



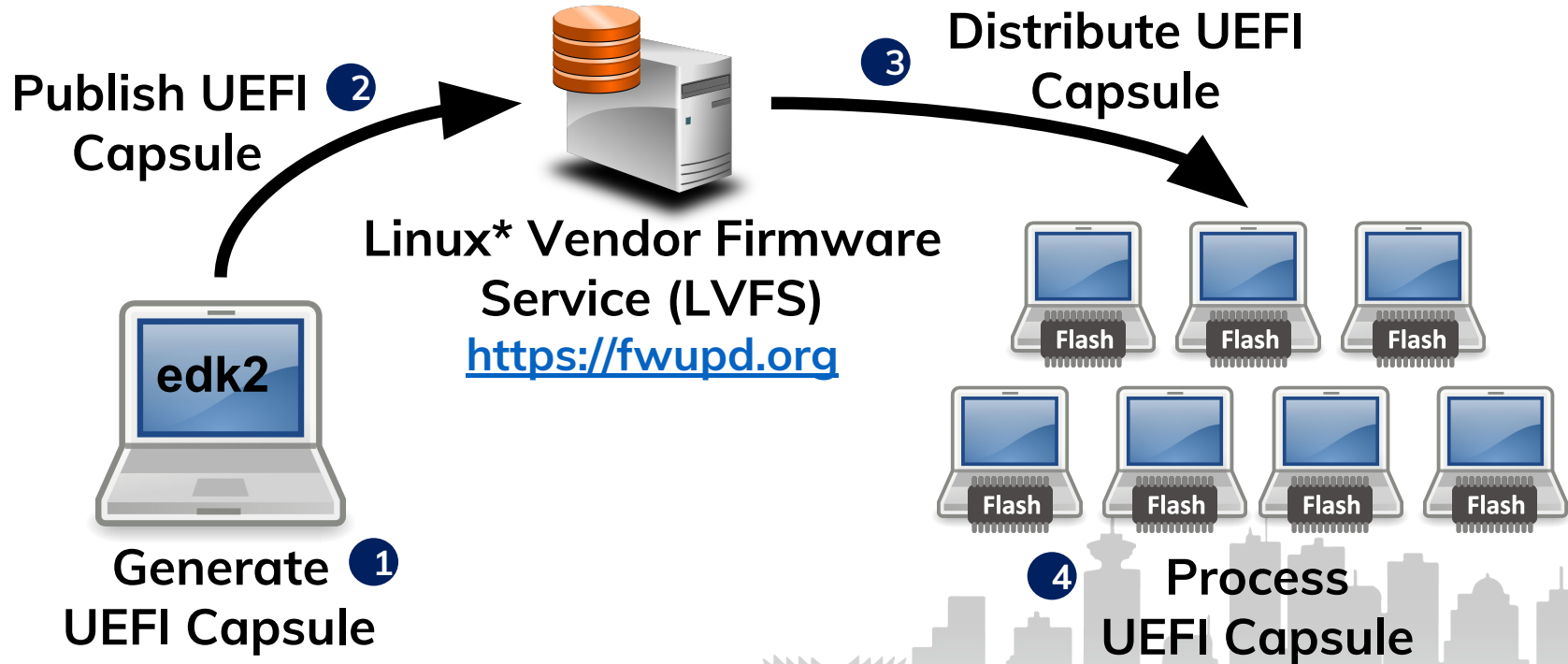
**Linaro
connect**
Vancouver 2018

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

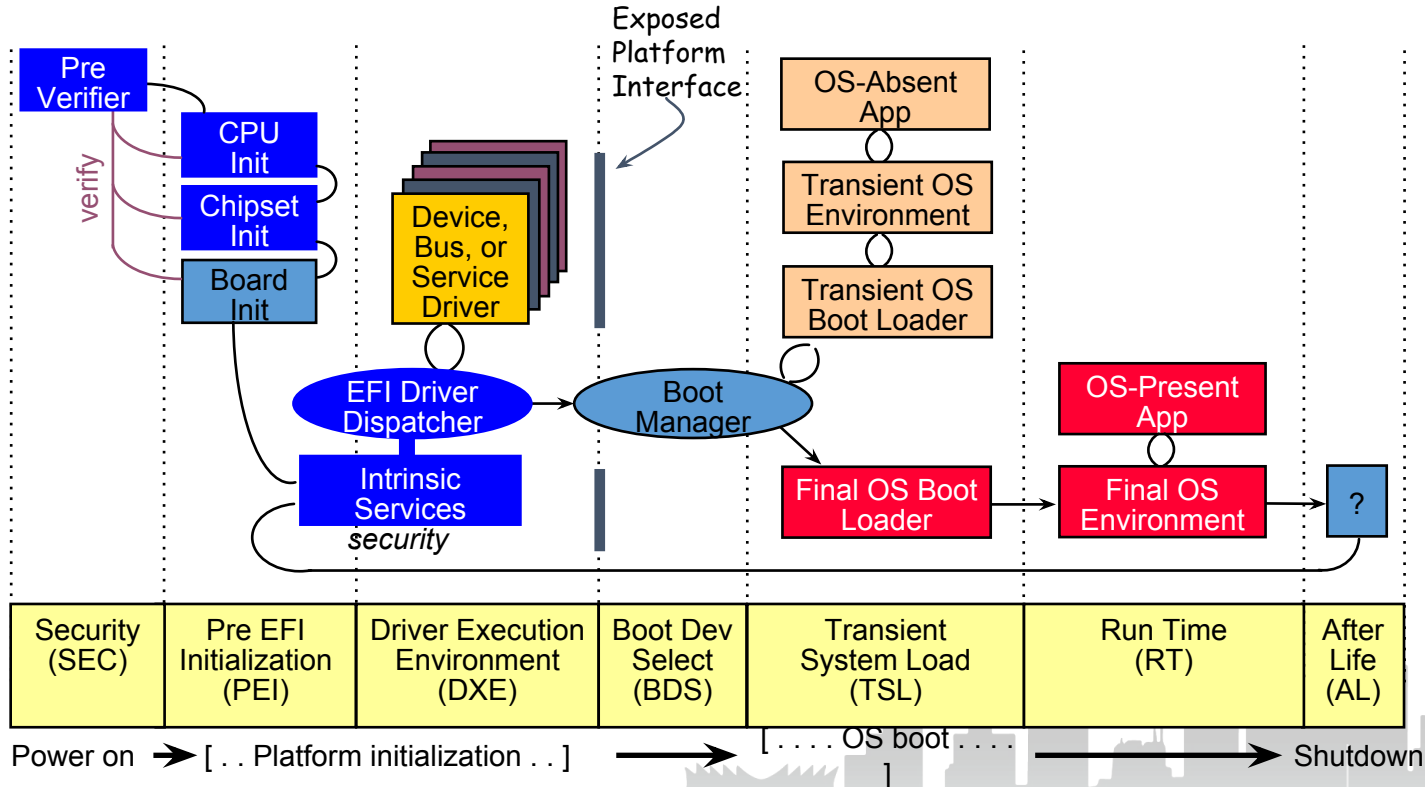
Michael Kinney



Building and Distributing UEFI Capsules for Firmware Update

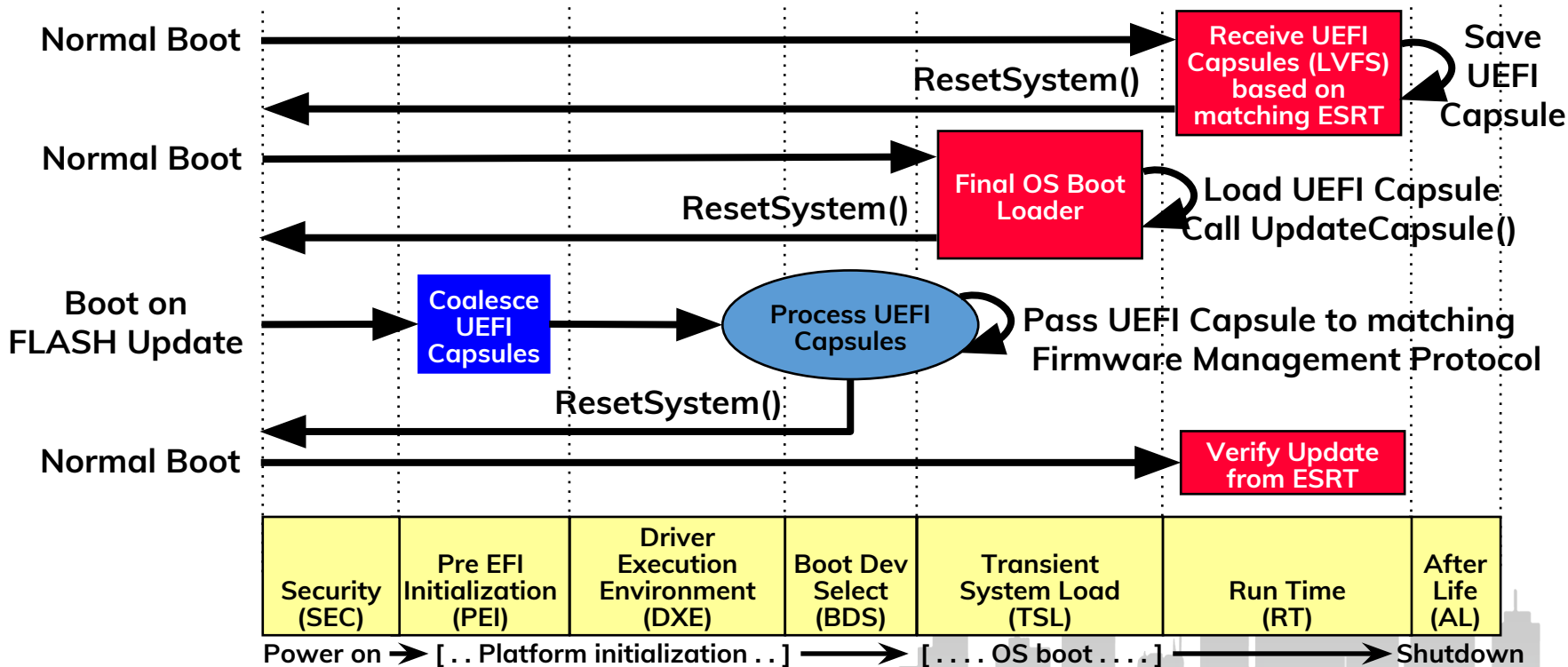


Platform Initialization (PI) Architecture Firmware Phases



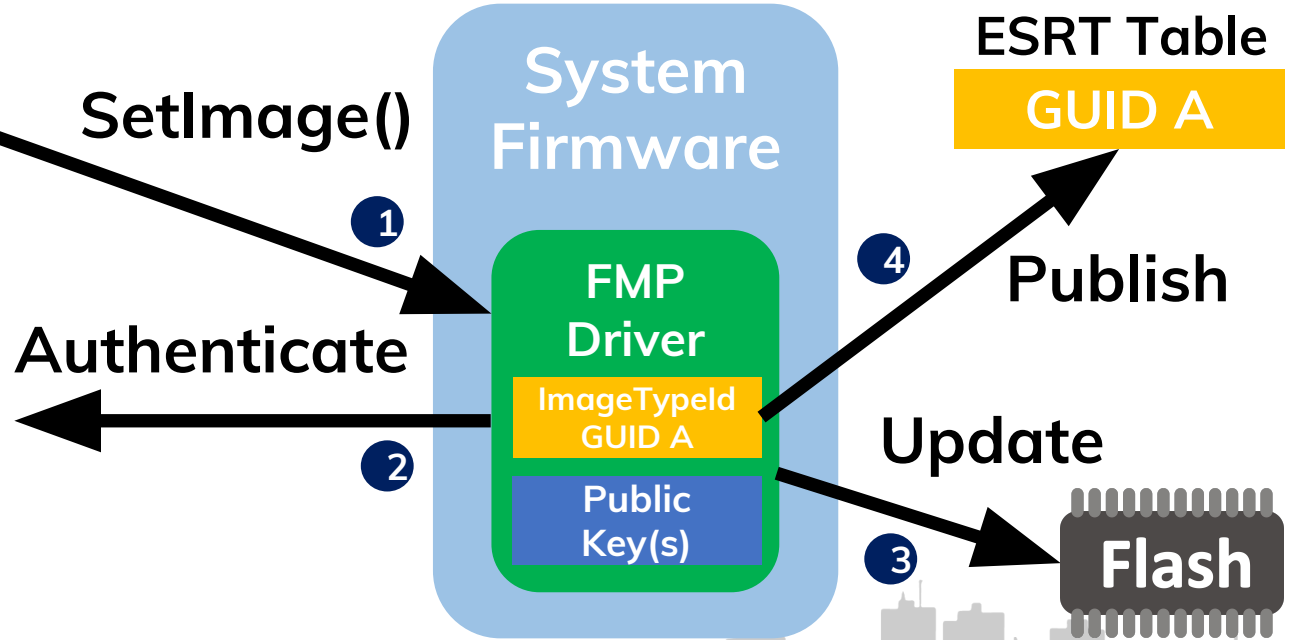
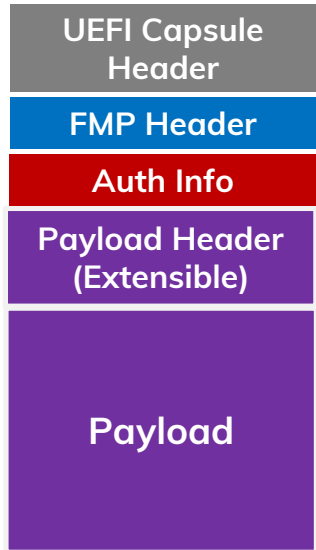
PI Architecture Firmware Phases

Example UEFI Capsule Processing



Process UEFI Capsule

UEFI Capsule



FMP = UEFI Firmware Management Protocol
GUID = Globally Unique Identifier

EDK II UEFI Capsule Features

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

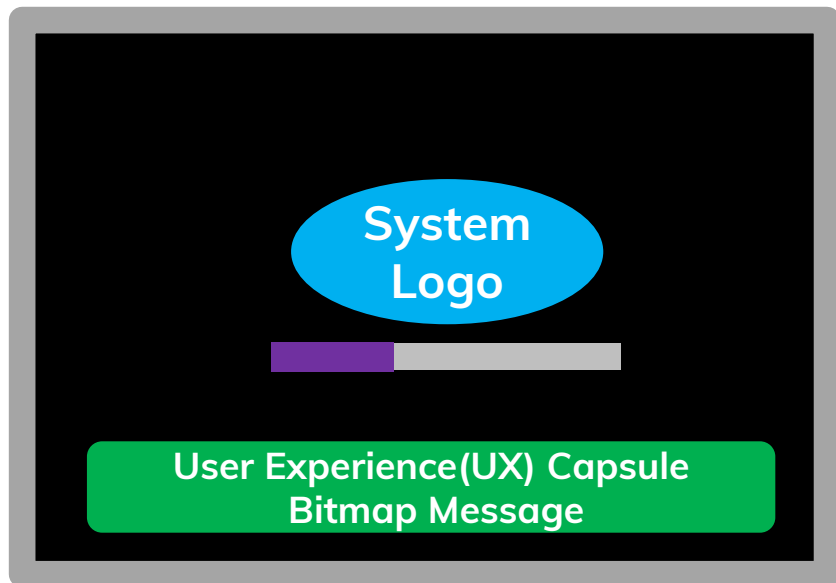
Feature	UDK2017 / UDK2018	edk2-stable201808
Generate UEFI Capsule	Integrated EDK II Build	Standalone Python* Script
Update Granularity	Focused on Monolithic	Designed to support Multiple Components
Authentication	PKCS7 Single Key	PKCS7 Multiple Keys
Pre Check	N/A	Power/Battery, Thermal, System
Update 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

* Other names and brands may be claimed as property of others

Firmware Update Indicators

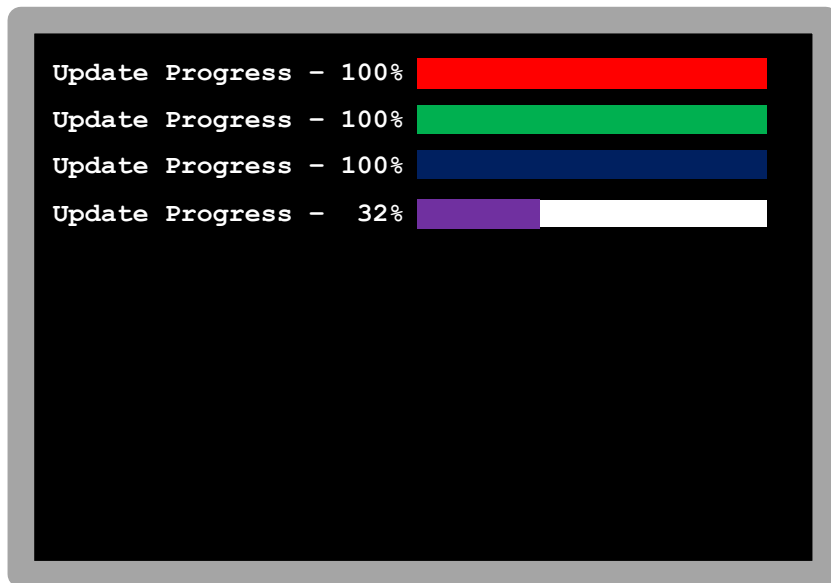
UEFI Graphics Console

EFI_GRAPHICS_OUTPUT_PROTOCOL



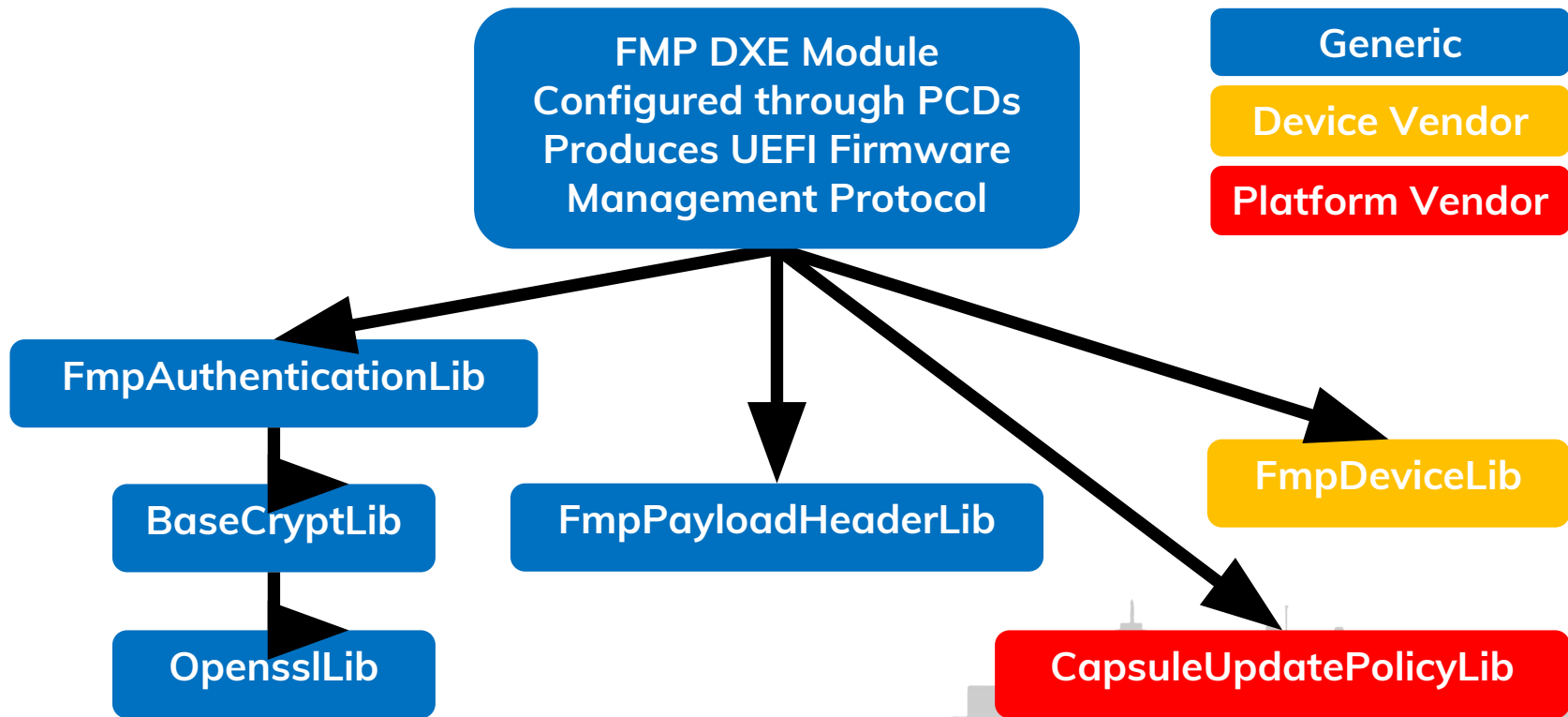
UEFI Text Console

EFI_SIMPLE_TEXT_OUTPUT_PROTOCOL



Customize with a new DisplayUpdateProgressLib instance

FmpDxe Module Overview



FmpDxe Module Configuration

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

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)



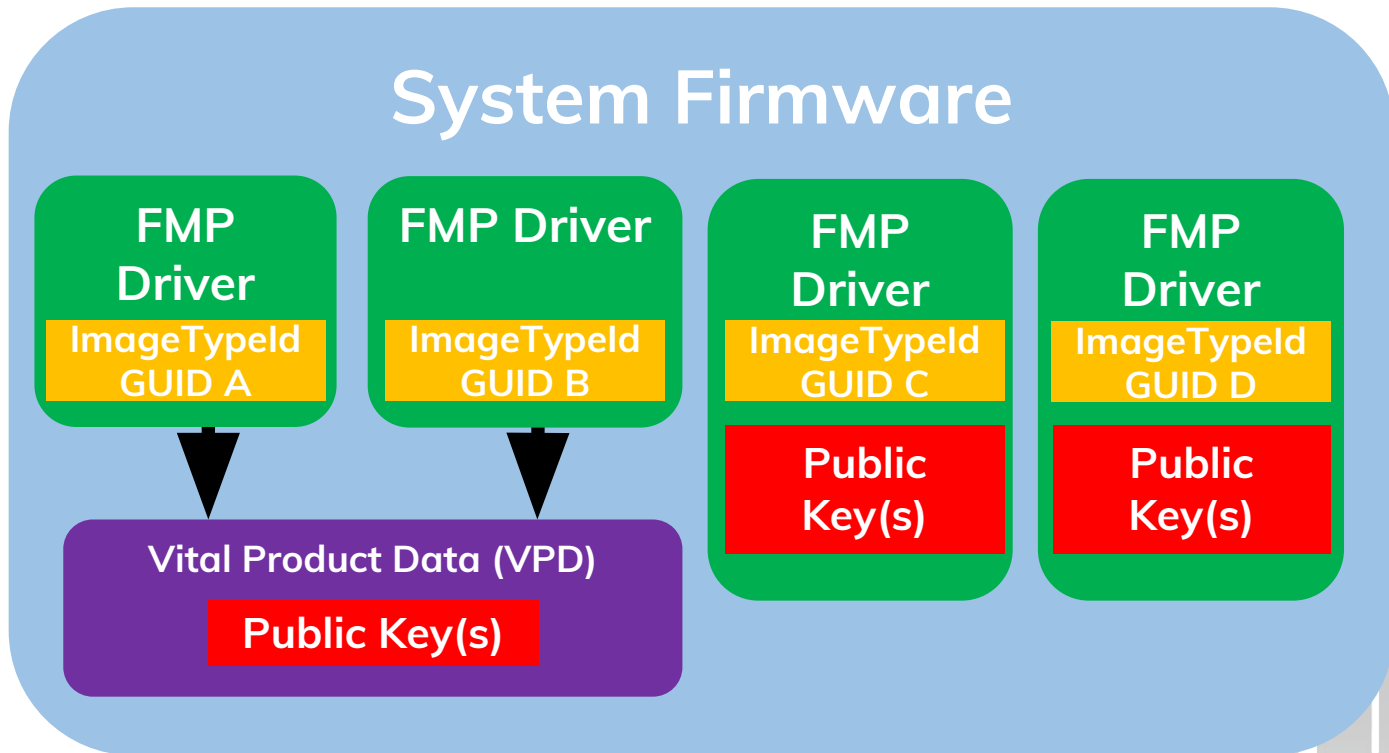
FmpDeviceLib APIs

Device Specific Library

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

ESRT GUIDs and Keys

Multiple Components

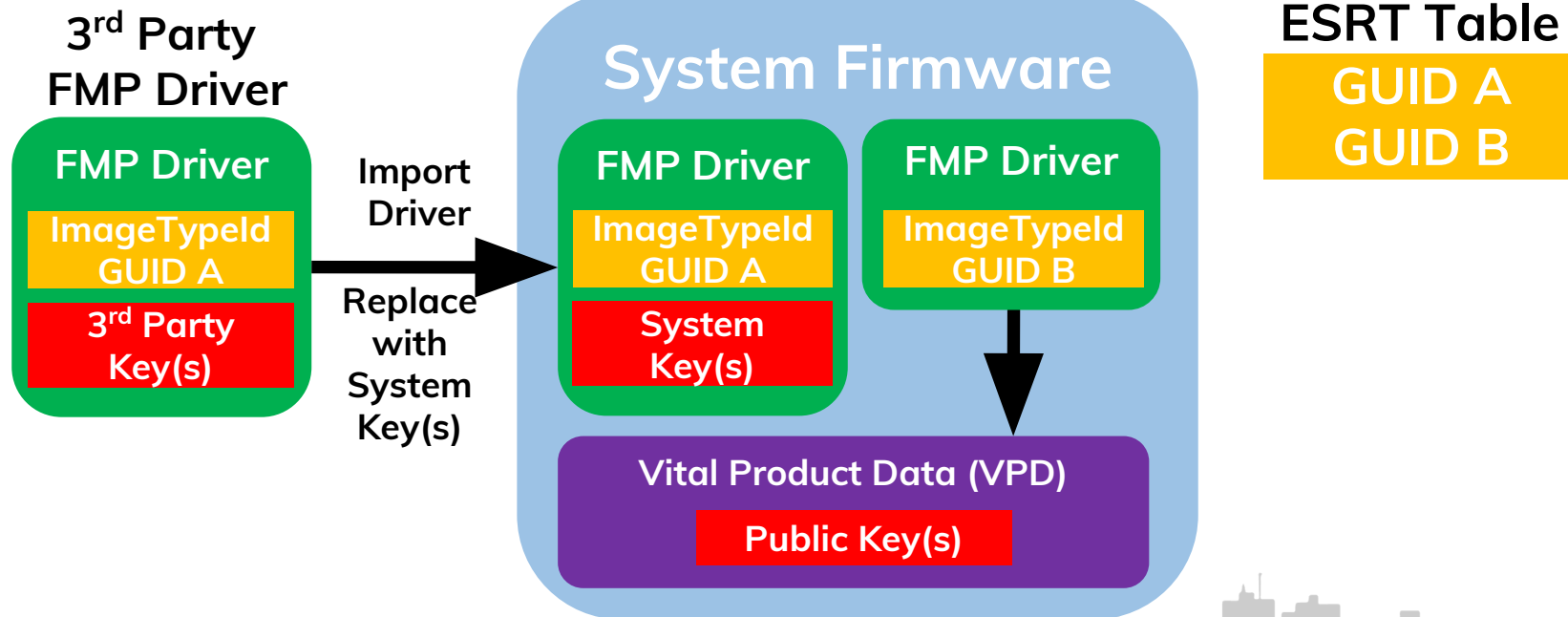


ESRT Table

GUID A
GUID B
GUID C
GUID D

ESRT GUIDs and Keys

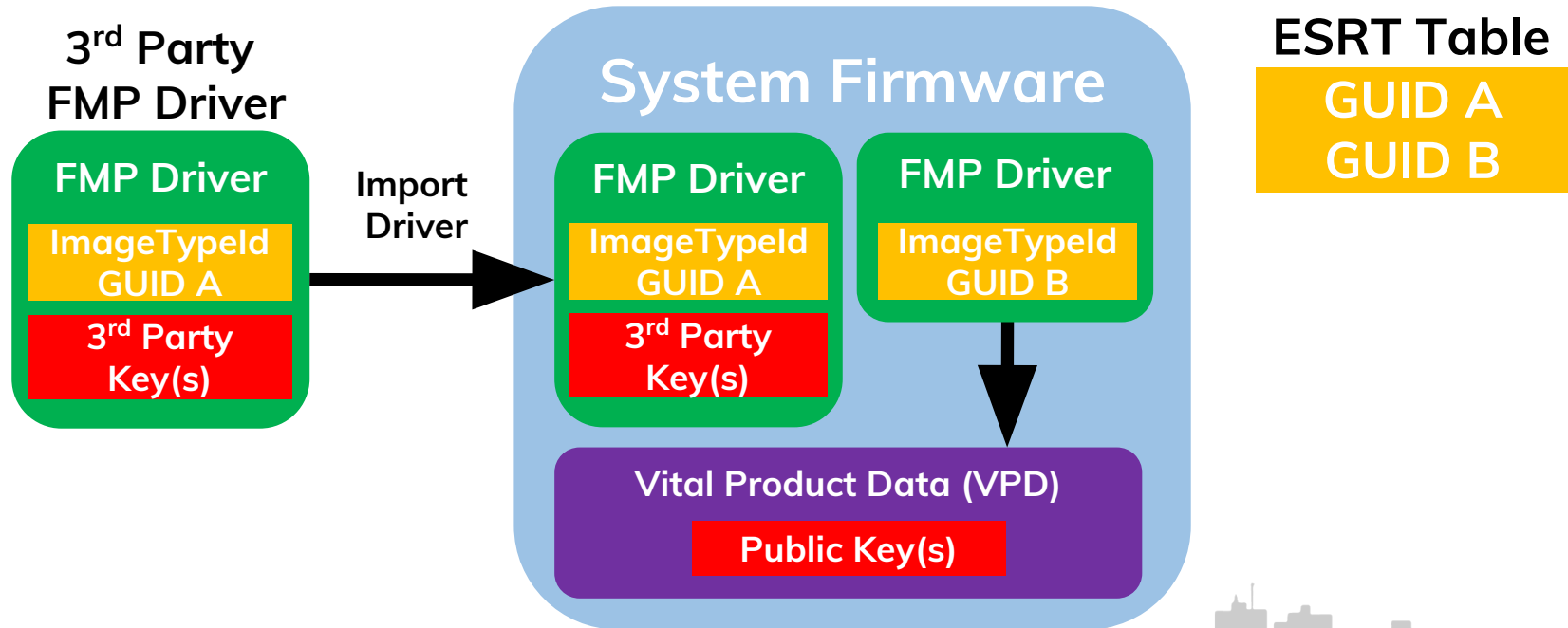
3rd Party FMP Driver



3rd Party UEFI Capsules must be resigned with System Key

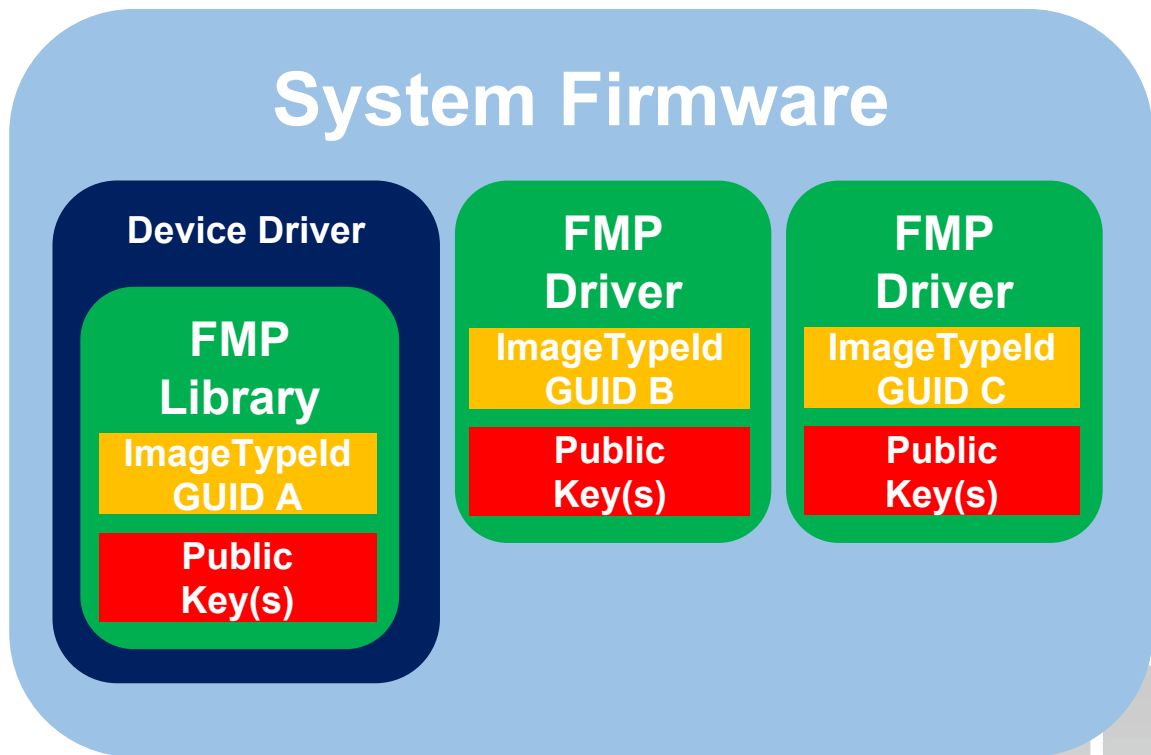
ESRT GUIDs and Keys

3rd Party FMP Driver



System allows UEFI Capsules from 3rd Party to be installed

Add FMP to Existing Device Driver



ESRT

Table

GUID A
GUID B
GUID C

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/>

