Trusted Substrate
Overview
Trusted Substrate: the fast path to SystemReady

- Marketing program
- Specifications & Test Suite
- Reference firmware implementations

Linux Reference Platform
- Security
- Trusted Substrate
  - IR
  - ES
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

- SystemReady-IR
- Trusted Firmware - A
- U-Boot
- STDMM
- OPTEE
- fTPM
- SCMI
- PlayReady
- Widevine
- tee-log

Non-secure to Secure

3rd party trusted apps/SP
Trusted Substrate add-on
SystemReady-IR
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

<table>
<thead>
<tr>
<th>Company</th>
<th>Board</th>
<th>SoC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Socionext</td>
<td>DeveloperBox</td>
<td>SC2A11</td>
</tr>
<tr>
<td>QEMU</td>
<td></td>
<td>BSA-ref64</td>
</tr>
<tr>
<td>QEMU</td>
<td></td>
<td>x86_64</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Company</th>
<th>Board</th>
<th>SoC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Texas Instruments</td>
<td>AM572x</td>
<td>Am57x Sitara</td>
</tr>
<tr>
<td>Texas Instruments</td>
<td>Beaglebone-x15</td>
<td>Am57x Sitara</td>
</tr>
<tr>
<td>STMicroelectronics</td>
<td>stm32mp157c-dk2</td>
<td>STM32MP157</td>
</tr>
<tr>
<td>QEMU</td>
<td></td>
<td>BSA-ref32</td>
</tr>
</tbody>
</table>

## To be added

<table>
<thead>
<tr>
<th>Company</th>
<th>Board</th>
<th>SoC</th>
</tr>
</thead>
<tbody>
<tr>
<td>NXP</td>
<td>LS2160-ARDB</td>
<td>LX2160A</td>
</tr>
<tr>
<td>Marvell</td>
<td>EspressoBin</td>
<td>Armada 3700LP</td>
</tr>
<tr>
<td>Marvell</td>
<td>MachiattoBin</td>
<td>Armada 8040</td>
</tr>
<tr>
<td>SolidRun</td>
<td>Honeycomb</td>
<td>LX2160A</td>
</tr>
<tr>
<td>Compulab</td>
<td>IOT-GATE-iMX8</td>
<td>iMX8-mini</td>
</tr>
</tbody>
</table>
Trusted Substrate

- **EBBR Runtime services:**
  - SetVariable
- **32bit SecureBoot(OPTEE/SIMM)**
- **Measured Boot in U-Boot**
- **TFA+OP-TEE A/B updates**
- **OP-TEE Asynchronous notification to normal world**
- **OP-TEE virtualization**
- **PKCS11 with OP-TEE**
- **System DT Demo**
- **DTB ABI, signatures, EFI fixup protocol**
- **BSA HW assessment**
- **RFP security constraints readiness (NIST, UN, ISO)**
- **Safety certification readiness**

**SystemReady IR productization**

**Heterogeneous OTA (SUIT)**

**iPXE EFI HTTP Boot**

**Binary releases**

**Microsoft Open Enclave with OP-TEE**

**PoC virtio-RPMB with supplicant**

**System DT Demo**

**Ongoing**

**Architecture**

**DTB**

**OP-TEE**

**Generic**

**Oct'21**

**DB**

**SVC20**

**Trusted Substrate for Arm SOAFEE**

**Binary releases**

**iPXE EFI HTTP Boot**

**U-Boot A/B updates**

**OP-TEE supplicant in EDK2**

**TFA+OP-TEE A/B updates**

**OP-TEE Asynchronous notification to normal world**

**PKCS11 with OP-TEE**

**System DT Demo**

**DTB ABI, signatures, EFI fixup protocol**

**BSA HW assessment**

**RFP security constraints readiness (NIST, UN, ISO)**

**Safety certification readiness**

**Jan '21**

**Apr'21**

**Oct'21**
Thank you