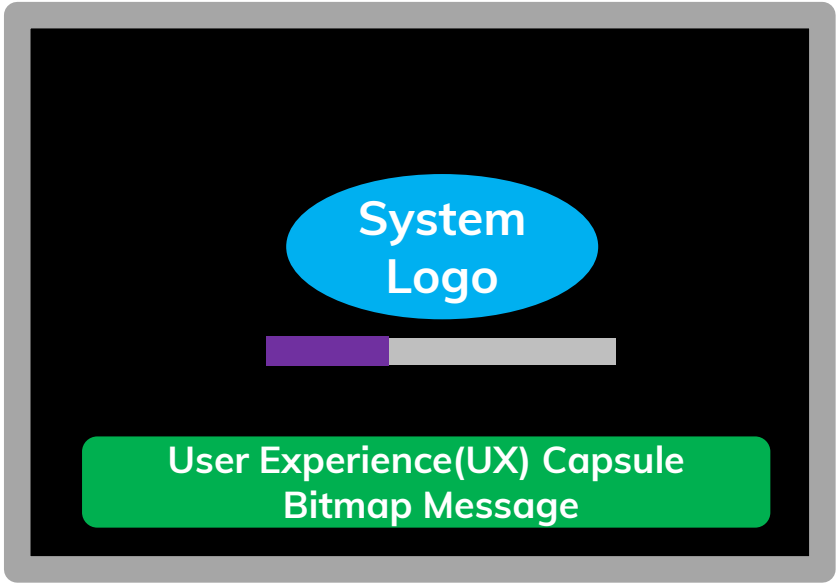
EFI Development Kit II (https://www.tianocore.org)

Feature	UDK2017 / UDK2018	edk2-stable201808
Generate UEFI Capsule	Integrated EDK II Build	Standalone Python* Script
Update Granularity	Focused on Monolithic	Designed to support Multiple Components
Authentication	PKCS7 Single Key	PKCS7 Multiple Keys
Pre-Check	N/A	Power/Battery, Thermal, System
Update Indicator	Requires platform code	Built-in with Consistent UX and Progress Bar
Firmware Management Protocol	Requires full implementation	Produced by FmpDxe module customized using configuration data and small libraries.
Test Key Detection	Requires platform code	Built-in
Watchdog	Requires platform code	Built-in
ESRT Driver	Legacy + FMP	Smaller/Simpler FMP only version

Firmware Update Indicators

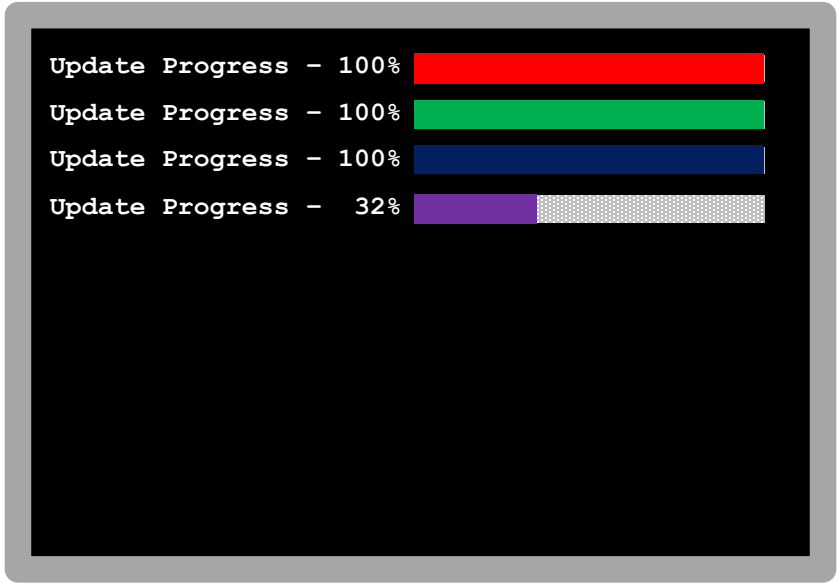
UEFI Graphics Console

EFI_GRAPHICS_OUTPUT_PROTOCOL



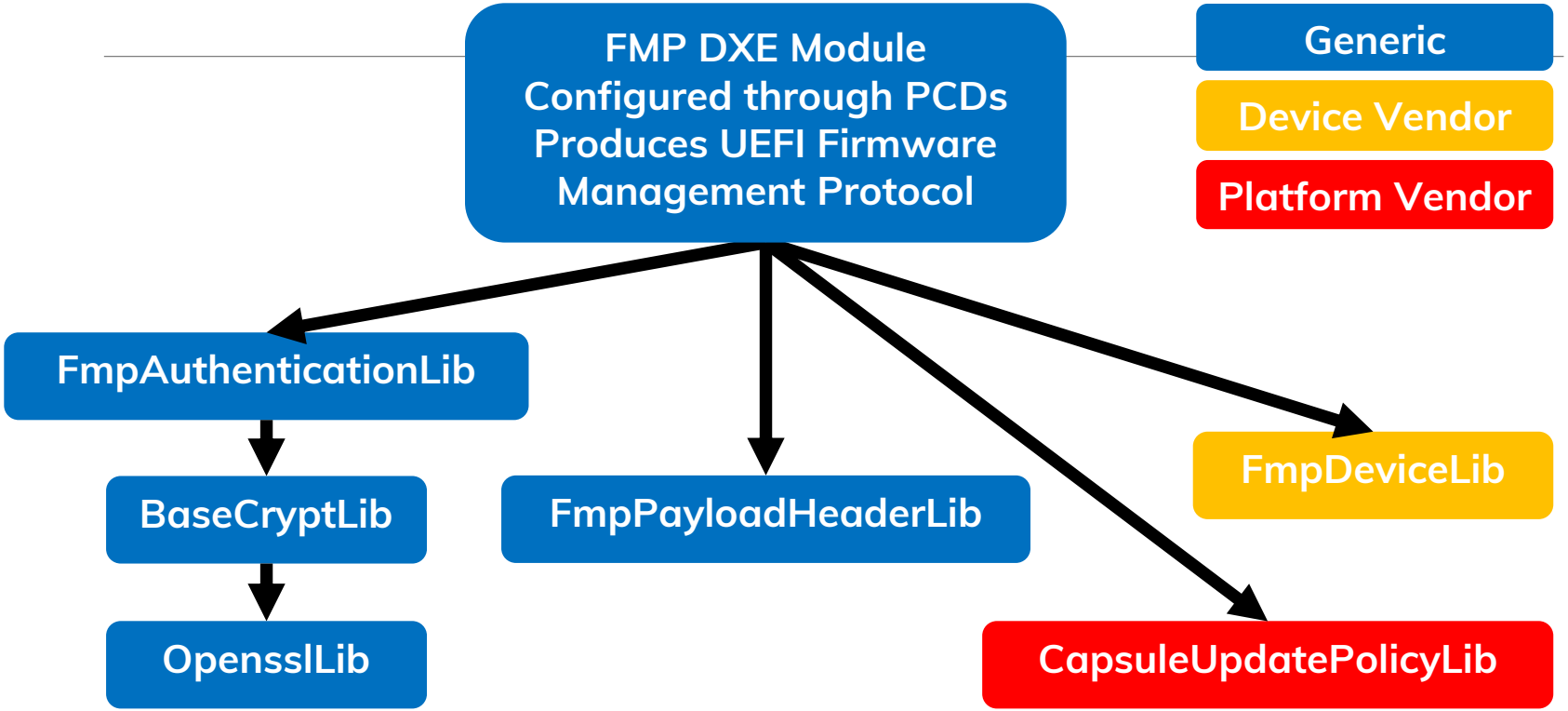
UEFI Text Console

EFI_SIMPLE_TEXT_OUTPUT_PROTOCOL



Customize with a new DisplayUpdateProgressLib instance

FmpDxe Module Overview



PCD = Platform Configuration Database

FmpDxe Module Configuration

Name	Description
`FILE_GUID`	ESRT GUID Value
`PcdFmpDeviceImageIdName`	FMP Image Descriptor - Unicode string
`PcdFmpDeviceBuildTimeLowestSupportedVersion`	Build time FMP/ESRT default value
`PcdFmpDeviceLockEventGuid`	Event GUID to lock FW storage device. Default is End of DXE.
`PcdFmpDeviceProgressWatchdogTimeInSeconds`	Watchdog armed on each progress update
`PcdFmpDeviceProgressColor`	24-bit Progress Bar Color (0x00rrggbb)
`PcdFmpDevicePkcs7CertBufferXdr`	One or more PKCS7 Certs in XDR format. Encode with `BaseTools/Scripts/BinToPcd`
`PcdFmpDeviceTestKeySha256Digest`	Set to `{0}` to disable test key detection

XDR = External Data Representation using Variable-Length Opaque Data format from RFC 4506

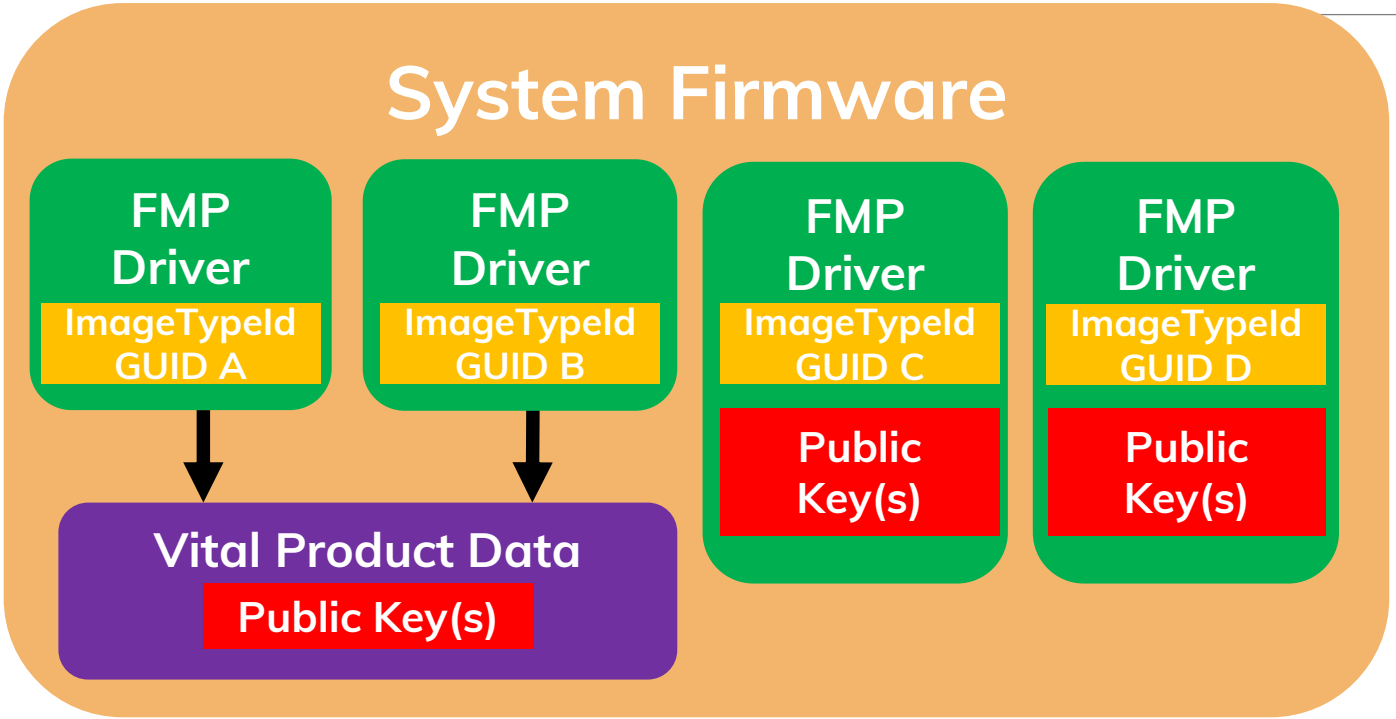
CapsuleUpdatePolicyLib APIs Platform Specific Library

Name	Description
`CheckSystemPower()`	Is system power/battery ok for FW update?
`CheckSystemThermal()`	Is system temperature ok for FW update?
`CheckSystemEnvironment()`	Is the system environment ok for FW update?
`IsLowestSupportedVersionCheckRequired()`	Skip lowest supported version check? (e.g. Service Mode)
`IsLockFmpDeviceAtLockEventGuidRequired()`	Skip firmware storage device lock action? (e.g. Manufacturing Mode)

FmpDeviceLib APIs
Device Specific Library

Name	Description
`RegisterFmpInstaller()`	Future expansion for add-in controllers.
`FmpDeviceGetSize()`	Size of ***currently stored FW image.***
`FmpDeviceGetImageTypeIdGuidPtr()`	ESRT/FMP GUID. Overrides FILE_GUID value.
`FmpDeviceGetAttributes()`	FMP Attributes Supported/Settings.
`FmpDeviceGetLowestSupportedVersion()`	LSV from ***currently stored FW image.***
`FmpDeviceGetVersionString()`	Unicode version string from ***currently stored FW image.***
`FmpDeviceGetVersion()`	32-bit version value from ***currently stored FW image.***
`FmpDeviceGetImage()`	Retrieve copy of ***currently stored FW image.***
`FmpDeviceCheckImage()`	Check if a new FW image is valid for this device.
`FmpDeviceSetImage()`	Update FW storage with a new FW image.
`FmpDeviceLock()`	Lock FW storage to prevent any further changes.

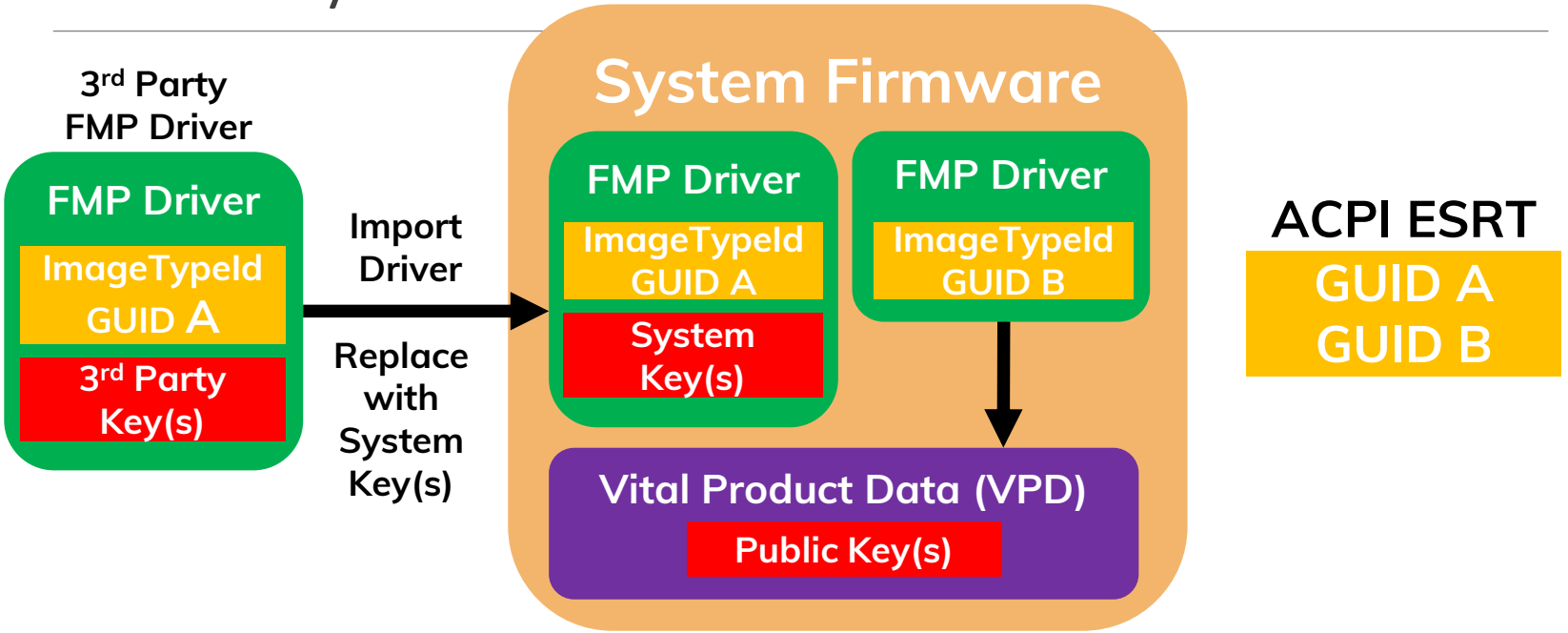
ESRT GUIDs and Keys
Multiple Components



ACPI ESRT

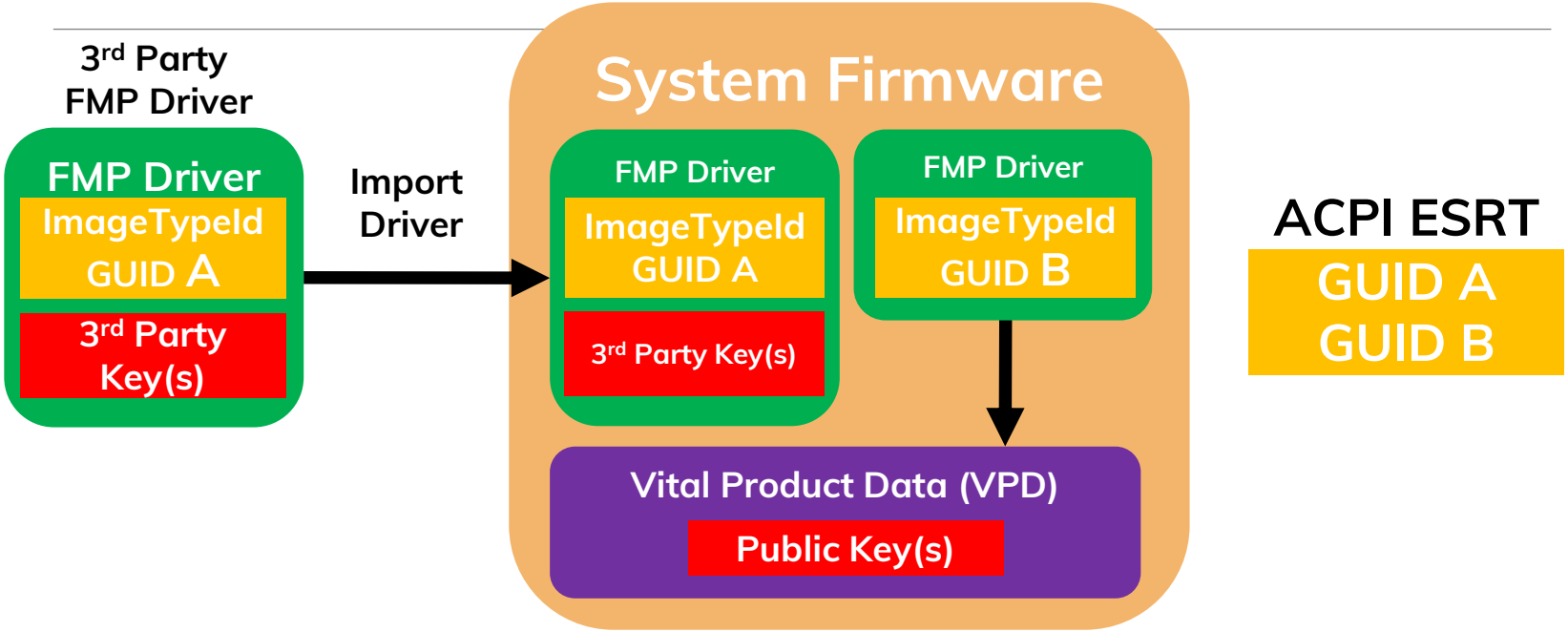
GUID A
GUID B
GUID C
GUID D

ESRT GUIDs and Keys
3rd Party FMP Driver



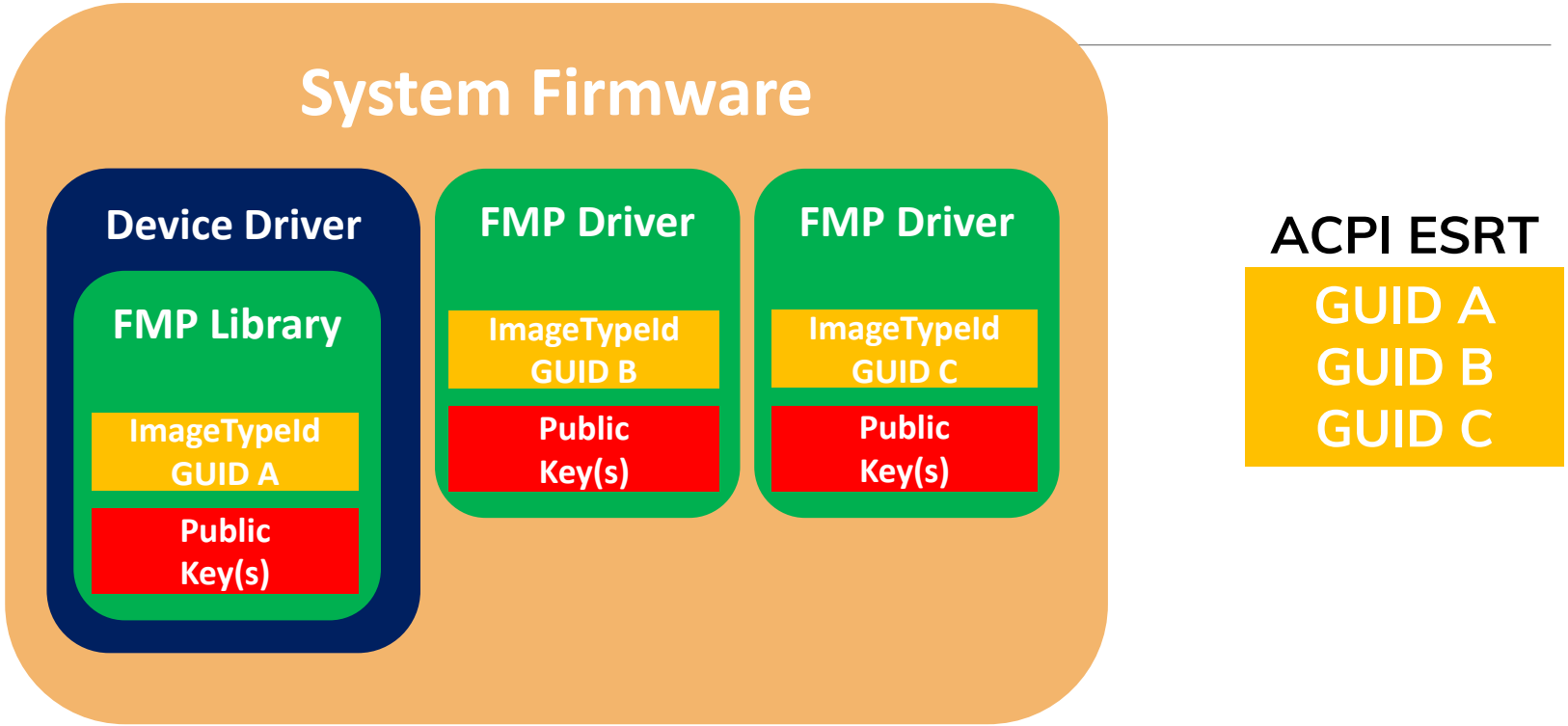
3rd Party UEFI Capsules must be re-signed with System Key

ESRT GUIDs and Keys
3rd Party FMP Driver



System allows UEFI Capsules from 3rd Party to be installed

Add FMP to Existing Device Driver



Summary

EDK II supports new UEFI Capsule Features for Firmware Update

- Simplifies FMP support for system firmware and integrated devices
- Multiple authentication keys with flexible key storage options.
- System update pre-check (Power/battery, thermal, and system).
- Improved UX with progress indicators during update.
- Built-in support for test key detection & watchdog timer.
- Simplified ESRT driver using FMP instances

EDK II GenerateCapsule.py used to Generate UEFI Capsules

Publish and Distribute UEFI Capsules for Firmware Updates using Linux Vendor Firmware Services (LVFS)

Call to Action

Add UEFI Capsule based Firmware Update to platforms

Implement UEFI Capsule based Firmware Update for devices

Take advantage of latest EDK II FmpDevicePkg features

Use Linux Vendor Firmware Service (LVFS) to publish and distribute UEFI Capsule based Firmware Updates

Provide feedback and contribute!

- TianoCore https://www.tianocore.org/
- LVFS https://fwupd.org/