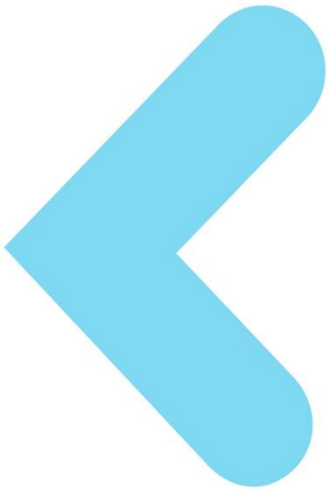
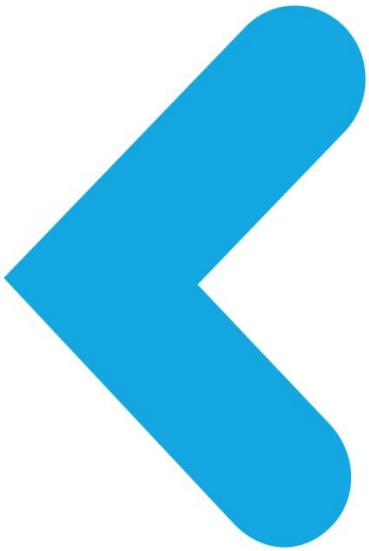
TRUSTONIC

Release Notes



Kinibi v400C for EXYNOS64

Release Notes



PREFACE

TABLE OF CONTENTS

1 INTRODUCTION

This document is the Release Notes for the Trustonic Kinibi product on Samsung S.LSI ARMv8 platforms with a normal world in 32 bits or 64 bits.

As a reminder the product versions Kinibi-400C for S.LSI platforms are specific maintenance versions built on top of Kinibi-400A_v017. Goal has been to keep unchanged the security reviewed SWd components and integrate all the NWd changes needed for Android P support (Treble/HIDL).

The exact version of the product is:
t-base-EXYNOS64-Android-400C-V002-20181101_223909_58281_87506

This version is a Commercial Release and it has been fully validated.

2 What's New in Kinibi

2.1 Kinibi v400C

2.1.1 New Integration Features

400C is the update of Kinibi for Android Pie. The TEE API level is unchanged.

2.1.1.1 Android P changes

It assures Android P official release compatibility:

- Updating RootPA and TUI components to match Android P/Treble isolation.
- Development of new system services to enable TEE access for OTA and System APKs.
- Update reference SE Linux rules to follow Android evolution.

3 PAST KINIBI RELEASES

3.1 Kinibi v400A

3.1.1 New Core Features

400A introduces new features. The TEE API level is changed to **11**.

This Kinibi version is compliant to:

- GlobalPlatform TEE Client API Specification ([Client API]) v1.0, GlobalPlatform TEE Client API Specification v1.0, Errata and Precisions v2.0, GPD_EPR_028.
- GlobalPlatform TEE Internal Core API Specification ([Internal Core API]) v1.1.1.

It passes the FIME GP compliance tool.

3.1.1.1 GP Properties

400A implements all the GP Properties defined by the GP internal API 1.1.1.

Note that `gpd.tee.description` does not anymore contain `<t-base`, but the product build id, e.g. `t-base-Arndale-Android-400A-20160501_011308_9060_36620`.

Note also that `gpd.tee.firmware.implementation.version` and `.binaryversion` are values that need to be provided by the underlying platform for a device to be GP compliant.

See the Kinibi API Documentation for the complete list of properties defined in each version of the product.

3.1.1.2 TEE Capabilities

400A implements new proprietary properties via the GP properties API that give information about the capabilities of the TEE on this specific device. For example:

`com.trustonic.tee.isa.arm.neon`	`Boolean`	`True if Kinibi supports NEON and Hardware Floating Point for TA` `Dynamic at build time`
`com.trustonic.tee.tui.available`	`Boolean`	`True if TUI is available` `Dynamic, will try to contact TUI driver`

See the Kinibi API Documentation for the complete list of properties defined in each version of the product.

3.1.1.3 GP Properties Enumeration

400A supports the GlobalPlatform properties enumeration API.

3.1.1.4 GP Time API

400A supports the full GP Time API, including the `TEE_Wait()` function that was previously not supported.

3.1.1.5 GP TA Instance Types

400A supports Single Instance Trusted Applications as well as Multi-Session and Keep-alive TAs. Respective configuration can be set via the new TA manifest.

3.1.1.6 GP Internal Client API

400A supports the GP TA-to-TA communication using the `TEE_OpenTASession()`, `TEE_InvokeTACommand()` and `TEE_CloseTASession()` functions.

Any GlobalPlatform TA can use this API to call another GP TA (any TA can be a *client*).

It depends on the way a TA is installed if the TA can be called in TA-to-TA communication (only some TAs can be a *server*).

For a GlobalPlatform TA to be a server, the TA must be already running or installed into Trusted Storage (TA-to-TA is not loading automatically System TA and SP TAs installed in mcRegistry). To make sure a TA can be called independently of the way the TA is installed, the developer has to use a multi-session TA and first open a session from a Client Application before opening a second session from a Trusted Application.

3.1.1.7 GP Crypto API

The following algorithmic key sizes have been added:

- `AES: 192 bits`
- `DES: 192 bits`

The following AES algorithms have been added:

- `TEE_ALG_AES_CTS`
- `TEE_ALG_AES_XTS`
- `TEE_ALG_AES_CCM`
- `TEE_ALG_AES_GCM`

The following ECDH algorithms have been added:

- `TEE_ALG_ECDH_DERIVE_SHARED_SECRET`

The following ECDSA_SHA algorithms have been added:

- `TEE_ALG_ECDSA_SHA1`
- `TEE_ALG_ECDSA_SHA224`
- `TEE_ALG_ECDSA_SHA256`
- `TEE_ALG_ECDSA_SHA384`
- `TEE_ALG_ECDSA_SHA512`

The following MAC algorithms have been added:

- `TEE_ALG_AES_CBC_MAC_NOPAD`
- `TEE_ALG_AES_CBC_MAC_PKCS5`
- `TEE_ALG_AES_CMAC`
- `TEE_ALG_DES_CBC_MAC_NOPAD`
- `TEE_ALG_DES_CBC_MAC_PKCS5`
- `TEE_ALG_DES3_CBC_MAC_NOPAD`
- `TEE_ALG_DES3_CBC_MAC_PKCS5`

The following missing GP APIs have been added or implemented:

- `TEE_GetOperationInfoMultiple()`
- `TEE_CopyOperation()`

- `TEE_ResetOperation()`
- `TEE_SetOperationKey2()`
- `TEE_AEInit()`
- `TEE_AEUpdateAAD()`
- `TEE_AEUpdate()`
- `TEE_AEEncryptFinal()`
- `TEE_AEDecryptFinal()`

3.1.1.8 Performance optimizations for cryptographic operations

Kinibi-400A leverages ARMv8 AARCH32 crypto acceleration instructions to increase the efficiency of cryptographic operations. Also ARMv7 NEON accelerations are used when available.

This improves the speed of reads and writes of GP SecureStorage API and the speed of GP Crypto API when the following base algorithms are being invoked:

- AES
- SHA1
- SHA256
- SHA512
- RSA key generation

3.1.1.9 Proxy enhancements

The proxy in 400A was enhanced to use zero-copy for shared buffers.

3.1.2 New Integration Features

3.1.2.1 TA downgrade protection

Kinibi-400A supports downgrade protection for System TAs that do not use the GlobalPlatform API. This feature is an extension of the RPMB support of 311A and requires that the Kinibi Daemon can access the efs partition. See the Kinibi Integration Guide for more information.

3.1.2.2 TEE Image builder

Kinibi-400A gives the SIP and OEM more flexibility to assemble and configure the TEE image. The new image builder in 400A allows exchanging the RPMB Monotonic Counter TA. The package contains a new folder SecureIntegration/t-base-kit that contains prebuilt TEE components and a python tool to assemble these files. This creates the TEE image. For more information, see the Kinibi Integration Guide.

3.1.2.3 New ATF Input Fastcalls for GlobalPlatform

For a device to be GlobalPlatform-compliant, the TEE must return the exact version of the firmware in the `gpd.tee.firmware.implementation.version` and `.binaryversion` properties. 400A adds a way for platform integrators to define these during the integration. In the case of ATF-based integrations, new IDs for TBASE_SMC_FASTCALL_INPUT have been defined to retrieve such version information.

3.1.2.4 TTS - Trustonic Test Suite

The Kinibi-400A package contains the TTS that SIP and OEMs must use to validate the product on development boards and production devices.

3.1.3 New SDK Features

3.1.3.1 TA Manifest file

400A SDK supports a manifest file for GP TAs that allows specification of static properties.

3.1.3.2 TUI double buffering for GP TAs

400A SDK supports the TUI double buffering API for TAs that use the GP API.

3.1.3.3 Downgrade protection flag for legacy System TAs

400A SDK supports the new MobiConvert flag `--downgrade-protected`. TAs that have this flag set will only be loaded on Kinibi versions that have the TA downgrade protection activated.

3.1.3.4 TeeClient

400A SDK contains the TeeClient, an in-APK library for downloadable and native proxy access.

3.1.3.5 Assembler support for TAs

400A SDK supports building and linking assembler files into TAs.

3.1.3.6 New samples

The following samples have been added:

- **CryptoCatalog_GP**: Demonstrate usage of cryptographic APIs using the GlobalPlatform APIs.
- **GP**: Demonstrate TA manifest, TA-to-TA communication, usage of Trusted Storage and GP Properties.
- **PinpadGP**: Implementation of the Pinpad sample using a GP TA and the Trustonic TUI APIs for GlobalPlatform.

3.1.4 Fixed Issues

3.2 Kinibi v311B

3.2.1 New Features

311B is the update of Kinibi for Android Nougat. The TEE API level is unchanged.

This release is not adding any new feature.

3.2.1.1 Performance improvements for GP registered shared memories

The management of the registered shared memories has been reworked in order to improve the performances of TEEC_InvokeCommand().

3.2.1.2 Paths in Android File System

The paths of the Kinibi binaries, libraries and registries had to be changed to follow the new recommendations.

Component	Name of the binary	Old Containing folder	New Containing folder
Kinibi Daemon *(32 or 64 bit)*	`mcDriverDaemon`	`/system/bin`	**`/vendor/bin`**
Kinibi Proxy *(32 or 64 bit)*	`trustonic_tee_proxy`	`/system/bin`	**`/vendor/bin`**
Root Provisioning Agent *32 bit*	`RootPA.apk`	`/system/app/`	`/system/app/`
Kinibi Client library *(32 or 64 bit)*	`libMcClient.so`	`/system/lib/` `/system/lib64/`	**`/vendor/lib/`** **`/vendor/lib64/`**
Kinibi Registry library *(32 or 64 bit)*	`libMcRegistry.so`	`/system/lib/` `/system/lib64/`	**`/vendor/lib/`** **`/vendor/lib64/`**
Keymaster1.0 library *32 and 64 bit*	`keystore.$DEVICE.so`	`/system/lib/` `/system/lib64/`	**`/vendor/lib/hw`** **`/vendor/lib64/hw`**
Gatekeeper library *32 and 64 bit*	`gatekeeper.$DEVICE.so`	`/system/lib/` `/system/lib64/`	**`/vendor/lib/hw`** **`/vendor/lib64/hw`**
Root Provisioning Agent Native library *32 bit*	`libcommonpawrapper.so`	`/system/lib/`	`/system/lib/`
Kinibi Read Only Registry		`/system/app/mcRegistry/`	**`/vendor/app/mcRegistry/`**

Kinibi Read Write Registry		`/data/app/mcRegistry/`	**`/data/misc/mcRegistry/`**

3.2.2 Fixed Issues

Core

- TBUG-868 System halt related to drApiWaitForIntr().

Keymaster 1.0

- TBUG-880 For RSA PSS signatures, do not hard code the salt length to 20 bytes even if it was compliant with the specifications, it does not work with the most recent versions of the CTS. The salt length is now equal to the digest length, except for MD5, it uses 20 because the digest is too short (16).
- TSEC-261 buffer overrun in TA
- (find_param): Fix preliminary error reporting
- (update): Fix chunking of operations
- (aes_finish): Set output length correctly
- (open) Don't use throwing `new'.
- Remove KM_TAG_ROOT_OF_TRUST from KEY_CREATION_ALLOWED_TAGS

Gatekeeper

- TBUG-757 throttling must be done on SWd and failure records must be stored in the SWd
- TBUG-744 Enroll() and Verify() should be implemented in TA

SDK

- TBUG-869 TEE_GetInstanceData() does not return NULL on first invocation, if TA API_LEVEL >= 8

Trusted User Interface

- TBUG-875 Support for NWd resolution change
- TBUG-863 Ghost TUI activity
- TBUG-837 TUI activity creation failure

ATF

- TBUG-866 memory corruption affecting FiqForward scenario due to misalignment between AFT/SPD and TEE

3.3 Kinibi v311A

3.3.1 New Features

311A introduces new features. The TEE API level is changed to **10**.

3.3.1.1 Trusted Storage with Rollback Protection

The Trusted Storage which is available using the GlobalPlatform Trusted Storage API has been enhanced to include support for Rollback Protection.

The silicon vendor and the OEM need to implement a RPMB driver and configure Kinibi image to use this feature. See the Kinibi Integration Guide for more information.

3.3.1.2 Trusted Storage Upgrade

Kinibi-311A introduces an automatic conversion tool that allows silicon vendors and device manufacturers to upgrade existing devices from previous versions to 311A.

This conversion tool reformats files stored using the GlobalPlatform Trusted Storage APIs with version 300A to the format of version 310A. The tool is integrated into the Kinibi image and into the Kinibi Daemon and is automatically run on each startup.

3.3.1.3 Post-Mortem Debug and Performance Analysis Tool

Kinibi-311A adds more system debugging support by the addition of tee-ps tool and the TEE DebugSession infrastructure.

The product package contains the **tee-ps** tool in **/t-base-dev-kit/Tools/TlcTeePs** with Src and Bin. See the Kinibi Integration Guide for more information on how to use this tool.

3.3.1.4 GP time API

Kinibi-311A supports more functions of the GP Time API:

The function TEE_GetSystemTime() is now monotonic between two resets.

The functions TEE_GetTAPersistentTime and TEE_SetTAPersistentTime are now supported.

3.3.1.5 Multiple OEM Keys

It is possible to inject up to 32 OEM keys in the Kinibi Core image.

3.3.1.6 GICv3

The Kinibi Core now supports the new generation of ARM Generic Interrupt Controller, GIC-500.

The boot loader must pass the GIC version to the Kinibi Core.

3.3.1.7 GP Client API in Kernel Module

The GP Client API is now available for the Linux kernel.

The API is defined in AndroidIntegration/Src/gud/MobiCoreDriver/public/GP/tee_client_api.h.

The name of the functions and types follow the Linux kernel coding rules.

3.3.1.8 Keymaster M-MR1

The Keymaster for Android M can now support up to 16 cryptographic operations in parallel.

3.3.2 Fixed Issues

Core

- TBUG-815 broken FastCall handling due to plat_fc_secondary_core_handler() corrupting regs->r1
- TBUG-820 drApiMapPhysicalBuffer can't map a physical address above 0xFFFFFFFF
- TBUG-802 The TA built with 302C TlSdk is not compatible with Kinibi 310A and later
- TBUG-722 MCP command timeout
- TBUG-777 Boot trace do not show anymore
- TBUG-784 Tee debug image too big
- TBUG-760 Memory leak in MTracker
- TBUG-711 Multiple vulnerabilities in drApiMapTaskBufferImpl
- TBUG-754 MTK does not update timeout for thread in special IPC case
- TBUG-747 SFS assert in L2
- TBUG-718 Integer overflow in RTM's llDecryptAndVerify_SP_TA()
- TBUG-719 RTM does not handle buffer offset correctly in llSafeCopyServiceBlob() and llSafeCopyAdditionalServiceBlob()

Crypto

- TBUG-673 HMAC and digest operations with short tags lead to buffer overruns
- TBUG-689 CR asserts on 0 length hash buffer
- TBUG-743 Insufficient bound checks in static_InjectAttribute
- TBUG-710 Integer overflow in map2Buffers
- TBUG-396 Wrong driver ID usage for the crypto driver

Keymaster

- TBUG-790 Keymaster M: Ignore KM_TAG_CREATION_DATETIME
- TBUG-793 Keymaster M,N: begin() should succeed if KM_TAG_AUTH_TOKEN is not present in the operation parameters and KM_TAG_AUTH_TIMEOUT is not present in the key parameters

Linux driver

- TBUG-804 The time field is not initialized when the MCP buffer is given to the SWd.
- TBUG-792 NWd driver mmap's memory beyond allocated .

Legacy Client API

- TBUG-782 NWd client: add support for MC_DRV_ERR_NO_FREE_INSTANCES

GP Client API

- TBUG-699 NWd client GP: fix memory leak and incorrect origin

Daemon

- TBUG-750 NWd daemon: need to close device on thread exit so driver can cancel pending requests

3.4 Kinibi v310C

3.4.1 New Features

310C introduces new features. The TEE API level is changed to **9**.

3.4.1.1 Trusted User Interface Service binding

The TUI service is no longer automatically started at boot time.

Client Applications must bind to the TUI Service before starting the communication with the Secure World. This can be transparently achieved by calling the new function TEEC_TT_RegisterPlatformContext() added in this release.

3.4.1.2 Proxy

The Kinibi proxy (trustonic_tee_proxy) is now a standalone process and must be started at boot time.

A new optional Authentication Service (TeeAuthServer) can be integrated in order to filter the access to the Secure World for the Client Applications.

3.4.2 Fixed Issues

Trusted User Interface

- TBUG-771 Tui session not stopped if TuiService killed during a TUI session.
- TBUG-767 TuiActivity is not killed if the framebuffer allocation is failing.
- TBUG-761 Memory leak in DrTui.

Crypto

- TBUG-758 During Secure Object creation, source data should not be copied into destination buffer.

Keymaster

- TBUG-706 Keymaster v0.4 testKeyStore_Encrypting_RSA_NONE_NOPADDING failed on Android M
- TBUG-762 Make KitKat Keymaster calls to tlApiWrapObject() immune to TBUG-758

Client Library (NWd)

- TBUG-715 When opening a session, return TEEC_ERROR_OUT_OF_MEMORY if errno is ENOSPC, not TEEC_ERROR_GENERIC.

Linux driver

- TBUG-714 Do not unblock caller for session close until [GP] session is closed in SWd.

Daemon

- TBUG-753 NWd daemon: fix check for user device presence

SDK

- TBUG-755 References to _stack_tlMain_* unprotected by TBASE_API_LEVEL check

3.5 Kinibi v310B

3.5.1 New Features

310B introduces new features. The TEE API level is changed to **8**.

3.5.1.1 Android SE Proxy

The default Google SEAndroid policy blocks access to Linux kernel devices by Android Java applications. 310B provides a proxy for these situations to allow such applications to talk via Unix sockets to a new proxy component that will then access the Linux kernel device on behalf of the application. The use of the proxy is transparent; it is libMcClient.so that tries to access the kernel device first and falls back to proxy if necessary. The application only uses libMcClient.so as before.

3.5.1.2 Android 6.0 Keymaster M and Gatekeeper

The Kinibi software package now includes support for Android 6.0 keymaster1 and gatekeeper with its implementations strengthened by ARM TrustZone® through Trusted Applications (TA) in the Secure World and shared libraries in the Normal World. It is up to the Kinibi integrator to include these TAs and shared libraries in the device software image.

This keymaster feature is optional to be integrated in a Kinibi integration.

The Kinibi software package for Marshallow Keymaster and Gatekeeper includes:

- shared library: `keystore.$DEVICE.so`
- shared library: `gatekeeper.$DEVICE.so`
- Trusted Application: `07060…04D.tlbin`
- Trusted Application: `070610…0.tlbin`

The implementation does not support optional or deprecated functions like:

- `delete_key()`
- `delete_all_keys()`

The implementation supports only the following import and export formats:

- Symmetric key
  - Import: `KM_KEY_FORMAT_RAW`
  - Export: not supported
- Asymmetric keys
  - Import: `KM_KEY_FORMAT_PKCS8`
  - Public key export: `KM_KEY_FORMAT_X509`
  - Private key export: not supported

Further documentation is described in the Kinibi integration guide.

3.5.1.3 Stack protection for Trusted Applications and Drivers

310B introduces MMU-protected stacks for Trusted Applications and Drivers that use TBASE_API_LEVEL=8. In the SDK, when you select TBASE_API_LEVEL <= 7, the stack is allocated in the BSS of the application binary. When you select level 8, the binary only contains an integer with the minimum stack size. The startup code of the application will allocate a stack with one unmapped MMU page before and after the stack area. That way, stack overflows and underflows will not silently overwrite global variables and heap, but cause a segmentation fault that helps discover stack problems during the development phase.

3.5.1.4 DebugFS interface for MCP timeout and core switching

The kernel module for 310A removed a feature to trigger a core switch on the command line. The new virtual file /trustonic_tee/active_cpu reintroduces this feature.

The kernel module for 310A implements a 50s watchdog for MCP commands in the SWd. With 310B, the /trustonic_tee/mcp_timeout virtual file allows to modify this timeout, e.g. for debugging purpose.

Find more information in chapter 8 "SYSTEM DEBUGGING WITH DEBUGFS" of the integration guide.

3.5.1.5 Calling the Firmware from a Driver

The new API, `DrApiCallTrustedFirmware()` can be used to call functionality of the Firmware from inside a driver. This is mostly intended for ARMv8 platforms that run the generic ARM Trusted Firmware in EL3 mode.

3.5.1.6 Add support for timeouts in TlApi

It is now possible to use a timeout value in ms for `tlApiWaitNotification`().

Only an immediate or infinite timeout was supported until now.

3.5.2 Fixed Issues

Core

- TBUG-135 drApiThreadSleep with a timeout value besides 0 and INFINITE is undefined
- TBUG-178 Separate Code and Data pages in MTK
- TBUG-470 SWd Kernel clips thread priority and this causes ISR not to run in expected order
- TBUG-645 random failures when using DSA key generated with TEE_GenerateKey()

Normal world

- TBUG-600 The Client Library is not able to map the same buffer multiple times
- TBUG-623 TUIActivity creation problem
- TBUG-657 A loop is required for send() or sendmsg() for Unix socket in the Daemon

3.5.3 Deprecations

Kinibi 310B deprecates the use of API LEVEL 1-4 for Secure Drivers. Driver developers must use the new APIs for memory extension introduced in Kinibi 302A and the stack protection introduced in Kinibi 310B. The next major Kinibi release will not support API LEVELS 1-4 for Secure Drivers.

3.6 Kinibi v310A

WARNING: the new format of the Trusted Storage introduced in version 310A is not compatible with previous version. This means data stored on a device using the GlobalPlatform Trusted Storage API with version 302A or earlier cannot be read if the device is upgraded to 310A. Therefore Trustonic recommends silicon vendors and device manufacturers to only apply version 310A on new devices and not to upgrade existing devices with 310A. Trustonic will provide a compatibility tool to fix this issue in forthcoming 310B release. Note this issue does not affect data stored with the Secure Object API.

3.6.1 New Features

310A introduces new features. The TEE API level is changed to **7**.

3.6.1.1 Trusted Storage

The Trusted Storage which is available using the GlobalPlatform Trusted Storage API from GP Trusted Applications has been optimized.

The Trusted Storage is using a sophisticated B+ tree which allows an efficient retrieval of the persistent objects with a reduced number of I/O operations.

The persistent object enumeration functions are now fully supported. It is also possible to rename a persistent object.

The Trusted Storage API is now also available for Secure Drivers (DrApi).

The following functions have been added:

- `TEE_AllocatePersistentObjectEnumerator()`
- `TEE_FreePersistentObjectEnumerator()`
- `TEE_GetNextPersistentObject()`
- `TEE_ResetPersistentObjectEnumerator()`
- `TEE_StartPersistentObjectEnumerator()`

The following functions defined in the GP1.1 Internal Core API specification have been added:

- `TEE_GetObjectInfo1()`
- `TEE_RestrictObjectUsage1()`
- `TEE_CopyObjectAttributes1()`
- `TEE_CloseAndDeletePersistentObject1()`

3.6.1.2 Trustonic KPHv2 support

Device manufacturers can use KPHv1 or KPHv2 with this version of the product in order to provision the TEE Device Binding key with the Key Provisioning Host during device manufacturing.

The CMTL and the MobiConfig tool have been updated in order to support the KPHv2.

3.6.1.3 Legacy Crypto API

The following RSA OAEP algorithms have been added:

- `TLAPI_ALG_RSA_SHA1_OAEP`
- `TLAPI_ALG_RSA_SHA224_OAEP`
- `TLAPI_ALG_RSA_SHA256_OAEP`
- `TLAPI_ALG_RSA_SHA384_OAEP`
- `TLAPI_ALG_RSA_SHA512_OAEP`
- `TLAPI_ALG_RSACRT_SHA1_OAEP`

- TLAPI_ALG_RSACRT_SHA224_OAEP
- TLAPI_ALG_RSACRT_SHA256_OAEP
- TLAPI_ALG_RSACRT_SHA384_OAEP
- TLAPI_ALG_RSACRT_SHA512_OAEP

The following RSA PKCS1 algorithms have been added:

- TLAPI_SIG_RSA_SHA1_PKCS1
- TLAPI_SIG_RSA_SHA224_PKCS1
- TLAPI_SIG_RSA_SHA256_PKCS1
- TLAPI_SIG_RSA_SHA384_PKCS1
- TLAPI_SIG_RSA_SHA512_PKCS1
- TLAPI_SIG_RSACRT_SHA224_PKCS1
- TLAPI_SIG_RSACRT_SHA256_PKCS1
- TLAPI_SIG_RSACRT_SHA384_PKCS1
- TLAPI_SIG_RSACRT_SHA512_PKCS1

The following RSA PSS algorithms have been added:

- TLAPI_SIG_RSA_SHA224_PSS
- TLAPI_SIG_RSA_SHA384_PSS
- TLAPI_SIG_RSA_SHA512_PSS
- TLAPI_SIG_RSACRT_SHA224_PSS
- TLAPI_SIG_RSACRT_SHA384_PSS
- TLAPI_SIG_RSACRT_SHA512_PSS

The following HMACs algorithms have been added:

- TLAPI_ALG_HMAC_SHA224
- TLAPI_ALG_HMAC_SHA256
- TLAPI_ALG_HMAC_SHA384
- TLAPI_ALG_HMAC_SHA512
- TLAPI_ALG_HMAC_MD5

The following digest algorithms have been added:

- TLAPI_ALG_MD5
- TLAPI_ALG_SHA224
- TLAPI_ALG_SHA384
- TLAPI_ALG_SHA512

3.6.1.4 GP Crypto API

The following RSA OAEP algorithms have been added:

- TEE_ALG_RSAES_PKCS1_OAEP_MGF1_SHA1
- TEE_ALG_RSAES_PKCS1_OAEP_MGF1_SHA224
- TEE_ALG_RSAES_PKCS1_OAEP_MGF1_SHA256
- TEE_ALG_RSAES_PKCS1_OAEP_MGF1_SHA384
- TEE_ALG_RSAES_PKCS1_OAEP_MGF1_SHA512

The following RSA PKCS1 algorithms have been added:

- TEE_ALG_RSASSA_PKCS1_V1_5_MD5
- TEE_ALG_RSASSA_PKCS1_V1_5_SHA224
- TEE_ALG_RSASSA_PKCS1_V1_5_SHA384
- TEE_ALG_RSASSA_PKCS1_V1_5_SHA512

The following RSA PSS algorithms have been added:

- TEE_ALG_RSASSA_PKCS1_PSS_MGF1_SHA224
- TEE_ALG_RSASSA_PKCS1_PSS_MGF1_SHA384
- TEE_ALG_RSASSA_PKCS1_PSS_MGF1_SHA512

The following HMACs algorithms have been added:

- TEE_ALG_HMAC_MD5
- TEE_ALG_HMAC_SHA224
- TEE_ALG_HMAC_SHA384
- TEE_ALG_HMAC_SHA512

The following digest algorithms have been added:

- TEE_ALG_MD5
- TEE_ALG_SHA224
- TEE_ALG_SHA384
- TEE_ALG_SHA512

The following DSA algorithms have been added:

- TEE_ALG_DSA_SHA1
- TEE_ALG_DSA_SHA224
- TEE_ALG_DSA_SHA256

The support for `TEE_DeriveKey()` has been added in this release for the `TEE_ALG_DH_DERIVE_SHARED_SECRET` algorithm.

RSA key size up to 4096 bits is supported.

The TEE Arithmetical API is supported. TEE_BigIntXXX().

3.6.1.5 Normal World refactoring

The Normal World components have been refactored in order to simplify the design and ease the integration.

The UNIX socket between the user space client API (`libMcClient`) and the daemon (`mcDriverDaemon`) has been removed.

The NETLINK socket between the kernel space client API (KernelApi) and the daemon has been removed.

The kernel module `MobicoreKernelApi` was merged into the `MobicoreDriver` module.

A new directory `trustonic_tee` was added to Linux debugfs to help in system debugging.

3.6.1.6 DRM API

Two new functions `tlApiDrmProcessContentEx()` and `TEE_TBase_DRM_ProcessContentEx()` have been added to the DRM API. They allow passing more parameters to the DRM driver.

More links (HDCP 2.1 and 2.2) can be checked with `tlApiDrmCheckLink()` or `TEE_TBase_DRM_CheckLink()`.

3.6.1.7 Power management notifications to drivers

Drivers can register themselves with `drApiEnablePowerEvents()` in order to receive Power management transitions notifications.

For example, this is needed if the hardware must be turned off when the system is going to be suspended.

The driver will receive two new messages, `MSG_SUSPEND` and `MSG_RESUME`.

3.6.1.8 Threading

Two new APIs, `drApiGetCurrentThreadId()` and `drApiGetThreadNo()` can be used to retrieve current the thread identifier and number.

3.6.1.9 FIQ forward

It is now possible to customize which FIQs are forwarded by the TEE (EL1) to the Trusted Firmware (EL3).

The documentation for the FIQ forward mechanism can be found in the Kinibi integration guide.

3.6.1.10 GP Time API

The following functions are supported:

- `TEE_GetSystemTime()`
- `TEE_GetREETime()`

The system time is based on REE-controlled timers.

3.6.1.11 GP Login API

It is now possible to specify a `connectionMethod` for `TEEC_OpenSession()` different than `TEEC_LOGIN_PUBLIC`.
The following logins are supported:

- `TEEC_LOGIN_PUBLIC`
- `TEEC_LOGIN_USER`
- `TEEC_LOGIN_GROUP`
- `TEEC_LOGIN_APPLICATION`
- `TEEC_LOGIN_USER_APPLICATION`
- `TEEC_LOGIN_GROUP_APPLICATION`

In the TA, the function TEE_GetPropertyAsIdentity("gpd.client.identity") can be used to retrieve the identity of the client and perform access control.

3.6.1.12 debugfs

In order to ease the debug of issues which are difficult to reproduce (random, long run, freeze…) the Linux driver now creates new entries under the `trustonic_tee` directory of the debugfs.

It is possible to retrieve the state of the TEE and a recent history. For example, the last SMCs, the last MCP commands or the sessions can be listed.

Please have a look at chapter 8 “SYSTEM DEBUGGING WITH DEBUGFS” of the integration guide.

4 What's new in Kinibi for EXYNOS64

The following lists the deltas of all the Early Access, Feature Complete and Commercial Releases performed to Samsung LSI.

4.1 Trustonic Kinibi-400C-EXYNOS64-v002 (build 87409)

Release status: Commercial Release

From a feature point of view, this Kinibi version is aligned on previous items introduced by NWd changes in 400c-v001 and v002. It is however rebuilding the correct link with Kinibi-400A_v017 SWd.

It's also including the following fixes:

- TBUG-1422: TeeService vendor does not cope correctly with TeeService Framework life cycle (Hidl services, TEEServiceJava).
- TD-1388: Adding support for onConfigurationChange reference code to support specific OEM usecase for screen size update (TEE ServiceJava).
- TBUG-1403: use fsync in FSD2 to ensure partition file and containing dir creation (mcDaemon).

This version of the product has been fully validated and no issue found. As a commercial Release quality, it is fully approved for production (NWd and SWd parts).

4.2 Trustonic Kinibi-400C-EXYNOS64-v002 (build 83578)

Release status: Commercial Release

This Kinibi version is adding the support of TUI on Android P (still based on Kinibi-400B, *Warning*).

It contains also several fixes in Normal World components:

- TD-1400: AndroidIntegration/Src/Patches folder contains 2 patches to apply on RootPA
- TD-1388: TUI support have been integrated to TeeService
- TBUG-1385: libMcRegistry have been fixed for OTAv1 failures
- TD-1404: libteeservice_client.so renamed to libteeservice_client.trustonic.so to be white-listed in /system/lib/public.libraries-trustonic.txt
- TD-1389: Updated SELinux policies recommendations.
- TBUG-1386: Adding security checks when allocating space for TEE object.

This release has been done mainly to provide a NWd reference code base to start early customer integration (SWd is based on Kinibi-400B and so not aligned with latest 400A_v017).

4.3 Trustonic Kinibi-400C-EXYNOS64-v001

Release status: Feature Complete

This Kinibi version is adding on top of Kinibi-400B (*Warning*):

- The support of Android P and new HIDL interfaces and services for ClientApp running from Android System Partition (Complete documentation to found into the Integration Guide).
- This release has been done mainly to provide a NWd reference code base to start early customer integration (SWd is based on Kinibi-400B and so not aligned with latest 400A_v017).

As a Feature Complete, this package as successfully passed sanity checks and overall stability is already good. However, it has not yet been fully validated and thus, is not approved for Production.

4.4 Trustonic Kinibi-400A-EXYNOS64-v017 (build 78721)

This version of Trustonic TEE is a Commercial Release update of Kinibi-400.

SWd Changes:

- Commenting out the PLAT_TRACE_EVENT feature as it is showing un-expected side effect in case of stress test (internal memory corruption, feature was only in TEE Debug image, TBUG-1353 and 1342).
- Fix to correctly support blacklisting of 64bit memory range (TBUG-1351).

4.5 Trustonic Kinibi-400A-EXYNOS64-v017

This version of Trustonic TEE is a Commercial Release update of Kinibi-400.

SWd Changes:

- SWd binary: Lots of SSIQ IRQ generated, even when Kinibi is idle (TBUG-1307)
- SWd binary: Samsung TA/Driver dumping notifications in case of un-expected abort and TEE raising error message in case of memory blacklist access, even in release binary (TBUG-1285)
- Fix to avoid loss of Readable attribute, if Writeable is set, in GP APIs TEE_PARAM_TYPE_MEMREF_WHOLE case (TBUG-1336).

NWd Changes:

- NWd TEE driver: use %pK i.o. %p to show kernel pointers in debugfs (TBUG-1273, already shared as patch)
- NWd TEE drivers: fix build and checkpatch on Linux v4.14 (TD-1302, already shared as patch)
- NWd TEE driver: do not consider TEE Proxy/client_fd option in openSession command (TBUG-1310).
- NWd TEE driver: start TEE channel at TEE Linux driver probe on platforms that don't ask otherwise (TD-1321, already shared as patch)
- NWd driver: wait for TEE to be started before opening device (TBUG-1316, already shared as patch)
- NWd TEE driver: prevent infinite daemon reconnection loop after TEE crash (TBUG-1180).
- NWd TEE driver: fastcall parameter overwritten in the log of 'mc_exec_core_switch()' (TBUG-1339)
- mcDriverDaemon, kick TUI thread before entering in mcDaemon wait. (TBUG-1309 again, fix already integrated as patch)

4.6 Trustonic Kinibi-400A-EXYNOS64-v016 (build 76762)

Release status: Commercial Release

This version of Trustonic TEE is a Commercial Release update of Kinibi-400 (emergency production change).

SWd Changes:

- Behavior of Kinibi SFS changed for partition 1 and in case of corruption detected, the Store1.tf will simply be reformatted (instead of returning "corrupted", TD-1341).
  Follow up of TBUG-1328.

4.7 Trustonic Kinibi-400A-EXYNOS64-v016 (~~build 75908~~)

Release status: Commercial Release

This version of Trustonic TEE is a Commercial Release update of Kinibi-400 (emergency production change).

SWd Changes:

- Upgrade the version of the RPMB partition to 3.0. The consequence is a reformat of the partition for devices with previous version (TBUG-1328). This happens once at very first boot in the lifetime of a device.

Warning: release DISCARDED and never deployed, code deleted.

4.8 Trustonic Kinibi-400A-EXYNOS64-v016

Release status: Commercial Release

This version of Trustonic TEE is a Commercial Release update of Kinibi-400.

SWd Changes:

- Modifying TA blob openSession sequence, checking 1st from NWd blob before looking into the Secure Storage. Goal is to prevent conflict between Android filesystem decryption and TEE SecureStorage file access (TBUG-1264).
- Changing Exynos SWd RPMB UUID (changed from 0x020A 0000…0000 to 0xFFFF FFFF 0000… 0000 0001).

NWd changes:

- Reporting back an "old/missed" fix to kick Trusted UI main thread only after the drivers (RPMB...) are loaded (mcDriverDaemon, TBUG-1267).

4.9 Trustonic Kinibi-400A-EXYNOS64-v015

Release status: Commercial Release

This version of Trustonic TEE is a Commercial Release update of Kinibi-400.

SWd Changes:

- Fix MMU flags inconsistency, bit "AP permission", between user and kernel space descriptors, causing random abort on Cortex-A75 (TBUG-1248 and TBUG-1252).
- Minor fix in RPMB activation detection in our Secure Storage Driver (badly detecting some use-mask/persistent-mask configurations (TBUG-1250).
- RPMB marshalling parameters potentially overwritten on return from tlApCallDriverEx (TBUG-1262).

drTui fixes:

- Fix platform hang due to DrTui and very early MSG_CLOSE_TRUSTLET notification (TBUG-1263, drTui.a)

NWd changes:

- NWd Linux driver post mortem logs improved (TD-1269, TEE Linux driver).

- TBUG-1173 NWd driver: lock list in put functions when de-listing is done in release, to avoid unlikely race condition (reporting Zendesk #3456).
- Following Android O update, support libgralloc1 library added in TUI Service(TD-1199).
- Add also reference version for the Kinibi Android Oreo SE Linux rules.

4.10 Trustonic Kinibi-400A-EXYNOS64-v014

Release status: Commercial Release

This version of Trustonic TEE is a Commercial Release update of Kinibi-400.

SWd Changes:

- The Secure Filesystem driver is able to call Samsung's RPMB driver directly to store the entire TA versioning in the RPMB partition

4.11 Trustonic Kinibi-400A-EXYNOS64-v013

Release status: Commercial Release

This version of Trustonic TEE is a Commercial Release update of Kinibi-400. In addition of several fixes it's introducing the support of an Embedded RPMB driver.

See below for full details:

SWd Changes:

- Adding drRPMB support as part of the System image.
  - TA loading sequence updated to be: embedded, SFS, Android FS.
  - ImageBuilder script updated to now consider DrRPMB path (new param *[--rpmb RPMB driver binary]*).
- TBUG-1165: Kinibi is now no more impacted by heavy NWd IRQ flow (previously unable to execute Trusted App in these specific cases).

t-base-dev-kit updates (sdk & ddk):

- Enabled optional Stack Smashing Protection for TAs and DRVs in TlSdk and DrSdk:
  - TASampleRot13 and DrSampleRot13 updating accordingly to demonstrate usage.
  - Kinibi_Developers_Guide.pdf Updated to add Stack Smashing Protection (*§3.1.3 Trusted Application Address Space*).

DrTui fixes:

- TBUG-1202 DrTui panic if it gets spurious notifications from the NWd.

Reporting Keymaster fixes shared in Zendesk:

- TBUGAPP-4 TLC and TA, KM_TAG_BLOB_USAGE_REQUIREMENTS may be set by caller.
- TBUGAPP-3 TLC, TEE_Begin() failed when trying to map a ReadOnly buffer from dev_tee_keymaster

It also integrates a list of NWd fixes:

- TD-1152: TEE Linux driver, minor fix to build that does not define MC_FASTCALL_WORKER_THREAD
- TBUG-1212: TEE Linux driver, handle ERESTARTSYS error in wait notification from kernel API
- Android O support improved:
  - Updating RootPA and TUI components to match Android O/Treble isolation.

- TBUG-1190, libMcClient, Android protobuf version conflicts for Android O (removing native TEE proxy, as feature not used and no more needed).

This version of the product has been fully validated and no issue found. As a commercial Release quality, it is approved for production.

4.12 Trustonic Kinibi-400A-EXYNOS64-v012

Release status: Commercial Release

This version of Trustonic TEE is a Commercial Release update of Kinibi-400.

SWd Changes:

- TBUG-1158 Miscalculation of parameter in DES key generation
- blacklist feature manageable by SMC from all cores
- Support for new MPIDR formats.

It also contains DrTui fixes:

- TBUG-1138 NULL pointer dereference in the drTuiCore driver
- TBUG-1138 Fix touch thread queue initialization

It also integrates a list of NWd Security fixes:

- TD-1079 NWd driver: only log CPU status when actually switching
- TBUG-1137 NWd driver: protect driver against TA size overflows
- TBUG-1143 NWd driver: lock around file->private_data
- TBUG-1159 NWd driver: do not blindly reset client on close in clientlib

It assures Android O preview 2 compatibility:

- Support for all Linux kernels up to v4.9
- NWd client: use ANDROID rather than LOG_ANDROID in log.h, to solve Android O preview 2 issue

This version of the product has been fully validated and no issue found. As a commercial Release quality, it is approved for production.

4.13 Trustonic Kinibi-400A-EXYNOS64-v011

Release status: Commercial Release

This version of Trustonic TEE is a Commercial Release update of Kinibi-400.

SWd Changes:

- Integer overflow check added in RTM at TA loading time (FIX TBUG-1078).
- Page pool maximum increased to go from 32MB to 128MB (TD-1011).

Overall TEE package has also been updated with minor fixes in SDK samples:

- A new SamplePinPad, showing TUI usage in GP Trusted App.
- ECDSA sample disabled for old TEE version.

This version of the product has been fully validated and no issue found. As a commercial Release quality, it is approved for production.

4.14 Trustonic Kinibi-400A-EXYNOS64-v010

Release status: Commercial Release

This version of Trustonic TEE is a Commercial Release update of Kinibi-400.

Changes of this delivery affect only the Secure World image:

- Reject TA if it uses the first page of the virtual address space (TBUG-1085).
- Forbid loading a non-downgrade protected system TA with version >=0.1 when the UUID.version file exist (REV-1792).
- Increasing number of SWd L2 descriptors from 65 to 110 (TBUG_1087).

This version of the product has been fully validated and no issue found. As a commercial Release quality, it is approved for production.

4.15Trustonic Kinibi-400A-EXYNOS64-v009

Release status: Commercial Release

This version of Trustonic TEE is a Commercial Release update of Kinibi-400.

Changes in Secure World image and in Normal World:

- Removed the automatic conversion tool that allowed silicon vendors and device manufacturers to upgrade existing devices from Kinibi-302A (TD-989, SWd image and mcDriverDaemon).
- Coverity issues fixed (TBUG-1071, NWd components)

This version of the product has been fully validated and no issue found. As a commercial Release quality, it is approved for production.

4.16Trustonic Kinibi-400A-EXYNOS64-v008

Release status: Commercial Release

This version of Trustonic TEE is a Commercial Release update of Kinibi-400.

Changes in Secure World image and in Normal World:

- Restoring "Contiguous world shared memory buffer" feature that was removed in V006.

This version of the product has been fully validated and no issue found. As a commercial Release quality, it is approved for production.

4.17Trustonic Kinibi-400A-EXYNOS64-v007

Release status: Commercial Release

This version of Trustonic TEE is a Commercial Release update of Kinibi-400.

Changes in Secure World image:

- Possible integer underflow in IWS buffer parsing in RTM (TBUG-1052).

This version of the product has been fully validated and no issue found. As a commercial Release quality, it is approved for production.

4.18Trustonic Kinibi-400A-EXYNOS64-v006

Release status: Commercial Release

This version of Trustonic TEE is the Commercial Release of Kinibi-400.

This version is introducing a new feature for the System TA Antirollback protection, the TA version check can be disabled through efuse burning (EL3 call/ PLAT_TBASE_INPUT_SYS_TA_RP_ENABLED)

It's also fixing few issues:

Changes on the Normal World components:

- Mobicore driver: dead code removed and ARMv8/GP issue fix for input parameters in shared buffed (file mmu.c, TBUG-1045)
- mcDaemon: Fix start issue in case of option `-r` with persistent SWd driver (TBUG-1039)
- t-base-dev-kit/Sample GP: fixing issues to have a correct GP example.

Changes in Secure World image:

- CBC IV generation is not uniformly random in SFS implementation (TBUG-984).
- RTM crash via un-sanitized signature data from the NWd (TBUG-906).
- RTM memory allocator does not unmap memory in case of insufficient RTM heap (TBUG-1040)

This version of the product has been fully validated and no issue found. As a commercial Release quality, it is approved for production.

4.19Trustonic Kinibi-400A-EXYNOS64-v005

Release status: Commercial Release

This version of Trustonic TEE is the Commercial Release of Kinibi-400. From the previous delivery, no new feature introduced. It's mainly fixing issues to improve overall TEE stability and Global Platform compliance:

Changes on the Normal World components:

- Mobicore driver: Update of low level SWd communication protocol to improve GP Time management (TBUG-970).
- Client Lib: Several minor updates to fix remaining issues in GP Compliance.
- Client Lib / Proxy: Shared Memory management refactored, fix for memory leak in proxy client and improve support of different SDK versions.
- tlcTui: Report code update to dynamically provide screen resolution to the NWd (Not applicable on Exynos platform).

Changes in Secure World image:

- Update of low level SWd communication protocol to improve GP Time management (TBUG-970).
- Fix for RTM threads synchronization issue on L2 table allocation (TBUG-957).
- Fix for RTM invalid check and free of L2 tables in case of overlapping buffer (TBUG-1031).
- Traces Cleanup and add trace for RPMB upgrade (TBUG-1016).
- Memory leak fix in some TA loading error cases (TBUG-967).

This version of the product has been fully validated and no issue found. As a commercial Release quality, it is approved for production.

4.20 Trustonic Kinibi-400A-EXYNOS64-v004

Release status: Feature Complete

This version of Trustonic TEE is a Feature Complete release of Kinibi-400. This version is fixing the following issue:

- Invalid parameters returned by API drApiFastCall (SWd binary).

4.21Trustonic Kinibi-400A-EXYNOS64-v003

Release status: Feature Complete

This version of Trustonic TEE is the 2nd Feature Complete release of Kinibi-400. This version is mainly fixing a lot of issues and improving the overall TEE stability:

- SWd API DrAPI_GetSecureTimeStamp was returning a random value and, by consequence, was also breaking all the SWd timeout mechanism (all the timeouts were mostly considered as "infinite")
- Several memory leaks fixed in the SWd, leading to OUT_OF_MEMORY TEE error in case of intensive usage of GP APIs.
- Many changes in TEE Linux driver to fix/adapt behaviour to pass the GP Compliance.
- TTS component update to support kinibi-400A.

4.22 Trustonic Kinibi-400A-EXYNOS64-v002

Release status: Feature Complete

This version of Trustonic TEE is the Feature Complete release of Kinibi-400. It contains all the features and fixes described in generic Kinibi 400A version.

- Documentation has been updated, but not yet finalized.
- Product has been fully validated, no major regression found however several tests are still not passing.
- This version is also not yet passing the GP Compliance testing suite.

4.23 Trustonic Kinibi-400A-EXYNOS64-v001

Release status: Early Access

This version of Trustonic TEE is the first Early access version of Kinibgi-400.

It introduces the support Rollback Protection for System TA.

Main features not included:

- Documentation is not up to date and still aligned on Kinibi-311B.
- TA to TA communication is not present.
- GP properties are not yet supported.

It has not been fully validated and is not ready for production

‹

5 HARDWARE AND SOFTWARE TESTED

The hardware platform tested is:

- Joshua (Exynos 7870).
- Lauterbach t32 is optional

The software components used are listed in the table below:

SW Components & Tools	Source	Version
Operating System for development PC		Windows XP SP3 32bits, Ubuntu 12.04 64bit
Android NDK	Google	r7b
ARM RVCT	ARM	4.1
Joshua BSP	S.LSI BSP shared in SecuTrans	20151001_JoshuaSMDK
EL3/Trusted Firmware	S.LSI BSP shared in Secu Trans with Trustonic TEE SPD	Delivered in Trustonic TEE package

6 KNOWN ISSUES AND LIMITATIONS

Due to Wi-Fi availability issue on Exynos SMDK devices, few OTA test cases have not been passed.

This is mandatory that the OEM passes the complete Trustonic TEE test suite including the OTA tests.

Trusted UI tests are also impossible to pass as feature is today not implemented/available development platform.

7 TEST RESULTS