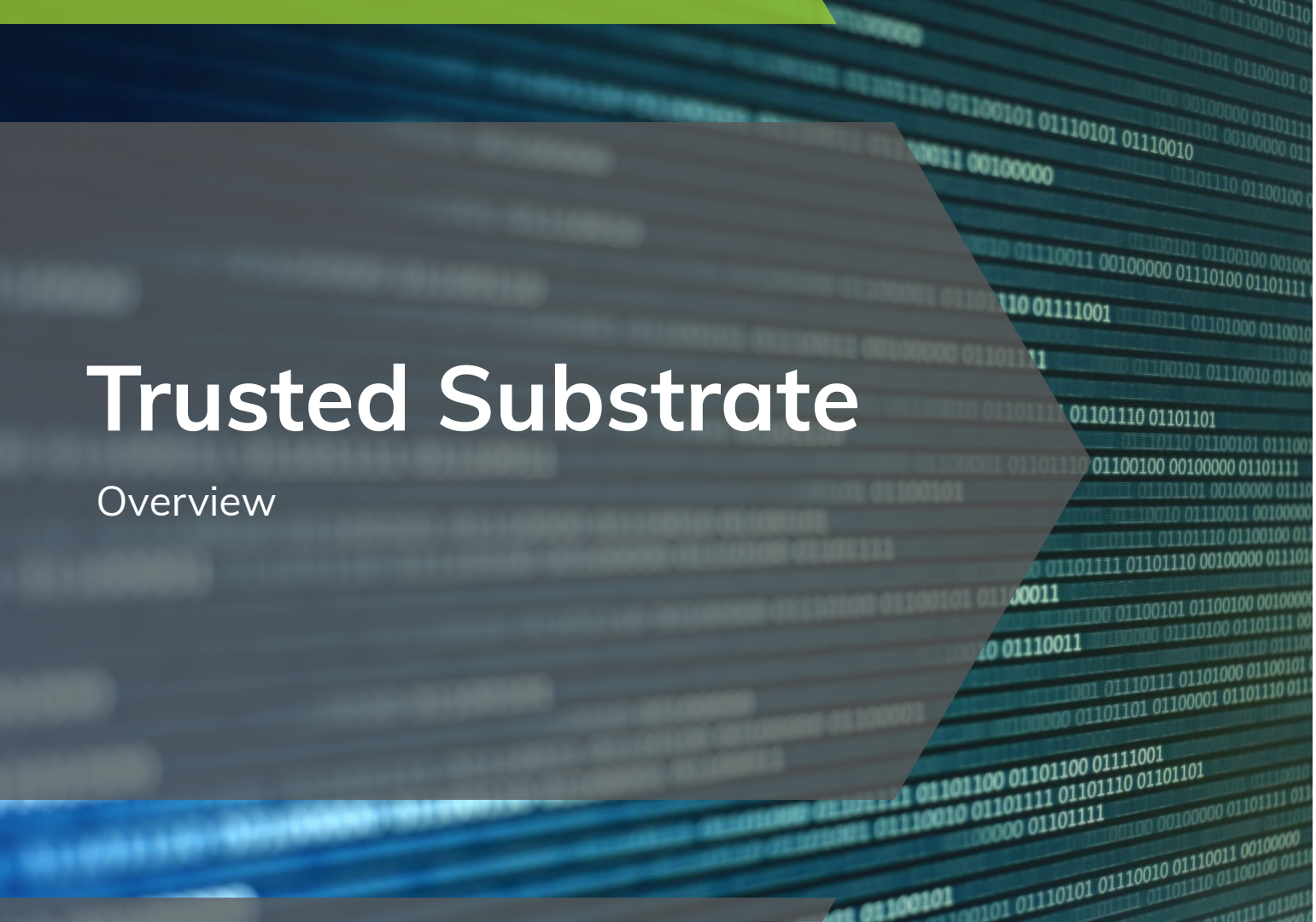
Trusted Substrate

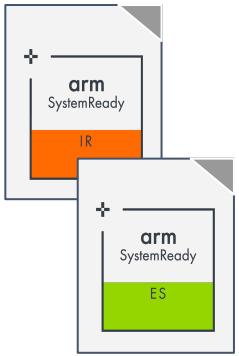
Overview



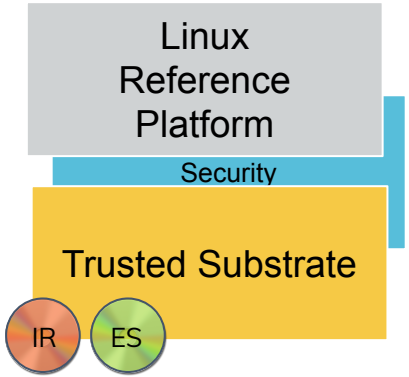
Linaro

Trusted Substrate: the fast path to SystemReady

Marketing program



Specifications &
Test Suite



Reference firmware implementations

Linaro

Simplified sales for ODMs: beyond base specs

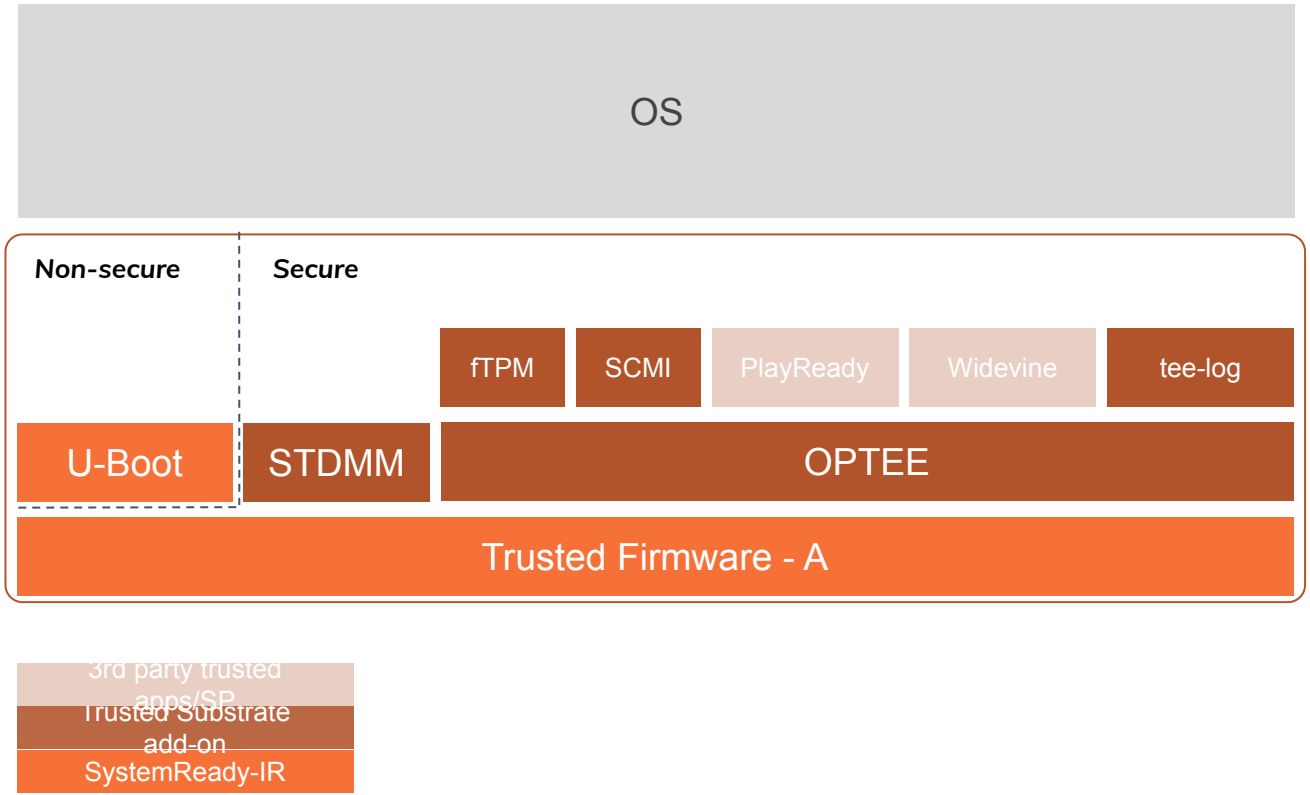
Trusted Substrate - IR = (IoT Ready)

- Arm Cassini related interfaces or recommendations
  - **SystemReady-IR (independent from BSA hardware specifications)**
  - Mandatory Base Board Security Requirements (optional in base SystemReady)
  - Mandatory Arm PSA level 3 readiness (no requirement for this in SystemReady)
- Industry interfaces and recommendations
  - Global Platform (TEE)
  - United Nations vehicle cybersecurity WP.29 readiness
  - USA NIST 800-193 & 800-155 firmware security and update readiness

Trusted Substrate - ES = (Embedded Server)

- Arm & industry interfaces
  - SystemReady-ES
  - Base Board Security Requirements
  - Global Platform (TEE)

Trusted Substrate components



Linaro

Linaro orchestrates integration for ecosystem

Similar to tool chain: integrate interdependent projects that do not synchronize

- Trusted Firmware A
- U-Boot for SystemReady-IR, EDK2 for SystemReady-ES
- OP-TEE plus TEE application catalog (in CI and/or in delivery)
  - firmware tpm
  - SCMI server
  - tee-log

SiPs can leverage Linaro tooling for internal production

Hardware support

In CI

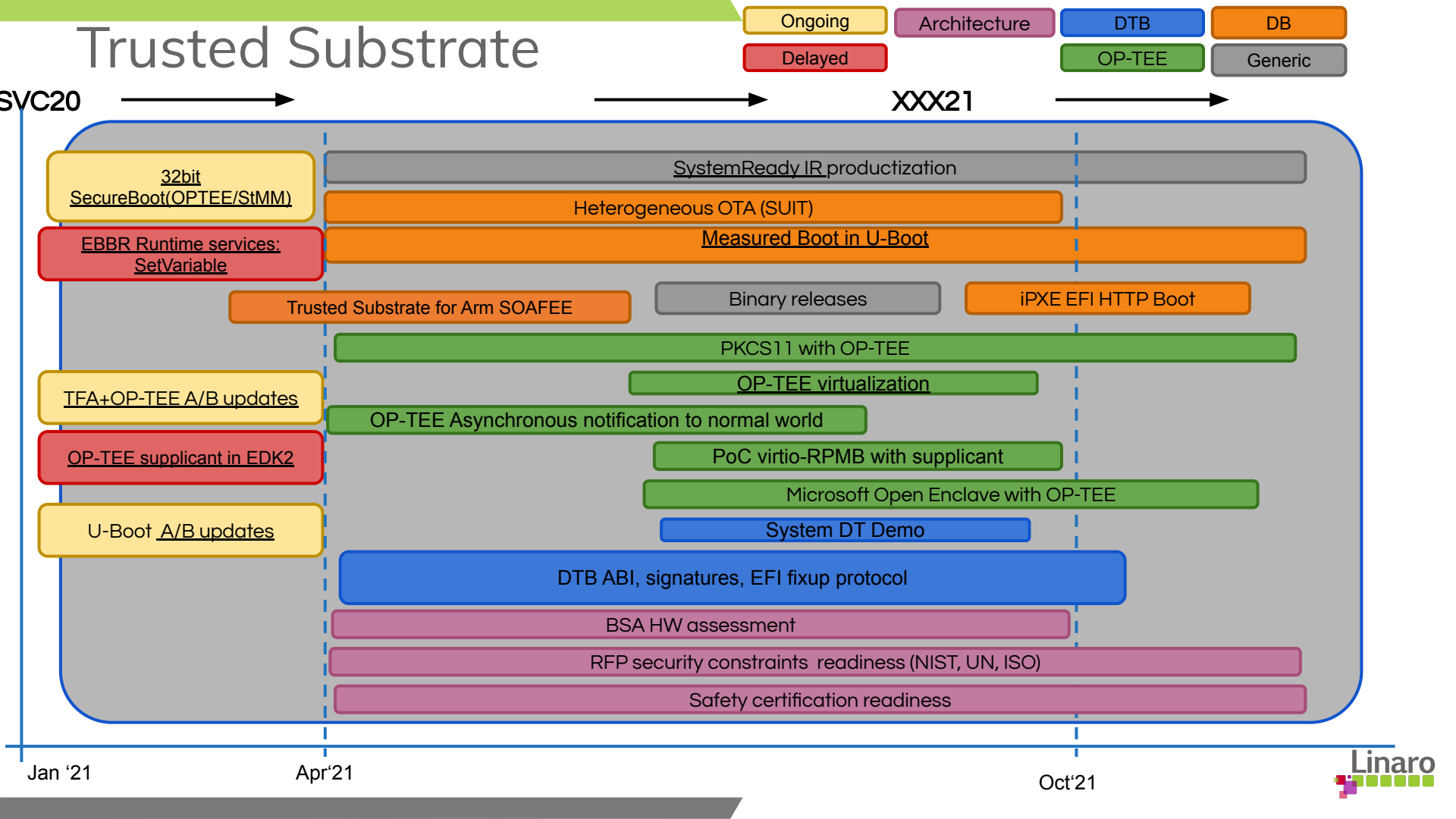
Company	Board	SoC
Socionext	DeveloperBox	SC2A11
QEMU		BSA-ref64
QEMU		x86_64

Company	Board	SoC
Texas Instruments	AM572x	Am57x Sitara
Texas Instruments	Beaglebone-x15	Am57x Sitara
STMicroelectronics	stm32mp157c-dk2	STM32MP157
QEMU		BSA-ref32

To be added

Company	Board	SoC
NXP	LS2160-ARDB	LX2160A
Marvell	EspressoBin	Armada 3700LP
Marvell	MachiattoBin	Armada 8040
SolidRun	Honeycomb	LX2160A
Compulab	IOT-GATE-iMX8	iMX8-mini

Trusted Substrate



Linaro

Thank you