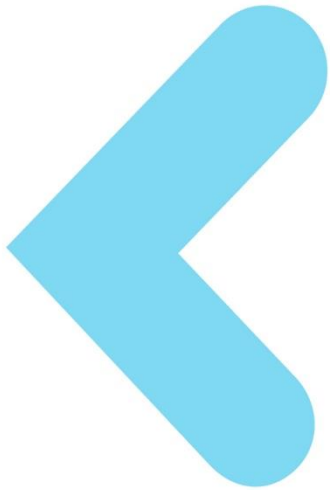
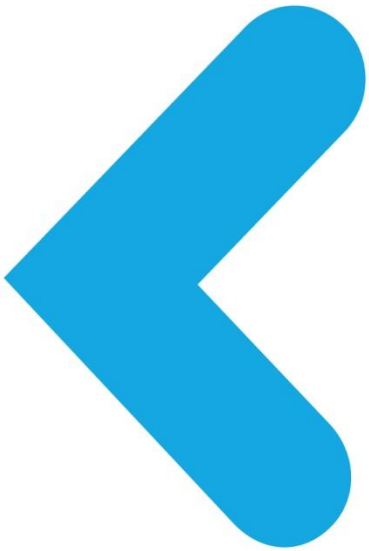
TRUSTONIC



Kinibi Integration Guide



PREFACE

DOCUMENT HISTORY

Date	Modification
January 5th, 2013	First version
May 22nd, 2013	Update for Kinibi-202
November 21st, 2013	Updated for Kinibi-300
June 9th, 2014	Updated for Kinibi-301
December 1st, 2014	Updated for Kinibi-302A: Integration information for Android 64 bit OS added Android CTS waiver information and SEAndroid information added. General improvements. Fix the paths of the Tui components. Remove sections about DrSecureStorage Detail on Registry and Factory Reset. Added missing information for the location of the keymaster in the Android File System. Fixed the error codes returned by the DRM driver. Security warnings added in TUI integration sections
February 19th, 2015	Updated for Kinibi-303A Updated permissions for the mcRegistry directories. TUI normal world architecture change to optimize memory consumption.
August 12th, 2015	Updated for Kinibi-310A: - Remove kernel module `MobicoreKernelApi` - Update kernel Makefile and Kconfig options - Add ueventd information for TUI driver - Add a new debugfs directory `trustonic_tee` for system debugging - Document FIQ forward
October 27th, 2015	Updated for Kinibi-310B: - Add Android SE Proxy - Add Android Keymaster M and Gatekeeper support - New entries in debugFS - IRAM support

February 9th, 2016	Updated for Kinibi-310C: - Add standalone Android SE Proxy
March 30th, 2016	Updated for Kinibi-311A: - Add Android M Verified Boot - Add Rollback Protected Storage - Add tee-ps tool for performance analysis and post-mortem debug -Add missing TUI HAL functions
May 19th, 2016	Fixed the number of instances of the Keymaster TA.
May 24th, 2016	Remove all mentions of TeeAuthService
May 30th, 2016	Add information about the Normal World daemon's light mode for recovery
June 6th, 2016	The number of threads of the TUI driver can be 5 or 6.
July 27th, 2016	Update for Android Nougat
September 9th, 2016	Added guidance on checking the Kinibi version Updated the Chapter on Validating the product to include Kinibi version verification check.
September 28th, 2016	Updated for Kinibi-400A: - Add System TA Downgrade Protection to Rollback Protection - Changes in NWd for access to /efs and multi-partition support - Add TEE Image Builder - Add ATF fastcalls for GlobalPlatform compliance
December 9th, 2016	Added System TA Downgrade Protection disable option
February 28th, 2017	Added System TA Downgrade Protection diagram and behavior without -dp flag.
June the 22nd, 2017	Xen integration patches and Yocto build information added

June 23rd, 2017	Adding Blacklist feature description
October 31st, 2017	RPMB changes for Kinibi-400b
November 24, 2017	Update SEAndroid section for Android O
March 22, 2018	Updated for Kinibi 410A: - Image Builder support - Remove support for Keymaster - Remove support for IRAM - Remove support for fastcall identity mapping
April 17, 2018	Review following 1st k-410 deliveries: - Review of Image Builder and integration into SWd components - FastCall Hook/u-boot integration section cleanup - System Debug completed with TEE Kernel halt dump
July 5, 2018	Updated for 2nd Kinibi-410 delivery: - Add changes for Android P HIDL services and SELinux - Add Key injection process for System TA encryption - Move System Debug into proper document - Add mcDriverDaemon usage
August 1, 2018	Updated for Android P delivery - Add changes in device.mk and BSP

TABLE OF CONTENTS

LIST OF FIGURES

1 INTRODUCTION

This document explains how to integrate Trustonic's Kinibi Trusted Operating System into a hardware platform. Kinibi integration consists of:

- Integrating the Kinibi Normal World components into the main Operating System
  - Default one is Google's Android OS.
  - Kinibi also supports other embedded Linux distribution like Debian, CentOS, Yocto.
- Integrating the Kinibi Secure World components.
- Implementing support of pluggable DRM framework.
- Implementing Kinibi Trusted User Interface (TUI).
- Implementing and integrating RPMB Driver.
- Running and passing the Trustonic Test Suite to verify the integration.

Note that in order to enable Kinibi-4xx and the OTA-Operated Containers on a Device, the device manufacturer must install and integrate Trustonic's Key Provisioning Host (KPH) into the manufacturing line. The KPH is a tool that injects the TEE Authentication Token into the device, storing a copy in the Trustonic backend system, Trustonic Directory. For details of this process and how to integrate the KPH please consult the document entitled *Kinibi_Provisioning_Manual.pdf*.

To encrypt System TAs and secure drivers, a key injection must be performed in the factory.

The Kinibi product package is structured as follows:

- `/Documentation`, this directory contains documentation detailing how to integrate Kinibi into a device and how to use Kinibi provisioning tools.
- `/AndroidIntegration`, this directory contains all the Normal World components to be integrated into Android.
- `/LinuxIntegration`, this directory contains all the Normal World components to be integrated into Linux – for non-Android BSPs.
- `/SecureIntegration`, this directory contains all the Secure World components including the Kinibi core binary and Trustonic System Trusted Applications.
- `/t-base-dev-kit`, the Kinibi software development kit (SDK) with documentation and Samples for Trusted Applications developers.
- */TTS*, a comprehensive test suite allowing integrators to quickly validate that all the critical features of Kinibi have been successfully integrated.

2 KINIBI NORMAL WORLD COMPONENTS

Trustonic's Kinibi OS is supplied with a number of components that need integrating into the Android or Linux image. These Normal World (NWd) components are:

In the Linux or Android User space:

- The Kinibi Daemon: in charge of filesystem access for the Secure World Around two axes: secure filesystem and Kinibi registry.
- The Kinibi Proxy: provides local socket access to the Secure World when the driver access is denied.
- The Root Provisioning Agent (RootPA): used to install Service Provider Trusted Applications. The RootPA includes the Curl library, for XML manipulations and a log library.
- The Kinibi Client library: A selection of user space APIs available for Normal World application developers. Tries to use the Kinibi Linux driver for Secure World access and falls back to using the proxy on access denied.
- The Kinibi registry interface: API's for the management of the Kinibi registry.

In the Android P onwards User space:

The Kinibi System service: A Framework service used by Android System or Service Providers applications to access the TEE. This system service is the only component allowed to use ITee HIDL interface.

The Kinibi Vendor Service : A vendor service implementing the ITee HIDL interface

In Linux Kernel space:

- The Kinibi Linux driver: A component in charge of communication between the Normal World user space client and the Secure World. There are two interfaces available: one reserved for the Kinibi Daemon and one allocated to direct communication with all the user space clients.
- The Kinibi Linux driver kernel API: kernel level APIs available to Normal World driver developers.

All Normal World components for the Kinibi product are provided in source code and binary forms, with support for 32-bit and 64-bit Android versions and 32-bit Linux, in the `/AndroidIntegration` directory for Android, in the `/LinuxIntegration` directory for Linux . The purpose of this folder is to provide a simple way of integrating the Kinibi Normal World components into an existing Android source tree.

2.1 BUILDING NORMAL WORLD COMPONENTS

For Android, Source Code the source code can be found in */AndroidIntegration/Src*.

For generic Linux, the Source Code can be found in */LinuxIntegration/Src*.

This Source Code folder contains two sub-folders:

- A `mobicore` sub-folder which contains the Android user space components (executables and libraries).
- A `gud` sub-folder which contains the Linux kernel components.

2.1.1 Kinibi user-space components

2.1.1.1 Android Compilation

The standard way of building the Kinibi user space components is to use a complete Android source tree. Simply copy the `mobicore` folder into the Android source tree `external` folder.

You should end up with the following files and folders:

```
Android root/
    external/
      mobicore/
        CAKeyInjection/
        ClientLib/
        TeeClient/
        TeeProxyClient/
        curl/
        Daemon/
        hardware/
        rootpa/
        tlcm/
        TeeService/
        TeeServiceJava/
         Android.mk
```

To build the Kinibi components, simply launch an Android tree full build.

2.1.1.2 Linux Compilation

Linux compilation is based on CMake. In each component sub-folder, you can find a CMakeLists.txt file that contains the rules to build the Kinibi components, as shown below:

```
mobicore/
├──── ClientLib
│     ├──── CMakeLists.txt
│     ├──── include
│     └──── src
└──── Daemon
      ├──── CMakeLists.txt
      ├──── include
      ├──── src
      └──── systemd
```

For the Daemon we also provide a system (the standard Linux init program) script to launch the daemon service on boot.

For the ClientLib, CMake generates a pkgconfig to be used by packages that depend on it (pkgconfig files contain the paths to the include and lib directory).

On your PC, you want to install CMake, pkgconfig and your arm toolchain used to cross-compile the component.

Information about CMake variables:

Variable	Description
CMAKE_PROJECT_NAME	Defines the name used in the pkgconfig files
CMAKE_C_COMPILER	Path to your C cross-compiler.
CMAKE_CXX_COMPILER	Path to your C++ cross-compiler.
CMAKE_INSTALL_PREFIX	Path where cmake installs the compilation result (headers, libs and pkgconfig files). You should use the same folder for ClientLib and Daemon compilation. Example configuration of prefix: `export CMAKE_INSTALL_PREFIX=~/install/`
TEE_VERSION	Defines the component version in pkgconfig files, should be aligned on Kinibi version (311A, 311B, …).
PKG_CONFIG_PATH	Path where libs and bins are installed, same folder as CMAKE_INSTALL_PREFIX with pkgconfig folder. Example configuration of pkgconfig for finding dependencies : `export PKG_CONFIG_PATH=~/install/lib/pkgconfig/`

Table 1 - CMake variables

2.1.1.2.1 ClientLib

For example, go into `mobicore/ClientLib/` folder then:

```
cmake . -DCMAKE_PROJECT_NAME=ClientLib -DCMAKE_C_COMPILER=arm-linux-
gnueabihf-gcc -DCMAKE_CXX_COMPILER=arm-linux-gnueabihf-g++
-DCMAKE_INSTALL_PREFIX=~/install/ -DTEE_VERSION=XXX -Wno-dev
```

2.1.1.2.2 `make` && `make install` Daemon

For example, go into `mobicore/Daemon/` folder then:

```
cmake . -DCMAKE_PROJECT_NAME=McRegistry -DCMAKE_C_COMPILER=arm-linux-
gnueabihf-gcc -DCMAKE_CXX_COMPILER=arm-linux-gnueabihf-g++
-DCMAKE_INSTALL_PREFIX=~/install/ -DTEE_VERSION=XXX -Wno-dev
make && make install
```

2.1.2 Kinibi Linux-kernel-space components

The Linux driver directory `gud` within the Kinibi package is designed to be directly dropped in the Linux kernel source tree, specifically the `drivers` folder.

It contains one module:

- The Kinibi Linux driver.

Once the `gud` directory has been copied, you should have the following organization:

```
Linux kernel/
    drivers/
        gud/
            Kconfig/
            Makefile/
            MobicoreDriver/
            TlcTui/
```

Please note that copying the `gud` directory to a different folder within the Linux source tree will not work.

To enable automatic building inside the kernel follow these steps:

- Update the Linux kernel configuration file `linux/drivers/Kconfig` with the following line which must be inserted before the last `endmenu` entry:

```
source "drivers/gud/Kconfig"
```

- Add the Kinibi Linux driver to the Linux kernel build file `linux/drivers/Makefile` :

```
obj-y += gud/
```

- Run `make menuconfig` and in the `Device Drivers` page of the configuration menu, please select:
  - `Trustonic TEE Driver`

```
<*> Trustonic TEE Driver
[ ]   Trustonic TEE uses LPAE
[ ]   Trustonic TEE driver debug mode
[ ]   Trustonic Trusted UI
[ ]  Trustonic Trusted UI with fb_blank
```

- Finally, run `make` again and the Kinibi's Linux kernel components will be included in the Linux kernel image.

2.2 INTEGRATION IN ANDROID (32 AND 64 BIT)

2.2.1 Integration in an Android Source Tree

All the Kinibi user-space components are located in the package inside AndroidIntegration/Src/mobicore. This folder should be copied in BSP_ROOT/external/mobicore.

Since Android P, 3rd-party services need to be declared in several places.

In BSP_ROOT/device/<OEM>/<platform >/manifest.xml:

```
    <hal format="hidl">
        <name>vendor.trustonic.tee</name>
        <transport>hwbinder</transport>
        <version>1.0</version>
        <interface>
            <name>ITee</name>
            <instance>default</instance>
        </interface>
    </hal>
    <hal format="hidl">
        <name>vendor.trustonic.teeregistry</name>
        <transport>hwbinder</transport>
        <version>1.0</version>
        <interface>
            <name>ITeeRegistry</name>
            <instance>default</instance>
        </interface>
    </hal>
```

In the top makefile of the plaform (usually located in /device/<OEM>/<platform>/device.mk:

```
PRODUCT_PACKAGES += mcDriverDaemon
PRODUCT_PACKAGES += vendor.trustonic.tee@1.0-service
PRODUCT_PACKAGES += vendor.trustonic.teeregistry@1.0-service
PRODUCT_PACKAGES += RootPA
PRODUCT_PACKAGES += TeeService
PRODUCT_PACKAGES += libTeeClient
```

2.2.2 Integration in Device File System

The tables below give the directories in the Android file system where Kinibi components must be placed.

2.2.2.1 Android OS file system:

Component	Name of the binary	Containing folder
TEE Vendor Components		
Kinibi Daemon	`mcDriverDaemon`	`/vendor/bin/`
Kinibi Client library	`libMcClient.so`	`/vendor/lib[64]/`
TEE HIDL Components		

Kinibi Framework Service	TeeService/TeeService.apk	/system/priv-app/
Kinibi AIDL Native Client side of Framework Service	libteeservice_client.trustonic.so	/system/lib[64]/
Kinibi Framework Service JNI lib	libTeeServiceJni.so	/system/lib[64]/
TEE HIDL clientlib	vendor.trustonic.tee@1.0.so	/system/lib[64]/
TEE HIDL service	Vendor.trustonic.tee@1.0-service	/vendor/bin/hw
TEE HIDL server init	vendor.trustonic.tee@1.0-service.rc	/vendor/etc/init/
Trustonic OTA Components		
Root Provisioning Agent	RootPA.apk	/system/app/
RootPA Native library	libcommonpawrapper.so	/system/lib/
Curl library	libcurl.so	/system/lib/
Trustonic OTA HIDL Components		
Registry HIDL clientlib interface	libMcRegistry.so	/system/lib/
Registry HIDL clientlib	vendor.trustonic.teeregistry@1.0.so	/system/lib[64]/
Registry HIDL service	Vendor.trustonic.teeregistry@1.0-service	/vendor/bin/hw
Registry HIDL server init	vendor.trustonic.teeregistry@1.0-service.rc	/vendor/etc/init

The RootPA.apk and TeeService.apk apps are System Android app and need to be signed like any System apps (the version provided by Trustonic is not signed).

2.2.2.2 32 bits and 64 bits Android OS file system

If the Kinibi Linux driver modules are not built within the Linux kernel tree you must place them in the following locations:

Component	Name of the binary	Containing folder
Kinibi user device (gud driver)	`mcDrvModule.ko`	`/system/lib/modules/`

A number of Trusted Applications have to be placed into the registry folder:

Component	Name of the binary	Containing folder
Content Management Trusted Application	`07010000…0000.tlbin` *(tlcm.axf)*	`/vendor/app/mcRegistry`

In addition, since Android N (7.0), in order to support 3rd party Trusted Application (Service provider TA) accessing the TEE interfaces, it is mandatory for the integrator to include the `libMcClient.so` in the list of Android vendor specific public libraries:

```
/vendor/etc/public.libraries.txt
```

In addition, since Android P (9.0), in order to support 3rd party Trusted Application (Service provider TA) accessing the TEE interfaces, it is mandatory for the integrator to include the `libteeservice_client.trustonic.so` in the list of Android system specific public libraries:

```
/system/etc/public.libraries-trustonic.txt
```

2.2.3 Permissions and Access Rights

To enable the correct operation of Kinibi and any Trusted Applications it is mandatory to ensure all Kinibi components have the correct permissions and access rights. The following section highlights the required settings.

- Kinibi Daemon (`mcDriverDaemon`):
  The Kinibi Daemon should have permissions `0755`.
- Kinibi libraries (`libMc*, libcurl, libcommonpawrapper`):
  No specific permissions are needed for libraries.
- Kinibi Linux driver:
  The Linux driver needs two device nodes in `/dev` for the two different access mechanisms: `/dev/mobicore` for administration purpose, and `/dev/mobicore-user` for client access. Permissions for these two nodes must be defined in the following way:

```
/dev/mobicore       0600 system:system
/dev/mobicore-user 0600 system:system
```

  This should be done by adding the following lines to your ueventd.<hardware>.rc file:

```
# Trustonic TEE
/dev/mobicore      0600 system system
/dev/mobicore-user 0600 system system
```

2.2.4 Directories Requirements

There are two directories that must be created in the device file-system for Kinibi. These paths are used by Kinibi components at runtime.

2.2.4.1 mcRegistry directory

This directory is used by Kinibi to store non-permanent data that can be deleted with a factory reset or device wipe.

The mcRegistry directory stores content relating to Device Binding, including:

- TEE Authentication Token (also known as the AuthToken)
- TEE Authentication Token backup (also known as the AuthToken backup)

Note that the TEE Authentication Token backup is an exception, and it must be preserved across factory reset or device wipe (see section 2.2.4.3.1)

The mcRegistry directory also stores content relating to the OTA-management of third-party content, including:

- Kinibi Root Containers
- Service Provider Containers
- Service Provider TA Containers
- Service Provider TA binaries (used only for TAs using GP APIs)

Service Provider and System TAs making use of GP Trusted Storage APIs automatically store Secure Objects in sub-folders of the mcRegistry directory.

The mandatory path is:

```
/data/vendor/mcRegistry
```

Permissions should be as follows:

- User: `system`, can read/write/execute
- Group: `system`, can read/write/execute
- Others can read/execute

In UNIX speak, permissions `0775`, user/group `system:system`.

2.2.4.2 Persistent Trusted Applications and Secure Drivers

System Trusted Applications and Secure Drivers can be stored anywhere in the device file system. However, Persistent Non-GP Trusted Applications or Secure Driver binaries must be placed in a non-volatile (factory reset proof) partition of the file system in order to survive a factory reset or device wipe.

GP Trusted Applications stored in the Secure File System by OTAv2 will not survive Factory Reset.

Trustonic System Trusted Applications like the Content Management Trusted Application (CMTL) must be placed in:

```
/vendor/app/mcRegistry
```

Permissions should be as follows:

- User: `system`, can read/write/execute
- Group: `system`, can read/execute
- Others can read/execute

In UNIX speak, permissions `0755`, user/group `system:system`.

Please note that there is no content generated here at runtime by Kinibi, the directory is only used to store persistent System Trusted Applications.

The files of the System Trusted Applications and Secure Drivers in the mcRegistry directory should have the following access permissions:

- User: `system`, can read/write
- Group: `system`, can read/write
- Others can read

In UNIX speak, permissions `0664`, user/group `system:system`.

2.2.4.3 Persistent read-write directory (/efs)

Kinibi needs to store system data in a location that is persistent across factory reset or device wipe.

This requirement presently applies only to the following files:

- TEE Authentication Token backup (also known as the AuthToken backup)

Since locations that are retained permanently are often highly OEM-specific, the OEM has to customize this location. A common location for this directory is:

```
/efs
```

2.2.4.3.1 AuthToken backup

The OEM has to customize the backup behavior. There is presently no environment variable governing the location of this container, and persistence is often achieved by restoring the container at each device boot, or as part of the factory reset procedure.

Note that, for implementation reasons, while the Containers held in this location must be persistent across factory reset and device wipe, there is a requirement for Kinibi to occasionally write these Containers at runtime.

2.2.5 Starting up Kinibi

2.2.5.1 Standard mode

To start the Kinibi daemon and proxy services automatically at start-up, the following lines must be added to one of the `/init.*.rc` files on the Android device:

```
service trustonic-daemon /vendor/bin/mcDriverDaemon
    class core
    user system
    group system
```

The daemon must have system permissions for `user` and `group`. The OEM is responsible to set the correct parameters for the service. The proxy must be user system to be accepted by the driver.

The OEM is also responsible for deciding how the system should behave in the event of an error, for example, if the device fails to correctly initialize Kinibi or if the Kinibi daemon crashes.

2.2.5.2 Recovery mode

In recovery mode, the proxy is not expected to be needed. Also, some services such as Secure File System and Trusted UI are not necessary. The daemon can thus be started without those two services, in "light" mode:

```
service trustonic-daemon /vendor/bin/mcDriverDaemon -l
    class core
    user system
    group system
```

2.2.6 SEAndroid Configuration

This section gives information about how to set the SE Linux Policies in order to allow all the Trustonic's elements working correctly.

The SE Linux Policies are on OEM responsibilities. This document is a guide line to help the OEM's implementation.

2.2.6.1 Interaction between Android components on Android P

As the Normal-World components for Kinibi can be configured by the OEM, the directories and naming of binaries in the figure below are mostly instructive, and can vary between installations. The exact configuration is left to the OEM although the permissions must be implemented correctly for normal OTA operation. It is essential that after any policy change the Kinibi Test Suite is executed to ensure there are no adverse effects on application provisioning via Trustonic's Directory servers.

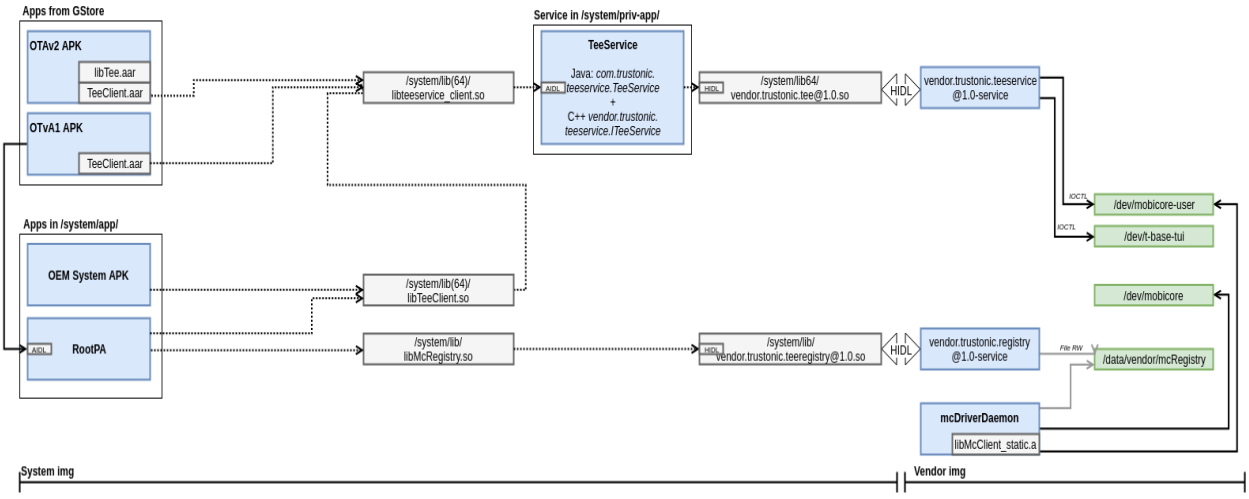


Figure 1 System description

The main flow of program installation (OTAv1 protocol only) is as follows and depicted in graphical form above. The Android program X (downloaded from a store) leveraging a Kinibi service first installs the usage rights for its Kinibi trusted application (TA). This is done as follows:

a) **OTAv1 APK** communicates over a **binder interface** with the **RootPA** application. This is an Android (Java)-internal operation.

b) The **RootPA** communicates with the **vendor.trustonic.teeregistry@1.0-service**. This communication is established over HIDL binder interface.

c) **OTAv1 APK OTAv2 APK** and will initiate network communication with a remote Trusted Application Manager server, but parts of the protocol messages will be handled by a Kinibi TA. For this to happen, the **vendor.trustonic.tee@1.0-service**, needs to **access the** /dev/mobicore-user**.** Device access is done over ioctls, reads and write, in all cases.

d) The **RootPA** gets protocol results that need to be stored on flash / disk. This is achieved by the **vendor.trustonic.teeregistry@1.0-service** reading and writing into a directory, typically /data/vendor/mcRegistry

At this point, the installation of the program rights has completed, and files have appeared in /data/vendor/McRegistry.

For OTAv1 APK, OTAv2 APK, System APK and **RootPA to execute**, it accesses the **TeeService via libteeservice_client.trustonic.so** which forward the call to the **ven vendor.trustonic.tee@1.0-service** via HIDL interface which then use /dev/mobicore-user device to communicate with its TA.

TUI (Trusted UI): TrustedUI integration is part of **vendor.trustonic.tee@1.0-service** and adds a new kernel driver device `/dev/t-base-tui`. In order to work properly, **vendor.trustonic.tee@1.0-service** needs to access `/dev/t-base-tui`.

RSU (T-Mobile Remote SimUnlock): Its integration brings a new Android application `RSU` and a new system service `tsDaemon`. In order to work properly, `RSU` application needs to connect to `tsDaemon` through a Unix socket.

2.2.6.2 SEAndroid Policy Requirements

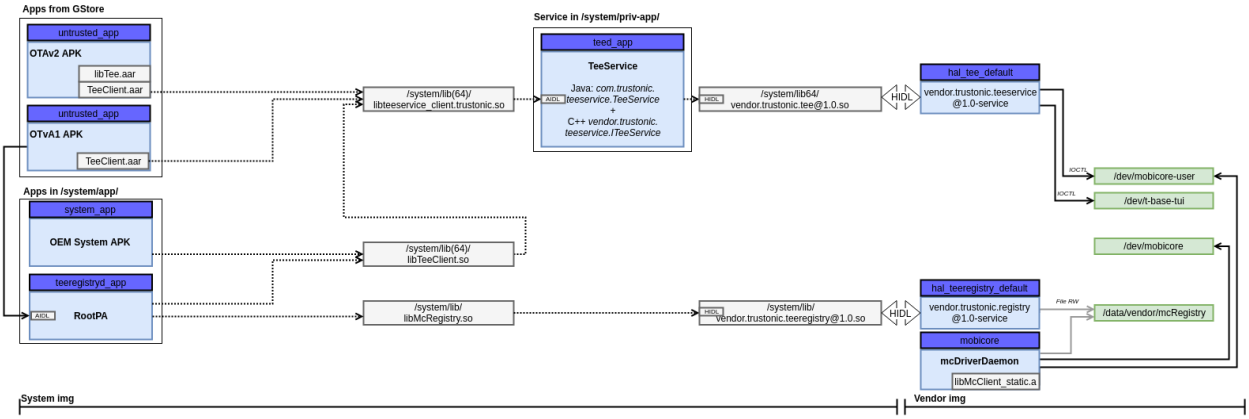


Figure 2 SELinux for Android Kinibi integration

The Kinibi system does not today leverage SEAndroid policy for its own protection. Therefore we state no requirements for enforcement.

Instead, the requirements purely stem from accessibility, i.e. which communication channels need to be available for what kinds of system stakeholders in order for the Kinibi system to be fully working.

2.2.6.3 SELINUX Types

File related types:

- `mobicore_user_device`: file type for kinibi driver device `/dev/mobicore-user` which provides access to the TEE features
- `mobicore_admin_device`: file type for kinibi driver device `/dev/mobicore` used by `vendor registry service` for provisionning and OTAv1 features
- `mobicore_tui_device`: file type for kinibi driver device `/dev/ t-base-tui` used by `vendor tee service` for TUI features.
- `mobicore_data_file / mobicore_vendor_file`: file type for data files handled by `mcDriverDaemon` and `vendor registry service` (mcRegistry, TA binaries)

File path – selinux type mapping can be found in `file_contexts` integration file.

Process related types:

- `mobicore`: service process type for `mcDriverDaemon` process (and RSU `tsDaemon` too)
- `mobicore_app`: Vendor Android application process type for `RSU`.
- `teed_app`: Android application process type for `TeeService`.
- `teeregistryd_app`: Android application process type for `RootPA`.
- `hal_tee_default`: Android vendor service process type for `vendor.trustonic.tee@1.0-service`.
- `hal_teeregistry_default`: Android vendor service process type for `vendor.trustonic.teeregistry@1.0-service`.

2.2.6.1 SELINUX Allow rules

2.2.6.1.1 Mobicore daemon rules

1) `/dev/mobicore` needs to be accessible from any `mcDriverDaemon`.
   The SEAndroid class needed for communication is `chr-dev`.
   Needed permissions are `ioctl, read, write, open`

2) `/dev/mobicore-user` needs to be accessible from `mcDriverDaemon`, `vendor.trustonic.teeregistry@1.0-service`, `vendor.trustonic.tee@1.0-service` and any vendor application.
   The SEAndroid class needed for communication is `chr-dev`.
   Needed permissions are `ioctl, read, write, open`

3) The directory `/data/vendor/mcRegistry` needs to be readable and writable by the `mcDriverDaemon` AND `vendor.trustonic.teeregistry@1.0-service`.
   Relevant SEAndroid classes are `dir` and `file`.

All SELinux rules needed can be found in AndroidIntegration/Src/SELinux/AndroidP directory.

2.2.6.1.2 Android applications rules

All vendor Android applications (installed in /vendor/app) need to be able to access `/dev/mobicore-user` via `libMcClient.so`

```
allow specific_app mobicore_user_device:chr_file rw_file_perms ;
```

For example `RSU` is `mobicore_app`.

Domain transition for Android applications is made automatically by registering their package name in `seapp_contexts` file. Here a sample for `RootPA`, `TeeService`:

```
# RootPA
user=_app seinfo=platform name=com.gd.mobicore.pa
domain=teeregistryd_app type=app_data_file levelFrom=user
# TeeService
user=_app seinfo=platform name=com.trustonic.teeservice
domain=teed_app type=app_data_file levelFrom=user
```

2.3 INTEGRATION IN LINUX

Note: this section does not apply to Android device integration projects.

2.3.1 Integration in Device File System

The table below gives the directories in the Android file system where Kinibi components must be placed:

2.3.1.1 Linux OS file system:

Component	Name of the binary	Containing folder
Kinibi Daemon	`mcDriverDaemon`	`/usr/bin/`
Kinibi Proxy	`trustonic_tee_proxy`	`/usr/bin/`
Kinibi Client library	`libMcClient.so`	`/usr/lib/`
Kinibi registry interface	`libMcRegistry.so`	`/usr/lib/`

If the Kinibi Linux driver modules are not built within the Linux kernel tree you must place them in the following locations:

Component	Name of the binary	Containing folder
Kinibi user device (gud driver)	`mcDrvModule.ko`	`/usr/lib/modules/`

A Trusted Applications have to be placed into the registry folder:

Component	Name of the binary	Containing folder
Content Management Trusted Application	`07010000…0000.tlbin` *(`tlcm.axf`)*	`/usr/share/trustonic_tee/registry/`

2.3.2 Permissions and Access Rights

To enable the correct operation of Kinibi and any Trusted Applications it is mandatory to ensure all Kinibi components have the correct permissions and access rights. The following section highlights the required settings.

- Kinibi Daemon (`mcDriverDaemon`):
  The Kinibi Daemon should have permissions `0755`.
- Kinibi libraries (`libMc*`):
  No specific permissions are needed for libraries.
- Kinibi Linux driver:
  The Linux driver needs two device nodes in `/dev` for the two different access mechanisms: `/dev/mobicore` for administration purpose, and `/dev/mobicore-user` for client access. Permissions for these two nodes must be defined in the following way:

```
/dev/mobicore-user 0666 XXX:XXX
/dev/mobicore      0600 XXX:XXX
```

Note: `/dev/mobicore-user` is only created when the TEE has started successfully, which is triggered by the first daemon's connection to `/dev/mobicore`.

2.3.3 Directories Requirements

There are two directories that must be created in the device file-system for Kinibi. These paths are used by Kinibi components at runtime.

2.3.3.1 mcRegistry directory

This directory is used by Kinibi to store non-permanent data that can be deleted with a factory reset or device wipe.

The mcRegistry directory stores content relating to Device Binding, including:

- TEE Authentication Token (also known as the AuthToken)
- TEE Authentication Token backup (also known as the AuthToken backup)

Note that the TEE Authentication Token backup is an exception, and it must be preserved across factory reset or device wipe

The mcRegistry directory also stores content relating to the OTA-management of third-party content, including:

- Kinibi Root Containers
- Service Provider Containers
- Service Provider TA Containers
- Service Provider TA binaries (used only for TAs using GP APIs)

Service Provider and System TAs making use of GP Trusted Storage APIs automatically store Secure Objects in sub-folders of the mcRegistry directory.

The mandatory path is:

```
/usr/share/trustonic_tee/registry/
```

Permissions should be as follows:

- User: `XXX`, can read/write/execute
- Group: `XXX`, can read/write/execute
- Others can read/execute

In UNIX speak, permissions `0775`, user/group `XXX:XXX`.

2.3.3.2 Persistent Trusted Applications and Secure Drivers

System Trusted Applications and Secure Drivers can be stored anywhere in the device file system. However, Persistent Non-GP Trusted Applications or Secure Driver binaries must be placed in a non-volatile (factory reset proof) partition of the file system in order to survive a factory reset or device wipe.

GP Trusted Applications stored in the Secure File System by OTAv2 will not survive Factory Reset.

Trustonic System Trusted Applications like the Content Management Trusted Application (CMTL) are must be found in:

```
/usr/share/trustonic_tee/registry/
```

Permissions should be as follows:

- User: XXX, can read/write/execute
- Group: XXX, can read/execute
- Others can read/execute

In UNIX speak, permissions 0755, user/group XXX:XXX.

Please note that there is no content generated here at runtime by Kinibi, the directory is only used to store persistent System Trusted Applications.

2.3.4 Starting up Kinibi

For automatically running the Kinibi daemon at start-up a systemd script is given tee-daemon.service:

```
[Unit]
Description=Trustonic TrustZone daemon

[Service]
Type=simple
ExecStart=/usr/bin/mcDriverDaemon -b -p /usr/share/trustonic_tee/registry/
Restart=always

[Install]
WantedBy=multi-user.target
```

Copy tee-daemon.service in /etc/system/system and launch this command:

```
systemctl enable tee-daemon.service
```

The daemon has to have system permissions for user and group otherwise the OEM is responsible to set the correct parameters for the service.

The OEM is also responsible for deciding how the system should behave in the event of an error, for example, if the device fails to correctly initialize Kinibi or if the Kinibi daemon crashes.

2.3.5 Build In Yocto Environment

The Kinibi package is providing full reference version of Yocto recipes under LinuxIntegration/YoctoLayer/meta-trustonic/.

Then, to automatically compile Kinibi Normal World Components within the baseport and ensure their presence in generated RootFS:

- The bblayer.conf file of the platform environment should be updated to contains and point to Kinibi directory meta-trustonic/.
- Recipe file name under meta-trustonic\recipes-core\images\image-name.bbappend must be changed to match image recipe name used in bitbake command.

2.4 XEN INTEGRATION

2.4.1 Hypervisor patches

The Xen hypervisor requires patches (under `AndroidIntegration/Src/xen/patches/` or `LinuxIntegration/Src/xen/patches/` inside the Kinibi package) to work with Kinibi while providing the necessary level of security. These patches apply to releases 4.8 and 4.8.1 of the Xen hypervisor as provided by the Xen project (https://xenbits.xen.org/).

2.4.2 Integration in Xen Dom0

The integration in Xen Dom0 is the same as without Xen, so please refer to the section that applies to integrate in either Android or Linux.

2.4.3 Integration in Xen DomU

The integration in Xen DomU is simplified because DomUs don't have a daemon running, and thus neither a mcRegistry directory nor a libMcRegistry library is required. The only two components here are the Linux driver and the libMcClient library.

Once the Linux driver has initialized, either because it is built-in or because its module has been inserted into the Linux kernel, it needs to be probed by the system. This does not happen automatically, so a script named `activate.sh` is provided (under `Hikey/xen_domu/` inside the Kinibi package) to perform the necessary actions. This script **runs on Xen Dom0** takes the Xen DomU ID as argument.

Important note: there is a Xen limitation to how much memory can be shared between DomU and Dom0, which impacts the memory sharing between DomU and the Secure World. By default, the limit is 64MiB.

2.5 KINIBI DAEMON USAGE

Help output:

```
$ mcDriverDaemon -h
TEE Driver Daemon 7.0. "t-base-HIKEY-Android-999A-
20180517_193251_49242_78646"
usage: mcDriverDaemon [OPTIONS]
Start the TEE Daemon

  -h            show this help and exit
  -v            print version and exit
  -b            fork to background
  -d            specify the path to the decryption key
  -l            do not start FSD/TUI services
  -p REGISTRY   specify path to registry (may be repeated)
  -r DRIVER     secure driver to load at start-up (may be repeated)
  -r DRIVER     It could be a /path/to/secure/driver.tlbin or a UUID
000102030405060708090A0B0C0D0E0F
  --Px PARTITION[x] PATH    specify the directory where the secure
partition is stored, 0 <= x <= 15
```

3 KINIBI SECURE WORLD COMPONENTS

Secure World components of Kinibi are available in the package directory `/SecureWorldIntegration`. It contains:

- The Kinibi image binary (secure operating system running in Secure World).
- The Content Management trusted application (System trusted application responsible for Containers management).
- Secure World drivers in skeleton form that the SIP and OEM have to integrate.
  - RPMB driver
  - Trusted User Interface Driver
  - DRM Driver (t-play)
  - Key Injection TA
- The ARM Trusted Firmware patch (spd, optional , for ARMv8 only)
- The TEE image builder (t-base-kit)
- The MobiConfig tool.

The Kinibi images are provided in binary (Debug and Release) under the *`SecureIntegration/t-base/bin/MobiCore/`* directory.

Please note that the `DEBUG` version is much slower than the `RELEASE` version as it prints all Kinibi traces to the Linux Kernel log (`dmesg`). You can always get traces from Trusted Applications if they are compiled as Debug).

The images are un-configured (`mobicore.raw.img`) and should be configured with a hash of a System Trusted Application public key before using them. For reference the package contains also images signed with Trustonic test keys (`.img`).

The Content Management trusted application is provided in binary form (`DEBUG` and `RELEASE`) under `SecureIntegration/tbase/bin/TlCm`. The trusted application is provided un-configured (`tlCm.axf`) and should be configured with the Kinibi KPH request signing key and signed with the System trusted application key pair.

3.1 VERIFYING THE KINIBI VERSION

Before integrating Kinibi on a device, please verify the version tag in the binary. This version tag is changed each time Kinibi is built, so it offers a way to distinguish between different Kinibi versions and also between engineering and commercial releases.

To check the Kinibi version, look for the string `"t-base-"` in the binary image:

```
$ strings SecureIntegration/t-base/Bin/MobiCore/*/Release/t-base.img |
grep t-base-
```

This displays several version tags because the Kinibi image is made of several components that each have their version string. All the version strings inside the same image are identical.

A Kinibi package includes both a release and a debug build, located in directories named `Release` and `Debug` respectively. To distinguish between a release and a debug build in isolation, search for strings that are only present in the debug build. The following command shows a way to distinguish the two variants:

```
$ strings SecureIntegration/t-base/Bin/MobiCore/*/Release/t-base.img |
grep "MTK: sigma0 size"
$ strings SecureIntegration/t-base/Bin/MobiCore/*/Debug/t-base.img |
grep "MTK: sigma0 size"
S0CBMTK: sigma0 size: code=0x%08x data/bss=0x%08x
```

To verify the running version during development and testing, call the function `tlApiGetMobiCoreVersion` from a Trusted Application or `mcGetMobiCoreVersion` from a Client Application as described in the Kinibi API Documentation. See also Section 8.1 Basic verification and version check.

3.2 KINIBI IN BOOT CHAIN

To maintain security it is important that the Kinibi image is started up in the boot flow as early as possible. Booting up with Kinibi is a critical task in the system design and it should be implemented in co-operation with the silicon vendor and Trustonic. There are several options for implementing Kinibi in the boot chain so the purpose of this chapter is to give a basic level of understanding as to what needs to be done.

- It is recommended to store Kinibi at a permanent location in the Boot partition or some other permanent storage as early in the boot chain there is often no access to a regular file system.
- The Kinibi image must be signed by the OEM or ODM.
- The Kinibi image should be securely loaded to secure memory (internal or DRAM) by a bootloader.
- After Kinibi is loaded into secure memory its signature must be verified.
- Before calling Kinibi, the caller must correctly set the boot configuration block which is used for exchanging predefined data with Kinibi.
- Calling Kinibi can usually be just a basic jump instruction.

Please note that as the initialization routine of Kinibi returns to the caller, the caller environment (bootloader/uboot) should be saved and restored for the time period execution is in TrustZone side.

If the Kinibi signature check or boot fails it is up to OEM or SOC vendor to decide whether or not the device can continue to boot.

3.2.1 IRAM support

Trustzone memory protection hides secure memory from Android. On-chip memory (internal memory, or IRAM) provides additional protection against probing attacks and should be used to store cryptographic keys and similar secrets. However, many Trustzone use cases require megabytes of memory, whereas IRAM only has kilobytes. There is no more explicit support for IRAM in Kinibi.

When the bootloader passes an IRAM region to Kinibi via the boot parameters (see 3.5), Kinibi will not use this memory.

3.3 TRUSTED APPLICATIONS AND DRIVERS

In a Kinibi environment, there are 3 types of secure components:

- System Trusted Applications,
- Service Provider Trusted Applications,
- Drivers.

System Trusted Applications and drivers are pre-integrated into the device before release. Conversely, Service Provider Trusted Applications are deployed at runtime, over the air, by a Trusted Application Manager (TAM). This document focuses on pre-integrated applications.

To ensure the security of these Trusted Applications or drivers they need to be signed and verified at runtime by Kinibi. To do this the hash of the System Trusted Application's public key is inserted into the Kinibi raw-image.

By convention, Trusted Applications are named as `UUID`***`.tlbin`*** and drivers as `UUID`**`.drbin`**, where UUID is a 16-byte hex value generated according to RFC-4122.

Any UUID value can be used by an OEM however UUID's with the least significant 12 bytes all zero are reserved for Trustonic:

- *0000 0000 0000 0000 0000 0000 0000 0000*,
- *0000 0001 0000 0000 0000 0000 0000 0000*,
- … ,
- *FFFF FFFF 0000 0000 0000 0000 0000 0000*.
- *[Most Significant Octet] … [Least Significant Octet]*

For more details on Trusted Application and driver development please consult the `Kinibi_Developer's_Guide.pdf`.

Note that other specifications reserve particular UUID's and UUID structures, and that in environments that interact with those other UUID's and UUID structures the rules of those specifications must also be taken into account. For example, see Section 5.6 and Annex A.3 of the GlobalPlatform Device Technology TEE Management Framework v1.0.

3.4 CONFIGURING AND SIGNING KINIBI COMPONENTS

The following section describes how to manage the different private and public keys to ensure the authenticity and integrity of the Kinibi binary, drivers, and System Trusted Applications.

It is mandatory for the OEM to go through all the steps in this section to customize the keys involved for the correct and secure operation of Kinibi.

3.4.1 Keys in Kinibi Environment

There are four keys involved in the Kinibi environment that are of special importance during the integration phase:

- `PrK.Vendor.Boot` and `PuK.Vendor.Boot`:
  A PKI key pair used during boot for verifying the integrity of the Kinibi image. This Key pair must be generated and managed by the SiP, OEM or ODM (whichever owns the relevant stage for the boot process).
- `PrK.Vendor.TltSig` and `PuK.Vendor.TltSig`:
  A PKI key pair used for signing System Trusted Applications and drivers that are installed by default on the device. This Key pair must be generated and managed by the OEM or ODM.
- `PuK.Trustonic.Endorsement`
  Trusted Applications use this key to sign data that can be proven to originate from a genuine TEE and the right Trusted Application. This key is provided by Trustonic as part of the Kinibi package.
- `Prk.Kph.Request` and `PuK.Kph.Request`:
  A PKI key pair used in message exchanges with the Kinibi Content Management Trusted Application in a production environment. Further details of how this key is used can be found in the documentation titled `Kinibi_Provisioning_Manual.pdf`.

OpenSSL is the recommended way to generate the key pairs described above:

```
$ openssl genrsa -3 -out VendorBoot.pem 2048
$ openssl rsa
    -in VendorBoot.pem
    -pubout
    -outform PEM
    -out VendorBoot_pub.pem
$ openssl genrsa -3 -out VendorTltSig.pem 2048
$ openssl rsa
    -in VendorTltSig.pem
    -pubout
    -outform PEM
    -out VendorTltSig_pub.pem
```

(PEM format is expected by Kinibi components).

Different settings can be changed as required. Especially the size of the key, Kinibi supports sizes up to 4096 bit. The exponent of the RSA key can also be changed, below we find an example of 4K key generation with an exponent equal to 17:

```
$ openssl genpkey
      -algorithm RSA
      -out pairVendorTltSigWithDesc.pem
      -pkeyopt rsa_keygen_bits:4096
      -pkeyopt rsa_keygen_pubexp:17
$ openssl rsa -in pairVendorTltSigWithDesc.pem > pairVendorTltSig.pem
```

3.4.2 Configuring Kinibi

3.4.2.1 Configuring the Kinibi Image

The first step in configuration is to inject a hash of the System Trusted Application signing public key (`PuK.Vendor.TltSig`) into the raw Kinibi image. The goal of this is to guarantee the origin of System Trusted Applications and drivers. Secondly the Trustonic endorsement key, located in the directory: *`SecureIntegration\t-base\bin\MobiCore\endorsementPubKey.pem`*, should be included to enable authenticity checks on Trusted Application data. To develop applications using this feature please refer to the `Kinibi Developer's Guide` for details about the Endorsement API. An additional configuration step has to be performed on the Kinibi image to make the Trusted Storage driver use Rollback Protection. See chapter Appendix I, **Error! Reference source not found.** for more details.

The MobiConfig tool is provided to inject keys hashes into a binary such as the Kinibi Image and can be found in the directory: `SecureIntegration/tools/MobiConfig`:

```
$ cd SecureIntegration/tools/MobiConfig
$ java -jar Bin/MobiConfig.jar
    -c
    -i mobicore.img.raw
    -o mobicore.img
    -k VendorTltSig_pub.pem
    -ek endorsementPubKey.pem
```

See also Appendix II for full list of MobiConfig options.

3.4.2.2 Signing the System Trusted Applications and Drivers

All System Trusted Applications and drivers must be signed with the signing key `PuK.Vendor.TltSig`.

The MobiConvert tool is provided to sign a Trusted Application and can be found in the directory: *`t-base-dev-kit/t-sdk/TlSdk/Bin/MobiConvert`*.

```
$ cd t-base-dev-kit/t-sdk/TlSdk/Bin/MobiConvert
$ java -jar MobiConvert.jar
    -b my_system_trustlet.axf.conf
    -servicetype 3
    -output 00010002000300040005000600070008.tlbin
    -k VendorTltSig.pem
```

3.4.2.3 Signing the Kinibi Image

Signing Kinibi with `VendorBoot.pem` has to be done by the OEM or ODM and a signature check of must be performed before starting up.

3.4.3 Configuring Content Management Trusted Application

The Content Management trusted application is the secure peer of the Normal World component RootPA. It is involved:

- In production, during device manufactory, to generate the Authentication Token.
- At runtime, once the device is deployed, for Content Management on the Secure side (containers creation).

3.4.3.1 Configure the Content Management Trusted Application

The goal of this step is to inject the KPH request signing key (`PuK.Kph.Request`) into the Content Management Trusted Application so that Kinibi can authenticate the requests coming from the KPH.

Each key comes with a KID to identify it (in some use cases, several keys can be supported):

```
$ cd SecureIntegration/tools/MobiConfig
$ java -jar MobiConfig/Out/Bin/MobiConfig.jar
    -c
    -i tlCm.axf
    -o tlCm.axf.conf
    -k MobiConfig_GuD_KPH_public_key.pem
    --kid 0
```

3.4.3.2 Signing the Content Management Trusted Application

The Content Management Trusted Application is a System Trusted Application. Once configured with the KPH request signing key and its KID, it must be signed with the usual System Trusted Application Signing key (`PrK.Vendor.TltSig`):

```
$ cd t-base-dev-kit/t-sdk/TlSdk/Bin/MobiConvert
$ java -jar MobiConvert.jar
    -b tlCm.axf.conf
    -servicetype 3
    -output 07010000000000000000000000000000.tlbin
    -k VendorTltSig.pem
```

The signed Content Management Trusted Application must be installed on the device in the Registry and must survive a device factory reset or wipe.

3.4.4 Signing the Trusted User Interface Driver

The Trusted User Interface driver is an optional new driver in Kinibi-300 that must be signed and installed on the device.

As a platform dependent component, the number of threads of the TUI driver is variable depending of the implementation. It is **5** for the reference TUI integration on Arndale (DCI, IPC, Exception, touch and VSYNC thread). It may be more if integration specific code launches additional threads. For instance, TUI integration on Qualcomm based devices has **6** threads (DCI, IPC, Exception, touch and Blitter and SafeKeeper thread).

```
$ cd t-base-dev-kit/t-sdk/DrSdk/Out/Bin/MobiConvert
$ java -jar MobiConvert.jar
    -servicetype 1
    -numberofthreads 5 or 6
    -bin drTui.axf
    -output 070c0000000000000000000000000000.drbin
    -d 257
    -memtype 2
    -flags 0
    -interfaceversion 1.0
    -keyfile VendorTltSig.pem
$ cp 070c0000000000000000000000000000.drbin
070c0000000000000000000000000000.tlbin
```

The signed driver must be installed on the device in the Registry and must survive a device factory reset or wipe.

3.4.5 Signing the DRM Driver

The DRM driver is an optional driver that must be signed and installed on a compatible device when required.

```
$ cd t-base-dev-kit/t-sdk/DrSdk/Out/Bin/MobiConvert
$ java -jar MobiConvert.jar
    -servicetype 1
    -numberofthreads 3
    -bin tlDrTplayDrm.axf
    -output 070b00000000000000000000000000000.drbin
    -d 1536
    -memtype 2
    -flags 0
    -interfaceversion 1.0
    -keyfile VendorTltSig.pem
$ cp 070b00000000000000000000000000000.drbin
070b00000000000000000000000000000.tlbin
```

The signed driver must be installed on the device in the Registry and must survive a device factory reset or wipe.

3.4.6 Signing the Key Injection Tool Trusted Application

The Key Injection Tool Trusted Application is an optional new System Trusted Application in Kinibi-410a that must be signed and installed on the device.

```
$ cd t-base-dev-kit/t-sdk/TlSdk/Bin/MobiConvert
$ java -jar MobiConvert.jar
    -b taKeyInjectionTool.axf
    -servicetype 3
    -gp_level GP
    -output 10c9cd73b89a5dd3941a1783390bbde4.tabin
    -k VendorTltSig.pem
    -numberofthreads 1 -numberofinstances 16 -memtype 2
    -flags 8 -interfaceversion 0.0
    -initheapsize 16384 -maxheapsize 65536
```

The signed Key Injection Tool Trusted Application must be installed on the device in the Registry and should be removed after key injection in the factory.

3.5 TEE IMAGE BUILDER

In Kinibi-410, Kinibi allows embedding of TAs and SWd drivers into the TEE binary image. That way such TAs can start right after TEE boot and before Linux (sometimes called 'Early TAs'). This is an alternative to storing System TAs in the mcRegistry folder and passing the TA blob during the mcOpenSession call.

The loading time/order of these SWs embedded services can be customized by property flags described in next section.

Typical output of Kinibi image builder tool:

```
TEE image:
  0x00000000:  84 KiB kernel
  0x00015000:   4 KiB image header
  0x00034000: 124 KiB core module: McLib
  0x00035000: 136 KiB core module: RTM
  0x00057000:  56 KiB service: sth2
  0x00065000:   4 KiB service: stproxy
  0x00066000:  56 KiB service: drcrypto
       xx000:  xx KiB service: SIP Driver
       xy000:  yy KiB service: OEM TA
  0x00074000: end of TEE image, size 464 KiB
```

The product package contains the TEE image builder under `SecureIntegration/t-base-kit/Build` directory. The content of the directory is as follows:

```
t-base-kit/
    Locals/
      Build/
      Code/
      Objects/
        driver-rpmb/
        CHIP_ID/
    Out/
```

The respective folders in Objects/ contain the stripped ELF/binary files of the components that make up the Kinibi TEE image.

Note that the highlighted components are considered as "TEE core" components. If those folders aren't present in the package, it means that they are delivered as part of the TEE image. In this case the initial TEE image shouldn't be altered (eg: remove a core service), as it would comprise the validity of the final product. The Image Builder offers the possibility to add a non-core service to the initial TEE image (eg: driver-rpmb).

The TEE image builder depends on python and the python ELF library from:

https://github.com/eliben/pyelftools

On an Ubuntu/Debian system, you can install them with the following command:

```
$ sudo apt-get install python-pip
$ sudo pip install pyelftools
```

Sample command line:

```
$ python imageBuilder.py \
   --input <in_path>/tee.img \
   --output <out_path>/tee.img \
   --services TA_NAME:flags:none:UUID.tlbin
```

This tool can be executed several times, before or after having called MobiConfig. There is no specific usage restriction and both tools are fully independent.

3.5.1 How to use

3.5.1.1 Help outputs

```
$ python imageBuilder.py -h
usage: imageBuilder.py [-h] [--quiet] [--verbose] [--cfg <tee.cfg>]
                       [--output <tee.img>] [--input <tee.img>]
                       [--mustMatchImage <tee.img>] [--kernel <kernel.elf>]
                       [--rtm <rtm.elf>] [--mclib <mcLib.elf>]
                       [--services <name:flags:caps:binary>
[<name:flags:caps:binary> ...]]
                       [--removeServices <name> [<name> ...]]
optional arguments:
  -h, --help            show this help message and exit
  --quiet, -q           don't print anything
  --verbose, -v         print details
  --cfg <tee.cfg>, -c <tee.cfg>
                        TEE config (Trustonic use only)
  --output <tee.img>, -o <tee.img>
                        TEE image to create
  --input <tee.img>, -i <tee.img>
                        TEE image to modify or print information about
  --mustMatchImage <tee.img>
                        existing TEE image to compare newly created image to
                        (Trustonic use only)
  --kernel <kernel.elf>
                        kernel AXF/ELF
  --rtm <rtm.elf>       RTM AXF/ELF
  --mclib <mcLib.elf>   McLib AXF/ELF
  --services <name:flags:caps:binary> [<name:flags:caps:binary> ...]
                        services to add/overwrite in image
  --removeServices <name> [<name> ...]
                        services to remove from image
```

3.5.1.2 Service options

The service option should fit the next template: `<name:flags:caps:binary_path>`. Note that the `name` of the service is automatically truncated to an 8 characters long string.

When specifying a service, following `flags` can be defined:

Flags	Behavior
`startOnBoot`	The TEE will start the Service (TA or Driver) directly after initialization of RTM and other embedded services.: - This flag is not supported for GP-TAs (NWd client mandatory in GP spec.).

	- With this flag, loading order is defined by order in the image (or concatenation order)
`startableAfterBoot`	When the TEE receives an open-session request, the TEE searches the respective UUID in the list of embedded services and starts the embedded service with priority over a service in SFS or in mcRegistry.

The `caps` field is now only available for Trustonic internal use and must remain “none”.

The `binary_path` configuration field should point to the driver binary (output of the MobiConvert tool). Note that if this binary was signed during the MobiConvert step, the Image Builder will truncate the service signature when adding it to the TEE image (meaning no TA signature check done when loaded a service from the embedded image).

3.5.2 Specific case to embed the SWd RPMB driver

The RPMB SWd driver is a specific SWd Driver as it is used directly by the Kinibi Secure Filesystem. Kinibi need a way to identify this particular RPMB service and the way to do this identification is based on Image Builder field `name`.

SWd RPMB driver MUST be called “**drrpmb**”. It’s the only way for the TEE to uniquely identify it, UUID and DrID can be customized without any constrains.

In order to integrate it into the TEE image, TEE package is offering 2 solutions:

- Either use directly the standard ImageBuilder python script:

```
$ python imageBuilder.py \
 --input ./t-base/Bin/MobiCore/$TARGET/$MODE/tee.img \
 --output SecureIntegration/t-base-kit/Out/$PLATFORM/$MODE/tee.img \
 --services drrpmb:startOnBoot:none:07050000…0021.tlbin
```

With `$TARGET` and `$MODE` set to the relevant targeted platform name and build mode (Usually TEE package is only containing one platform mode, root directory under `./t-base/Bin/MobiCore/`)

- Either use Trustonic drrpmb sample build helper script (finally only a wrapper script):

```
$ cd SecureIntegration/t-base-kit
$ TARGET=HUAWEI_AARCH32_HIKEY \
  ./Locals/Build/build.sh --rpmb-bin 07050000…0021.tlbin \
                          --rpmb-drv-flags startableAfterBoot
```

With `TARGET` environment variable set again to relevant targeted platform name.

Both options should create the final TEE image in:

```
SecureIntegration/t-base-kit/Out/$PLATFORM/$MODE/tee.img
```

The resulting image then has to undergo usual others configuration as described in other parts of this guide.

3.6 KINIBI BOOT PARAMETERS ON 32 BIT HARDWARE

The entity that starts up Kinibi, usually a platform secure bootloader, should use the boot configuration block as an interface to Kinibi. The configuration block can be customized according to needs but must transfer at least the following information to Kinibi.

Example of Kinibi boot arguments on an Uboot integration:

Register	Values
r0	0, Cold boot. 1, Wake up from sleep.
r1	Pointer to MCSysInfo block (physical address, MCSysInfo_ptr). Defined below.
r13 / sp	MC boot stack (physical address) / 20 words available
r14 / lr	Start address of NWd. Kinibi jumps to this NWD address after changing the NS bit.

For reference here is the definition of the Kinibi system information structure:

```
typedef struct {
    uint32_t            magic;       //
    uint32_t            version;     // 0x00010000
    uint32_t            length;      // 0x00000030 (bytes)
    uint32_t            flags;       // Reserved
    struct mem_info_t   dram_total;  // Total DRAM area
    struct mem_info_t   dram_sec;    // Secure DRAM area
    struct mem_info_t   sram_total;  // Total SRAM area
    struct mem_info_t   sram_sec;    // Secure SRAM area
} MCSysInfo_t, *MCSysInfo_ptr;

typedef struct {
    uint32_t       base; // physical address (32bits)
    uint32_t       size;
} mem_info_t;
```

3.7 KINIBI ON ARM64 HARDWARE

On this type of hardware platform, the entity that starts up Kinibi is the *Trusted Firmware* (reference version provided by ARM). To start a new integration, Trustonic will provide a reference version that includes an implementation of the *Secure Payload Dispatcher (spd)* in charge of the Kinibi component.

3.7.1 Kinibi Boot Parameters on 64 bit Hardware

For reference, here is the definition of the Kinibi system information structure:

```
typedef struct {
    uint32_t magic;         // magic value from information
    uint32_t length;        // size of struct in bytes.
    uint64_t version;       // Version of structure
    uint64_t dRamBase;      // NonSecure DRAM start address
    uint64_t dRamSize;      // NonSecure DRAM size
    uint64_t secDRamBase;   // Secure DRAM start address
    uint64_t secDRamSize;   // Secure DRAM size
    uint64_t secIRamBase;   // Secure IRAM base
    uint64_t secIRamSize;   // Secure IRAM size
    uint64_t conf_mair_el3;// MAIR_EL3 for memory attributes sharing
    uint32_t RFU1;
    uint32_t MSMPteCount;   // Number of MMU entries for MSM
    uint64_t MSMBase;       // MMU entries for MSM
    uint64_t gic_distributor_base;  // GIC dist base address
    uint64_t gic_cpuinterface_base; // GIC CPU base address
    uint32_t gic_version;           // GIC version
    uint32_t total_number_spi;      // Total SPI number in the system
    uint32_t ssiq_number;           // interrupt used for TEE comm.
    uint32_t RFU2;
    uint64_t flags;
} bootCfg_t;
```

3.7.2 SMC from SWd to ATF monitor

3.7.2.1 SMC_TEE_FC_INPUT

Kinibi uses the fastcall input to read platform-specific properties from the monitor.

Register	Value	Explanation
R0	0xB2000005	
R1	DataId	Identifier for data to be read, see below for possible IDs
R2	Length	Requested data length in bytes

Data is returned as follows:

Register	Value	Explanation
R0	Status	Status code, 0=ok.
R1	Offset	Offset to MSM
R2	realLen	Real length of data in MSM.

DataId indicates read data as follows:

ID	Value	Explanation
1	HWIdentity	Chip identity information (SUID), total of 96 bits.
2	HWKey	Chip –specific random key value.
3	RNG	Read random number based on true random number generator.
4	Freq	Platform frequency in kHz, divisor for CNTPCT.
5	Firmware version	Get ATF version information string, official version.
6	Firmware binary version	Get ATF version information string, exact version like git revision.
7	SysTA RP disabled	Get fuse value to see if should be disabled (see Chapter Appendix I).

The sample code in SecureIntegration/spd shows how to implement these callbacks.

To start a new integration, Trustonic will provide additional documentation.

3.8 FASTCALLS HOOK MECHANISM

A FastCall is a call to the ARM SMC instruction with some specific parameters that allow the execution of some routines in Kinibi without performing a complete context switch.

Kinibi makes use of this to communicate to the ARM ATF, if that is present in the SWd.

Kinibi also provides a mechanism to allow Secure World drivers installed in Kinibi to react to FastCalls from the Normal world or the Secure World.

FastCalls are always executed in IRQ Mode with FIQ and IRQ masked and must therefore execute as little, carefully designed, code as possible.

The calling convention for the ARM SMC instruction for performing FastCalls is as follow:

FastCall Parameters (Input)

```
r0          FastCallID (always < 0)
r1 – r3     FC parameters depending on the FastCallID
```

Return Values (Output)

```
r0          FastCallID (always < 0) of the FC which has been executed
            (r0 from input data)
r1 - r3     status information / data (depending on FC)
            (r1 returns status "0" or error)
```

Kinibi already supports either generic or platform-specific internal FastCalls. They are mainly used for Kinibi initialization and common operations that have to be done by the Normal World but can only be performed in the Secure World.

FastCalls have the following limitations:

- They cannot call any TlApi or DrApi functions
- They may be executed concurrently on several CPUs
- They must not cause any exception. There is no means to recover in case an exception is triggered by a FastCall.

3.8.1 Handling FastCalls

Kinibi allows two Secure Drivers known as Firmware Drivers to register an additional FastCall handler that will be called for FastCall IDs that are not known to Kinibi. "*Firmware Driver*" is a naming convention for the two drivers to install a FastCall handler during Kinibi runtime. It is intended to act as a system integration means, compared to other hardware peripherals' drivers. One Firmware Driver is intended to be developed by the Silicon Provider (SiP) to handle FastCalls related to the silicon platform and the second Firmware Driver is intended to be developed by the OEM to handle FastCalls related to the device.

As it must always be available as soon as the FastCall handler has been registered, the Firmware Driver **must** be marked as permanent in the driver flags defined in its `Makefile`:

```
DRIVER_FLAGS := 1 # 0: no flags; 1: permanent; […]
```

The Firmware Driver routine gets called whenever Kinibi kernel's FastCall handler receives an ID designated by ARM as a SIP or OEM fastcall ID:

- SiP fastcall ID > 0x81000000
- OEM fastcall ID > 0x83000000

By calling the `drApiInstallFc()` function, the Firmware Driver indicates which FastCall ID it is handling.

Regarding the information shared between the Firmware driver and the Fastcall handlers: the Fastcall handlers get Firmware driver memory mappings in the range of 0-2MB at the time the handler is installed. As there is absolutely no synchronization mechanism between the Firmware driver and the FastCall handlers once installed, it is mandatory for the Firmware driver to not unmap any of these mappings.

In addition, if new mappings are made by the Firmware driver after FastCall installation, they cannot be relied upon to be visible in Fastcall hook functions.

3.8.2 Additional Secure Driver APIs

The main header file for the Driver API extension is `DrApiFastCall.h`.

```
#include "DrApi/DrApiFastCall.h"
```

3.8.2.1 Types

3.8.2.1.1 FastCall Registers

```
typedef uint32_t *fastcall_registers_t;
```

Depending on the platform, a FastCall handler may have access to at least 4 registers (r0 to r3).

Each time an SMC is sent and caught by the Firmware driver, they are forwarded by Kinibi to the Firmware driver through the `fastcall_registers_t` table. The size of this table can be determined by field, `registers`, from FastCall context structure (`struct fcContext`)

3.8.2.1.2 FastCall Context

```
struct fcContext {

      /* Size of the context */
      uint32_t size;

      /*Callback to modify L1 MMU mapping */
      void *(*setL1Entry)(fcContext_t context,
                          uint32_t idx,
                          uint32_t entry);

     void *(*setL1Entry64)(struct fcContext *context,
                           uint32_t idx,
                           uint64_t entry);

      /* Number of registers available in FastCalls handler */
      uint32_t registers;

      void (*prepareIdenticalMapping)(struct fcContext *context,
                                      addr_t start,
                                      uint32_t length,
                                      uint32_t flags);   void
(*generateFcNotification)(struct fcContext *context);
};
```

The FastCall context structure, `fcContext_t`, is filled when the Firmware driver is initialized in Kinibi and forwarded as a parameter to the FastCall hook initialization function.

Note: This context is shared between FastCalls and all the CPUs of the application processor.

The `setL1Entry` callback can be used at runtime to map additional memory in the FastCall context:

- `context`: The context parameter to the fastcall hook.
- `idx`: The Index of the section in the table of L1 descriptors; this is highly system dependent. In the current Kinibi version values from 0 to 7 are valid.
- `entry`: The L1 descriptor that will be used for the mapping.

The value returned by the function `setL1Entry` is the virtual address of the mapped area (`NULL` in case of error).

However, these mappings, done in the FastCall context, will not be visible from the Firmware driver.

The `prepareIdenticalMapping` callback is not supported as of Kinibi-410a.

The `generateFcNotification` callback can be used at runtime to generate a notification interrupt from the FastCall hook context to a Secure World driver (by default this feature is based on SGI 8).

Both of the above features, `prepareIdenticalMapping` and `generateFcNotification`, are highly system dependent and may not be available in all Kinibi versions.

3.8.2.2 Specific FastCall Entry Points

3.8.2.2.1 FastCall Handler Initialization

```
typedef uint32_t (*fcInitHook)(
      struct fcContext *context
);
```

This entry point is called once when FastCall Hooking is enabled through a call to the `drApiInstallFc` driver API (Firmware driver initialization). It is executed in Secure SVC mode.

This function must **never** cause any exception.

Parameters

- `context`: FastCall context structure.

Returns

It must return 0 if initialization is successful otherwise, with any other value, the FastCall will not be allowed.

3.8.2.2.2 FastCall Handler

```
typedef uint32_t (*fcEntryHook)(
      fastcall_registers_t *regs,
      struct fcContext *context
);
```

This is the actual FastCall handler. It may be executed concurrently on several CPUs and is executed only in IRQ mode.

This function must **never** cause any exception.

Parameters

- `regs`: Normal World registers' values:
  - On entry, `regs[0]` to `regs[context->registers - 1]` contain input parameters. `regs[0]` is always the FastCall identifier.
  - On exit, `regs[0]` to `regs[3]` store output results.
    - `regs[0]` is always the FastCall identifier.
    - `regs[1]` can be used to store a return value.
    - `Regs[2]` free to use
    - `Regs[3]` free to use
    - Other registers **must not** be modified; the result of any modification is unpredictable.

    By convention, if the FastCall identifier is unknown the value `MC_FC_RET_ERR_INVALID` should be returned in r1.
- `context`: FastCall context structure.

Returns

A non-zero value should be returned when a FastCall is handled internally and zero when the FastCall is not known.

3.8.2.3 Specific Firmware Driver APIs

3.8.2.3.1 drApiInstallFc

```
_DRAPI_EXTERN_C drApiResult_t drApiInstallFc(
      void *entryTable,
      uint32_t fastcallOwner)
```

Install the custom FastCall handler.

Parameters:

- `entryTable`: table of function pointers to FastCall Hooking entry points (see section 3.8.3, "Firmware Driver Structure").
  - `entryTable[0]` should point to a function of type `fcInitHook`
  - `entryTable[1]` should point to a function of type `fcEntryHook`
- `fastcallOwner`: define which FastCall IDs will be handled by the hook. Currently supported values :
  - `FASTCALL_OWNER_SIP`
  - `FASTCAL_OWNER_OEM`

Returns:

- `DRAPI_OK` if the FastCall handler has been correctly set
- `E_DRAPI_NOT_PERMITTED` if this function is called from a non-driver context
- `E_DRAPI_INVALID_PARAMETER` if `entryTable` does not point to code in the driver
- `E_DRAPI_CANNOT_INIT` if the driver has not been configured as permanent
- `DRAPI_ERROR_CREATE(E_DRAPI_CANNOT_INIT, E_MAPPED)` if another FastCall handler has already been installed

3.8.3 Firmware Driver Structure

3.8.3.1 FastCall Hook Initialization

Initialization of FastCall handling is done by the Firmware driver, it boils down to building a 2-entries table where:

- the first element is a pointer to the FastCall initialization function,
- the second one is a pointer to the actual FastCall handler.

```
void *entryVector[2] = { &fcInit, &_fcMain };

_DRAPI_ENTRY void drMain(
    const addr_t    dciBuffer,
    const uint32_t  dciBufferLen
){
      drApiResult_t ret = drApiInstallFc(entryVector);
      if (E_OK != ret)
      {
          drDbgPrintf("Initialization failed: %x\n", ret);
          ...
      }

      /* Start IPC handler */
      drIpchInit(dciBuffer, dciBufferLen);
}
```

3.8.3.2 Assembly Glue for the FastCall Handler

The FastCall handler, once installed, will be executed in the context of the Monitor and eventually on any CPUs available. While the main Monitor might have a decent stack, it might not be the case for the secondary monitors. For this reason, it's required to setup a new stack before entering in the FastCall Handler

The following piece of assembly code is an example of how to reserve specific stacks for each CPU on which the FastCall handler may run and use the correct one when it is executed (`_fcMain` is the function installed, it then calls the real FastCall Handler, `fcMain`):

```
      export _fcMain
      import fcMain

CORES_MAX   equ  48
STACK_SIZE  equ  256 * 4

      area stack, noinit, readwrite
fcStackBottom
      space CORES_MAX * STACK_SIZE
fcStackTop

      area text, code, readonly
      preserve8
      arm
_fcMain
      push { r6-r8, r12, lr}
      mov r12, sp

      ; get affinity level 0 core number in r1
      mrc    p15, 0, r7, c0, c0, 5    ; get mpidr
      ubfx   r6, r7, #0, #4           ; cpu id(1-3)
      ubfx   r7, r7, #8, #4           ; cluster id (8-11)

      ; set own core-specific stack
      ldr    r7, =fcStackTop
      mov    r8, #STACK_SIZE
      ; calculate stack-start for this core
      mul    r6, r6, r8
      ; by sp = top - (core_num * size_core)
      sub    r7, r7, r6
      mov    sp, r7

      ; save the old stack in the new stack
      push {r12}
      blx fcMain
      ; get the old stack back
      pop {r12}
      mov sp, r12
      ; restore the context from the old stack
      pop { r6-r8, r12, lr}
      bx lr

      end
```

3.8.3.3 FastCall Handler Example

The FastCall Handler is divided into two steps:

- The initialization function, called by Kinibi when the Firmware driver installs the FastCall hook:
- `uint32_t` fcInit(fcContext *context)

```
{
    /* Initialization code here…
     * Runs in Kernel context */

    /* optionally map things… */
    void *virt = context->setL1Entry(context, 0,
fcMakeL1PTE(phys_addr));
    return 0;
}
```

- The FastCall Handler, called each time an SMC is not recognized by Kinibi Monitor:

```
uint32_t fcMain(
    fastcall_registers_t *regs,
    fcContext *context)
{
    uint32_t mpidr;
    uint32_t fastCallID = regs[0];

    switch(fastCallID){
        case FASTCALL_SOMETHING:
            doFCSomething(regs);
            return 1;        default:
            break;
    }
    return 0;
}
```

3.8.4 u-boot Integration Example

Trustonic can provide on demand specific bootloader/u-boot sample code to demonstrate integration of the Firmware driver in u-boot.

The goal of this a this approach would be that the FastCall hook is available for u-boot and for the very early boot sequence of the Normal World OS. However, Trustonic is today considering this solution as **deprecated** and would recommend relying on Kinibi `ImageBuilder` tool to integrate this type of services directly into the TEE binary image.

3.9 FIQ FORWARD MECHANISM (ARMV8)

Trustonic TEE allows forwarding a FIQ (usually processed at EL1 level) to the ARM Trusted Firmware in order to process it with the maximum privileged level (EL3).

Even if this mechanism allows virtually any processing to be done at EL3 level for a given interrupt, developer must keep in mind the following things:

- At the time the dedicated callback is reached at EL3 level (plat_tbase_forward_fiq(), more details in chapter FIQ Forward handling), **the FIQ is already acknowledged and terminated from a GIC perspective (GICC_EOIR has been written for this interrupt)**.
- Developer must NOT trigger a world-switch from this place.

As detailed in following chapters, using this feature requires some effort during integration phase in order to

1. configure the forward mechanism
2. implement the associated handler for forwarded FIQs.

3.9.1 FIQ Forward configuration

Configuring the FIQ forward mechanism can be achieved by calling the following function for each FIQ that has to be forwarded and processed at EL3 level.

```
void tbase_fiqforward_configure(uint32_t intrNo, uint32_t enable);
```

Parameters

```
intrNo:
      this data must be set to the interrupt ID to be configured
enable:
      TBASE_FLAG_SET will enable the FIQ forward mechanism for the
target interrupt
      TBASE_FLAG_CLEAR will disable the FIQ forward mechanism for the
target interrupt
```

Returned value

```
      Not applicable
```

Calling this function must be done during the Trustonic TEE initialization phase from the Secure Payload and Dispatcher.

In order to keep the SPD structure simple and agnostic of this process, another function has been added to plat_tbase.c file as a dedicated placeholder for FIQ forward configuration calls:

(note: plat_tbase.c is the common placeholder for platform abstraction of Trustonic TEE's SPD to the silicon platform)

```
void plat_tbase_fiqforward_init(void)
{
        printf( "Configuring TEE forwarded FIQs...\n");

        /* Watchdog FIQ configuration */
```

```
        tbase_fiqforward_configure( WDT_IRQ_BIT_ID,    /* interrupt id
*/
                                    TBASE_FLAG_SET ); /* enable
forward */

        /* Another forwarded FIQ, just for testing purpose */
        tbase_fiqforward_configure( 162,               /* interrupt id
*/
                                    TBASE_FLAG_SET ); /* enable
forward */
}
```

Previous implementation is an example on how to configure the mechanism to enable forwarding interrupts WDT_IRQ_BIT_ID and 162 to the ARM Trusted Firmware.

Default implementation will be empty, and it's up to the silicon partner or the OEM to enable/disable FIQ forwards during the platform integration step by calling appropriately `tbase_fiqforward_configure()` from the `plat_tbase_fiqforward_init()` function.

3.9.2 FIQ Forward handling

At runtime, each time a FIQ is triggered, Trustonic TEE kernel will check if it has to be forwarded to the ARM Trusted firmware.

1. If IT IS NOT the case, it will be normally processed by the kernel and dispatched to the task waiting for it (if any).
2. If IT IS the case, the kernel will not dispatch this interrupt further to any tasks running in the TEE and will trigger a dedicated fastcall (hidden to the developer), finally calling the following function with the forwarded interrupt number as parameter :

```
uint32_t plat_tbase_forward_fiq(uint32_t fiqId)
```

Parameters

```
fiqId:
      this data holds the interrupt number of the forwarded FIQ.
```

Returned value

```
      PLAT_TBASE_INPUT_OK if the appropriate processing was done
successfully.
      PLAT_TBASE_INPUT_ERROR otherwise.
```

Please note the returned value is ignored by the Trustonic TEE kernel as of today, but could potentially be used in later versions.

As an example, for the same interrupts as in FIQ Forward Configuration chapter, the following code could be used:

```
uint32_t plat_tbase_forward_fiq(uint32_t fiqId)
{
        uint32_t Status = PLAT_TBASE_INPUT_OK;
        uint32_t linear_id = platform_get_core_pos(read_mpidr());

        /* Verbosity */
        printf( "core %d EL3 received forwarded FIQ %d from the TEE
!\n", (int)linear_id, (int) fiqId);
```

```
        /* Handle forwarded FIQ */
        switch (fiqId)
        {
        case WDT_IRQ_BIT_ID:
                /* Dump the platform… */
                platformDump();
                break;
        case 162:
                /* just a simple test */
                printf("%s: That's a test !\n",__func__);
                break;
        default:
                /* Unknown FIQ */
                printf("%s: FIQ %d was forwarded but no processing was
associated to it.\n",__func__,fiqId);
                Status = PLAT_TBASE_INPUT_ERROR;
                break;
        }


        return Status;
}
```

 Default implementation will be empty and it's up to the silicon partner to implement the expected processing in **`plat_tbase_forward_fiq()`**, during the platform integration step.

3.10 BLACKLIST MEMORY FEATURE

Trustonic TEE allows EL3 and EL2 to send SMC to manage blacklisting of memory. Once a memory area is blacklisted, it can't be mapped by any component of the TEE such as TA, Drivers and even TEE itself. It can be useful to isolate some critical segments of memory.

3.10.1 Definitions

2 SMC can be sent to the Trustonic TEE from EL3 or EL2.

```
#define TEE_FC_SMC_FASTCALL_BLACKLIST_ADD        (0xFF00003A)
#define TEE_FC_SMC_FASTCALL_BLACKLIST_REMOVE     (0xFF00003B)
```

TEE_FC_SMC_FASTCALL_BLACKLIST_ADD <start_address>, <length>, <flag>, <unused>

This fastcall, when succeeding, will blacklist the memory segment starting at <start_address> and ending at <start_address> + <length> - 1.

(First non-blacklisted byte will be <start_address>+<length>).

When a memory segment is blacklisted, then the TEE kernel, its drivers and TAs cannot map it. This memory segment will remain inaccessible from the TEE until it is un-blacklisted by a call to TEE_FC _SMC_FASTCALL_BLACKLIST_RM fulfilling requested conditions.

TEE_FC _SMC_FASTCALL_BLACKLIST_REMOVE <start_address>, <unused>, <flag>, <unused>

Memory can be un-blacklisted by the Execution Level which has first blacklisted it or a higher Level.

3.10.2 Parameters

Arguments for the "ADD" SMC will be <start address>, <length>, <flags>

Arguments for the "REMOVE" SMC will be <start address>, <unused>, <flags>

- <**start address**> and <**offset**> should be 4KB aligned addresses
- <**length**> indicates size of the memory chunk to be blacklisted.

  The first non-blacklisted block available for the TEE will be <start address> + <length>

- <**flags**> can be used to store whatever information needed by the caller. The 8 upper bits are reserved to Trustonic use to store the Execution Level of the caller.

  Caller should only use the lower 24-bits.

3.10.3 Possible return code

```
MC_FC_RET_OK              0   /**< No error. Everything worked fine. */
MC_FC_RET_ERR_INVALID     1   /**< FastCall was not successful. */
TEE_FC_RET_ERR_NOABILITY  6    /**< Call is not allowed. */
```

3.10.4 Limitations

Blacklist entries are limited to 512. If the limit is reached, the TEE will reject all "ADD" until an entry on the list is deleted by a "REMOVE" call.

Only EL3 and EL2 NWd can send those 2 SMCs. Call from other Level of execution will be rejected.

EL2 cannot "REMOVE" memory blacklisted by EL3. Call will be rejected.

<start_address> and <offset> parameters should be 4K aligned. Otherwise, call will be rejected.

3.10.5Examples

Examples on ATF using Trustonic generic `tbase_monitor_fastcall` can be found in the SPD sample code.

1) Blacklist 1 memory page.

```
tbase_monitor_fastcall(TEE_FC_SMC_FASTCALL_BLACKLIST_ADD, 0x1000000,
0x1000, 0x1234,0x0, &resp);
```

➔ Here we blacklist 1 4K page of memory starting from 0x1000000 physical address. Flag to be stored will be 0x1234 (meaningless here), 4th parameter is unused.

2) To un-blacklist it, and so allow the TEE and its components to map the memory:

```
tbase_monitor_fastcall(TEE_FC_SMC_FASTCALL_BLACKLIST_REMOVE,
0x1000000, 0x0, 0x1234, 0x0, &resp );
```

➔ On REMOVE call the offset is pointless. If the <start_address> AND the <flag> matches an item in the blacklist array, then the whole memory block is un-blacklisted.

Here both conditions are met so the RM will succeed.

3) Blacklist 5 memory pages

```
tbase_monitor_fastcall(TEE_FC_SMC_FASTCALL_BLACKLIST_ADD,0x1000000,
0x5000,  0x0, 0x0,  &resp );
```

As the <start_address> is not already present in the list, the block will be added to the blacklisted memory.

4 RPMB INTEGRATION

Kinibi protects against the following rollback attacks:

- Replacing a Secure Filesystem partition with an old version
- Replacing a System TA with an old version

See for the different components and partitions:

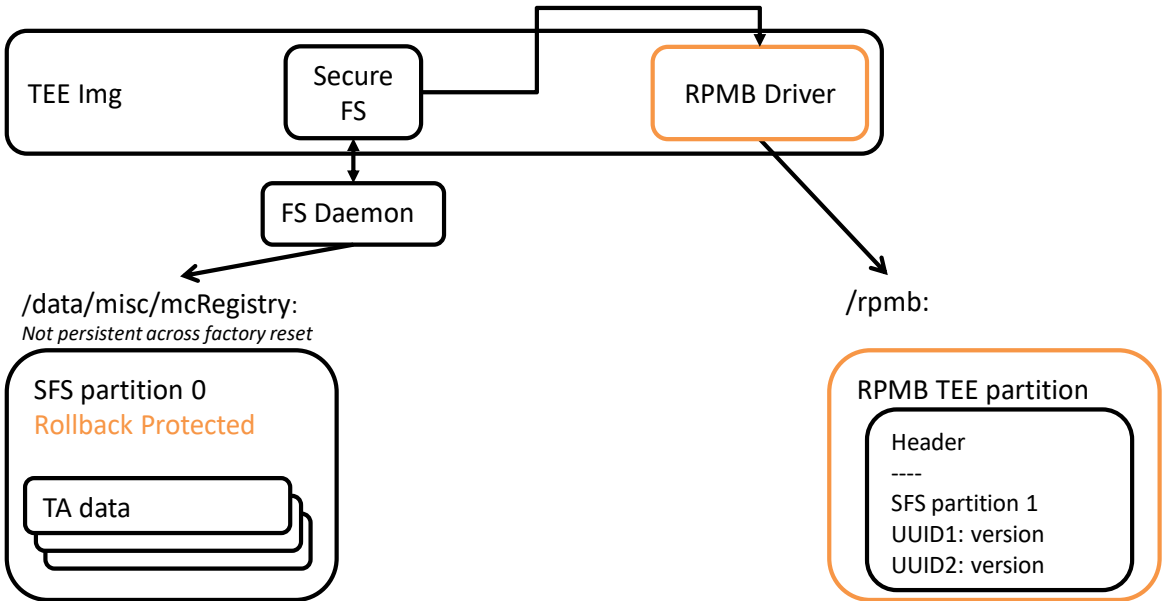


Figure 3: Secure Storage System

4.1 SECURE STORAGE SYSTEM

The Kinibi Secure Filesystem provides the GlobalPlatform Trusted Storage API to Trusted Applications and Secure Drivers. The Secure Filesystem handles file accesses using a sophisticated B+ tree that allows an efficient retrieval of the persistent objects with a reduced number of I/O operations. The underlying partitions are stored in the Normal world with the help of the Filesystem Daemon (FSD). The FSD is part of the Kinibi Daemon and connects to the Secure Filesystem at Daemon startup. FSD will then wait for requests from the TEE to modify the partition backend files.

Kinibi-400A supports two partitions:

- partition 0: user data and TA binaries
  - persistent objects accessed via the GlobalPlatform Trusted Storage API
  - TA binaries installed via TAMv2
  - user-specific
  - wiped during factory reset
  - e.g. “/data/misc/mcRegistry”
  - Daemon parameter -p <path>
  - Should be TEE rollback protected
- partition 1: System TA version information
  - version information for system TAs that are not using the GlobalPlatform API
  - system-specific
  - persist factory reset
  - Stored directly in RPMB partition

4.2 CONFIGURING KINIBI IMAGE FOR RPMB USE CASES

By default, the RPMB support in Kinibi image is disabled.

The integrator has to integrate an RPMB driver and configure the Kinibi image with the desired RPMB behavior using MobiConfig. The MobiConfig Rollback Protected Storage(--rps) mode is based on bitmasks matching SFS partitions and can set the flags for up to the 16 partitions.

If an RPMB driver is integrated into Kinibi, partition 1 is stored in RPMB directly.

Currently there is one option/mask:

MobiConfig option	**Behavior**
`--rollback_protected_partitions`	Enable Rollback Protection for partitions in mask. When the Rollback Protection is activated, the Secure Filesystem recognizes if the backend partition was rolled back to a previous state and returns respective error codes in the GlobalPlatform Trusted Storage API.

Below are two examples demonstrating few example of configurations:

4.2.1 Rollback Protection for partition 0 and 1:

The integrator has to configure the TEE image with MobiConfig:

```
$ cd SecureIntegration/tools/MobiConfig
$ java -jar Bin/MobiConfig.jar
    --rps
    -i tee.img
    -o tee_rps.img
    --rollback_protected_partitions 3
    --chunk-id 0
```

Value 3 is a SFS partition ID bitmask, who in this particular case means:

- Partition 0, the one used by GP Secure Storage is RPMB globally protected (`--rollback_protected_partitions [0000 0011]`)
- Partition 1, the one used by TEE to store System TA versions is RPMB globally protected (`--rollback_protected_partitions [0000 0011]`)

Complete behavior in the example configuration:

- If you remove Secure Storage 0, you will lose your data for sure, but partition will be reformatted (system will not be blocked by TEE and it's up to the TA to react when they will see that data are no more present).
- Partition 1 will be created in RPMB directly, no way for attacker to remove it.

4.2.2 No Rollback Protection for partition 0:

The integrator has to configure the TEE image with MobiConfig:

```
$ cd SecureIntegration/tools/MobiConfig
$ java -jar Bin/MobiConfig.jar
    --rps
    -i tee.img
    -o tee_rps.img
    --use_mask 2
    --chunk-id 0
```

In this setup, only SFS Partition 1 will be Rollback Protected and and stored in RPMB. As no Rollback Protection is set for partition 0, if Store0.tf removed, rolled back or corrupted, SFS will detect the corruption and simply reformat a new store (data previously stored inside would be lost for sure).

For more information about MobiConfig, see Appendix II.

4.3 INTEGRATING RPMB HARDWARE

For the Kinibi Rollback Protection to work, the device must have an RPMB-compatible peripheral and Kinibi must access it. The integrator has to implement a custom secure channel between the RPMB driver and the RPMB peripheral. The RPMB driver must be adapted to the Kinibi Secure Filesystem.

Kinibi has two ways to integrate the platform RPMB driver:

- Use the skeleton DrRPMB driver and implement the Trustonic RPMB interface
- Use its own SIP-proprietary RPMB driver and share the marshalling structure with Trustonic

The Secure Filesystem Driver communicates with the RPMB driver to read and write a rollback counter for partition 0 and to access partition 1. The SFS driver needs to know the marshalling structure for RPMB read and write commands and the RPMB driver ID.

4.3.1 Integrating RPMB Driver

The product package contains the **DrRPMB** sample driver in SecureIntegration/rpmb/DrRPMB directory.

DrRPMB Secure Driver UUID

The DrRPMB UUID is :

0705-0500-0000-0000-0000-0000-0000-0021

DrRPMB driver ID

The DrRPMB Driver ID is : 0x0700

Commands

The DrRPMB must implement the following commands:

```
RPMB_MESSAGE_TYPE_OPEN        1
RPMB_MESSAGE_TYPE_CLOSE       2
RPMB_MESSAGE_TYPE_WRITE       3
RPMB_MESSAGE_TYPE_READ        4
```

Marshalling Parameters Structure

The driver must implement the following interfaces:

```
typedef struct {
    uint32_t size;    /* Size of the exchange buffer message: 16 + n */
    uint16_t version;  /* Must be 0. Reserved for future extensions */
    uint16_t command;     /* Command identifier */
    uint32_t status;      /* Return status */
    uint32_t handle;      /* Object handle */
    union {
        struct {
            addr_t   data;
            uint32_t data_size;
        }
        cmdRPMBOpen_t cmdRPMBOpen;
        rspRPMBOpen_t rspRPMBOpen;
        cmdRPMBRead_t cmdRPMBRead;
        rspRPMBRead_t rspRPMBRead;
        cmdRPMBWrite_t cmdRPMBWrite;
        rspRPMBWrite_t rspRPMBWrite;
    } payload;
} rpmbExchangeBuffer_t,*rpmbExchangeBuffer_ptr;
```

To start a new integration, Trustonic will provide an additional document explaining the interface in more detail.

Startup integration

The integrator has to embed the RPMB driver into the TEE image using the TEE image builder (See Appendix I).

The integrator should start the RPMB driver as the first driver loaded by mcDriverDaemon -r.

4.3.2 Integrating Custom RPMB driver using marshalling structure

The product package contains the drRPMB.lib sample code in SecureIntegration/rpmb/DrRPMB directory.

RPMB marshalling

This is the sample implementation:

File name	Behavior
`Locals/Code/drRpmbApi.h`	Interface definition of tlApiRpmbRead() and tlApiRpmbWrite()
`Locals/Code/platforms/Generic/drRpmbApi.c`	Sample implementation of tlApiRpmbRead() and tlApiRpmbWrite()
`Locals/Code/drRPMBMarshal.h`	Sample marshalling structure

The integrator should update the marshaling structure and share with Trustonic.

Trustonic needs to know:

- RPMB driver ID
- RPMB marshalling for RPMB read and RPMB write
- RPMB driver UUID

TEE Image integration

The integrator has to use the TEE image builder to include the platform-specific DrRPMB in the TEE image (See Appendix I). The image builder will take the following file to include in TEE image:

```
SecureIntegration/rpmb/DrRPMB/Out/Bin/ARM_V7A_STD/GNU/$(MODE_DIR)/drRPMB.axf
```

Startup integration

The integrator has to embed the RPMB driver into the TEE image using the TEE image builder.

The integrator should start the RPMB driver before starting any other TA or Driver that requires the Rollback protection.

The RPMB driver should be started by the mcDriverDaemon using –r option.

4.4 SYSTEM TA DOWNGRADE PROTECTION

Kinibi protects legacy System TAs and GP TAs as well against downgrade attacks. Respective TAs and Secure Drivers must be specifically marked with a version > 0 and the downgrade-protection flag. Kinibi will then automatically enroll them, automatically upgrade the last known version and fail opening a session to the service if an attacker downgrades the TA.

See for an overview of the feature:

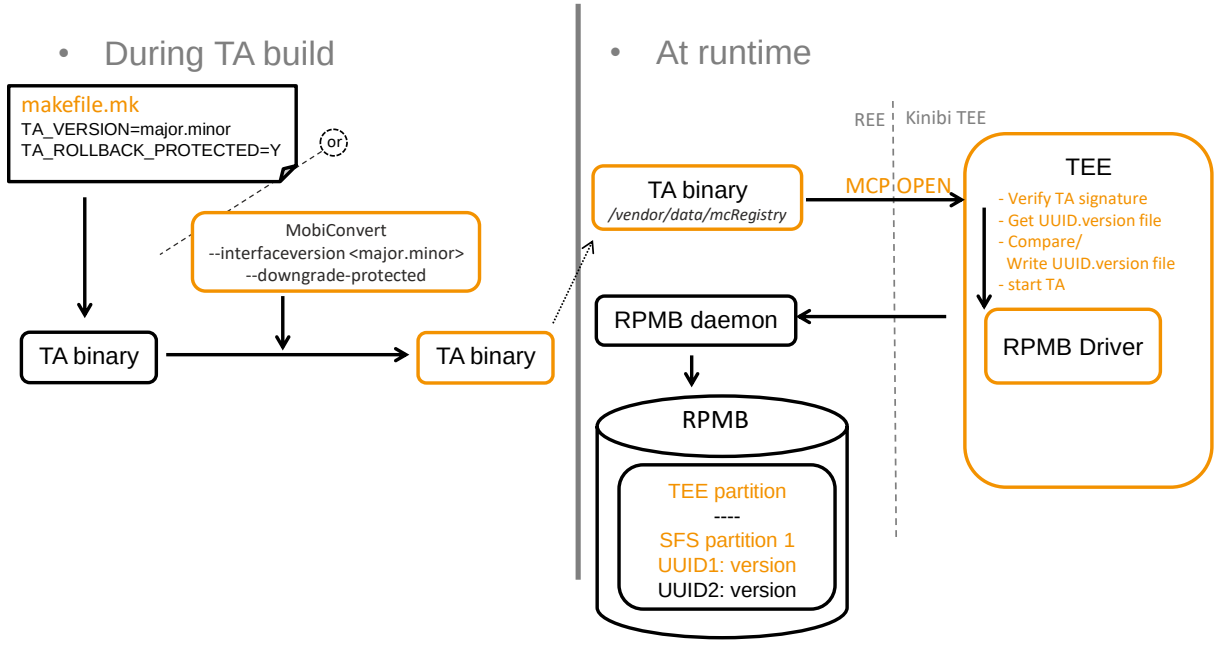


Figure 4: System TA Downgrade Protection

The integrator has to do the following steps to enable TA downgrade protection:

1. Integrate an RPMB driver (see Appendix I)
2. Inject a minimum version into the TA (see Appendix I)
3. Activate automatic enrolment of the TA by setting the dp flag in the TA (see Appendix I)

Note that Kinibi now checks the version of each TA. If the version is not 0.0, a lookup in the SFS Partition 1 is performed to find a minimum version. This can fail during early boot. Trustonic advises Integrators to set TA version to 0.0 for early-boot TAs that need to start before the Daemon.

4.4.1 Marking TAs for downgrade protection

Set a minimum version

With MobiConvert:

```
-iv 0.1, --interface-version <major.minor> : activate downgrade
                                             protection for the TA
```

In TlSdk makefiles:

```
TA_VERSION:=0.1
```

Enable automatic enrolment

MobiConvert, TlSdk and DrSdk makefiles accept new options:

New MobiConvert option:

```
-dp, --downgrade-protection: activate automatic enrolment for STADP
```

New TlSdk option:

```
TA_ROLLBACK_PROTECTED:=Y
```

New DrSdk option:

```
DR_ROLLBACK_PROTECTED:=Y
```

Sample

Sample call to create a downgrade protected TA with version 0.1:

```
java -jar MobiConvert.jar -b <pathToBinary> -o <pathToOutput> -k
<pathToKeyFile> -s 3 --downgrade-protected --interface-version 0.1
```

4.4.2 Disabling System TA downgrade protection with a hardware Fuse

While TA downgrade protection is an important aspect of overall device security, it creates some hurdles during the development cycle, similar to secure boot. Integrators usually overcome this hurdle with a hardware fuse that they burn only on development devices.

Kinibi supports disabling of the System TA downgrade protection feature via a fuse.

- Platform-dependent code needs to read this fuse.
- By default, the fuse is read as System TA Rollback Protection enabled.

- On ATF-based platforms, Kinibi calls the new PLAT_TBASE_INPUT_SYS_TA_RP_ENABLED call to retrieve the value of the fuse. See also 3.7.2.1.

5 SYSTEM TA ENCRYPTION

Kinibi-410a supports System TA and Secure Driver encryption. The integrator must do three things:

1) encrypt its TAs and Drivers,
2) in the factory, inject the decryption key into the device using the TAKeyInjectionTool, and
3) on startup of the mcDriverDaemon, pass the wrapped decryption key for loading into the TEE.

5.1 ENCRYPTING TRUSTED APPLICATIONS AND DRIVERS

The Kinibi Developers Guide, *Kinibi_Developers_Guide.pdf*, shows how to encrypt a signed System TA or Driver using `MobiConvert -encrypt` mode with a key file or an HSM.

The OEM first has to sign the TAs and then encrypt them.

5.2 USING THE KEY INJECTION TOOL

Kinibi comes with a template key injection tool used to inject a key in clear text in the factory.

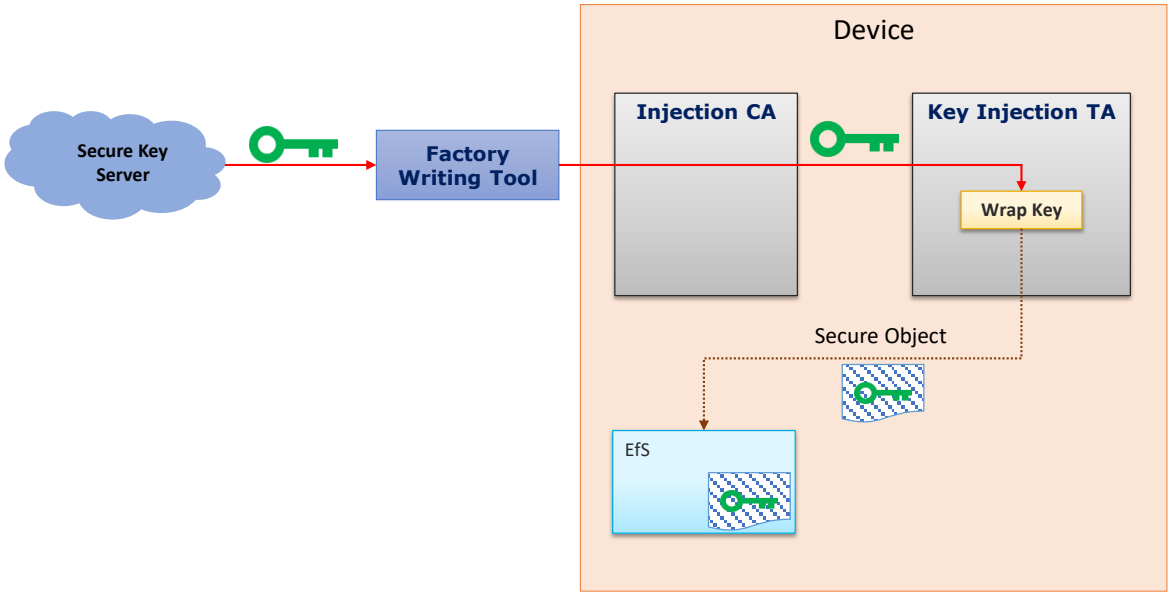


Figure 5: Key Injection Tool

The Key Injection Tool consists of a GP Client Application and a GP System TA. The System TA cannot be encrypted itself. The Key Injection TA creates a secure object which is linked to the UUID of the TA. The OEM cannot change this UUID. The Client Application transfers the key in clear text to the TA, the TA wraps it and then the CA stores the secure object in a partition that survives the factory reset. In the next step, the Kinibi Daemon retrieves the secure object from this location.

The OEM has to ensure to remove the key from the device after the manufacturing phase. All traces of the key and also the key injection tool should be removed before delivery of the device.

5.2.1 Integrating TAKeyInjection

The product package contains the **TAKeyInjectionTool** template in SecureIntegration/KeyInjectionTool/TAKeyInjection directory.

TAKeyInjectionTool Trusted Application UUID

The TAKeyInjectionTool UUID is:

10c9-cd73-b89a-5dd3-941a-1783-390b-bde4

Note that the UUID must not be changed.

5.2.1 Integrating CAKeyInjection

The product package contains the CAKeyInjectionTool template in AndroidIntegration/Src/mobicore/CAKeyInjection.

5.3 LOADING THE KEY ON EACH BOOT

After key injection, the wrapped key must be loaded into the TEE on each boot using the Kinibi Daemon. See the following figure:

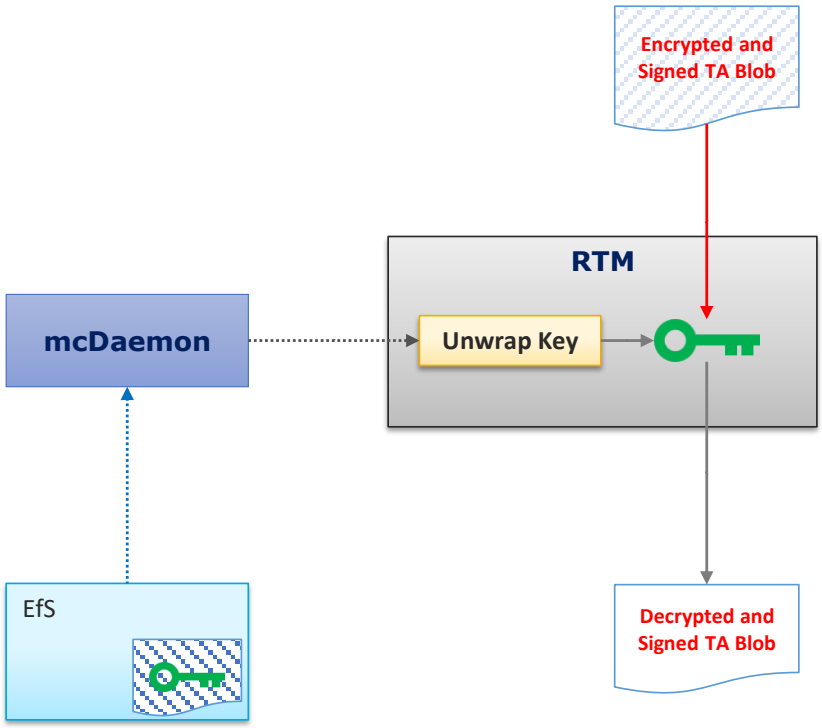


Figure 6: Loading decryption key into TEE

The OEM can use the Kinibi Daemon to load the wrapped key into the TEE by adding the path to the decryption key to the command line when starting the Daemon:

```
mcDriverDaemon -d /efs/encryptionKey.bin.so
```

6 DRM INTEGRATION

Kinibi supports a Secure Driver for DRM which allows Trusted Applications to process DRM content through a set of standard APIs. The Secure Driver once implemented must provide a means for the DRM Trusted Applications to decrypt encrypted content data and store the resulting data in protected regions of memory. The Secure Driver is responsible for verifying that the entire process is kept secure, this includes:

- Verifying the entire address range for output data is protected.
- Verifying integrity of decoder firmware (if required, according to design)
- Managing multiple sessions if multiple DRM sessions are supported concurrently.

6.1 HIGH LEVEL FLOW

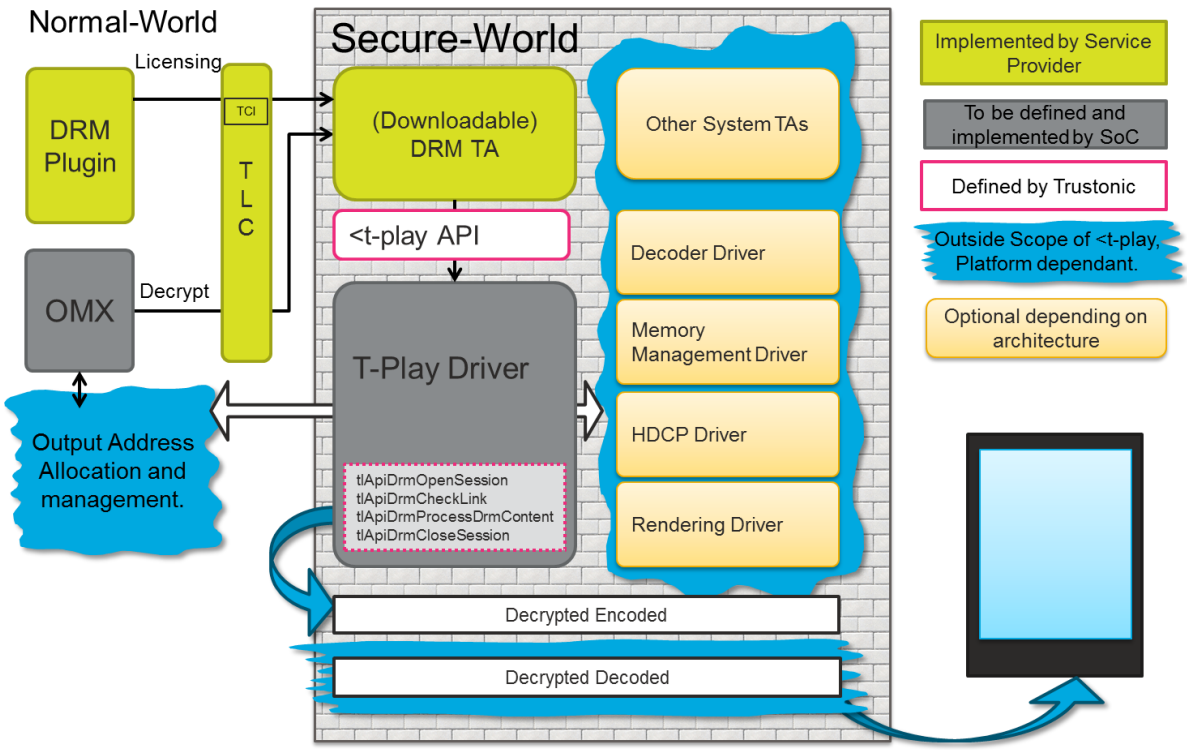


Figure 7: DRM components overview

The following is an example of one possible high level sequence :

1. The DRM Secure Driver will be authenticated by the secure OS.
2. During runtime the application is passed a DRM protected Stream.
3. The DRM Plugin handles the license acquisition with the DRM Trusted Application.
4. ACodec::allocateBuffersOnPort is called by the OMX component and a platform dependent mechanism is initiated to identify the output buffer to be used for the decrypt.
5. The value returned from allocateBuffersOnPort is set as the output reference and shall be passed unmodified to the DRM driver when the decryption is being processed.

6. The NW Client will allocate a region of world shared memory and place the encrypted content in it.
7. The Trusted Application calls the DRM Driver `openSession` function. If multiple sessions are going to be supported the session handle can be passed if known, and null if a new session is being opened.
8. The driver must initialize any hardware that will be required for example the crypto accelerator, decoder hardware, and raise the firewalls to protect any pre-defined memory regions.
9. If the encryption algorithm is not supported by the driver the Trusted Application will decrypt the content itself (software based) and call the DRM driver's `processDrmContent` function passing the clear data and the function's 'processmode' parameter set to 'PLAIN'. The DRM Secure Driver will need to copy this data into the predefined protected buffer and signal the media framework.
10. If the encryption algorithm is supported, the `processDrmContent` function will be called with processMode set to decrypt, the output address will be resolved according to format of the parameter passed via output and the data decrypted to this address. The media framework will then be signaled to know the encoded clear data is ready.
11. The decryption of data will continue until it has been fully successfully decrypted at which point the Trusted Application will call `closeSession` and finalize the operation by cleaning buffers and disabling firewalls.
12. The handling of the decoding and rendering is outside the scope of this document and of the DRM APIs.

6.2 T-PLAY ASSUMPTIONS

1. Mixed Input Data

It is assumed that if the buffer received by the TA contains mixed clear and encrypted segments, all data must be passed to the driver to be managed. The same restriction applies as above, in that the output address is not known by the TA. This can be done using the APIs defined to first copy the clear data to the output buffer and then decrypt the rest to overwrite the relevant segments.

6.3 DRIVERS OVERVIEW

6.3.1 Framework Support

The APIs defined by this document are provided in a stub form. If the DRM functionality is required it is necessary to implement a driver for the platform according to the hardware specifications. If the functions are not implemented the error `DRIVER_NOT_IMPLEMENTED` will be returned by default to any calls to the driver.

6.3.2 TLC and TA Driver Access

A trusted driver can only have one normal world client, therefore if we wish to communicate with the driver from both a TLC and a Trusted Application we must open the session using the TLC that will use the DCI directly with the driver. The session must then remain open which will allow the TA to access the driver.

It is advised that the session be opened and the driver be loaded at boot time, and then it can remain loaded and be accessible when required. It would also be recommended to implement the TLC as a kernel module, to restrict the access rights on who can use the driver APIs.

6.3.3 Driver-Client Access Control

Access control is not required in the driver as no assets are available to the Trusted Application in clear. If an unauthorized Trusted Application attempts to access the driver it cannot gain access to protected content. Please see Section 4. Security and Evaluation Considerations.

6.3.4 Threads

Below, the threads required in the implementation of the drivers are described, for more information on their usage please see [DrDrvGuide].

6.3.4.1 Exception Handler Thread

This is the main thread and runs with higher priority than IPC handler thread. Its main responsibility is to handle exceptions caused by the IPC handler thread. The exception handler is implemented in 'drTplayExcHandler.c'. When the IPC handler thread is started in drTplayIpcHandler.c (see `drIpchInit()`), the exception handler thread is registered as local exception handler. When the IPC handler thread causes an exception, the Kinibi kernel informs the exception handler. Then the IPC handler thread is restarted if exception is segmentation fault. If it is caused by, for example, undefined instruction, etc, the DRM Driver shuts down.

6.3.4.2 IPC Handler Thread

This is the second thread and it handles IPC messages sent by Trusted Applications. The IPC handler thread runs with lower priority than the exception handler thread and it is implemented in 'drTplayIpcHandler.c'. When it receives IPC messages from Trusted Applications, it checks function id, processes incoming requests accordingly and responds to Trusted Applications with relevant status code. For various operations such as AES encrypt/decrypt and data copy requests, the driver should maps Trusted Application's address space to access Trusted Application data. '`drApiAddrTranslateAndCheck()`' API call can be used for this purpose.

6.3.4.3 DCI Handler Thread

This is the third required thread and it intercepts IPC messages sent by Trusted Application Connectors. The DCI handler thread runs with lower priority than the exception handler thread but a higher priority than the IPC thread and it is implemented in 'drTplayDciHandler.c'. When it receives IPC messages from the normal world, it should parse the incoming data, and process incoming requests accordingly, finally responding to Trusted Application Connector with relevant status code.

6.3.5 Protected Buffers

The address at which the protected buffers lie must be within a predefined range which must be retrieved by the driver at runtime. This can either be passed as a parameter from the normal world, hardcoded within the driver or passed from the kernel through a Kinibi interface. The chosen method is platform dependent. For more information on the protected buffers and security concerns see section 4 of this document.

6.4 DRM DRIVER PROTOCOL

The DRM agent Trusted Application will call the DRM tlApi.

The driver will call drApiMapClientAndParams which returns a marshaling parameter which is given in more detail in the following sections according to the driver and the command being executed.

DRM Driver
/** * Function IDs */ typedef enum { FID_DR_OPEN_SESSION 1 FID_DR_CLOSE_SESSION 2 FID_DR_PROCESS_DRM_CONTENT 3 FID_DR_CHECK_LINK 4 } Sec_FuncID_t;

Table 2: Driver Command IDs

DRM Secure Driver UUID

The DRM Secure Driver UUID is :

070b-0000-0000-0000-0000-0000-0000-0000

Secure Playback driver ID

The DRM Secure Driver ID is : 1536

Marshalling Parameters Structure

```
/**
 * Union of marshaling parameters. */
/* If adding any function, add the marshaling structure here
 */
typedef struct {
    uint32_t     functionId;  /* Function identifier. */
    union {
        uint8_t                 *returned_sHandle;
        uint8_t                 sHandle_to_close;
        tlDrmApiDrmContent_t    drmContent;
        tlDrmApiLink_t          link;
        int32_t                 retVal;      /* Return value */
    } payload;
} tplayMarshalingParam_t, *tplayMarshalingParam_ptr;
```

Commands

The DRM driver supports the following commands:

```
0x00000001 (FID_DR_OPEN_SESSION)
0x00000002 (FID_DR_CLOSE_SESSION)
0x00000003 (FID_DR_PROCESS_DRM_CONTENT)
0x00000004 (FID_DR_CHECK_LINK)
```

6.4.1.1 FID_DR_OPEN_SESSION

Command ID

0x00000001

Effect

This command is used to set hardware and context configurations according to what will be required depending on the content that will be decrypted. Buffers and structures can be organized and initialized with values if required.

The firewalls must also be enabled by this command.

Error Code

- `TLAPI_DRM_OK` if operation was successful.
- `E_TLAPI_DRM_INTERNAL` general error in case of crypto problem
- `E_TLAPI_DRM_MAP` in case of error mapping memory to driver.
- `E_TLAPI_DRM_PERMISSION_DENIED` in case of rights access related issue
- `E_TLAPI_DRM_SESSION_NOT_AVAILABLE` in case the driver is busy and cannot open a session.
- `E_TLAPI_DRM_DRIVER_NOT_IMPLEMENTED` in case the function is not implemented.

6.4.1.2 FID_DR_CLOSE_SESSION

Command ID

0x00000002

Effect

The DRM Agent sends this command to the DRM Secure Driver to disable the firewalls and carry out any necessary cleanup required. The driver does not free any memory, it merely changes the property and raises a flag to indicate the firewall is enabled.

Any buffers used by the secure driver should be reset so that their content is not readable after the firewalls have been disabled.

Error Code

- `TLAPI_DRM_OK` if operation was successful.
- `E_TLAPI_DRM_INTERNAL` in case of failure.
- `E_TLAPI_DRM_DRIVER_NOT_IMPLEMENTED` in case the function is not implemented.

6.4.1.3 FID_DR_PROCESS_DRM_CONTENT

Command ID

0x00000003

Structure passed in Marshaling Parameter

```
typedef struct {
    uint8_t                         sHandle,
    TL_DRM_DecryptContext           decryptCtx,
    uint8_t                        *input,
    TL_DRM_InputSegmentDescriptor   inputDesc,
    uint16_t                        processMode,
    uint8_t                        *output
} tlDrmApiDrmContent_t, *tlDrmApiDrmContent_ptr;
```

Effect

The DRM Agent sends this command to the DRM Secure Driver to either send decrypted content to the protected buffer, or to pass encrypted content for the driver to decrypt into a protected buffer so as to be processed by the media framework.

The function takes an offset as parameter within the InputSegmentDescriptor structure that is used to calculate the exact location in the output buffer to place the clear data. The output buffer must be known to the driver at this point. This can be done by a number of ways depending on the implementation, for example the protected region may always be static and the address can be hardcoded within the driver, the kernel can pass the address dynamically via a Kinibi interface, or the values could be stored in a secure registry and read out only when required.

The driver must ensure that the data to be decrypted falls within the limits of the firewalled region.

Error Code

- `TLAPI_DRM_OK` if operation was successful.
- `E_TLAPI_DRM_INVALID_PARAMS` incorrect parameters in input.
- `E_TLAPI_DRM_INTERNAL` general Error in case of crypto problem
- `E_TLAPI_DRM_MAP` in case of error mapping memory to driver.
- `E_TLAPI_DRM_PERMISSION_DENIED` in case of rights access related issue
- `E_TLAPI_DRM_REGION_NOT_SECURE` if the memory for output is not protected
- `E_TLAPI_DRM_ALGORITHM_NOT_SUPPORTED` in case the algorithm is not supported.
- `E_TLAPI_DRM_DRIVER_NOT_IMPLEMENTED` in case the function is not implemented.

6.4.1.4 FID_DR_CHECK_LINK

Command ID

0x00000004

Effect

The DRM Agent sends this command to the DRM Secure Driver to check the external link information like HDCPv1, HDCPv2, AirPlay, and DTCP.

Error Code

- `TLAPI_DRM_OK` if operation was successful.

- `E_TLAPI_DRM_INTERNAL` in case of failure.
- `E_TLAPI_DRM_DRIVER_NOT_IMPLEMENTED` in case the function is not implemented.

6.5 SECURITY AND EVALUATION CONSIDERATIONS

6.5.1 Video Buffer Protection

Trustzone technology allows for two methods of protecting buffers, we will use the naming conventions as follows:

1. *Protected Memory* : The memory region is protected by an access control that is based on the Bus ID.
2. *Secure Memory :* The security bit of the memory region is enabled.

Depending on the implementation there will be up to three buffers to protect, a buffer to contain the decrypted encoded data, one for decrypted decoded and another for the display. An implementation may choose to use the same buffer for multiple uses if desired.

The memory can be protected by one of the following methods:

1. *A Trusted Normal World Component.*
   If we receive notification from a normal world component that the memory is protected it is imperative that the trust has already been established with that component.

2. *Bus master filtering.*
   In this case we enable the security at boot time and filter the access to the protected region according to Bus ID and thus can give access to only particular hardware such as the VPU.

3. *Using TZASC at runtime.*
   In this case the secure bit is enabled directly from within the driver.

In each of these cases there must be a check to ensure that the range of protected/secure memory is large enough to contain completely the input data so as not to leak any sensitive data to unprotected region.

6.5.2 Checking of Pointers

All pointers passed to the driver functions must be verified to ensure a bad address is not being used.

6.5.3 Input to Crypto Hardware

It must be verified that all sensitive inputs being passed to the crypto hardware (if used) are coming from secure memory.

6.5.4 Integrity of System Components

It is recommended that the video firmware is authenticated when loaded, and that it is loaded during the openSession command. This will ensure that the firmware is correct for each decrypt and avoids an attack where the firmware could be replaced after bootup.

The authenticity of any component can be verified with a hash/signature check, but it must be ensured that it is done using a public key stored in secure memory on the device.

6.5.5 Trusted Application Isolation

In order to protect the secrets between different DRM schemes sharing the same drivers, Kinibi implements isolation between Trusted Applications. Each trusted application executes in its own memory space and any persistent secure objects stored by the Trusted Application are only accessible by the Trusted Application thus protecting sensitive key data.

If multiple Trusted Application's require access to the Secure Driver then some form of session management or resource permissions must be implemented so as to avoid any denial of service.

6.5.6 Debug Attack

It is assumed that in any platform for commercial release that JTAG or similar debug functionality is disabled.

6.5.7 Reset Buffers

It is imperative that the memory used to store buffers, keys and any other assets during any part of the secure processes are correctly reset after use.

7 TRUSTED USER INTERFACE INTEGRATION

Kinibi comes with components and templates for integrating the Trusted User Interface (TUI) feature. The following diagram shows the Trusted User Interface architecture.

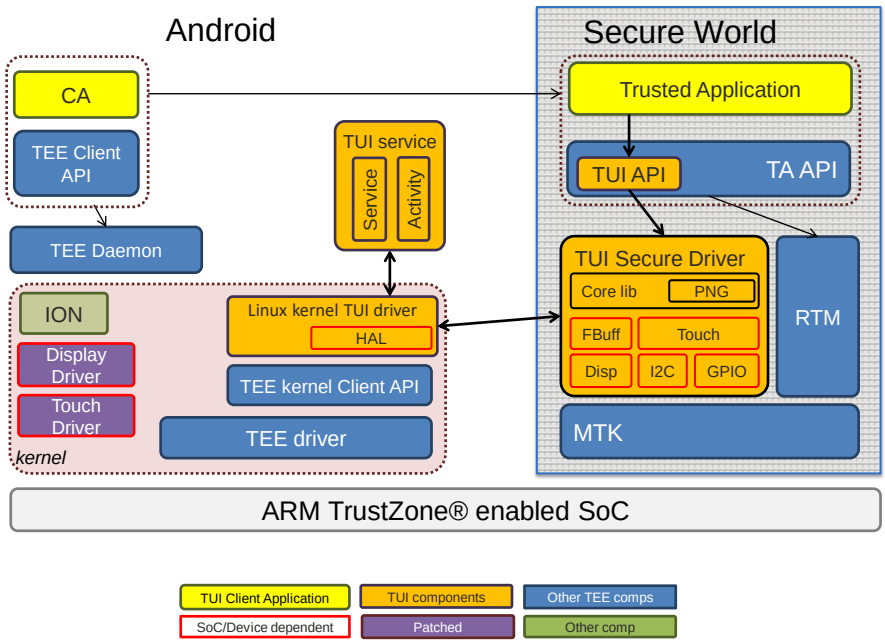


Figure 8: TUI components overview.

- The TUI application developer uses a TUI API as an extension of the TA API. This extension is hardware independent.
- The TUI secure driver in TZ Secure World is the core of the TUI implementation. It fully handles UI hardware within TUI session. It consists of a generic core part and a hardware abstraction layer (HAL) to be ported to the actual hardware. It is also internally linked with a TUI kernel driver running in the normal world.
- The TUI kernel driver is a proxy that links the TUI secure driver to the UI Linux drivers and a TUI Android service. It also contains a HAL to be ported to the actual kernel. The UI Linux drivers – typically touch, i2c and GPIO drivers for input, and display drivers – should be disabled and must not access the hardware within TUI session. They may need to be patched for this.
- Some system events must cancel an ongoing TUI session there is one. The TUI Service running in Android is designed to notice them and trigger the cancellation of the TUI session.
  The TUI service is started at boot time.
  Within TUI sessions the TUI service starts a TUI activity. The `android:keepScreenOn` attribute is set to true in TUI activity manifest and disables the Android screen timeout within TUI sessions.

Because TUI highly depends on the hardware of the device the TUI template cannot be considered as out-of-the-box product. The integrator must complete the porting for its own device.

7.1 SECURITY CONSIDERATIONS

The integrator must remember that the UI resources handled by the Secure-World (both hardware and software) manage sensitive information. This sensitive information must not be disclosed to the Normal-World during or after the TUI session. As part of ensuring this security requirement, Kinibi TUI has been designed to have exclusive access to UI resources within TUI session.

7.1.1 Framebuffer

Securing the display consists of securing the framebuffers, and optionally the display controller.

In case the framebuffers are allocated from secure world memory, the secure bootloader is responsible for setting up the TZASC and the framebuffers should not appear in any normal world mapping. The porting effort is limited to obtaining the physical address from the secure bootloader.

In case the framebuffers are allocated from normal world memory, they must be wiped before closing the TUI session. The TUI secure driver does it at every regular closing of the session. Furthermore, in case of a warm reset, the TUI secure driver may not have wiped the previous content of the buffers, therefore the secure bootloader must wipe the secure framebuffers from the previous boot before any normal world component is executed.

In case the framebuffers are allocated at fixed address the secure bootloader can just wipe it unconditionally. But in case it is allocated at variable address this address must be stored by the secure world in a location that is not lost after a warm reset. For this reason, it is recommended to locate the secure framebuffers at a fixed address.

If the framebuffers are allocated from the normal world, it is the responsibility of the secure integrator code to properly protect the buffer for secure-only access, for instance via TZASC. When the TUI driver receives the pointer and size of the framebuffer from the normal world, it passes it to a HAL function tuiHalFBProtect which should do the following:

- Check that the designated region consists entirely of normal world memory. If not, return a failure status.
- Change the TZASC configuration to make the buffer locked for secure access only.

These two steps must be done atomically. Failing to do it atomically may lead to race conditions if the framebuffers are shared with other secure services, like DRM.

7.1.2 Input devices

The input devices generally consist of an external touchscreen device linked to the main chip by an i2c interface and an additional GPIO as interrupt line.

The i2c bus is here critical because input data will transit on this bus. It must be fully protected during the TUI session. It means particularly that if the i2c bus is shared with other devices these other devices may not work properly during the TUI session.

The GPIO interrupt may be shared with many other devices in an interrupt decoding chain, making it very difficult to secure. The GPIO interrupt line is less critical as it only reveals that something has happened in input device. However it is sensitive because it may disclose the timing of key or button presses. It should be protected and managed by the secure world during TUI session.

The external touchscreen is critical too because it contains the last input events. It must be fully managed by the secure world during the TUI session. Furthermore particular attention must be paid to the sequence of operations when closing the TUI session. The touchscreen device should be reset before the closing completes, to ensure that the normal world cannot obtain any data on the last input events during the session. From a higher-level perspective, the input device should not be in use when closing the TUI session, to avoid disclosing the last action by the user. As the sequence of

operations to reset the device is hardware-specific, it needs to be customized by the hardware integrator. The following operations need to be performed:

1. Wait until the device state indicates that no finger is pressed.

2. Reset the input device so that it is subsequently impossible to read any information about past touch events.

7.2 TUI SECURE DRIVER

The TUI Secure Driver is provided as part of the Secure-World Integration components. It contains a part in source code – the HAL – and a part in binary – the core library. The integrator must complete the development of the HAL according to its platform and must recompile and sign the TUI Secure Driver image.

The following section give what needs to be taken care of in the Secure Driver.

7.2.1 Memory requirement

Double buffering:

The TUI driver requires three times the size of a full screen buffer as secure buffer.

This memory requirement is depending on both the resolution of the screen and the driver implementation.

- To reach the expected security level we are not considering any overlay or partial display. The secure display must be exclusive and full screen. The actual framebuffer size is then directly calculated from the display resolution.

  The current TUI driver implementation uses two framebuffers for rendering.

- The TUI core part needs a working buffer to uncompress images given by the TA. As images size can be up to full screen the working buffer is the same size as the framebuffer.

In case the secure buffers are allocated from Secure World memory (see Security Considerations) they must be reserved at boot time. Their addresses and size are recovered independently and successively using the function `tuiHalFBOpen`.

In case the secure buffers are allocated from Normal World memory (see Security Considerations) they must be contiguous. Their address and size are recovered at TUI session opening from the TUI kernel driver.

Drawing raw buffers of pixels:

The TUI driver allows Trusted Applications to draw raw buffers of pixels. They are allocated from TA memory space which is included in the whole TEE memory. To take benefit of drawing raw buffers the integrator should increase the permanent secure memory allocated for the whole TEE.

The recommended additional memory is about the same size as one frame buffer.

7.2.2 Lifecycle

The following entry point must be implemented by the integrator:

- `tuiHalGetVersion`: called at TUI driver loading to recover the version of the HAL software. If it does not match the version of the core library the initialization will fail.
- `tuiHalBoardInit`: called at TUI driver loading to give an initialization opportunity to the HAL software.

- `tuiHalHandleNwdMessage`: called when the TUI Secure Driver receives a message from the HAL of the NWd TUI kernel driver. The message contains one uint32_t of payload, whose meaning and interpretation is up to the integrator. If the TUI SWd HAL is not supposed to get any message from the TUI NWd HAL, then this function should do nothing.

The following callback is implemented by the core driver:

- `drTuiCoreCancelSessionRequest`: called at any time by the HAL to cancel a running TUI session if any.

7.2.3 Secure display

The entry points described in this section must be implemented by the integrator.

The following entry point is called at TUI secure driver loading:

- `tuiHalFBOpenV2`:
  - It is called at least three times, one for the working buffer, two for the framebuffers.
  - It must return the display metrics. Note that it includes the screen orientation: the integrator is responsible for returning the natural orientation of the device. It will not be changed by the TUI core driver.
  - It may return the physical address and size of the buffer in case the buffer is allocated from the Secure World memory. It only returns the size of the buffer in case it is allocated from Normal World memory.

The following entry points are called at TUI session opening:

- `tuiHalDisplayMapController`: setup MMU for the display system.
- `tuiHalDisplayProtectController`: setup TZPC for the display system.
- `tuiHalDisplayInitialize64`: initialize the display system for the Secure World.
- `tuiHalFBProtectV2`: setup TZASC for the framebuffer in case it is not taken from the Secure World memory. If you implement this function, please see guidelines from the “Security considerations” section.

The following entry points are called within TUI session:

- `tuiHalFBImageBltV2`: copy an image to a framebuffer. It may be a partial update of the framebuffer. The input format of raw image at this point is always the same: 32-bit per pixel (RGBA, where R is LSB). This function must support clipping.
- `tuiHalFBFillRect`: draw a rectangle filled with a given color to the destination framebuffer.
- `tuiHalFBPost`: post the framebuffer and wait until it is displayed.
- `tuiHalFBCopyArea`: copy a rectangle area of the source framebuffer to a place in the destination framebuffer. This function must support clipping.

The following entry points are called at TUI session closing:

- `tuiHalFBUnProtectV2`: release TZASC for the framebuffer in case it is not taken from the Secure World memory. If you implement this function, please see guidelines from the “Security considerations” section.
- `tuiHalDisplayUnmapController`: release MMU for the display system.
- `tuiHalDisplayUnprotectController`: release TZPC for the display system.
- `tuiHalDisplayUninitialize`: release the display system.

The following callbacks are implemented by the core driver as a reference software implementation. They can be called by the integrator if no hardware implementation is available:

- `drTuiFBBlit`: draw a clipped rectangle area of an image to the destination FrameBuffer.
- `drTuiFBCopyArea`: copy a rectangle area of the source FrameBuffer to a place in the destination FrameBuffer.
- `drTuiFBFillRect`: draw a rectangle filled with a given color to the destination FrameBuffer.

7.2.4 Secure input

The TUI driver handles a particular thread fully dedicated to the secure input. This thread is referred as touch thread.

The touch thread has to be created and started by the HAL when opening the TUI session and killed by the core driver when closing the TUI session.

The following entry point must be implemented by the integrator:

- `tuiHalTouchOpen`: called from the core driver main thread at session opening. It must manage the input device during TUI session and particularly implement the touch thread. The synchronization of main and touch thread can be done using some callbacks. This function is responsible for the touch device initialization and should not return before it is done.
- `tuiHalTouchGetInfoV2`: called from the core driver main thread at session opening after `tuiHalTouchOpen`. The integrator must give the touch resolution and the desired size of touch event queue.
- `tuiHalTouchClose`: called from core driver main thread at TUI session closing. It should kill the touch thread and release the touch hardware.
  Before returning this function must particularly wait until the device state indicates that no finger is pressed and reset the input device so that it is subsequently impossible to read any information about past touch events.

The following callbacks are implemented by the core driver and must be called by the integrator to synchronize the touch thread:

- `drTouchReportV2`: called from the touch thread to signal a touch event to the core driver. The reported events are queued in the core driver until the TA reads them. In case of an overflow the oldest events in the queue will be overwritten. The size of the touch event queue should be tuned at integration time using the touch interactive tests.
- `drTouchLock`: called from the touch thread to signal to the core driver that the touch hardware is being used and it must not be interrupted or stopped.
- `drTouchUnlock`: called from the touch thread to signal to the core driver that the touch hardware is not being used anymore. It also means that the i2c interrupt must not be attached anymore to the touch thread when calling this.

  The integrator must take care not to call this function while the touch device state indicates that a finger is pressed.

  After calling this the touch thread may be killed and the touch device reset.

7.2.5 Building the TUI secure driver

The TUI core library `SecureIntegration/tui/DrTui/Out/Bin/Release/drTuiCore.a` implements the platform-independent part of the TUI driver. It is provided as binary only.

The integrator must complete the source part of the TUI secure driver and link it against the core library to generate the TUI driver.

In case the TUI driver UUID has to be changed it must be updated in `SecureIntegration/tui/DrTui/Locals/Code/public/dciTui.h` and `SecureIntegration/tui/DrTui/Locals/Code/driver.mk`.

For any new device the integrator must create a new `makefile.<device>.mk` in `SecureIntegration/tui/DrTui/Locals/Code` and update the source files and options for his particular device. The driver should be built using a new makefile variable `<DEVICE>`:

```
$ cd SecureIntegration/tui/DrTui
$ DEVICE=<DEVICE> ./Locals/Build/build.sh
```

7.2.6 Integrating the TUI secure driver

The TUI secure driver must be installed into the mcRegistry makefilepath, which is located in `/vendor/app/mcRegistry`

```
$ adb push SecureIntegration/t-
base/bin/DrTui/<PLATFORM>/<MODE>/<driver>.tlbin /vendor/app/mcRegistry
```

7.3 TUI KERNEL COMPONENTS

7.3.1 TUI kernel driver

The TUI kernel driver is a proxy between the TUI secure driver and the Normal world components – TUI service and Linux drivers.

The entry points described in this section must be implemented by the integrator.

The following entry point is called at TUI kernel driver loading:

- `uint32_t hal_tui_init(void)`
  This function is called when the TUI kernel driver is initialized, either at boot time, if built statically in the kernel, or when the kernel is dynamically loaded if built as a dynamic kernel module. This function may be used by the integrator, for instance, to get a memory pool that will be used to allocate the secure framebuffer and work buffer for TUI sessions. The function must return 0 on success, or non-zero on error. If the function returns an error, the module initialization will fail.
- `uint32_t hal_tui_exit(void)`
  This function is called when the TUI kernel driver exits. It is called when the TUI kernel driver is unloaded, if built dynamically, and never called if built-in into the kernel. It can be used to free any resources allocated by `hal_tui_init()`.

The following entry points are called at TUI session opening:

- ```
  uint32_t hal_tui_alloc(
                tuiAllocBuffer_t  *allocbuffer,
                size_t             allocsize,
                uint32_t           number
  )
  ```
  This function is called when the module receives a CMD_TUI_SW_OPEN_SESSION message from the secure driver. The function must allocate '`number`' buffer(s) of physically contiguous memory, where the length of each buffer is at least '`allocsize`' bytes. The physical address of each buffer must be stored in the array of structure '`allocbuffer`' which is provided as arguments. Physical address of the first buffer must be put in `allocate[0].pa`, the second one on `allocbuffer[1].pa`, and so on.
  The function must return 0 on success, non-zero on error.
  ```

For integrations where the framebuffer is not allocated by the Normal World, this function should do nothing and return success (zero).

- `uint32_t hal_tui_free(void)`
  This function is called at the end of the TUI session, when the TUI module receives the CMD_TUI_SW_CLOSE_SESSION message. The function should free the buffers allocated by `hal_tui_alloc(…)`.
- `uint32_t hal_tui_deactivate(void)`
  This function should stop the Normal World display and, if necessary, Normal World input. It is called when a TUI session is opening, before the Secure World takes control of display and input.

  It must return 0 on success, non-zero otherwise.
- `uint32_t hal_tui_activate(void)`
  This function should enable Normal World display and, if necessary, Normal World input. It is called after a TUI session, after the Secure World has released the display and input.
  It must return 0 on success, non-zero otherwise.
- `void hal_tui_post_start(struct tlc_tui_response_t *rsp)`
  This function is called after framebuffer allocation, when allocation is done using the Android Native Window API. If the HAL does not use Android Native Window API for framebuffer allocation, this function is not called.

The following functions are used for communication with the TUI Secure Driver HAL:

- ```
  uint32_t hal_tui_process_cmd(
        struct tui_hal_cmd_t *cmd,
        struct tui_hal_rsp_t *rsp)
  ```
  This function is called when a message is received from the TUI Secure Driver HAL. It receives as input the parameter '`cmd`', which contains the message payload and whose meaning is up to the HAL. The output parameter '`rsp`' must be filled with the response to the message to be forwarded to the TUI Secure Driver HAL. Its interpretation is up to the HAL.
- `uint32_t hal_tui_notif(void)`
  this function is called when the TUI Secure Driver HAL notifies the TUI Kernel driver HAL. If the HAL is not expecting any notification from the TUI Secure Driver HAL, this function should do nothing.

The communication between TUI kernel module and TUI secure driver has several channels:

- Commands from the driver:
  - `CMD_TUI_SW_OPEN_SESSION`: TUI session is opening.
    - The TUI service must start watching the events that may cancel the TUI session.
    - In case the secure buffers are allocated from Normal World, they must be allocated now. The secure buffers must be contiguous and the total requested size is received as a parameter of this command.
    - The Linux drivers should stop using the UI hardware.
  - `CMD_TUI_SW_CLOSE_SESSION`:
    - The TUI service must stop watching the events that may cancel the TUI session.
    - The Linux drivers can use the UI hardware again.
    - In case the secure buffers are allocated in normal world they may be freed.
  - `CMD_TUI_SW_HAL`:
    - A message coming from the Secure HAL is received.
    - Actions to be done are up to the HAL. The callback `hal_tui_process_cmd` is called with the payload of the message and the response to be filled. The meaning and interpretation of the both the response and the response is up to the HAL.
  ```

- Responses from the normal world:
  - Each command from the secure driver must be acknowledged with a response from TUI kernel module. In particular the response to the CMD_TUI_SW_OPEN_SESSION command must contain the physical address of the secure buffer in case it is allocated from normal world memory.
- Notifications to the driver:
  - NOT_TUI_CANCEL_EVENT: notify the secure driver that an event that should cancel the TUI session was triggered in the TUI service.

7.3.2 Patching Linux drivers

The Linux drivers involved in UI – typically touch, i2c and GPIO drivers for input, and display drivers – must not access the hardware within TUI session. If not, security exceptions may be raised. The Linux drivers should be patched to avoid this and keep a safe behavior.

7.3.3 Building the kernel

This section is an addition of section 2.1.2 Kinibi Linux-kernel-space components.

It is assumed that input and video drivers have been patched according to the previous section.

The Kinibi TUI module can be found in `AndroidIntegration/Src/gud/TlcTui`

To enable automatic building inside the kernel follow these steps:

- Update Linux kernel configuration file `linux/drivers/gud/Kconfig` with following line (must be inserted at the end):

```
config TRUSTONIC_TRUSTED_UI
    tristate "Trustonic Trusted UI"
    depends on TRUSTONIC_TEE
    ---help---
      Enable Trustonic Trusted User Interface


config TRUSTONIC_TRUSTED_UI_FB_BLANK
    bool "Trustonic Trusted UI with fb_blank"
    depends on TRUSTONIC_TRUSTED_UI
    ---help---
    Blank the framebuffer before starting a TUI session
```

- And add the Kinibi TUI module to the Linux kernel build file `linux/drivers/gud/Makefile`:

```
obj-$(CONFIG_TRUSTONIC_TRUSTED_UI) += TlcTui/
```

- Then, run `make menuconfig` and in the *Device Drivers* page of the configuration menu, please select:
  - *Trustonic TEE Driver*
  - *Trustonic Trusted UI*
  - *Trustonic Trusted UI with fb_blank*

```
<*> Trustonic TEE Driver
[ ]   Trustonic TEE uses LPAE
[ ]   Trustonic TEE driver debug mode
<*>   Trustonic Trusted UI
```

```
<*>   Trustonic Trusted UI with fb_blank
```

- Finally, run `make` again and the Trustonic Trusted UI kernel components will be included in the kernel image.

7.3.4 Integrating the TUI kernel driver

The TUI kernel driver has one device for user access that need to be accessed by the TUI service. Access permissions for this device are defined by *udev* following way:

```
/dev/t-base-tui 0666 system:system
```

7.4 TUI ANDROID COMPONENTS

7.4.1 Customizing the TUI Service

Some system events must cancel an ongoing TUI session there is one. The TUI Android service is designed to notice them and trigger the cancellation of the TUI session.

The list of events can be customized in `com/trustonic/tuiservice/TuiService.java`:

- Add dynamic registration of intent in OnCreate()
- Add filtering of event in onReceive() of broadcastReceiver

Add required permission for intent reception if any in `AndroidManifest.xml`.

7.4.2 Integrating the TUI service

The usual way to build Kinibi TUI Android component is from a complete Android source tree:

Simply copy the contents of the folder `AndroidIntegration/Src/mobicore/TuiService/Locals/Code/` to an Android source tree. You should have the following organization:

```
Android root/
    External/
      mobicore/
        MobiCoreDriverLib/
        ProvisioningLib
        RootPA/
        TuiService
```

Add the following lines at the end of the file `External/mobicore/Android.mk`:

```
# Include the TUI Service
include $(MOBICORE_PROJECT_PATH)/TuiService/Android.mk
```

All Kinibi components – including TUI service – will be automatically built within the next build of full Android source tree.

Else usual Android command can be used to build only TUI component is:

```
$ mmm external/mobicore/Tuiservice/
```

7.4.3 SEAndroid configuration for TUI

SEAndroid integration for TUI components is described in SEAndroid Configuration.

7.5 TUI FLOW CHARTS

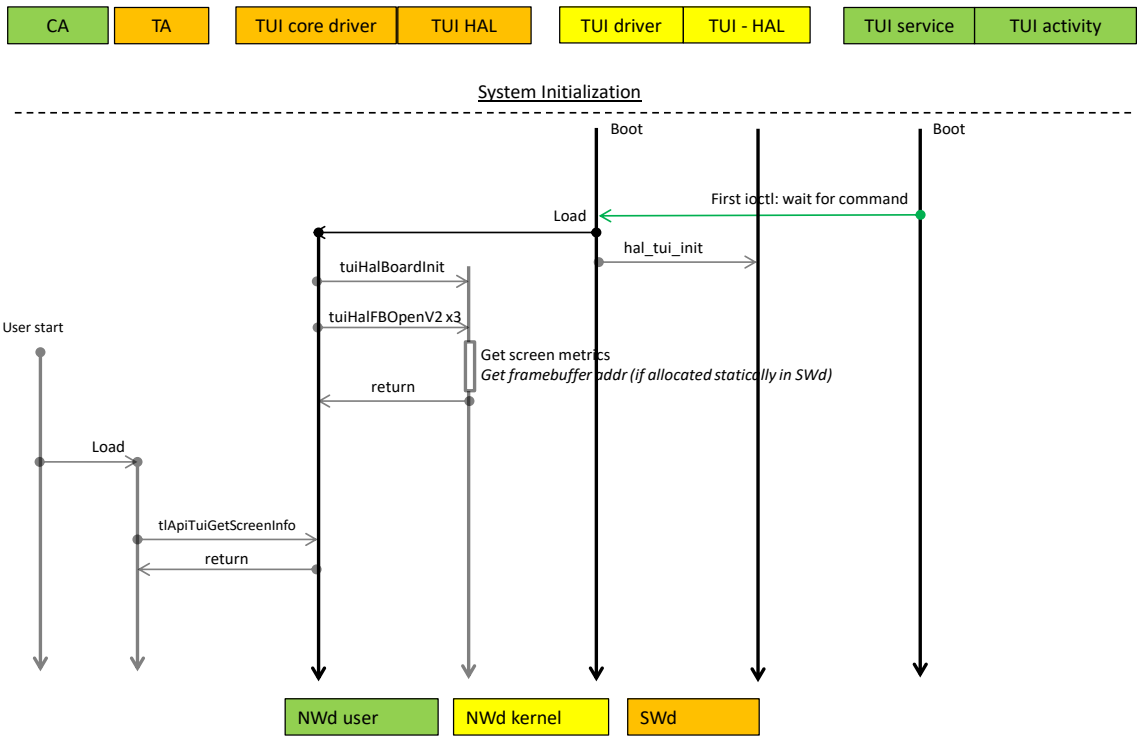


Figure 9: TUI flow chart: initialization.

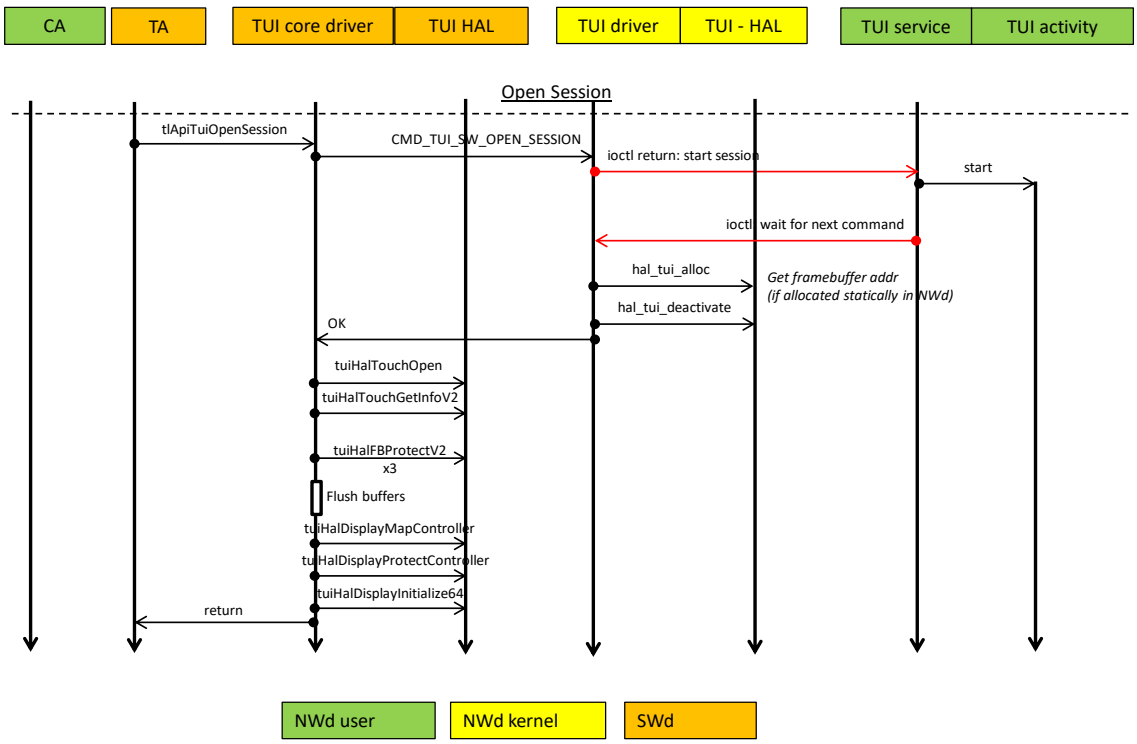


Figure 10: TUI flow chart: session opening.

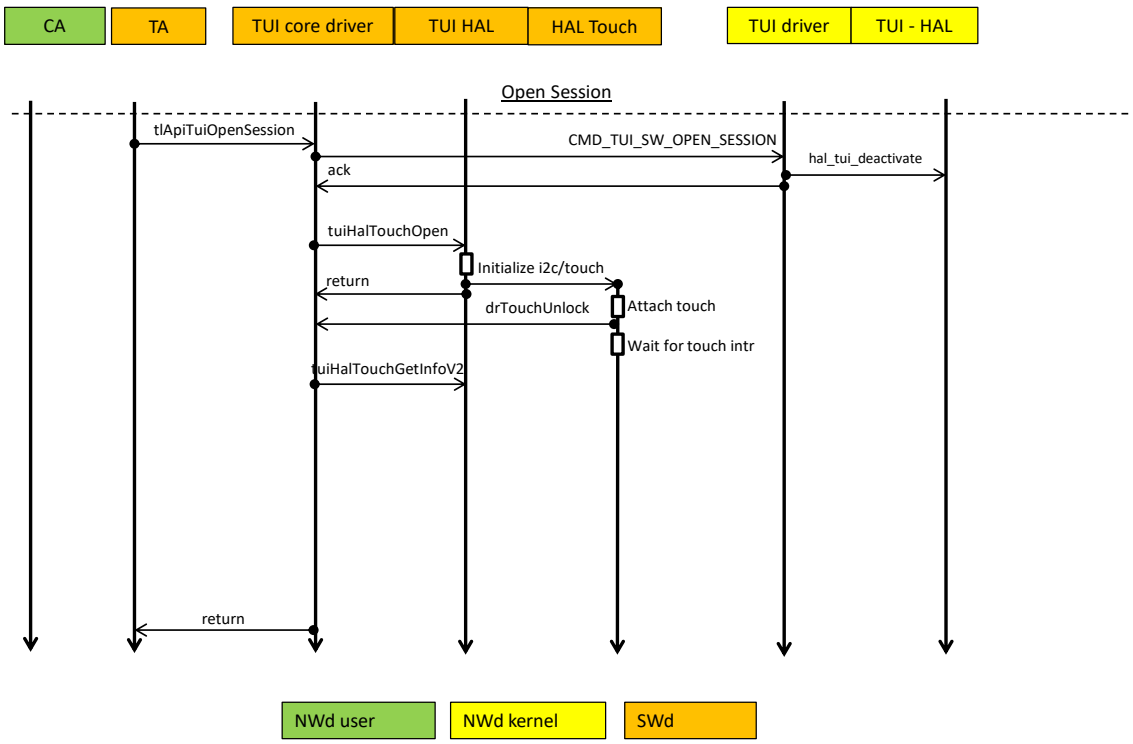


Figure 11: TUI flow chart: touch opening.

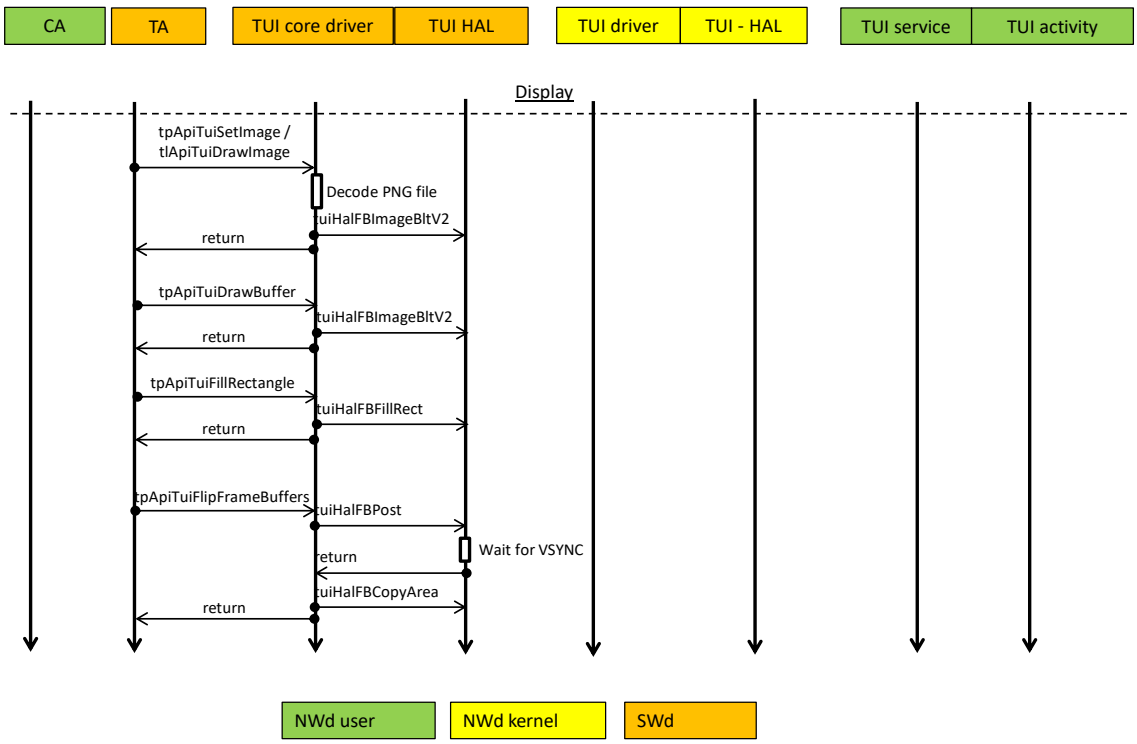


Figure 12: TUI flow chart: displaying.

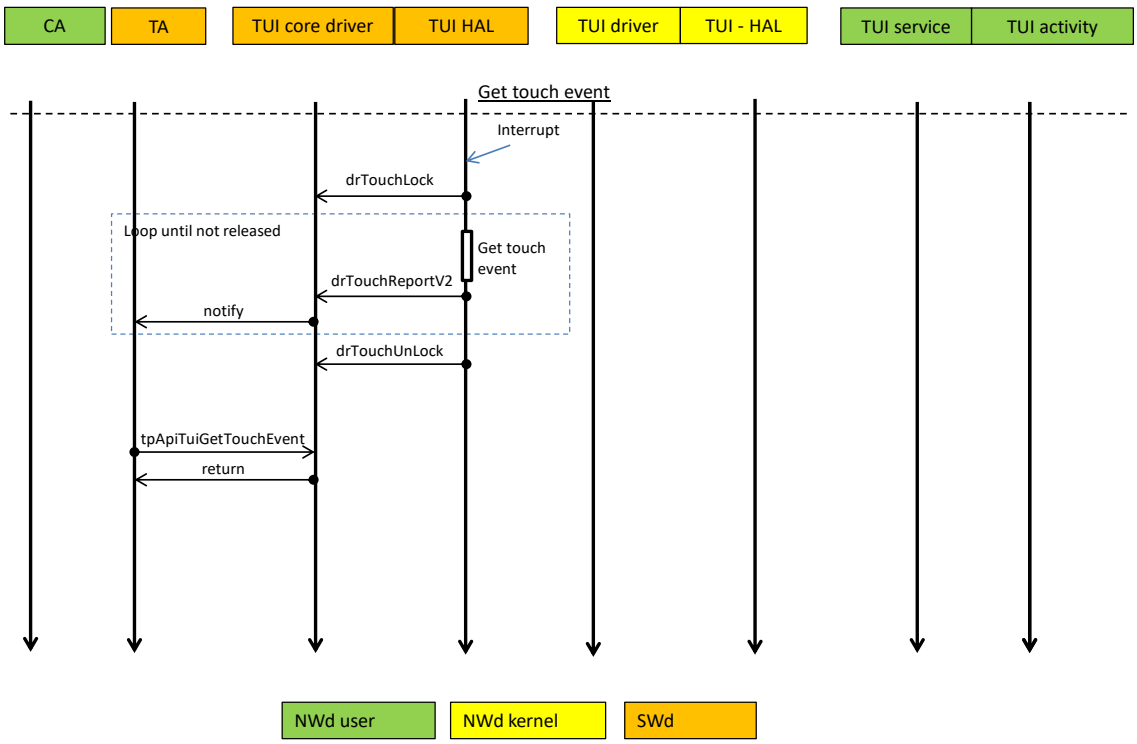


Figure 13: TUI flow chart: getting touch event.

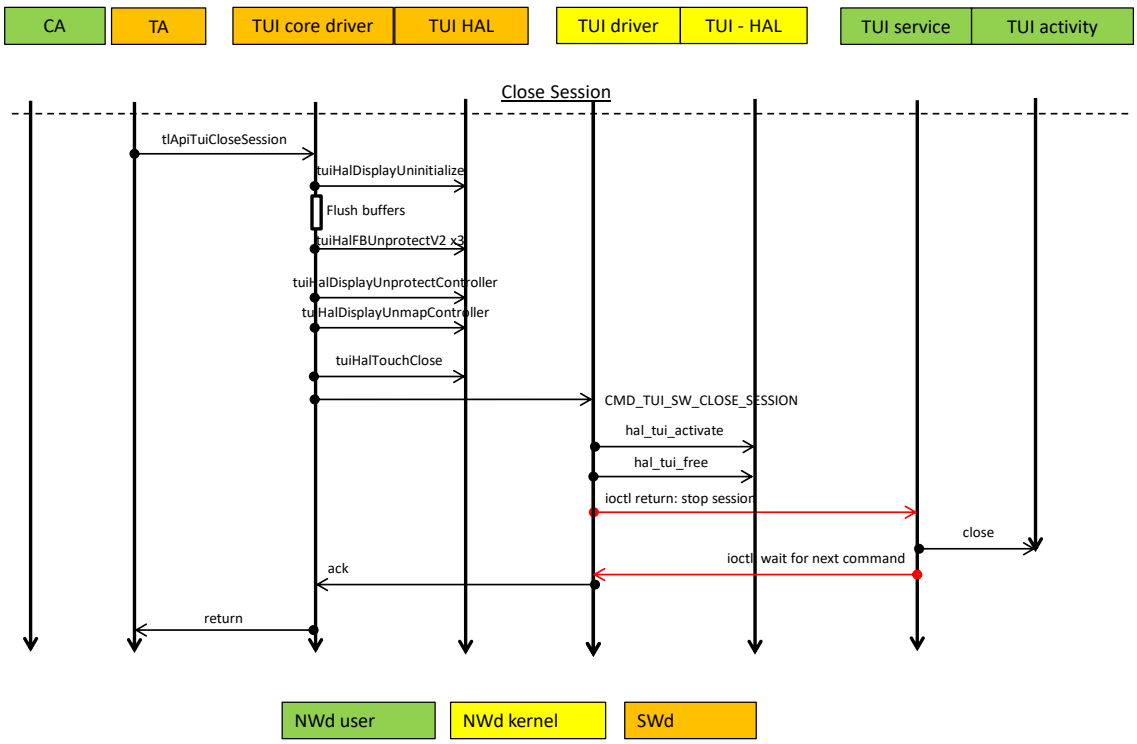


Figure 14: TUI flow chart: session closing.

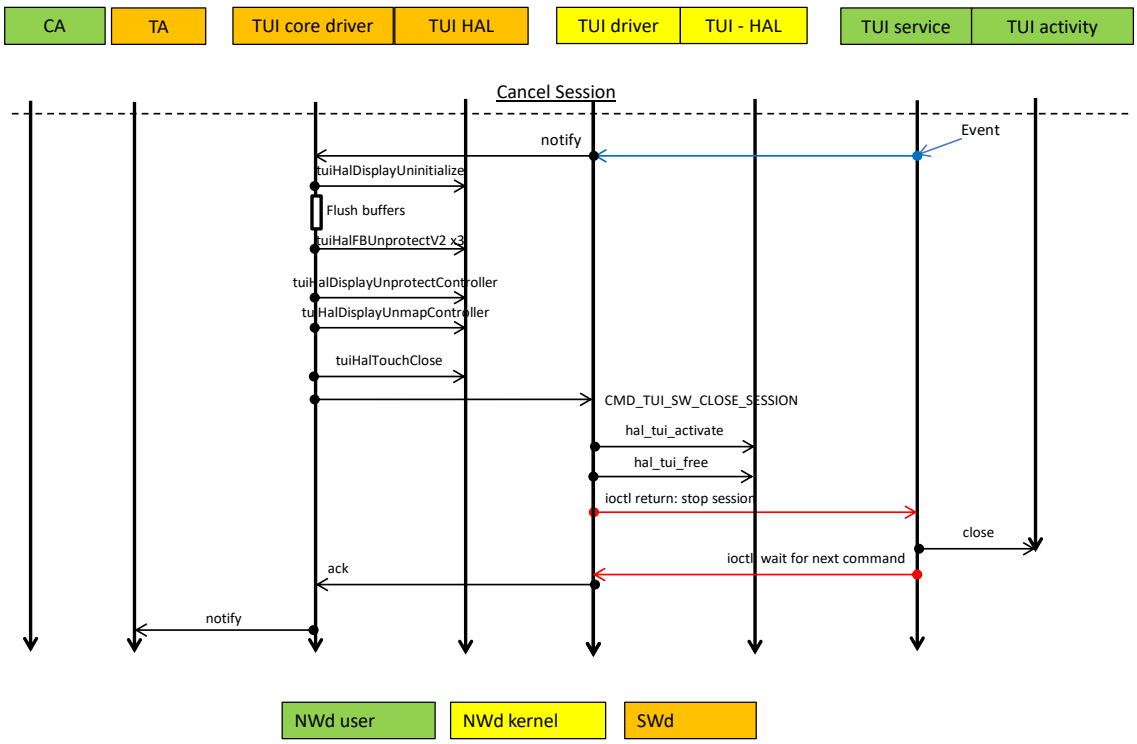


Figure 15: TUI flow chart: session cancellation.

8 VALIDATING THE PRODUCT

8.1 BASIC VERIFICATION AND VERSION CHECK

The Kinibi product comes with several samples and informative applications. It is recommended to install and run them to verify basic functionality and to check the Kinibi version.

To verify that the basic functionality works, follow this integration guide and then boot the device. This should have installed the Content Management Trusted Application *(tlcm.axf)* `07010000…0000.tlbin` in `/system/app/mcRegistry`. This TA will be used to test that TA loading works and to get the Kinibi version. To do so, you need to install the `tlcInfo` tool that is provided in the product package.

Installing the `tlcInfo` tool:

```
$ adb push t-base-dev-kit/Tools/Info/<TOOLCHAIN>/<MODE>/tlcInfo
/data/misc
```

Running the `tlcInfo` tool:

```
$ cd /data/misc/
$ ./tlcInfo
```

Expected output:

```
Copyright (c) Trustonic Limited 2013-2015.
Test-Package-ARNDALE-311A-20160831_184510_13773_45507, Aug 31 2016,
19:29:18.

mcGetMobiCoreVersion:
productId        = t-base-EXYNOS64-Android-311A-V004-20160527_225213_11082_
38854
versionMci       = 0x00010005
versionSo        = 0x00020002
versionMclf      = 0x00020005
versionContainer = 0x00020001
versionMcConfig  = 0x00000003
versionTlApi     = 0x00010013
versionDrApi     = 0x00010004
versionCmp       = 0x00060001

CMP GetSuid:
SUID             = 0x020000001000052438428 56AC76010000
SUID.SiP         = 0x00000002
SUID.SoC         = 0x43520010
SUID.CSN         = 0x842856AC76010000
CMP GetVersion:
productId        = t-base-EXYNOS64-Android-311A-V004-20160527_225213_11082_
38854
versionMci       = 0x00010005
versionSo        = 0x00020002
versionMclf      = 0x00020005
versionContainer = 0x00020001
versionMcConfig  = 0x00000003
versionTlApi     = 0x00010013
```

```
versionDrApi      = 0x00010004
versionCmp        = 0x00030000
```

Note the Kinibi product version in productId field that must match the version from the release notes and the release zip file name.

8.2 RUNNING THE TTS

The Kinibi product comes with the TTS apk, the Trustonic Test Suite which contains tests to validate the Kinibi integration on the platform.

The test suite is located in the `TTS` folder that contains complete documentation explaining how to run the tests.

9 System Debugging

Trustonic is now providing a more complete and independent documentation for system debug, for more information, please refer to *Kinibi_System_Debug_Guide.pdf*

10 TEE KEYMASTER AND GATEKEEPER

Trustonic is providing the complete support for the Google/Android KeyMaster and Gatekeeper Applications. These services are provided in a dedicated package, independent of the TEE.

Appendix I.
Appendix I.
Appendix I.
Appendix I.

Appendix I. Google Compliance Test Suite

1 Details of the CTS waiver request

In general any Android application that wants to communicate with a Trusted Application running in Kinibi needs to be able to share read/write memory with the Trusted Application. Applications can be downloaded from the Google Play Market with the functionality to communicate with a Trusted Application running in Kinibi.

The only way to share memory between an Android Application and a Kinibi Trusted Application is through the Linux device node `/dev/mobicore-user`. The Android application needs to send at least 2 calls to the Linux kernel to prepare shared memory buffers (L2 MMU tables) for Kinibi, an IOCTL call and a mmap (`PROT_READ | PROT_WRITE`) call. Because of these 2 calls the Android application needs Read & Write access to the `/dev/mobicore-user` device node.

Because we assume any application from the Google Play Market should be allowed to communicate with the Secure World there is no way to assign a Group ID (GID) to the application in order for it to access Kinibi. Because the node cannot assume any GID for all the applications the node needs the extended permissions of `0666`.

Please note that write is only required for the mmap (PROT_READ | PROT_WRITE) call as this is a definition in the Linux kernel. The write method is not implemented for the `/dev/mobicore- user` and no write is actually allowed from user space.

This method of accessing the Secure World through the /dev/mobicore-user device node has been fully approved by Google and a waiver is in place for their Compliance Test Suite (CTS). Details of Google's approval process for this waiver can be found at:

https://android-review.googlesource.com/#/c/63940/

The code of the CTS where this waiver is implemented can be found at:

https://android.googlesource.com/platform/cts/+/3e29e6b0916db3f4b59657dabde9a40815244097/tests/tests/permission/src/android/permission/cts/FileSystemPermissionTest.java

Appendix II. MobiConfig Manual

Help output

```
java -jar MobiConfig.jar
MobiConfig V3.3 Build by lukhan01@DE0015 01/26/16 17:55:13
  Copyright (c) 2013-2015 TRUSTONIC LIMITED. All rights reserved.

java -jar MobiConfig.jar <command> <options>...

<command>
  -h,--help                   Show help
  -c,--config <config-opts>  Configuration options, see below
  -p,--preconfig <preconfig-opts> Pre-configuration options, see below
  --rps Rollback-protected storage configuration options, see below
  -d,--dump <image>      Dump configuration settings of image and exit
  -de,--dump-endorsement <image> Dump endorsement configuration
settings of image and exit
  -ds,--dump-sipid <image> Dump Silicon provider ID of image and exit
  -dr,--dump-rps <image> Dump Rollback-protected storage configuration

<config-opts>
  -i,--in <in-image> -o,--out <out-image>
  [-k,--key <keyfile> [--kid <keyid>]  |
   [--kphkey1 <keyfile1> --rekey1 <rekeyfile1> --kid1 <keyid1>
    --kphkey2 <keyfile2> --rekey2 <rekeyfile2> --kid2 <keyid2>
  ]]
  -ek,--ekey <ekeyfile>  | [-xc,--xml-config <xml-manifest> ]

<preconfig-opts>
  -i,--in <in-image> -o,--out <out-image> -ek,--ekey <ekeyfile> -si,--
sipid <sipid>-df,--dflags <dflags>
  <keyfile>      PEM file containing public key
  <keyid>        Puk.Kph.Request Key-ID (keyid >= 1; default:1)
  <ekeyfile>     PEM file containing endorsement server public key
  <sipid>        Silicon provider ID
  <xml-manifest> XML file containing the key list with access
permission flag and reserved uuid list

<Rollback-protected storage configuration options>
  --use_mask <Rollback-protected storage for a partition enabled mask>
  --reset-persistent_mask <Blanking by erasure configuration mask>
  --chunk-id <First Rollback-protected storage chunk ID>
   <in-image>     Input image file
   <out-image>    Configured output image file

Device binding key-related options:
  <kphkeyfile[n]>   PEM file containing Device Binding request signing
key
                    (PuK.Kph.Request) public key at table entry n.
  <rekeyfile[n]>    PEM file containing Receipt Encryption
(PkP.Root.Transport)
```

```
                    public key at table entry n.
  <keyid[n]>      Key ID for table entry n;
                  defaults to Key ID 1 (Trustonic).

                  Note that use of multiple table entries requires
                  a version of CMTL that supports the structure.
                  If n is not specified, it defaults to table entry #1.
```

I. Multi OEM keys

Since Kinibi-311A, the SIP and the OEM can configure up to 32 OEM keys into the Kinibi image.

The MobiConfig tool has a new option --xml-config that accepts an XML file with a list of keys and options:

```
<?xml version="1.0"?>
<parameters>
<!-- manifest used for test -->
  <oem-keys>

    <oem-reserved-uuid-list>
        <!-- list with up to 16 different UUIDs:
            Allow the OEM to restrict a certain key to a limited number of UUIDs.
            To make use of this list, define a key without the ALLOW_ANY_UUID flag.
         -->
        <uuid value="08010000000000000000000000000011"/>
    </oem-reserved-uuid-list>

    <key-list>
        <!-- list with up to 32 different hashes:

             <key filename=... flags=.../>
             <key hash=... flags=.../>

Attributes:
"filename": is a path to a PEM file, where the hash will be generated over the public
key
"hash":     a hexadecimal byte string of the form "xxxx...xx", length is 64 chars,
each char must be [0-9,A-F,a-f]
"flags":    case insensitive comma separated list of
        "ALLOW_DRIVER",    # This key signs drivers
        "ALLOW_MIDDLEWARE # This key signs middle ware
        "ALLOW_SYSTEM_TA" # This key signs system TA
        "ALLOW_ANY_UUID"  # This key signs any UUID, otherwise UUID must NOT be in
<oem-reserved-uuid-list>

Either "hash" or "filename" should be used. If both attributes present, "hash" must
match the hash generated from the PEM file. If not, the program will abort with an
error. This can be used as a fail-safe checkto ensure the correct PEM file is used and
there is a key pair for a hash.
         -->
        <key filename="key_driver_pub.pem" flags="ALLOW_DRIVER"/>
        <key filename="pairVendorTltSig.pem"
flags="ALLOW_DRIVER,ALLOW_MIDDLEWARE,ALLOW_ANY_UUID,ALLOW_SYSTEM_TA"/>

    </key-list>

  </oem-keys>
</parameters>
```