Application Note Jacinto7 HS 器件客户退货流程

TEXAS INSTRUMENTS

Biao Li, Linjun Meng, and Yong Zhang

摘要

目前,在路上行驶的汽车中,装载有 TI ADAS 处理器的已达数亿辆。随着 TI 最新一代的 Jacinto 7 汽车处理器大规模生产并进入市场,各个细分市场都出现了极具竞争力的器件,比如 DRA8x/TDA4x 系列处理器。对于德州仪器 (TI)来说,客户满意度非常重要,因此我们对待客户退货的问题时,始终以谨慎且迅速的态度处理。为了能够及时解决客户的问题,TI 为希望退货的客户设立了一套客户退货流程。

与其他器件的退货相比,Jacinto7系列芯片的退货流程更为复杂,因为需要解锁高安全性 (HS)设备等,这不仅增加了流程的复杂性,也延长了整个流程的时间。本应用手册详细介绍 Jacinto7系列 HS 器件退货流程所需的其他解锁操作,旨在更大限度简化 CRP、加快 CRP 周期并优化客户体验。

表格清单

商标

所有商标均为其各自所有者的财产。



1 简介

在客户进行研发和大规模生产的阶段,可能会遇到许多与硬件或软件相关的问题。当客户怀疑问题源自芯片内部 模块时,首先需要联系我们的支持窗口。TI 对自家产品的质量有高度的信心,大部分问题很可能与客户的硬件或 软件设计有关。在大多数情况下,TI 能够帮助客户解决问题,所以通常没有必要退回器件。

在某些特殊情况下,如果客户确实需要退回器件,那么就需要根据 TI 的 通用 CRP 标准来判断您的芯片是否符合 TI 退货分析标准。以上便是退回有问题的 TI 器件的标准流程,向 TI 提交退货申请前,您需要先了解这个流程。您需要在系统中填写并提交相应的 CRP 申请表。提交申请后,系统将自动安排相应的 TI FQE 同事来跟进相关事 宜。

除了标准退货流程之外,客户还需要协助 TI 进行一些实验或在客户系统层面进一步分析以找到具体模块故障,包括但不限于 ABA 实验、X 射线焊点照片、TI 默认软件测试、信号波形测量等。这些实验需要根据具体情况来实施。由于处理器非常复杂且难以分析,因此我们需要客户的大力配合。这有助于加快器件分析过程。

总之, Jacinto7 器件需要按照图 1-1 来推进该流程。如有任何疑问, TI 支持窗口将随时为您提供帮助。



图 1-1. Jacinto7 器件退货流程图

2 提供的器件类型和关键信息

您可以从器件表面获取器件型号,也可以在您向 TI 下达的订单中搜索器件型号。然后,可以从 ti.com 下载数据 表。以 TDA4VM 为例。如需更多信息,请参阅适用于 ADAS 和自动驾驶汽车的 TDA4VM Jacinto™ 处理器器件 修订版 1.0 和 1.1 中的器件和文档支持一节。您可以明确自己拥有的是哪种器件。此处提供了大量有关器件类型 的详细信息。您只需关注表 2-1 中所示的三种器件类型。

表 2-1. GP/HS 器	表 2-1. GP/HS 器件的 JTAG 状态			
型号	DMSC/SMS JTAG 状态			

器件类型	型号	DMSC/SMS JTAG 状态	R5F JTAG 状态
通用 (GP)	不适用	开路	开路
高安全性	强制安全型 (SE)	闭路 (TI)	闭路(客户)
高安全性-Prime	强制安全型 (SE)	闭路(客户)	闭路(客户)

例如:TDA4VM88TGBALFRQ1-通用器件可以直接退回 TI。

TDA4VM88T5BALFRQ1 - 高安全性器件需要解锁准备,不要直接退回。

这三种器件类型的退货流程是不同的。尤其是通用芯片和高安全性芯片的区别更大,HS器件的退货会更加复杂。

2.1 通过 MCU UART 获取其他关键信息

在从客户电路板上拆下器件并发回进行测试之前,必须事先读取 UID(唯一 ID)、DIE ID 等关键信息。本文建议 使用 UART 引导模式来分析 MCU UART 打印的字符。具体操作步骤如下。

- 1. 获取 UID。
 - a. 将电路板的引导模式配置为 UART 引导模式,并将电路板的第二个 MCU UART 串行端口连接到主机 PC,请参阅 J721E 的 EVM 设置,然后为 EVM 加电。
 - b. 终端会显示如下所示的一些日志。您需要移除末尾的额外 CCC 并另存为日志文件。默认 HS 电路板日志 如下所示。
 - C. 1aa67a56d53b06f250d75cb2a9cf7a52d6eb5e21b5e824250d7e09c22d997f09dc9389ecaa3f7d2b64d3a76d6163a a09e928ea050e1da95507e661f6002b07cd9b0b7c47d9ca8d1aae57b8e8784a12f636b2b760d7d98a18f189760dfd 0f23e2b0cb10ec7edc7c6edac3d9bdfefe0eddc3fff7fe9ad875195527df02f2a23c0ed9d5fcf6dfb3a097ee4207c b1e2a5956e07ba144b73fe71143982cccccccccc
 - d. 下载 python 脚本来解析步骤 2 中的日志。
 - e. 在获取上述两个文件后,使用以下命令解析日志。解析后的信息如下所示:

@Ubuntu18:~/Documents/summary/parse_uart_log\$ python 7080.uart_boot_socid.py default_uart_hs.log SoC ID Header Info: NumBlocks : [2] SOC ID Public ROM Info: SubBlockId SubBlockSize : j7es DeviceName DeviceType : HSSE DMSC ROM Version : [0, 1, 0, 2] R5 ROM Version : [0, 1, 0, 2]SoC ID Secure ROM Info: Sec SubBlockId : 2 Sec SubBlockSize : 166 : 0 Sec Prime : 1 Sec Key Revision Sec Key Count : 1 Sec TI MPK Hash 33c74f0c8631aa67a56d53b06f250d75cb2a9cf7a52d6eb5e21b5e824250d7e09c22d997f09dc9389ecaa3f7d2b64



d3a76d6163aa09e928ea050e1da95507e66 Sec Cust MPK Hash : 1f6002b07cd9b0b7c47d9ca8d1aae57b8e8784a12f636b2b760d7d98a18f189760dfd0f23e2b0cb10ec7edc7c6eda c3d9bdfefe0eddc3fff7fe9ad875195527d Sec Unique ID : f02f2a23c0ed9d5fcf6dfb3a097ee4207cb1e2a5956e07ba144b73fe71143982

2. 获取 DIE ID。

本文档建议在进入客户电路板的 Linux 后,输入命令行,使用以下命令行读取 DIE ID。

echo `devmem2 0x43000020 w | tail -n1` echo `devmem2 0x43000024 w | tail -n1` echo `devmem2 0x43000028 w | tail -n1` echo `devmem2 0x4300002c w | tail -n1`

获得上面列出的所有关键信息后,您需要将其共享到支持窗口。这将有助于完成 HS 器件退货的后续流程。如果您的器件是通用 (GP) 型,请将这些关键信息提供给您的 TI 支持窗口,然后即可直接退回该器件,无需提供以下用于 HS 器件退货的文件。否则,您需要按照节3中的步骤生成更多二进制文件以供 TI 进一步测试您的器件。

3 HS 器件退货

HS 器件退货情况更为复杂,因为 JTAG 接口已关闭,TI 无法访问并对此进行更多测试。TI 需要在客户的帮助下 生成"复位中等待"(WIR)证书、SBL/SPL 证书和 DMSC 固件。这些二进制文件将帮助 TI 解锁 JTAG 并登录 HLOS 以继续执行后续流程。Jacinto7 系列器件的退货测试流程如图 3-1 所示。要启用 HS 器件测试,必须进行 HS 凭据握手。



图 3-1. TI 中的客户退货单元测试流程

需要客户签名的 WIR 证书才能启用以下两种测试:ATE 测试和基准测试。在开发阶段,客户可以在 Boardcfg 文件中使用 allow_wildcard_unlock = 0x5A 来跳过 UID 验证,但在大规模生产阶段,该参数必须设置为 0 以启用 UID 验证。CRP 主要针对大规模生产项目。TI 提供的相应固件 (allow_wildcard_unlock = 0x0) 用于启用 UID 验证。客户为固件签名后,需要在固件进入系统之前验证 UID。只有通过验证后才能成功启动系统。因此,该固件 只能用于解锁您提供的 UID 对应的器件以进一步保护客户的信息安全。每个器件的器件 UID 都是唯一的。证书仅 允许在一个器件上进行调试。这涉及客户和 TI 之间就每个退回的器件交换相关信息。辅助应用程序调试需要额外 的签名映像。客户必须使用器件根密钥(私钥)为 TI 引导加载程序和固件映像签名。

创建新的 QTS 作业后, CRP 无法启动, 直到 TI:

- 接收到器件(客户从电路板上拆下器件并发货)
- 对器件重新植球
- 提取器件 UID 并创建证书输入并发送给客户联系人
- 接收到客户签名的证书



3.1 CRP 脚本工具

为了标准化和简化客户提供二进制文件的流程,TI提供了 CRP 脚本工具。目前该工具参考 tar 仅支持 TDA4VM,更多的器件需要选择 SDK 路径来生成签名的二进制文件。该 CRP 脚本的运行逻辑如图 3-2 所示。



图 3-2. TI CRP 脚本工具签名和生成流程

设置生成二进制文件的环境后,TI将提供参考环境 tar (基于 TDA4VM SDK8.6),客户只需要输入 KEY_FILE 路径(这意味着客户需要能够访问私钥)、器件 UID 和输出路径,该工具将帮助进行签名并生成 TI CRP 需要的 所有二进制文件。请添加 override.bin、SBL/SPL 证书二进制文件和 DMSC 证书二进制文件。该工具可以选择除 tiboot3.bin 和 tifs.bin 或 sysfw.itb 以外的其他二进制文件是否需要签名。对于 HS 器件和 HS-Prime 器件的不同签 名流程,该工具也可以处理这种情况。

使用该工具可以一次性生成需要在 CRP 流程中签名的所有文件,并可以修改参数来配置该工具生成的文件数量, 且该工具仍在不断改进。该工具的具体使用步骤如下:

- 1. 下载 j7_crp_tool.zip tar 并将其解压到 ubuntu PC 上。
- 2. 转到该工具的安装路径,并使用以下命令执行脚本工具: / j7_crp_spl_tool.sh。
- 3. 输入私钥路径:KEY_FILE 路径,该工具中提供了 TI 虚拟密钥,例如:{cwd}/j7_crp_spl_too_for_reference/ core-secdev-k3/keys/custMpk.pem。
- 4. 您需要输入器件类型 (hs/hsp)。该工具将检查密钥文件是否存在,如果不存在,则会立即退出。
- 5. 您需要输入器件 UID 和已签名二进制文件的输出路径。
- 6. 您可以在输出路径中找到该工具生成的所有二进制文件,并需要将这些文件打包到一个文件 (tar) 中并发送到TI 联系窗口。

3.2 独立生成 WIR 证书二进制文件 (override.bin) 并为其签名

所有 Jacinto7 HS 器件退货 ATE 测试都必须执行该过程。WIR 证书用于在 ATE 测试阶段解锁 JTAG 调试端口。 JTAG 解锁后,可以继续进行 ATE 测试,也可以运行一些基本的裸机测试程序。但是,该测试只能针对特定的故 障模块进行单模块测试。如果上述所有测试都通过,则有必要进入高级操作系统 (HLOS) 以执行基准系统级测 试,并根据客户故障场景进行有针对性的系统级测试。为了生成 WIR 证书,您需要使用以下模板代码替换粗体显 示的 UID,然后将其另存为 x509_sec_override.txt。

在以下代码模板中,certType = INTEGER:2147483649 (十进制为 0x80000001)表示覆盖证书 (Override Cert) 模式。debugType = INTEGER:4 表示 DEBUG_FULL,用于解锁 JTAG 功能并启用完整调试功能。

```
[ req ] distinguished_name =
    req_distinguished_name x509_extensions = v3_ca prompt = no dirstring_type = nobmp [
    req_distinguished_name ] C = gc ST = CW L = y6qqF9wh61 O =
    vGtcXq5gItAeCDXDyVCtdVayXh OU = tcDeqFyxG4r CN = rgH4qFPTF emailAddress =
    lQeqF8F1HQuc2@lrIP7hPUyQ03x.com [ v3_ca ] basicConstraints = CA:true
    1.3.6.1.4.1.294.1.1=ASN1:SEQUENCE:boot_seq 1.3.6.1.4.1.294.1.8=ASN1:SEQUENCE:debug [
    boot_seq ] certType = INTEGER:2147483649 bootCore = INTEGER:0 bootCoreOpts =
    INTEGER:0 destAddr = FORMAT:HEX,OCT:00000000 imageSize = INTEGER:0 [ debug ]
    debugUID =
    FORMAT:HEX,OCT:486227340651ed7670e840191e064dbb8d0ad5164737980ed860ebd81672b8cc
    debugType = INTEGER:4 coreDbgEn = INTEGER:0 coreDbgSecEn = INTEGER:0
```

使用以下命令生成名为 override.bin 的 WIR 证书文件。以下命令中的 custkey.pem 是客户的根私钥,并需要在同一路径中运行该命令。

\$ openssl req -new -x509 -key custkey.pem -nodes -outform DER -out override.bin -config x509_sec_override.txt -sha512

这已集成到 CPR 脚本工具中。

3.3 为基准测试独立生成二进制文件

所有 Jacinto7 HS 器件退货基准测试都必须执行该过程。TI 可能需要登录 HLOS 系统来运行更多测试以便进一步 分析。需要更多签名的二进制文件来解锁器件。原因在于,在基准测试中,TI 需要进入 HLOS (如 Linux)来获取 更多日志信息,因此需要更多签名的二进制文件。下文主要介绍 SPL 引导模式。

1. 生成签名的 cfg 文件。

TI 将为您准备 board-cfg.bin、sec-cfg.bin、rm-cfg.bin、pm-cfg.bin(位于 /ti-processor-sdk-linux-j7-evm-xx_xx_xx/board-support/k3-image-gen-2021.01a/out/soc/j721e/evm),并请求您通过 secure-binary-image.sh 为这些文件签名。然后,返回签名的映像。使用以下命令生成签名的二进制文件:

/ti-processor-sdk-linux-j7-evm-07_03_00_05/board-support/core-secdev-k3/scripts/secure-binaryimage.sh out/soc/j721e/evm/board-cfg.bin out/soc/j721e/evm/board-cfg.bin-signed

2. 生成签名的 sysfw.bin-hs。

通过 ./gen_x509_cert.sh 使用 custMpk.pem 为 sysfw 内部证书签名。该过程在 HS 和 HS-Prime 器件之间存 在差异。您只需选择一种生成方式。

a. HS 器件:

TI 将准备 ti-fs-firmware-j721e_sr1_1-hs-enc.bin 和 ti-fs-firmware-j721e_sr1_1-hs-cert.bin 供客户签名。

```
./gen_x509_cert.sh -d -c m3 -b /home/chris/J7/J721e/86/hs/board-support/prebuilt-images/ti-
fs-firmware-
j721e_sr1_1-hs-cert.bin -o ti-fs-firmware-j721e_sr1_1-hs-certs.bin -l 0x40000 -k /home/
chris/J7/J721e/86/hs/board-
support/core-secdev-k3/keys/custMpk.pem -r 1
```



您需要通过 cat 命令生成 sysfw.bin-hs。

```
cat ti-fs-firmware-j721e_sr1_1-hs-certs.bin /home/chris/J7/J721e/86/hs/board-support/
prebuilt-images/ti-fs-
firmware-j721e_sr1_1-hs-enc.bin > out/soc/j721e/evm/sysfw.bin-hs
```

b. HS-Prime 器件:

TI 将仅准备 ti-fs-firmware-j721e-hs.bin 供客户签名。

```
./gen_x509_cert.sh -d -c m3 -b /home/chris/J7/J721e/86/hs/board-support/prebuilt-images/ ti-
fs-firmware-j721e-hs.bin -o out/soc/j721e/evm/sysfw.bin-hs -l 0x40000 -k /home/chris/J7/
J721e/86/hs/board-support/core-secdev-k3/keys/custMpk.pem -r 1
```

客户只需为该二进制文件签名。无需再执行 cat 命令。

3. 通过脚本 gen_its.sh 生成其文件,最后返回 sysfw.itb。

所有类型的 HS 器件都必须执行该过程。首先使用以下命令生成其文件。

```
./gen_its.sh j721e_sr1_1 hs evm out/soc/j721e/evm/sysfw.bin-hs out/soc/j721e/evm/board-cfg.bin-
signed
out/soc/j721e/evm/pm-cfg.bin-signed out/soc/j721e/evm/rm-cfg.bin-signed out/soc/j721e/evm/sec-
cfg.bin-signed >
out/soc/j721e/evm/sysfw-j721e_sr1_1-evm.its
```

使用此 mkimage 命令生成 sysfw-j721e_sr1_1-evm.itb 并重命名为 sysfw.itb。

mkimage -f out/soc/j721e/evm/sysfw-j721e_sr1_1-evm.its -r sysfw-j721e_sr1_1-evm.itb
move out/soc/j721e/evm/sysfw-j721e_sr1_1-evm.itb out/soc/j721e/evm/sysfw.itb

4. 生成 tiboot3.bin 以用于 SPL 引导。

您需要先使用下面的补丁来执行 U-boot, 然后重新生成 u-boot-spl.bin。该补丁跳过了对后续内核或应用程序 文件进行签名的需求。

```
diff --git a/arch/arm/mach-k3/security.c b/arch/arm/mach-k3/security.c
index 092588f4b5..c55d1da689 100644
--- a/arch/arm/mach-k3/security.c
+++ b/arch/arm/mach-k3/security.c
@@ -53,6 +53,14 @@ void ti_secure_image_post_process(void **p_image, size_t *p_size)
       if (!image_size)
            return;
        if
           (get_device_type() == K3_DEVICE_TYPE_HS_SE &&
 +
            !ti_secure_cert_detected(*p_image)) {
+
            printf("warning: Did not detect image signing certificate. "
"Skipping authentication to prevent boot failure for CRP. "
"This will fail on Security Enforcing(HS-SE) devices\n");
+
+
+
            return;
+
       }
+
       if (get_device_type() == K3_DEVICE_TYPE_GP) {
                (ti_secure_cert_detected(*p_image)) {
    printf("Warning: Detected image signing certificate on GP device. "
```

使用 k3_gen_x509_cert.sh 生成 tiboot3.bin。

```
u-boot-2021.01+gitAUTOINC+62a9e51344-g62a9e51344/tools/k3_gen_x509_cert.sh -c 16 -b s -o tiboot3.bin -l 0x41c00000 -r 1 -k /home/chris/J7/J721e/86/l/board-support/core-secdev-k3/keys/custMpk.pem
```

只需向 TI 提供 tiboot3.bin 和 sysfw.bin。

4 总结

本应用手册总结了 J7 HS 器件客户退货流程,并为客户提供了 CPR 脚本工具来标准化和简化客户签名流程,从 而更大限度为行使退货测试权利的客户提供便利。当退回 HS 器件时,由于器件解锁等问题,客户退货流程的周 期会大大延长,导致客户体验受到影响。目前,针对 Jacinto7 系列的最常见 HS 版本 TDA4VM,开发了 CRP 脚 本工具。适用于 Jacinto7 系列其他器件类型的工具将在未来更新。

5 参考文献

- 1. TDA4VM 产品页面
- 2. 德州仪器 (TI): DRA829/TDA4VM 技术参考手册
- 3. TISCI 用户指南
- 4. 德州仪器 (TI): Jacinto7 HS 器件开发
- 5. 德州仪器 (TI): K3 安全硬件架构用户指南 (SPRUIMOC)
- 6. 如何检查器件类型是 HS-SE、FS 还是 GP

重要声明和免责声明

TI"按原样"提供技术和可靠性数据(包括数据表)、设计资源(包括参考设计)、应用或其他设计建议、网络工具、安全信息和其他资源, 不保证没有瑕疵且不做出任何明示或暗示的担保,包括但不限于对适销性、某特定用途方面的适用性或不侵犯任何第三方知识产权的暗示担 保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任:(1) 针对您的应用选择合适的 TI 产品,(2) 设计、验 证并测试您的应用,(3) 确保您的应用满足相应标准以及任何其他功能安全、信息安全、监管或其他要求。

这些资源如有变更,恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的应用。严禁对这些资源进行其他复制或展示。 您无权使用任何其他 TI 知识产权或任何第三方知识产权。您应全额赔偿因在这些资源的使用中对 TI 及其代表造成的任何索赔、损害、成 本、损失和债务,TI 对此概不负责。

TI 提供的产品受 TI 的销售条款或 ti.com 上其他适用条款/TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

邮寄地址:Texas Instruments, Post Office Box 655303, Dallas, Texas 75265 Copyright © 2024,德州仪器 (TI) 公司