This document instructs how to deploy Smaug v1.0 in Android environment.

The configurations of the hardware/software used in our deployment are listed below.

- Ubuntu20.04
- Python3.8
- Python2.7
- GCC 9.4.0
- Android 9.0.0_r34
- OP-TEE 3.8.0
- Smaug v1.0
- Hikey620 with 8GB eMMC

Prerequisites

The following additional are needed. Please install them.

```
$ sudo apt install \
  android-tools-adb \
  android-tools-fastboot \
  autoconf \
  automake \
  bc \
  bison \
  build-essential \
  ccache \
  cscope \
  curl \
  device-tree-compiler \
  expect \
  flex \
  ftp-upload \
  gdisk \
  iasl \
  libattr1-dev \
  libcap-dev \
  libfdt-dev \
  libftdi-dev \
  libglib2.0-dev \
  libgmp3-dev \
  libhidapi-dev \
  libmpc-dev \
  libncurses5-dev \
  libpixman-1-dev \
  libssl-dev \
  libtool \
  make \
  mtools \
  netcat \
  ninja-build \
  python3-crypto \
  python3-cryptography \
  python3-pip \
  python3-pyelftools \
  python3-serial \
  rsync \
  unzip \
  uuid-dev \
  xdg-utils \
  xterm \
  xz-utils \
  zlib1g-dev
```

First, it needs to synchronize all the code of AOSP with OP-TEE. Reference link.

```
git clone https://github.com/linaro-swg/optee_android_manifest [-b <release_tag>]
# release tags come in the form of X.Y.Z, e.g. 3.8.0
$ cd optee_android_manifest
$ ./sync-p.sh
```

Build instructions

Need to switch python from python3 to python2. Also need to install pycryptodome for python2.

```
$ pip2 install pycryptodome
```

The code in several files needs to be modified to correct compilation errors.

- Edit /optee_android_manifest/device/linaro/bootloader/edk2/BaseTools/Source/C/GenVtf/GenVtf.c: Replace both strncpy() calls with memcpy(). Reference: [OE-core] [PATCH 3/4] ovmf: Fix build with gcc8

```
@@ -129,9 +129,9 @@ Returns:
   } else {
     Length = strlen(Str);
     if (Length < 4) {
-      strncpy (TemStr + 4 - Length, Str, Length);
+      memcpy (TemStr + 4 - Length, Str, Length);^M
     } else {
-      strncpy (TemStr, Str + Length - 4, 4);
+      memcpy (TemStr, Str + Length - 4, 4);^M
     }

     sscanf (
@@ -1529,7 +1529,7 @@ Returns:
   //
   FitStartPtr = (FIT_TABLE *) RelativeAddress;

-  strncpy ((CHAR8 *) &FitStartPtr->CompAddress, FIT_SIGNATURE, 8);  // "_FIT_   "
+  memcpy ((CHAR8 *) &FitStartPtr->CompAddress, FIT_SIGNATURE, 8);  // "_FIT_   "
   assert (((VtfInfo->CompSize & 0x00FFFFFF) % 16) == 0);
   FitStartPtr->CompSize     = (VtfInfo->CompSize & 0x00FFFFFF) / 16;
```

- Edit /optee_android_manifest/optee/optee_os/scripts/sign_encrypt.py:

```
@@ -128,9 +128,9 @@ def get_args(logger):


 def main():
-    from Cryptodome.Signature import pss
-    from Cryptodome.Hash import SHA256
-    from Cryptodome.PublicKey import RSA
+    from Crypto.Signature import pss
+    from Crypto.Hash import SHA256
+    from Crypto.PublicKey import RSA
     import base64
     import logging
     import os:q
```

- Add or change file into /optee/optee_os and /external/optee_client.
- Edit /optee_android_manifest/external/optee_client/tee-supplicant/tee_supplicant_android.mk:

```
@@ -23,7 +23,15 @@ LOCAL_SRC_FILES += src/handle.c \
                    src/tee_supp_fs.c \
                    src/tee_supplicant.c \
                    src/teec_ta_load.c \
-                   src/rpmb.c
+                   src/rpmb.c \
+                   src/tee_tpm.c \
+                   src/smaug_guorui.c \
+                   src/sqlite3.c \
+                   src/defs.c \
+                   src/dbqueue.c \
+                   src/mhtdefs.c \
+                   src/mhtfile.c \
+                   src/tee_supp_tzvfs.c

@@ -50,9 +58,10 @@ endif

 LOCAL_C_INCLUDES := $(LOCAL_PATH)/../public \
                     $(LOCAL_PATH)/../libteec/include \
-                    $(LOCAL_PATH)/src
+                    $(LOCAL_PATH)/src \
+                    $(LOCAL_PATH)/../../boringssl/include

-LOCAL_SHARED_LIBRARIES := libteec
+LOCAL_SHARED_LIBRARIES := libteec libcrypto
```

- Add Smaug files and my_test files in /external.
- Edit /optee_android_manifest/device/linaro/hikey/optee-packages.mk:

```
@@ -68,3 +68,10 @@ PRODUCT_PACKAGES += dba51a17-0563-11e7-93b1-6fa7b0071a51.ta
 PRODUCT_PACKAGES += 4d573443-6a56-4272-ac6f-2425af9ef9bb.ta
 PRODUCT_PACKAGES += wait_for_keymaster_optee
 PRODUCT_PACKAGES += KMGK_gtest
+
+#smaug
+PRODUCT_PACKAGES += smaug
+PRODUCT_PACKAGES += 1111fadd-99d5-4afb-a1dc-ee3e9c61b04d.ta
+
+#my_test
+PRODUCT_PACKAGES += 9aaaf200-2450-11e4-abe2-0002a5d5c51b.ta
```

In HiKey-620 8G:

```
$ ./build-p.sh
```

Flashing the image

The instructions for flashing the image can be found in detail under device/linaro/hikey/installer/hikey/README in the tree.

1. Set jumpers/switches 1-2 and 3-4, and unset 5-6.
2. Reset the board. After that, invoke:

```
$ sudo ./device/linaro/hikey/installer/hikey/flash-all.sh /dev/ttyUSBn
```