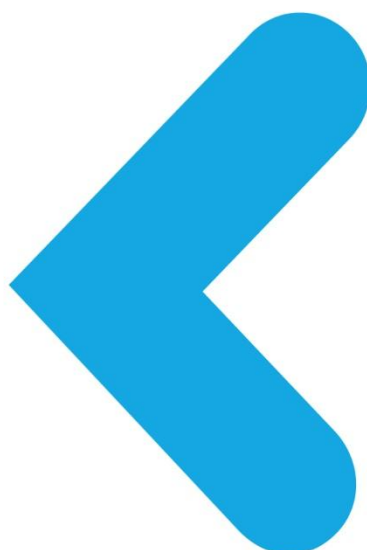
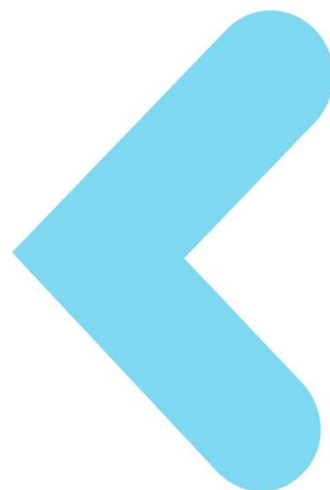


# vt-base

**<t-base-300 for MT6582**

**Commercial Release**

**Release Notes**



## TABLE OF CONTENTS

1	Introduction.....	2
2	What's New?.....	3
2.1	<t-base 300 V008 (Commercial Release).....	3
2.2	<t-base 300 V007 (Commercial Release).....	3
2.3	<t-base 300 V006 (Feature Complete) .....	3
2.4	<t-base 300 V005 (Feature Complete) .....	3
2.5	<t-base 300 V004 (Early Access).....	4
2.6	<t-base 300 V003 (Early Access).....	4
2.7	<t-base 300 V002 (Early Access).....	4
2.8	<t-base 300 V001 (Early Access).....	5
3	System Requirements .....	6
3.1	Hardware .....	6
3.2	Software for Developer PC .....	6
4	Test Results.....	7

# 1 INTRODUCTION

This document contains the Release Notes for the <t-base product on Mediatek MT6582 platform.

The version of the product is <t-base-300 V008 Commercial Release.

It has been fully validated and no critical issues found (detailed test results available in “Test Results” section).

## 2 WHAT'S NEW?

### 2.1 <T-BASE 300 V008 (COMMERCIAL RELEASE)

Product has been fully validated. TEE and OTA tests suites have been fully passed and no critical or unexpected error found.

It includes several fixes:

- DeviceKey generated by <t-base was corrupted after first use.
- Incorrect TciBuffer address returned in case of Trusted App. or Secure Drivers built with GCC (root cause localized in TISdk and DrSdk).
- <t-play documentation improvements

### 2.2 <T-BASE 300 V007 (COMMERCIAL RELEASE)

Product has been fully validated. TEE and OTA tests suites have been fully passed and no critical or unexpected error found.

This version also includes a minor fixes in GP Trusted Application storage (directory TbStorage now created in /data/app/mcRegistry, even if /system/app/mcRegistry is defined)

### 2.3 <T-BASE 300 V006 (FEATURE COMPLETE)

<t-base-300 V006 introduces the following new features and improvements:

- Fix issues in configuration of GIC for Secure World interrupts.
- Add support of UNCACHED mapping attribute for D9 area to driver API drApiMapPhys().
- Introduce new time API in TISdk: tlApiGetSecureTimestamp().
- Include the support of CPU0 Dormant Abort and L2Cache resize at t-base boot time.

### 2.4 <T-BASE 300 V005 (FEATURE COMPLETE)

<t-base-300 Feature Complete introduces the following new features and improvements:

- **Trusted User Interface (TUI):**  
The <t-base Internal API supports a new API for the Trusted User Interface. The TUI API allows Trusted Applications to retrieve securely inputs from the end-user and to securely displays data to the device display.  
This API is available to both Legacy and GlobalPlatform Trusted Applications  
  
<t-base comes with a new unified Secure Driver template for the Trusted User Interface to ease the porting of the TUI on the silicon platform.
- **<t-play DRM API**  
The <t-base Internal API supports a new DRM API for processing DRM content. This API allows Trusted Applications to decrypt and play media content through the secure media components of the platform.  
This API is available to both Legacy and GlobalPlatform Trusted Applications

<t-base comes with a new unified Secure Driver template for DRM to ease the porting on the silicon platform.

- **GlobalPlatform API**

<t-base-300 supports GlobalPlatform APIs including:

- GlobalPlatform Client API
- GlobalPlatform Cryptographic API
- GlobalPlatform Trusted Storage API
- GlobalPlatform Memory Management API

The list of functions which are supported is indicated in “t-base – API Documentation”.

- **Memory Management**

Trusted Applications can declare and use a heap for dynamic memory management.

- **Increased number of Trusted Applications and Secure Drivers**

Subject to memory availability, up to 19 Trusted Applications and 10 Secure Drivers can be loaded simultaneously.

- **Improvements for Secure Drivers**

- The virtual space for drivers has been increased to 24MB.
- Functions have been added to the DrAPI to do the cache maintenance on a specific range of memory.

- **Backward Compatibility**

<t-base-300 provides backward compatibility with the previous APIs and binary compatibility for Trusted Applications and Secure Drivers. This version also includes the support of CPU 0 Dormant Mode (MT6582 Power Management).

This delivery also include the support of CPU 0 Dormant Mode (MT6582 Power Management).

## 2.5 <T-BASE 300 V004 (EARLY ACCESS)

The early access v4 includes:

- Fix to support handling of multiple interrupts in one secure driver.
- Extension of virtual memory available for HW mapping (until 16MB).
- Partial support of CPU 0 Dormant mode.

## 2.6 <T-BASE 300 V003 (EARLY ACCESS)

This early access v3 of t-base is now able to executing trusted applications and secure drivers.

It also adds:

- SMP boot of Android.
- Power schemes supported: CPU hotplug of secondary cores.
- HW RNG integration done.

## 2.7 <T-BASE 300 V002 (EARLY ACCESS)

Changed IRQ used to notify NWd from SWd to be IRQ 80 (Shared Peripheral Interrupt).

Using software crypto driver instead of empty stubs as initially done (as it allows for primary validation while crypto driver development is done in parallel).

## 2.8 <T-BASE 300 V001 (EARLY ACCESS)

Initial <t-base integration allowing Android boot on CPU0 in normal world (replacing Mediatek's FakeTEE).

## 3 SYSTEM REQUIREMENTS





### 3.1 HARDWARE

Mediatek MT6582 devices.











### 3.2 SOFTWARE FOR DEVELOPER PC




SW Components & Tools	Source	Version
Operating System (including service pack):		Windows XP SP3 32bit, Ubuntu 12.04 64bit
Android NDK	Google	r7b
ARM RVCT	ARM	4.1
Android images	Mediatek	BSP images, release 20131120, with Pre-loader patch.
Linux Kernel	Mediatek	Kernel images, release 20131120, with Pre-loader patch.

## 4 TEST RESULTS

Test	<b>Product version:</b> t-base-300-MT6582-Android-V008 <b>Test Suite:</b> INTEGRATION <b>Test version:</b> jenkins-IntegrationBuildWrapper_trunk-2637 <b>Platform:</b> MT6582, CPU : 0x41: 0xc07 <b>Binaries version:</b> release <b>Execution date:</b> 20140110_123655		
	Results	Doc.	Time (s)
Total metrics	1134 1100 26 (26 documented)		1h7m
TrustletAPI_CryptoDriverAlgorithms	177 162 9 (9 documented)		14m49s
GP	133 129 4 (4 documented)		7m54s
TrustletAPI_CryptoDriver	230 230 0		3m9s
TPlayTest	5 5 0		53.83s



MemoryManagement	135 134 1 (1 documented)		16m3s
TrustletAPI_ContentManagement_3	78 78 0		2m29s
Runtime	38 36 1 (1 documented)		8m17s
TrustletAPI_ContentManagement_2	47 47 0		2m38s
TrustletAPI_Security	63 63 0		1m3s
Limitations	15 11 3 (3 documented)		2m54s
McDrvApi	95 95 0		2m34s
TrustletAPI_MemoryAlloc	9 9 0		20.97s
DaemonRuntime	7 0 7 (7 documented)		20.77s
daemonCommunication	81 81 0		1m56s

Registry	15 15 0		20.46s
TrustletAPI_System	2 1 1 (1 documented)		31.21s
CrashTests	4 4 0		59.82s


## Metric Legend


Testcases Total

Testcases Success

Testcases Failure ( Documented failures )

## Result Legend

 pass : The result of the test is the expected result

 fail : The result of the test is not the expected result

 : The test is not executed