Trusted Substrate Home

About this project

Trusted Substrate is an integrated firmware solution made of all necessary components to implement Arm SystemReady standards with all security options turned on.

Its ambition is to enable industrial grade off-the-shelf operating systems and hypervisors to run as is on compliant platforms and greatly augment supported platforms for vertical market targeted distributions such as Civil Infrastructure Platform, Automotive Grade Linux, OpenIL, Scientific Linux and its derivatives as well as LEDGE Reference Platform and other commercial versions.

SystemReady is very flexible and allows many different cases to be compliant. To achieve its goals in the intended industrial grade context, Trusted Substrate adds requirements to those assumed by SystemReady:

- mandates security option
- requires that UEFI update capsules become the standard vehicle to update any secure or device firmware in the system
- adds anti-rollback and anti-bricking requirements to Over-The-Air updates
- implement Global Platform compliant TEE interface

As a result Trusted Substrate interfaces requires:

- SystemReady compliance
- SystemReady BBSR compliance (optional in the main case)
- PSA Firmware Framework A / in progress Firmware Update specification compliance
- PSCI compliance
- SCMI compliance
- ParSec compliance
- Global Platform TEE compliance
- (future DTE project driven compliance)

In a nutshell, Trusted Substrate complements SystemReady functional aspects of boot, OTA and security with additional functions and add some "security performance" elements.

Trusted Substrate exists in two flavors that complement respective SystemReady counterparts: TrustedSubstrate-IR and TrustedSubstrate-SR:

- TrustedSubstrate-IR implementation is built on Trusted Firmware A, OP-TEE, U-Boot and uses Device Tree as hardware description.

Meetings

See: Trusted Substrate Calendar

SystemReady

Trusted Substrate supported...

Hardware

CI supported

64 bits
• TrustedSubstrate-SR implementation is built on EDK2, OP-TEE and uses ACPI as hardware description (main difference with typical datacenter firmware is the presence of OP-TEE)

The primary goal of the project is to upstream all necessary technologies in a number of open source projects to seed SystemReady compliance. Linaro Edge & Fog computing group hardware as well as Qemu (64 & 32 bits) will be used as reference platforms for the development.

Development of Trusted Substrate is “feature orientated” rather than upstream project orientated. In other words, when a feature is planned, activities in relevant upstream projects is identified and monitored for completion as a whole. Each upstream project has its own roadmap that is not related to SystemReady compliance and independent from other projects. So if you are evaluating what community to join, the decision criteria is whether your goal is holistic or just focused at an individual project.

NOTE: more details on Trusted Substrate: whys, what, how (note: This presentation was produced before SystemReady was announced. a new version will be authored)

Related Linaro software development projects

Trusted Substrate project covers a wide range of software components as stated above. To orchestrate engineering activities in manageable pieces, the development is split between the following projects (Trusted Substrate project leadership ensure coherency and completeness across projects):

• Dependable Boot - ensure SystemReady boot flow conformance across firmware projects (TF-A, OP-TEE, U-Boot, Linux kernel). This project collates work from different teams in Linaro (Kernel Working Group, Security Working Group, LEDGE)
• Device Tree Evolution - efforts to create a System Device Tree that covers asymmetric computing platforms and to change the lifecycle of Device Tree so that it is provided by firmware to operating systems
• Linaro OP-TEE Contributions - while most OP-TEE activities related to SystemReady are guided by Dependable Boot, some long term changes such as Trusted Application lifecycle and distribution scenarios may actually be driven by this project.
• SCMI Server - the service may be hosted in the SCP, as a TA or even as a VM. When it is distributed as a TA or in the SCP firmware, this service is integral part of the Trusted Substrate.

Deliverables

Trusted Substrate project deliverables are upstream patches in many upstream projects. The development is driven by the Linaro projects as said above.

Upstream activity can be found in:

• U-Boot, EDK2
• Trusted-Firmware A, OP-TEE
• Linux kernel
• FreeBSD

Currently TrustedSubstrate-IR for Qemu-BSA 32 bits (U-Boot/DT) and Qemu-BSA 64 bits (EDK2/ACPI and U-Boot/DT) are accessible through the LEDGE Reference Platform downloads.

In the future, and to simplify using Trusted Substrate, a multi-project build repository will be made available as well as binary versions of reference hardware for direct usage.

Services

Linaro is evaluating the opportunity to create SystemReady and Trusted Substrate services such as:

• Board SystemReady-IR readiness, i.e. making sure the board will pass SystemReady-IR certification
• include SystemReady-IR CI/CD loops
• Collaborative maintenance of Trusted Substrate project members defined LTSes (this is very early stages of thinking)

Should you want to have more information or more generally discuss any of the above, please contact us.

Get Involved

• Mailing List
- Linaro Boot Architecture mailing list subscription
- Project membership for roadmap steering and resources allocation
  - Please contact us
- Board integration in CI
  - Please contact us

---

**Structure**

If you get an error message, you can view the structure [here](https://collaborate.linaro.org/plugins/servlet/gadgets/ifr?container=atlassian&amp;amp;lang=en&amp;amp;view=default&amp;amp;view-params=%7B%22writable%22%3A%22false%22%7D&amp;amp;st=atlassian%3Aisw%2F9TmNaY%2BIT5RVByAGqgwkiOoMRlo%2F%7D%7C2BehNxy9Dli9Ka8AzP9CRj7uoYjoEOP0u75BsqiiMwrlzihX876YKoMFC7U5HIPUjgV%7C2FByG1K4Kz28WMJodhZiSPwPmTnt3eVYA2kylpiSHNR82TQGknT0mKeNGKNO%2B5yGdmjy4KcnouRnCItxRFbeQIbweWwPqc4cgg3DlqGQ7MB7CPNbBV0CXNYJw7Q8mig6QLmHkscgVgcvz24SrNgmNWc05LHZw%7D%7Damp;amp;up_structureId=289&amp;amp;up_viewId=10&amp;amp;up_filterId=&amp;amp;up_filterName=&amp;amp;up_customTitle=&amp;amp;up_numRows=15&amp;amp;up_isConfigured=true&amp;amp;up_allowChanges=true&amp;amp;up_useCanvasSettings=false&amp;amp;up_canvas-viewId=&amp;amp;up_canvas-rows=15&amp;amp;up_customTitle=Structure

---

**Backlog**

The following items are on the project backlog but not currently planned. If you are interested in contributing to any of these items, please state your intention on the project's mailing list (found above)

<table>
<thead>
<tr>
<th>key</th>
<th>summary</th>
<th>type</th>
<th>created</th>
<th>updated</th>
<th>due</th>
<th>assignee</th>
</tr>
</thead>
</table>
| ![Jira project doesn't exist or you don't have permission to view it.](https://collaborate.linaro.org/plugins/servlet/gadgets/ifr?container=atlassian&amp;amp;lang=en&amp;amp;view=default&amp;amp;view- params=%7B%22writable%22%3A%22false%22%7D&amp;amp;st=atlassian%3Aisw%2F9TmNaY%2BIT5RVByAGqgwkiOoMRlo%2F%7D%7C2BehNxy9Dli9Ka8AzP9CRj7uoYjoEOP0u75BsqiiMwrlzihX876YKoMFC7U5HIPUjgV%7C2FByG1K4Kz28WMJodhZiSPwPmTnt3eVYA2kylpiSHNR82TQGknT0mKeNGKNO%2B5yGdmjy4KcnouRnCItxRFbeQIbweWwPqc4cgg3DlqGQ7MB7CPNbBV0CXNYJw7Q8mig6QLmHkscgVgcvz24SrNgmNWc05LHZw%7D%7Damp;amp;up_structureId=289&amp;amp;up_viewId=10&amp;amp;up_filterId=&amp;amp;up_filterName=&amp;amp;up_customTitle=&amp;amp;up_numRows=15&amp;amp;up_isConfigured=true&amp;amp;up_allowChanges=true&amp;amp;up_useCanvasSettings=false&amp;amp;up_canvas-viewId=&amp;amp;up_canvas-rows=15&amp;amp;up_customTitle=Structure) View these issues in Jira

---

**Plan of Record**

Attach a PDF to the latest approved PoR

**Health Checks**

Attach a PDF to the project health deck

---

**Documentation**

**Code**

(List of project git repos)