

TrustBox BSP user guide

Description

This technical reference document serves as a guide on how to build and use the BSP for the Scalys TrustBox.



Introduction

This document serves as a technical reference document on how to build the Board Support Package (BSP) for the Scalys TrustBox. It is meant to supplement the available documentation already provided by NXP[1, 2] and Armbian[3]. Armbian is used as a build system and is tested and verified on a specific Ubuntu release only. Thus, the resulting firmware is an Ubuntu-based system with integrated NXP, Microsoft and Scalys components.

The TrustBox features a QorIQ LS1012A processor[4] that contains a single Arm Cortex-A53 core. This document assumes the reader has a basic knowledge of platform software and deployment, and it will not go into too much detail of the actions performed to build the BSPs. This document currently only describes building the Armbian-based BSP. Contact Scalys for more information on the Yocto based Software Development Kit (SDK). Additionally, this document only focusses on a specific release version. Contact Scalys when updates are desired.

Rev	Date	Description
2.1	11 th Feb, 2021	Update build and flash instructions
2.0	22 th Dec, 2020	Updated to Armbian
1.7	2 th Jul, 2020	Update with LSDK 2004 release
1.6	1 th Jun, 2020	Correct standalone u-boot build instructions
1.5	10 th Jun, 2019	RCW section changes
1.4	29 th May, 2019	Improved document structure
1.3	4 th May, 2019	Updated in accordance with new lsd19.03
1.2	18 th Oct, 2018	URL and FAQ update
1.1	28 th May, 2018	FAQ update
1.0	18 th May, 2018	First release

Contents

List of Tables	4
1 Preparation	5
1.1 Install the dependencies using the package manager	5
1.2 Git setup	5
2 Building images	6
2.1 Quick start with Armbian	6
2.1.1 Building image	6
2.2 Standalone Linux kernel build	8
3 Firmware components	9
3.1 U-Boot	9
3.1.1 Standalone U-boot build	9
3.2 Reset Configuration Word	9
3.2.1 Modifying the Reset Configuration Word	9
4 TrustBox flash configuration	11
4.1 Primary flash partitioning	11
4.2 Rescue flash partitioning	12
5 Installing and updating images	13
5.1 Flashing/updating the the SD card	13
5.2 Updating partitions on the primary flash	13
5.3 Recovering from the rescue flash	14
6 Configuration necessary for a TFTP boot	15
6.1 TFTP server installation and configuration	15
6.2 DHCP Server installation and configuration	16
7 Frequently asked questions	17
7.1 What is the default login of the Armbian?	17
7.2 How to connect to the TrustBox?	17
7.2.1 Serial port connection	17
7.2.2 SSH connection	17
7.3 Why doesn't my TrustBox seem to accept my commands on the serial port?	17
7.4 Why doesn't my TrustBox produce any output data on the serial interface?	18
7.5 The ethernet interfaces of the Packet Forwarding Engine (PFE) are not working?	18
7.6 Bluetooth can't find any devices?	18
7.7 PPA related kernel crash	19
A References	20
B List of Acronyms	21

List of Tables

4.1 Primary NOR flash Partitioning	12
--	----

1

Preparation

This document assumes the system used to build the BSP is a newly installed OS.

The presented build process has been verified on Ubuntu 20.04 host system. On other systems it is possible to use Armbian docker containerisation capabilities to run a build implicitly inside of an Ubuntu 20.04 builder container.

1.1 Install the dependencies using the package manager

A list of additional packages used throughout this user guide are as follows:

- curl
- git
- gawk
- wget
- tftpd
- tftp
- isc-dhcp-server
- nfs-kernel-server
- gcc-aarch64-linux-gnu
- device-tree-compiler
- libncurses5-dev
- libncursesw5-dev
- docker.io

You can install them through your package manager using the following command:

```
sudo apt-get install curl git gawk wget tftpd tftp isc-dhcp-server nfs-kernel-server \  
gcc-aarch64-linux-gnu docker.io device-tree-compiler libncursesw5-dev libncurses5-dev
```

1.2 Git setup

```
# Setup username and email for git if not already done  
git config --global user.name "Your Name"  
git config --global user.email "user@example.com"
```

2

Building images

2.1 Quick start with Armbian

2.1.1 Building image

The following guide primarily follows the steps given in an Armbian documentation. More in-depth information regarding an Armbian build environment can be found in the Armbian manual[3].

Note: this document describes a manual BSP image build. Unless you are interested in modifying sources, binary pre-build SD card images available at <https://scalys.com/downloads> (see Scalys pre-build BSP releases) can be used.

In this section we will build our Armbian image which includes the Linux kernel, device tree, Root File System (RFS) and firmware binaries. Note that only a subset of the default Armbian builder commands is supported for the TrustBox.

1. Begin with creating a working directory in your home directory:

```
mkdir -p ~/trustbox/ && cd ~/trustbox
```

2. Setup Docker on the host machine. If not already installed, then do so from your package manager. Add your user to the docker group.

```
sudo addgroup --system docker  
sudo usermod -aG docker <accountname>  
sudo gpasswd -a <accountname> docker  
sudo service docker restart
```

Make sure to logout once to apply the changes to your user.

3. Clone *bsp-armbian* repository from the Scalys github page to your working directory:

```
git clone https://github.com/Scalys/bsp-armbian.git -b armbian-2012 && cd bsp-armbian
```

4. Build the BSP.

Build BSP within docker build environment:

```
./compile.sh docker BOARD=trustbox
```

It is also possible to run build directly on a host system. But it should be noted that build procedure is tested on a Ubuntu host system and will try to install missing packages if there are any. To run build natively:

```
./compile.sh BOARD=trustbox
```

Refer to the Armbian documentation [5] to get more details about build options. Now that we have an image prepared, we have the option to go directly to [section 5.1](#) in order to prepare the SD card for the TrustBox or continue with the following sections to build manually U-boot and the Linux kernel manually if more in-depth customization is required.

Note: to add customize default packages included into the Ubuntu build modify the '*configs/boards/trusbox.csc*'.

2.2 Standalone Linux kernel build

Modifying the Linux kernel to your requirements is recommended to do within the Armbian builder. Refer to the Armbian documentation [3] to get more details on how to accomplish this. In this section we will show how to build a Linux kernel in a stand-alone fashion.

Start by cloning the correct Linux kernel repository (with the appropriate branch) from the Scalys github page. For this example we take the kernel used in the Layerscape Software Development Kit (LSDK) with the TrustBox patches, so make sure you also use the associated RFS for it to work.

```
git clone https://github.com/Scalys/linux-qoriq.git -b trustbox-2012 && cd linux-qoriq/
```

Configure the kernel:

```
CROSS_COMPILE=aarch64-linux-gnu- ARCH=arm64 make defconfig lsdk.config trustbox.config
```

Optionally, we can now configure and modify the kernel manually with:

```
CROSS_COMPILE=aarch64-linux-gnu- ARCH=arm64 make menuconfig
```

Build the kernel:

```
CROSS_COMPILE=aarch64-linux-gnu- ARCH=arm64 make -j 8
```

Install the generated files in the RFS, e.g. on the SD card:

```
sudo cp Image <path_to_rfs>/boot/Image  
sudo cp arch/arm64/boot/dts/freescale/trustbox.dtb <path_to_rfs>/boot/trustbox.dtb  
sudo CROSS_COMPILE=aarch64-linux-gnu- ARCH=arm64 make INSTALL_MOD_PATH=<path_to_rfs> modules_install
```


3

Firmware components

3.1 U-Boot

3.1.1 Standalone U-boot build

Download the Scalys U-boot repository:

```
git clone --recursive https://github.com/Scalys/u-boot-qoriq.git -b trustbox-2004 && cd u-boot-qoriq
```

Update external submodules:

```
git submodule update --init --recursive
```

Choose the corresponding TrustBox configuration:

```
ARCH=aarch64 CROSS_COMPILE=aarch64-linux-gnu- make trustbox_qspi_defconfig
```

Optionally run menuconfig and change any options you need:

```
ARCH=aarch64 CROSS_COMPILE=aarch64-linux-gnu- make menuconfig
```

Build U-boot image:

```
ARCH=aarch64 CROSS_COMPILE=aarch64-linux-gnu- make -j 8
```

3.2 Reset Configuration Word

The LS1012A processor requires a valid Reset Configuration Word (RCW) in order to be successfully initialized at boot time. The current revisions of the processor support reading the RCW from two sources only. Namely an external QSPI flash device and an internal hardcoded source. The TrustBox by default selects the QSPI device as the RCW source. The RCW is a set of 64 bytes, which define how the LS1012A and its interfaces are configured. The Pre-Boot Loader (PBL) reads these 64 bytes along with any appended Pre-Boot Instructions (PBI) from the chosen source.

The TrustBox by default comes with an RCW configuration with the following main features:

- SATA configuration on the M.2. port;
- I2C and DSPI configured on the 26-pins header.

3.2.1 Modifying the Reset Configuration Word

When the default RCW options are not sufficient it is possible to modify it.

1. Download bootloader sources as described in subsection 3.1.1;
2. Modify the RCW source file located at *board/scalys/trustbox/rcw.cfg* with the settings you need (at your own risk!);
3. Build the standalone U-boot binary;

4. Update bootloader firmware by following the [section 5.2](#) (*u-boot-with-spl-pbl.bin* binary should be renamed to *u-boot-with-pbl.bin*).

4

TrustBox flash configuration

4.1 Primary flash partitioning

The primary NOR flash has been partitioned into the following functional parts:

u-boot

Partition containing the PBL (RCW + PBI), SPL, and U-boot bootloader

env

Environment settings as used in U-boot

pfe

Primary firmware for the PFE under U-boot

ppa

Primary Protected Application (PPA) firmware.

spl_hdr

SPL header for secure boot

u-boot_hdr

U-boot header for secure boot

pfe_hdr

PFE header for secure boot

ppa_hdr

PPA header for secure boot

itb_hdr

Image Tree Blob header for secure boot

itb

Image Tree Blob header for placing the a small RFS

The partitioning may be modified to fit a specific application, as long as the requirement is met for the PBL binary to start at address 0x0. Altering these partitions requires updates to the offset(s) defined within the PBI and/or U-boot.

Table 4.1: Primary NOR flash Partitioning

No.	Name	Size	Offset
0	u-boot	0x00200000	0x00000000
1	env	0x00040000	0x00200000
2	pfe	0x00040000	0x00240000
3	ppa	0x00100000	0x00280000
4	spl_hdr	0x00040000	0x00380000
5	u-boot_hdr	0x00040000	0x003c0000
6	pfe_hdr	0x00040000	0x00400000
7	ppa_hdr	0x00040000	0x00440000
8	itb_hdr	0x00040000	0x00480000
9	itb	0x03b40000	0x004c0000

```
mtddparts: mtdparts=1550000.quadspi:2M@0x0 (u-boot) , 256k (env) , 256k (pfe) , 1M (ppa) , 256k (u-boot_hdr) , 256k (pfe_hdr) , 256k (ppa_hdr) , - (UBI)
```

4.2 Rescue flash partitioning

The rescue flash is read-only by default and contains a U-boot binary to recover the Trustbox primary flash. It also holds unique board configuration data, such as MAC addresses and manufacturing data. Contact Scalys for more information regarding the rescue flash memory.

5

Installing and updating images

5.1 Flashing/updating the the SD card

By default TrustBox will attempt to boot the Linux kernel from an SD card. Without modification it requires the first partition to be formatted as an *ext4* filesystem. Firmware image built in previous steps already has all needed partitions. You can write it with, for instance, the *dd* command line tool or the *Balena Etcher*, *USBImager* tools.

Find the block device of your SD card <DEV> (e.g. /dev/sda). If it mounted, unmount it:

```
sudo umount <DEV>
```

Next, go to your BSP directory and run the following in order to write image to SD card:

```
sudo dd if=output/images/trustbox-armbian-<version>.img of=<DEV> bs=4M conv=sync status=progress
```

After any major firmware update it is important to ensure that binary firmware (u-boot, pfe, ppa) are up to date. For that on the first boot with the updated SD card image stop the boot process during countdown in bootloader and perform:

```
run update_mmc_uboot_qspi_nor
run update_mmc_ppa_qspi_nor
run update_mmc_pfe_qspi_nor
reset
<once again stop boot during countdown>
env default -a
saveenv
reset
```

5.2 Updating partitions on the primary flash

The default U-boot image on the TrustBox has a set of environment variables to update the partition data in the primary flash memory from external sources. The default supported sources are:

tftp

Refer to [section 6.1](#) to setup the TFTP server.

mmc

By default the variables expect the first partition on the SD card to be formatted with an *ext4* filesystem.

usb

By default the variables expect the first partition on the USB memory stick to be formatted with a *ext4* filesystem.

If the updated files are put in a subdirectory on the source then you have to ensure that the '*update_files_path*' U-boot environment variable is matched correctly. By default this variable is set to '.'. It can be modified using the '*editenv*' command in U-boot.

Updating the *u-boot* target partition requires the file named '*u-boot-with-pbl.bin*' to be available on the chosen file source. The *ppa* target partition requires the file named '*ppa.itb*', and the *pfe* target partition requires the file named '*pfe_fw_sbl.itb*'^[6]. The *image* target requires the file named *trustbox_qspi_fw.itb*, it consists of a composite firmware (contains u-boot, pfe and ppa partitions) that could be generated in LSDK.

Each of these variables can be executed using the following command:

```
run update_<source>_<target>_qspi_nor
```

These variables can be modified to change the partition index or filesystem type using the U-boot *editenv <variable>* command.

5.3 Recovering from the rescue flash

The primary flash memory data may become corrupted during usage. The TrustBox therefore includes a back-up U-boot image on a read-only rescue flash memory, that may be used to write correct data onto the primary flash memory¹. To boot from this rescue flash the following two steps should be performed:

1. Connect the TrustBox to your host PC and open the terminal application.
2. Press and hold switch 'S2' on the TrustBox.
3. Power-up (or reset with switch 'S1') the TrustBox.
4. Release switch 'S2' once U-boot prints the message: '*Please release the rescue mode button (S2) to enter the recovery mode*'. Note that this will take a few seconds as this rescue flash is slower.

After performing these steps the user should be able to program the primary flash memory using the commands described in the previous [section 5.2](#).

¹Note that when burning specific secure boot fuses that this feature will become inaccessible unless the contents of the write protected rescue flash are updated

6

Configuration necessary for a TFTP boot

These steps are optional and only necessary when the target is connected directly to the computer used to build the BSP.

6.1 TFTP server installation and configuration

Install the TFTP server (if not already done):

```
sudo apt-get install tftpd-hpa
```

Enable and start *tftpd-hpa* service:

```
sudo systemctl enable --now tftpd-hpa
```

The default TFTP data folder is */srv/tftp* (it will be created automatically).

Warning: TFTP has no security so be aware this folder is NOT SECURE!

6.2 DHCP Server installation and configuration

Install the DHCP server (if not already done):

```
sudo apt-get install isc-dhcp-server
```

edit the '/etc/network/interfaces' file, where 'eth1' is the chosen interface to the board:

```
# Make sure the network ranges match your host system!  
auto <interface>  
allow-hotplug <interface>  
iface <interface> inet static  
address 192.168.1.1  
netmask 255.255.255.0
```

and edit the '/etc/dhcp/dhcpd.conf' file:

```
default-lease-time 600;  
max-lease-time 7200;  
  
# Optionally, we can assign static addresses for the targets  
host <target_hostname> {  
    hardware ethernet 00:11:22:33:44:55;  
    fixed-address 192.168.1.180;  
}  
  
subnet 192.168.1.0 netmask 255.255.255.0 {  
    range 192.168.1.150 192.168.1.200;  
    option routers 192.168.1.254;  
    option domain-name-servers 192.168.1.1, 192.168.1.2;  
}
```

Specify the interface in the '/etc/default/isc-dhcp-server' file:

```
INTERFACES="<interface>"
```

Restart the DHCP service.

```
sudo service isc-dhcp-server restart
```


7

Frequently asked questions

7.1 What is the default login of the Armbian?

The default login is *root* with the password *1234*. You will be prompted to change this password at first login. You will then be asked to create a normal user account that is sudo enabled.

7.2 How to connect to the TrustBox?

7.2.1 Serial port connection

Connect the TrustBox to your host PC with the micro usb port. Verify that a serial device has been successfully added. Note that for Windows 10 based hosts you may have to manually install the drivers from: <https://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers>. Using your favourite terminal program, e.g. PuTTY for Windows or Minicom/Kermit for Linux, you have to open the connection with the serial device with the following settings: *115200 8N1 with no flow control*.

7.2.2 SSH connection

There are several ways to achieve this, but for simplicity we will chose a setup without a DHCP server in the network. Note that by default this connection does not allow access to the U-boot bootloader.

Using the serial connection described subsection 7.2.1 you should configure the ethernet interface on your TrustBox with a static IP in the address range of your dedicated network port on your host PC. To do this we can add the following lines in the `/etc/network/interfaces` file:

```
auto eth0
allow-hotplug eth0
iface eth0 inet static
address 192.168.1.100
netmask 255.255.255.0
```

Now configure the network interface of your host PC with the 192.168.1.1 address and connect it directly to the TrustBox. Verify that it works by pinging the TrustBox's address. Note that it may takes several seconds for the TrustBox to boot completely before the SSH service become available. Once successfully connected we can open the SSH connection using PuTTY (under Windows) or the SSH command under Linux with the chosen TrustBox's address.

7.3 Why doesn't my TrustBox seem to accept my commands on the serial port?

As mentioned in subsection 7.2.1, make sure to have the correct serial settings and ensure that you have flow control set to none. For instance, in PuTTY you can achieve this as shown in figure 7.1 below.

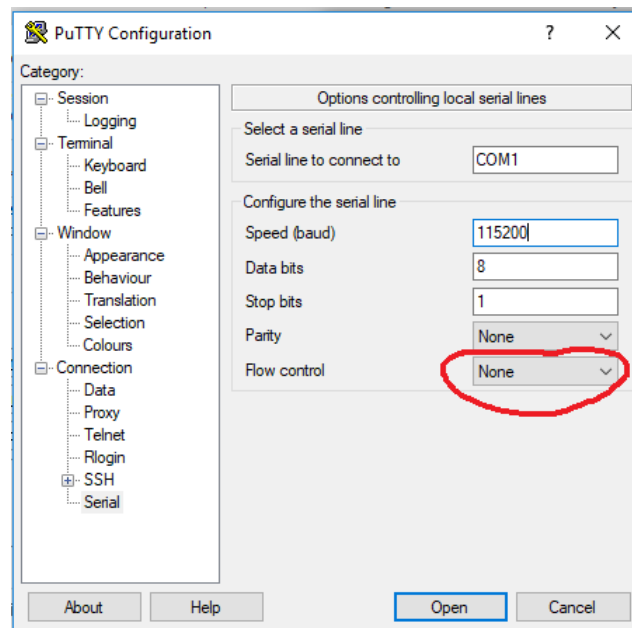


Figure 7.1: Flow control setting in PuTTY

7.4 Why doesn't my TrustBox produce any output data on the serial interface?

Firstly make sure you have the correct power supply for the TrustBox, or else it might not boot fully. Even though the green power LED is lit it might not be enough for all the interfaces on the TrustBox. Refer to the TrustBox User manual for specific information on the power supply.

Next we should also rule out any problem with the serial interface configuration. Refer to subsection 7.2.1 for more information.

One last option would be to verify that the rescue boot mode doesn't produce any output either. Refer to section 5.3 on how to achieve this. If this works then try reprogramming the primary flash from this rescue boot.

If none of these steps work then contact Scalys to resolve your issue.

7.5 The ethernet interfaces of the PFE are not working?

The PFE on the LS1012A processor requires firmware to operate. For U-boot it requires the '*pfe_fw_sbl.itb*' image (see section 5.2 on how to program it) and under Linux the '*ppfe_class_ls1012a.elf*' and '*ppfe_tmu_ls1012a.elf*' files in the '*/lib/firmware/*' directory. These files can be retrieved from the LSDK github page[7]. **Note that it is required to execute the command '*pfe stop*' in U-boot before booting a Linux kernel.** This has already been included for the default boot command(s) of the TrustBox.

7.6 Bluetooth can't find any devices?

The default bluetooth kernel driver doesn't initialize the RF-component of the combined WiFi/BT module properly. You first need to initialize it through the WiFi driver, e.g.:

```
ifconfig <wlXXXXXXXXXXXX> up
```

7.7 PPA related kernel crash

Note that the kernel expects a valid PPA firmware to be available to boot successfully. A default PPA image is included in the Armbian image and can be programmed in the primary flash under U-boot.

```
run update_<source>_ppa_qspi_nor
```

A

References

- [1] *SDK QorIQ online manual*. [Online]. Available: https://nxp.sdlproducts.com/LiveContent/web/pub.xql?c=t&action=home&pub=QorIQ_SDK&lang=en-US
- [2] *LSDK online manual*. [Online]. Available: https://nxp.sdlproducts.com/LiveContent/web/pub.xql?c=t&action=home&pub=LSDKUG_Rev19.03&lang=en-US
- [3] *Armbian Documentation*. [Online]. Available: https://docs.armbian.com/Developer-Guide_Build-Preparation/
- [4] *QorIQ® Layerscape 1012A Low Power Communication Processor*. [Online]. Available: <https://www.nxp.com/products/processors-and-microcontrollers/arm-based-processors-and-mcus/qorIQ-layerscape-arm-processors/qorIQ-layerscape-1012a-low-power-communication-processor:LS1012A>
- [5] *Armbian build options*. [Online]. Available: https://docs.armbian.com/Developer-Guide_Build-Options/
- [6] *Layerscape Software Development Kit github page*. [Online]. Available: <https://lsdk.github.io/>
- [7] *Layerscape Software Development Kit download link (requires registration)*. [Online]. Available: https://www.nxp.com/design/software/embedded-software/linux-software-and-development-tools/layerscape-software-development-kit:LAYERSCAPE-SDK?&tab=Design_Tools_Tab#nogo

B

List of Acronyms

BSP Board Support Package

LSDK Layerscape Software Development Kit

PBI Pre-Boot Instructions

PBL Pre-Boot Loader

RFS Root File System

RCW Reset Configuration Word

SDK Software Development Kit

PFE Packet Forwarding Engine

PPA Primary Protected Application