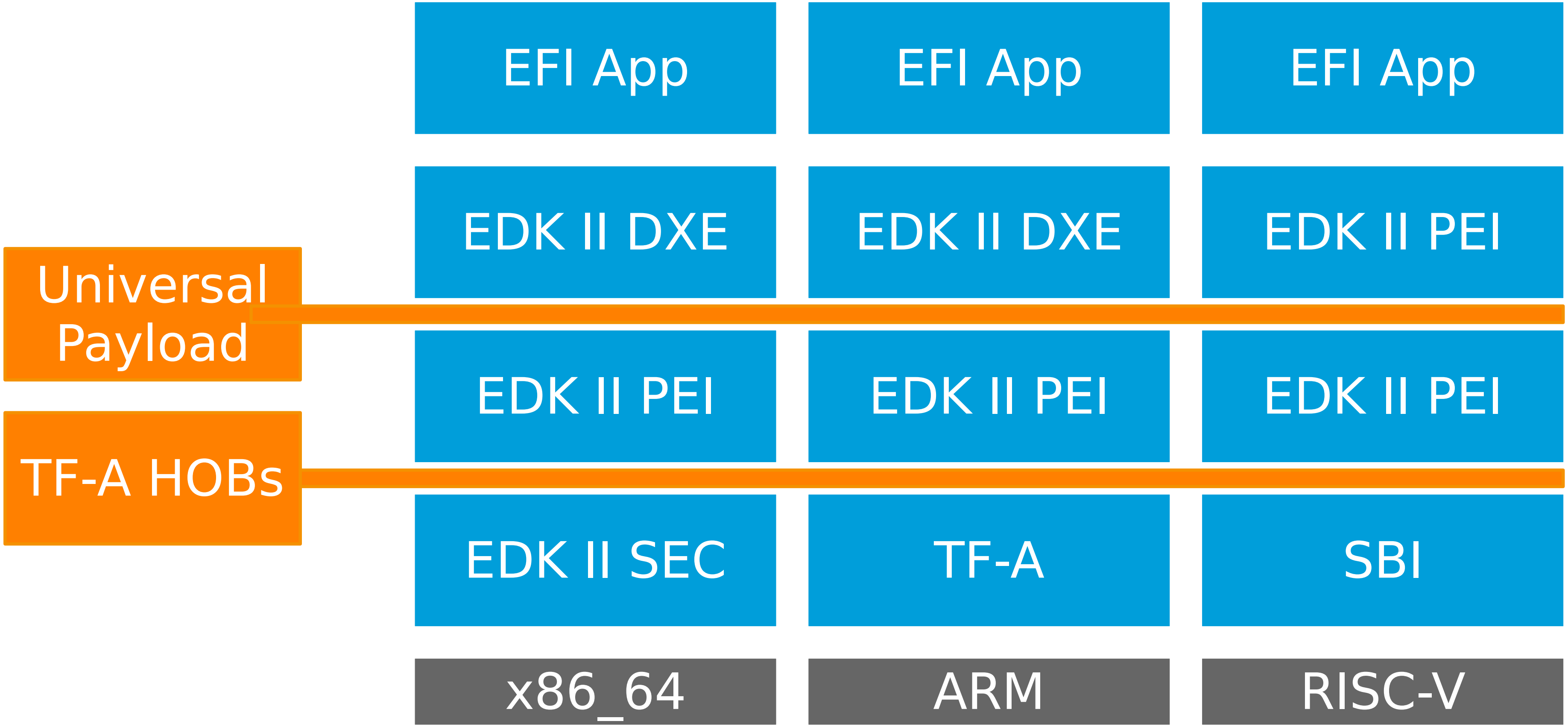
Handoff Between Firmware Stages

Heinrich Schuchardt

UEFI Software Stack

EFI App	EFI App	EFI App
EDK II DXE	EDK II DXE	EDK II PEI
EDK II PEI	EDK II PEI	EDK II PEI
EDK II SEC	TF-A	SBI
x86_64	ARM	RISC-V

Interface Discussions



EFI App | EFI App | EFI App

EDK II DXE | EDK II DXE | EDK II PEI

Universal Payload

EDK II PEI | EDK II PEI | EDK II PEI

TF-A HOBs

EDK II SEC | TF-A | SBI

x86_64 | ARM | RISC-V

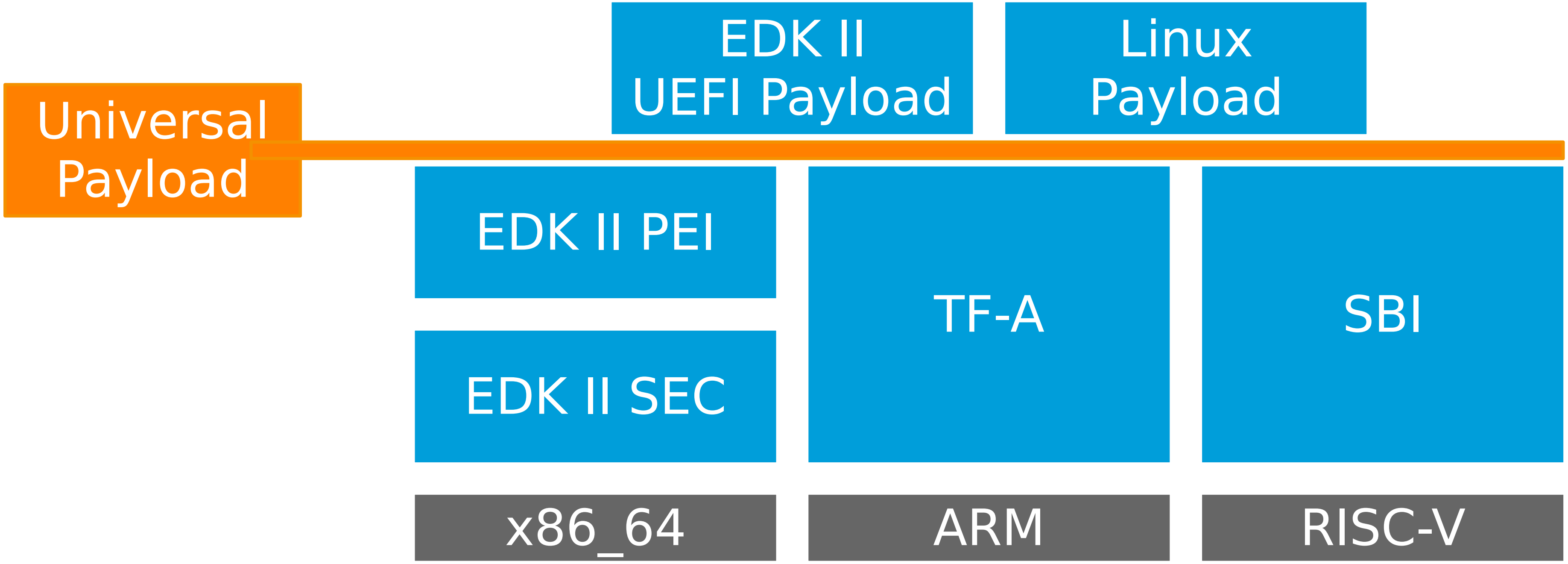
Do We Need a PEI?

Boot Flows

U-Boot SPL	TF-A/SBI	U-Boot	Linux
	TF-A/SBI	Linux	
	TF-A/SBI	LinuxBoot	Linux

TF-A: ARM_LINUX_KERNEL_AS_BL33 option

Interface Discussions



EDK II
UEFI Payload

Linux
Payload

Universal
Payload

EDK II PEI

EDK II SEC

TF-A

SBI

x86_64

ARM

RISC-V

Design Principles

- Execute at minimum privilege level
- Minimize number of software components
- Standardize software interfaces

Backup

Privilege Modes

Ring 3	PL0	EL 0	VU-mode U-mode
Ring 0	PL1	EL 1	VS-mode S-mode
Hypervisor Mode	PL2 (HYP)	EL 2	HS-mode S-mode
System Mgmt Mode	Secure PL1	EL 3	M-mode
x86_64	ARMv7	ARMv8	RISC-V