TOP-TECH 鼎科实业 程序文件		文件编号	RD-TBC
		版本	A/0
		制定日期	2012-7-30
文件名称	**调试报告**	页码	共 页，第 1 页

产品名称：	MSD308B	**调试类型：**	○ 软件 ○ **硬件**		
调试人员：	蔡敏淦	**调试时间：**	2013-12	**编制日期：**	2013-12-5

CI 分类：CI 有 CI 和 CI PLUS 之分，现在的 CI PLUS 已经升级为 1.3 版本，解密方式有普通解密和加密解密之分。一版的 mstar 的公版 code 中都有内置 smart CAM 的普通卡的解密 KEY。带加密的卡匹配的 key 需要客户提供。

此次问题碰到了客户的 CI+无法解密：

分析客户打印信息：

```
UART_115200

BIST0-OK
BIST1-FAIL
_U
Hello A7
[boot time] start of main

 <Utopia> | [MST] | [7.3.11] | [V37]
-->>NEW POWER ON SEQ: MApi_AUDIO_WritePreInitTable

 USB_Init_ConfigureUSB_Init_Configure done...
Flash is detected (0x0503, 0xC2, 0x20, 0x17)

Keypad Initialize OK
MDrv_PNL_Init u32PnlRiuBaseAddr = BF200000
MDrv_PNL_Init u32PMRiuBaseAddr = BF000000
[XC,Version] 00421206
 MApi_XC_Init, 515, pXC_InitData->stPanelInfo.eLPLL_Type=1
Init PWM1
Init PWM2
[Utopia] T9 is not support
GE_SetOnePixelMode
=====================
First GOP driver instance, flush GWIN HW
=====================



[GOP_ALL][Driver Version]: 0083, BuildNum: 0011, ChangeList: 00385765
[HAL_TSP_CPU_SetBase][2131] load firmware (address, size) = (0x0095DA00, 0x000028A8)
firmware 111 0x0095DA00 0x00000000 0x000095DA
```

```
[HAL_DSCMB_SetBank][160] Set bank 0xBF200000

m_acSATTableMap=FF
m_acSATTableMap=FF
m_acSATTableMap=FF
m_acSATTableMap=FF
m_acSATTableMap=FF
m_acSATTableMap=FF
m_acSATTableMap=FF
m_acSATTableMap= 3
m_acSATTableMap= 0Error> USB Download Search: port 2 connection timeout
xc: 3D has changed the H prescaling setting, need to skip PQ HSD_Sampling/HSD_Y/HSD_C loading

[-enDVBPreSelectType-]: 0bParallelTS==1Javy --- AVL_DVBSx_ExtAV2011_Initialize!!!

  Tuner slave address = 0xC4
>DVB-C DSP Loadcode fail!DVB-C Load DSP Code Fail
DSP code loaded successfully
init Shared

HAL_MAD_SetMemInfo[DSP_DEC] = 0x00CA9000

HAL_MAD2_SetMemInfo[DSP_SE] = 0x00B8D000
device/tuner/NXP_TDA18275.c, 513, i2c write Error
[CurrentStandard],0
_MAPP_EPGDB_Setup: [Current EPG DB occupy size: 0x83C218];    [Max EPG DB config. size: 0x840000]

  set tv type = 0
==>Delete Main Path, SRC =39, Dest=1
bParallelTS==1MDrv_IFDM_SetIF =B
===== Check Audio Decoder Protection from hash-key IP =====
Hash-key Support DD.
Hash-key Support DD+.
Hash-key Support Generic HE-AAC !!
Hash-key Support WMA.
===== Check Protection IP End                              =====
Audio DSP1 code is same(3), no need to reload
=== HAL_AUDIO_SPDIF_SetMode: 0, src:0 ===
>DVB-C DSP Loadcode fail!DVB-C Load DSP Code Fail

  set routing to (2) ok!!
[HAL_TSP_CPU_SetBase][2131] load firmware (address, size) = (0x0095DA00, 0x000028A8)
firmware 111 0x0095DA00 0x00000000 0x000095DA

========================================

DVB-T Software Version: 0.00
[Board]: BOARD_TYPE_P75_309BS2_V60A
[Panel]: FullHD_AUO_M270HVN02.1
```

```
[MEMORY_MAP]: MMAP_128MB
[DRAM SIZE]: 128 MB
[FLASH SIZE]: 8 MB
[ATV]: PAL
[Mirror]: 1
[ENABLE_PWS]: 1
[ENABLE_POWER_SAVING_DPMS]: 1
[DEMO_FINE_TUNE]: DFT_STD_FULLHD_M270HVN02
[ENABLE_DLC]: 1
[MWE]: 1
[FRONTEND_TUNER_TYPE]: NXP_TDA18275_TUNER

===================================
[12506 ms] [CI] Notify Current Service Info: TS_ID(0x03F9) | Service ID(0xEF74)
[CI+][HSS] MDrv_CI_HSS_SetSunningStatus: 1
[CI+][HSS] 5 sec Timeout Waiting for SDT (6).
HAL_VPU_EX_SetDbgLevel eLevel=0x1
===== Check Audio Decoder Protection from hash-key IP =====
Hash-key Support DD.
Hash-key Support DD+.
Hash-key Support Generic HE-AAC !!
Hash-key Support WMA.
===== Check Protection IP End                         =====
=== HAL_AUDIO_SPDIF_SetMode: 2, src:0 ===
=== HAL_AUDIO_SPDIF_SetMode: 2, src:0 ===
[.//msAPI_CI_common.c:1622][Warning!][CI+][HSS] SDTActual is not acquired after 5 seconds then service shunning is In-active (8)!
[CI+][HSS] MDrv_CI_HSS_SetSunningStatus: 0
Clear ES buffer
[24354 ms] [CI] Notify Service Exit...
[24357 ms] [CI] Notify Current Service Info: TS_ID(0xFFFF) | Service ID(0xEF10)
[CI+][HSS] MDrv_CI_HSS_SetSunningStatus: 1
[CI+][HSS] 5 sec Timeout Waiting for SDT (6).
=========> vdec_u8Idx=0x0, u32VdecStreamId=01010
HAL_VPU_EX_SetDbgLevel eLevel=0x1
  VDEC_USER_CMD_FORCE_INTERLACE_MODE    fail !
===== Check Audio Decoder Protection from hash-key IP =====
Hash-key Support DD.
Hash-key Support DD+.
Hash-key Support Generic HE-AAC !!
Hash-key Support WMA.
===== Check Protection IP End                         =====
=== HAL_AUDIO_SPDIF_SetMode: 0, src:0 ===
=== HAL_AUDIO_SPDIF_SetMode: 0, src:0 ===
[26389 ms] [CI] Notify Current Service Info: TS_ID(0x0421) | Service ID(0xEF10)
[CI+][HSS] MDrv_CI_HSS_SetSunningStatus: 1
[CI+][HSS] 5 sec Timeout Waiting for SDT (6).
[CI+][HSS] MDrv_CI_HSS_Set: TS ID(0421)|Service ID(EF10) 0 bytes
[CI+][HSS] Add SDT Cache(TS ID(1057)|Service ID(61200)).
```

```
[CI+][HSS] No CDP in SDT Table.
[CI+][HSS] MDrv_CI_HSS_Set: TS ID(0421)|Service ID(EF11) 0 bytes
[CI+][HSS] Add SDT Cache(TS ID(1057)|Service ID(61201)).
[CI+][HSS] No CDP in SDT Table.
[CI+][HSS] MDrv_CI_HSS_Set: TS ID(0421)|Service ID(EF14) 0 bytes
[CI+][HSS] Add SDT Cache(TS ID(1057)|Service ID(61204)).
[CI+][HSS] No CDP in SDT Table.
[CI+][HSS] MDrv_CI_HSS_Set: TS ID(0421)|Service ID(EF15) 0 bytes
[CI+][HSS] Add SDT Cache(TS ID(1057)|Service ID(61205)).
[CI+][HSS] No CDP in SDT Table.
[26460 ms] [CI] Notify Current Service Info: TS_ID(0x0421) | Service ID(0xEF10)
[CI+][HSS] MDrv_CI_HSS_SetSunningStatus: 1
[CI+][HSS] 5 sec Timeout Waiting for SDT (6).
[CI+][HSS] MDrv_CI_HSS_Set: TS ID(0421)|Service ID(EF10) 0 bytes
[CI+][HSS] Reset SDT Cache(TS ID(1057)|Service ID(61200)).
[CI+][HSS] No CDP in SDT Table.
[CI+][HSS] MDrv_CI_HSS_Set: TS ID(0421)|Service ID(EF11) 0 bytes
[CI+][HSS] Reset SDT Cache(TS ID(1057)|Service ID(61201)).
[CI+][HSS] No CDP in SDT Table.
[CI+][HSS] MDrv_CI_HSS_Set: TS ID(0421)|Service ID(EF14) 0 bytes
[CI+][HSS] Reset SDT Cache(TS ID(1057)|Service ID(61204)).
[CI+][HSS] No CDP in SDT Table.
[CI+][HSS] MDrv_CI_HSS_Set: TS ID(0421)|Service ID(EF15) 0 bytes
[CI+][HSS] Reset SDT Cache(TS ID(1057)|Service ID(61205)).
[CI+][HSS] No CDP in SDT Table.
[CI+][HSS] MDrv_CI_HSS_GetSunningStatus: 1
[26810 ms] [CI] Update CA PMT: CAFlag = 0 | HSS Status = 1
[31709 ms] [CI] Notify Service Exit...
[31712 ms] [CI] Notify Current Service Info: TS_ID(0x0421) | Service ID(0xEF10)
[CI+][HSS] MDrv_CI_HSS_SetSunningStatus: 1
[CI+][HSS] 5 sec Timeout Waiting for SDT (6).
HAL_VPU_EX_SetDbgLevel eLevel=0x1
===== Check Audio Decoder Protection from hash-key IP =====
Hash-key Support DD.
Hash-key Support DD+.
Hash-key Support Generic HE-AAC !!
Hash-key Support WMA.
===== Check Protection IP End                              =====
=== HAL_AUDIO_SPDIF_SetMode: 2, src:0 ===
=== HAL_AUDIO_SPDIF_SetMode: 2, src:0 ===
[33873 ms] [CI] Notify Current Service Info: TS_ID(0x0421) | Service ID(0xEF10)
[CI+][HSS] MDrv_CI_HSS_SetSunningStatus: 1
[CI+][HSS] 5 sec Timeout Waiting for SDT (6).
[CI+][HSS] MDrv_CI_HSS_Set: TS ID(0421)|Service ID(EF10) 0 bytes
[CI+][HSS] Reset SDT Cache(TS ID(1057)|Service ID(61200)).
[CI+][HSS] No CDP in SDT Table.
[CI+][HSS] MDrv_CI_HSS_Set: TS ID(0421)|Service ID(EF11) 0 bytes
[CI+][HSS] Reset SDT Cache(TS ID(1057)|Service ID(61201)).
[CI+][HSS] No CDP in SDT Table.
```

```
[CI+][HSS] MDrv_CI_HSS_Set: TS ID(0421)|Service ID(EF14) 0 bytes
[CI+][HSS] Reset SDT Cache(TS ID(1057)|Service ID(61204)).
[CI+][HSS] No CDP in SDT Table.
[CI+][HSS] MDrv_CI_HSS_Set: TS ID(0421)|Service ID(EF15) 0 bytes
[CI+][HSS] Reset SDT Cache(TS ID(1057)|Service ID(61205)).
[CI+][HSS] No CDP in SDT Table.
[CI+][HSS] MDrv_CI_HSS_GetSunningStatus: 1
[34378 ms] [CI] Update CA PMT: CAFlag = 0 | HSS Status = 1
bParallelTS==1[CI] ## E_CI_HWRST
[CI+][HSS] MDrv_CI_HSS_SetSunningStatus: 1
[CI] Delay 500 ms for H/W Reset of CI Init.
[CI] ## E_CI_INIT
[CI] PCMCIA CIS:
1D 04 00 DB 08 FF 1C 03
00 08 FF 15 30 05 00 53
6D 61 72 44 54 56 00 44
56 42 20 43 41 20 4D 6F
64 75 6C 65 00 24 63 6F
6D 70 61 74 69 62 6C 65
5B 63 69 70 6C 75 73 3D
31 5D 24 00 FF 20 04 FF
FF 01 00 1A 15 01 0F FE
01 01 C0 0E 41 02 44 56
42 5F 43 49 5F 56 31 2E
30 30 1B 11 C9 41 19 37
55 4E 5E 1D 56 AA 60 90
01 03 50 FF FF 1B 26 CF
04 19 37 55 4D 5D 1D 56
22 20 C0 09 44 56 42 5F
48 4F 53 54 00 C1 0E 44
56 42 5F 43 49 5F 4D 4F
44 55 4C 45 00 14 00 FF
6B 09 2B 4E 57 60 D3 46
E7 9E AA 9F 58 D0 37 51
B7 8A 1B 82 99 0B DC 00
38 E7 39 E0 38 DB 32 FF
07 76 93 51 11 49 97 5A
80 AF 10 6F 10 DF 24 DF
21 2E 61 A6 23 FF 38 CF
BF 5C 4B D6 A5 EA 7E 9C
4C D6 B1 14 BD 12 F5 68
49 A0 72 D0 3B 76 6C 42
DE A0 B7 16 8F 42 66 CD
98 3E 23 D7 96 DC 7B FC
3B 05 8E F7 84 3A 8C 00

[CI] ManufacturerName SmarDTV
[CI] ProductName DVB CA Module
[CI] ProductInfo1 $compatible[ciplus=1]$
```

```
[CI] ProductInfo2□
[CI] Reset Interface OK!
[CI] BufferSize 2046 bytes
[CI+] Up DAIE!!!
[CI] PCMCIA Config OK!
[CI] CI+ CAM: SmarDTV | DVB CA Module
[52024 ms] TX: 01 00 82 01 01
[52032 ms] RX: 01 00 83 01 01 80 02 01 00
[52079 ms] RX: 01 00 80 02 01 80
[52099 ms] TX: 01 00 81 01 01
[52119 ms] RX: 01 00 A0 07 01 91 04 00 01 00 41 80 02 01 00
[52139 ms] TX: 01 00 A0 0A 01 92 07 00 00 01 00 41 00 01
[52178 ms] TX: 01 00 A0 09 01 90 02 00 01 9F 80 10 00
[52222 ms] RX: 01 00 80 02 01 80
[52225 ms] TX: 01 00 81 01 01
[52233 ms] RX: 01 00 A0 09 01 90 02 00 01 9F 80 11 00 80 02 01 00
[52240 ms] TX: 01 00 A0 09 01 90 02 00 01 9F 80 12 00
[52254 ms] RX: 01 00 80 02 01 80
[52257 ms] TX: 01 00 81 01 01
[52265 ms] RX: 01 00 A0 09 01 90 02 00 01 9F 80 10 00 80 02 01 00
[52271 ms] TX: 01 00 A0 3D 01 90 02 00 01 9F 80 11 34 00 01 00 41 00 01 00 42 00 02 00 41 00 02 00 43 00 03 00
41 00 20 00 41 00 24 00 41 00 40 00 41 00 8C 10 01 00 8D 10 01 00 8E 10 01 00 41 00 41 00 10 00 41
[52299 ms] RX: 01 00 80 02 01 80
[52302 ms] TX: 01 00 81 01 01
[52310 ms] RX: 01 00 A0 07 01 91 04 00 24 00 41 80 02 01 00
[52315 ms] TX: 01 00 A0 0A 01 92 07 00 00 24 00 41 00 02
[52325 ms] RX: 01 00 80 02 01 80
[52328 ms] TX: 01 00 81 01 01
[52336 ms] RX: 01 00 A0 07 01 91 04 00 20 00 41 80 02 01 00
[52342 ms] TX: 01 00 A0 0A 01 92 07 00 00 20 00 41 00 03
[52357 ms] RX: 01 00 80 02 01 80
[52360 ms] TX: 01 00 81 01 01
[52368 ms] RX: 01 00 A0 07 01 91 04 00 8D 10 01 80 02 01 00
[52373 ms] TX: 01 00 A0 0A 01 92 07 00 00 8D 10 01 00 04
[52383 ms] RX: 01 00 80 02 01 80
[52386 ms] TX: 01 00 81 01 01
[52393 ms] RX: 01 00 A0 0A 01 90 02 00 02 9F 84 40 01 00 80 02 01 00
System Time=>DATE : 2013/11/5
[CI] System Updates UTC DT: DD 19 15 16 30
[52405 ms] TX: 01 00 A0 0C 01 90 02 00 04 9F 81 01 03 41 55 54
[52416 ms] RX: 01 00 80 02 01 80
[52419 ms] TX: 01 00 81 01 01
[52427 ms] RX: 01 00 A0 09 01 90 02 00 04 9F 81 10 00 80 02 01 80
[52433 ms] TX: 01 00 81 01 01
[52440 ms] RX: 01 00 A0 09 01 90 02 00 04 9F 81 10 00 80 02 01 80
[52447 ms] TX: 01 00 81 01 01
[52454 ms] RX: 01 00 A0 07 01 91 04 00 02 00 43 80 02 01 00
[52459 ms] TX: 01 00 A0 0C 01 90 02 00 04 9F 81 11 03 65 6E 67
[52470 ms] RX: 01 00 80 02 01 80
```

```
[52473 ms] TX: 01 00 81 01 01
[52481 ms] RX: 01 00 A0 09 01 90 02 00 04 9F 81 10 00 80 02 01 80
[52487 ms] TX: 01 00 81 01 01
[52494 ms] RX: 01 00 A0 07 01 91 04 00 8C 10 01 80 02 01 00
[CI+][CC] Content Control v1 Resource Connect
System Time=>DATE : 2013/11/5
[CI] System Updates UTC DT: DD 19 15 16 30
Credentials Bin Length: 4898 bytes
AES-128-CBC Decrypt:
    0x1F, 0x8A, 0xCF, 0x26, 0x4E, 0x67, 0x8F, 0x34, 0x2A, 0x0A, 0x15, 0x3B, 0xA2, 0xE1, 0xDD, 0x5E,
    0xCB, 0x1C, 0x5D, 0xEB, 0x51, 0xF9, 0x92, 0x62, 0x22, 0x1E, 0xAB, 0x30, 0x86, 0xA7, 0x7A, 0xA4,

AES-128-XCBC MAC:
    0x36, 0xC5, 0x46, 0x88, 0x01, 0xD7, 0xDF, 0xFF, 0x5C, 0xE7, 0x0D, 0x1C, 0x91, 0x00, 0x4C, 0x92,

Credentials Bin AES-128-XCBC MAC:
    0x00, 0xA0, 0xBA, 0xA3, 0x78, 0xB3, 0xE7, 0x9E, 0x98, 0x38, 0x39, 0xD9, 0x69, 0x88, 0x5A, 0x64,

[.//polarssl/library/polarssl_api.c:1237][Warning!][POLARSSL_API] CI+ Credentials Bin Auth NG!//这里可以看出 bin 没有 loading 进去
[.//msAPI_CI_cc.c:3431][Warning!][CI+][CC] Command CMD_LOAD_CREDENTIALS Fail!
[.//msAPI_CI_cc.c:1462][Warning!][CI+][CC] Fail to Load Credentials!
[.//msAPI_CI_common.c:624][Warning!][CI] Resource (ResourceID 0x008C1001 | SessNum 6) is refused because of Resource Init NG!
[52588 ms] TX: 01 00 A0 0E 01 90 02 00 02 9F 84 41 05 DD 19 15 16 30
[52599 ms] RX: 01 00 80 02 01 80
[52602 ms] TX: 01 00 81 01 01
[52609 ms] RX: 01 00 A0 07 01 91 04 00 03 00 41 80 02 01 00
[52614 ms] TX: 01 00 A0 0C 01 90 02 00 04 9F 81 11 03 65 6E 67
[52625 ms] TX: 01 00 A0 0C 01 90 02 00 04 9F 81 11 03 65 6E 67
[52635 ms] TX: 01 00 A0 0A 01 92 07 00 00 02 00 43 00 05
[52645 ms] TX: 01 00 A0 09 01 90 02 00 05 9F 80 20 00
[52654 ms] TX: 01 00 A0 0C 01 90 02 00 04 9F 81 11 03 65 6E 67
[52664 ms] RX: 01 00 80 02 01 80
[52667 ms] TX: 01 00 81 01 01
[52675 ms] RX: 01 00 A0 20 01 90 02 00 05 9F 80 21 17 01 00 00 00 00 11 48 44 2B 20 43 49 20 50 6C 75 73 20 4D 6F 64 75 6C 80 02 01 00
[52687 ms] TX: 01 00 A0 0A 01 92 07 00 00 8C 10 01 00 06
[52790 ms] TX: 01 00 A0 0E 01 90 02 00 02 9F 84 41 05 DD 19 15 16 30
[52801 ms] RX: 01 00 80 02 01 80
[52804 ms] TX: 01 00 81 01 01
[52812 ms] RX: 01 00 A0 09 01 90 02 00 06 9F 90 01 00 80 02 01 00
<<< [CI+][CC] CC Open Req
>>> [CI+][CC] CC Open Cnf
[52822 ms] TX: 01 00 A0 05 01 95 02 00 06
[52831 ms] TX: 01 00 A0 0A 01 92 07 00 00 03 00 41 00 07
[52841 ms] RX: 01 00 80 02 01 80
[52844 ms] TX: 01 00 81 01 01
[52851 ms] RX: 01 00 A0 06 01 96 03 00 00 06 80 02 01 00
```

```
[CI+][CC] Content Control Resource Close
[52860 ms] TX: 01 00 A0 09 01 90 02 00 07 9F 80 30 00
[52869 ms] TX: 01 00 A0 0A 01 90 02 00 06 9F 90 02 01 01
[52879 ms] RX: 01 00 80 02 01 80
[52882 ms] TX: 01 00 81 01 01
[52891 ms] RX: 01 00 A0 0F 01 90 02 00 07 9F 80 31 06 18 30 18 43 18 60 80 02 01 00
[CI+][HSS] MDrv_CI_HSS_GetSunningStatus: 1
```

我自己抓取的打印信息：

```
    [CI+] URI Copy Never....
[CI] ## E_CI_HWRST

[CI+][HSS] MDrv_CI_HSS_SetSunningStatus: 1

[CI] Delay 500 ms for H/W Reset of CI Init.

[CI] ## E_CI_INIT

[CI] PCMCIA CIS:

1D 04 00 DB 08 FF 1C 03

00 08 FF 15 30 05 00 53

6D 61 72 44 54 56 00 44

56 42 20 43 41 20 4D 6F

64 75 6C 65 00 24 63 6F

6D 70 61 74 69 62 6C 65

5B 63 69 70 6C 75 73 3D

31 5D 24 00 FF 20 04 FF

FF 01 00 1A 15 01 0F FE

01 01 C0 0E 41 02 44 56

42 5F 43 49 5F 56 31 2E

30 30 1B 11 C9 41 19 37

55 4E 5E 1D 56 AA 60 90

01 03 50 FF FF 1B 26 CF
```

```
04 19 37 55 4D 5D 1D 56
22 20 C0 09 44 56 42 5F
48 4F 53 54 00 C1 0E 44
56 42 5F 43 49 5F 4D 4F
44 55 4C 45 00 14 00 FF
C9 CB D3 34 59 65 5D B8
DB 73 0F B2 C1 65 E1 50
07 C9 FF A3 99 36 77 E6
BB F4 BB EF 8F 7D DB 50
02 C1 34 BB 35 AC 47 A6
C1 5D 94 30 A8 69 79 F7
56 FD B1 97 12 03 9C 4E
A5 30 3E 3F F9 BD A2 01
77 40 CC 53 EC A4 24 21
CE B8 39 D4 B7 D6 B6 32
9F 7B D0 B2 05 AB 4F B4
09 97 01 C6 7E 29 91 A0
C0 FC 84 37 4A 9E 64 00

[CI] ManufacturerName SmarDTV
[CI] ProductName DVB CA Module
[CI] ProductInfo1 $compatible[ciplus=1]$
[CI] ProductInfo2 Interface OK!
[CI] BufferSize 2047 bytes
[CI+] Up DAIE!!!
```

```
[CI] PCMCIA Config OK!

[CI] CI+ CAM: SmarDTV | DVB CA Module

[55134 ms] TX: 01 00 82 01 01

[55138 ms] RX: 01 00 83 01 01 80 02 01 00

[55455 ms] RX: 01 00 80 02 01 80

[55558 ms] TX: 01 00 81 01 01

[55660 ms] RX: 01 00 A0 07 01 91 04 00 01 00 41 80 02 01 00

[55765 ms] TX: 01 00 A0 0A 01 92 07 00 00 01 00 41 00 01

[55970 ms] TX: 01 00 A0 09 01 90 02 00 01 9F 80 10 00

[56374 ms] RX: 01 00 80 02 01 80

[56477 ms] TX: 01 00 81 01 01

[56579 ms] RX: 01 00 A0 09 01 90 02 00 01 9F 80 11 00 80 02 01 00

[56684 ms] TX: 01 00 A0 09 01 90 02 00 01 9F 80 12 00

[57088 ms] RX: 01 00 80 02 01 80

[57191 ms] TX: 01 00 81 01 01

[57293 ms] RX: 01 00 A0 09 01 90 02 00 01 9F 80 10 00 80 02 01 00

[57398 ms] TX: 01 00 A0 3D 01 90 02 00 01 9F 80 11 34 00 01 00 41 00 01 00 42 00 02 00 41 00 02 00 43 00 03 00
41 00 20 00 41 00 24 00 41 00 40 00 41 00 8C 10 01 00 8D 10 01 00 8E 10 01 00 41 00 41 00 10 00 41

[57816 ms] RX: 01 00 80 02 01 80

[57919 ms] TX: 01 00 81 01 01

[58021 ms] RX: 01 00 A0 07 01 91 04 00 8D 10 01 80 02 01 80

[58126 ms] TX: 01 00 81 01 01

[58228 ms] RX: 01 00 A0 07 01 91 04 00 24 00 41 80 02 01 80

[58333 ms] TX: 01 00 81 01 01

[58435 ms] RX: 01 00 A0 07 01 91 04 00 02 00 41 80 02 01 80
```

```
[58540 ms] TX: 01 00 81 01 01

[58642 ms] RX: 01 00 A0 07 01 91 04 00 8C 10 01 80 02 01 80

[CI+][CC] Content Control v1 Resource Connect

System Time=>DATE : 2014/10/24 //系统时间
[CI] System Updates UTC DT: DE 7A 20 33 14

From Date: 2011/3/29//系统时间一定要在此范围内
To Date    : 2099/12/31
Now Date : 2014/10/24 32:51:20
[CI+][X.509] Verify Certificate Pass!

From Date: 2013/6/19
To Date    : 2063/6/19
Now Date : 2014/10/24 32:51:20
[CI+][X.509] Verify Certificate Pass!

[58802 ms] TX: 01 00 81 01 01

[58904 ms] RX: 01 00 A0 07 01 91 04 00 20 00 41 80 02 01 00

[59009 ms] TX: 01 00 A0 0A 01 92 07 00 00 8D 10 01 00 02

[59114 ms] RX: 01 00 80 02 01 80

[59216 ms] TX: 01 00 81 01 01

[59318 ms] RX: 01 00 A0 07 01 91 04 00 40 00 41 80 02 01 80

[59423 ms] TX: 01 00 81 01 01

[59525 ms] RX: 01 00 A0 07 01 91 04 00 03 00 41 80 02 01 00

[59630 ms] TX: 01 00 A0 0C 01 90 02 00 02 9F 81 01 03 41 55 54

[59835 ms] TX: 01 00 A0 0C 01 90 02 00 02 9F 81 11 03 65 6E 67

[60040 ms] TX: 01 00 A0 0A 01 92 07 00 00 24 00 41 00 03

[60245 ms] TX: 01 00 A0 0A 01 92 07 00 00 02 00 41 00 04

[60450 ms] TX: 01 00 A0 09 01 90 02 00 04 9F 80 20 00

[60654 ms] TX: 01 00 A0 0A 01 92 07 00 00 8C 10 01 00 05

[60759 ms] RX: 01 00 80 02 01 80
```

```
[60862 ms] TX: 01 00 81 01 01

[60964 ms] RX: 01 00 A0 1F 01 90 02 00 04 9F 80 21 16 01 00 00 00 00 10 43 49 2B 20 53 6D 61 72 43 41 4D 33 20
41 50 50 80 02 01 80

[61119 ms] TX: 01 00 81 01 01

[61222 ms] RX: 01 00 A0 09 01 90 02 00 05 9F 90 01 00 80 02 01 00

<<< [CI+][CC] CC Open Req

>>> [CI+][CC] CC Open Cnf

[61332 ms] TX: 01 00 A0 0E 01 90 02 00 03 9F 84 41 05 DE 7A 20 33 14

[61538 ms] TX: 01 00 A0 0A 01 92 07 00 00 20 00 41 00 06

[61743 ms] TX: 01 00 A0 0A 01 92 07 00 00 40 00 41 00 07

[61948 ms] TX: 01 00 A0 0A 01 92 07 00 00 03 00 41 00 08

[62053 ms] RX: 01 00 80 02 01 80

[62156 ms] TX: 01 00 81 01 01

[62258 ms] RX: 01 00 A0 0B 01 90 02 00 07 9F 88 01 02 01 01 80 02 01 80

[62364 ms] TX: 01 00 81 01 01

[62466 ms] RX: 01 00 A0 59 01 90 02 00 07 9F 88 0C 50 00 9F 88 03 13 43 49 2B 20 53 6D 61 72 43 41 4D 33 20 4D
4F 44 55 4C 45 9F 88 03 18 47 65 6E 65 72 69 63 20 53 74 61 74 75 73 20 52 65 70 6F 72 74 69 6E 67 9F 88 03 18
50 72 65 73 73 20 4F 6B 20 6F 72 20 45 78 69 74 20 74 6F 20 71 75 69 74 80 02 01 00

[62592 ms] TX: 01 00 A0 09 01 90 02 00 08 9F 80 30 00

[62797 ms] TX: 01 00 A0 0A 01 90 02 00 05 9F 90 02 01 01

[62902 ms] RX: 01 00 80 02 01 80

[63005 ms] TX: 01 00 81 01 01

[63107 ms] RX: 01 00 A0 0F 01 90 02 00 08 9F 80 31 06 10 00 10 01 10 02 80 02 01 80

[CI+][HSS] MDrv_CI_HSS_GetSunningStatus: 1

[63214 ms] TX: 01 00 81 01 01

[63316 ms] RX: 01 00 A0 33 01 90 02 00 05 9F 90 03 2A 01 01 13 00 20 05 66 A3 A1 D0 F0 4D 7A 11 BE 1B 82 F3
```

```
64 C7 2D CB 91 BD 65 C5 C1 5A BB BF C8 3C 9E 74 86 60 BB 04 0D 11 0F 07 80 02 01 00

<<< [CI+][CC] CC Data Req

    <<< Auth Nonce

    [CI+][CC] Auth Nonce:

    05 66 A3 A1 D0 F0 4D 7A 11 BE 1B 82 F3 64 C7 2D

    CB 91 BD 65 C5 C1 5A BB BF C8 3C 9E 74 86 60 BB


    [CI+][CC] DHX:

    6E 4D 65 2E 82 66 9E B6 59 35 D3 33 C4 46 D3 9A

    E7 2F 08 4A EE 91 15 C2 97 DA BB 09 F3 C5 34 DA

    18 47 0F 40 2F 70 E3 74 4A A1 E0 60 B4 DD 99 3A

    86 20 B6 2F D7 69 EE E0 A5 B2 65 89 A6 55 61 5E

    51 37 E5 F5 7E 36 B2 AA D1 1E F8 EC 9D 99 31 00

    68 8C AF FC E7 C8 8F D7 72 CA A9 07 5C D0 6A 74

    8B C4 A3 10 DD 2E 12 CF 6A 1D C7 95 5C 24 C4 E6

    8A 7D 82 A5 26 2F 02 4E F2 B3 B2 30 EB 67 B1 1D

    2B 1A 57 63 50 BE 82 62 B7 85 11 1C 79 D1 E2 C9

    F7 16 EE F4 25 91 7C CF 1F 6A 76 A1 21 BD A0 D7

    E7 F9 E7 28 DB 90 FD 56 F2 12 E8 A7 F7 C5 A5 35

    03 00 22 64 E9 A5 B3 5F 07 35 BD 82 B1 A3 FE BB

    38 4B AD 64 A6 51 46 79 33 D5 EF A5 1E D7 E0 97

    EB AB D3 19 F0 2C 83 A6 A7 76 A4 55 0A 57 24 45

    CF 1A 5F 24 5E 48 3A 6B 8C 2B 1F C8 AE CF 49 D2

    5E A9 1D 21 1B A4 DE A3 3E E5 4B B8 4D FE 34 15
```

```
DHPH:

    2E B0 C2 E8 BC E4 F8 D9 CC 38 C2 20 BD 14 B0 2B

    68 8A 52 D0 73 2D 8F 53 C8 F3 BB 91 4A 26 49 80

    0C D8 CB 47 C3 CB 1B B3 AA 1D B4 8E 4F CA 7E 28

    62 68 55 FE C1 76 56 AD B0 82 40 29 7E AB 82 E1

    B8 0F 38 5F 3A 64 4C 79 32 3B E4 B1 27 D6 D1 BC

    F5 D9 56 95 72 23 0B B8 A0 F3 D8 E3 F2 A6 9F 49

    93 E4 18 D9 D2 9D 31 AA E0 51 13 B6 49 74 B3 C9

    20 07 C7 D2 96 71 BA 93 31 50 53 E4 DA EC 9A 69

    D3 53 FD 67 6B 34 6E 9C 1E 91 D1 8D 75 80 20 59

    B5 13 F6 6E ED F4 39 3C 31 1F 42 B9 86 DA CE D2

    4B 64 63 99 24 65 B2 8D A1 0C 3D 8B 58 EF D3 0A

    76 CD 1A 2E C7 2B 31 96 92 F5 13 B6 51 33 B9 94

    37 39 B6 95 AE 59 05 49 93 B7 4D 12 77 EF 47 F1

    87 B1 AD 98 50 FA CB 78 38 9A 83 44 55 83 D5 F5

    80 F1 FA BF D9 E7 70 BE 4B 3F 1C C5 A2 B1 35 B5

    05 3C 2C 16 61 57 F6 F6 7A 0E F5 7D 15 8B 29 9E


    [CI+][CC] version || msg_label || auth_nonce || DHPH:

    00 00 08 01 01 00 08 02 02 01 00 05 66 A3 A1 D0

    F0 4D 7A 11 BE 1B 82 F3 64 C7 2D CB 91 BD 65 C5

    C1 5A BB BF C8 3C 9E 74 86 60 BB 04 08 00 2E B0

    C2 E8 BC E4 F8 D9 CC 38 C2 20 BD 14 B0 2B 68 8A

    52 D0 73 2D 8F 53 C8 F3 BB 91 4A 26 49 80 0C D8
    CB 47 C3 CB 1B B3 AA 1D B4 8E 4F CA 7E 28 62 68
    55 FE C1 76 56 AD B0 82 40 29 7E AB 82 E1 B8 0F
    38 5F 3A 64 4C 79 32 3B E4 B1 27 D6 D1 BC F5 D9
    56 95 72 23 0B B8 A0 F3 D8 E3 F2 A6 9F 49 93 E4
    18 D9 D2 9D 31 AA E0 51 13 B6 49 74 B3 C9 20 07
    C7 D2 96 71 BA 93 31 50 53 E4 DA EC 9A 69 D3 53
    FD 67 6B 34 6E 9C 1E 91 D1 8D 75 80 20 59 B5 13
    F6 6E ED F4 39 3C 31 1F 42 B9 86 DA CE D2 4B 64
    63 99 24 65 B2 8D A1 0C 3D 8B 58 EF D3 0A 76 CD
    1A 2E C7 2B 31 96 92 F5 13 B6 51 33 B9 94 37 39
    B6 95 AE 59 05 49 93 B7 4D 12 77 EF 47 F1 87 B1
    AD 98 50 FA CB 78 38 9A 83 44 55 83 D5 F5 80 F1
    FA BF D9 E7 70 BE 4B 3F 1C C5 A2 B1 35 B5 05 3C
    2C 16 61 57 F6 F6 7A 0E F5 7D 15 8B 29 9E
Signature_A:
    51 1D AF 56 F7 00 44 DE B2 5B 61 73 F9 82 FB 75
    7C D4 33 7D 8B FA 83 8B 11 C5 55 0A 2E C5 C1 D7
    68 64 A3 68 45 D3 4A 03 B4 06 4F E7 4C 51 A8 8B
    DD 85 DB 9D 47 6A E4 5A 99 E1 F9 DC B7 4D 81 B7
    F1 55 A8 9C EE A6 A1 00 97 BE 47 A7 3F A9 2D 20
    FD 13 1A 42 A5 AA FE 13 B0 FE 1B 53 5F 73 57 66
    1E 2B 0E 0F 04 3B 11 93 26 D2 79 47 B1 FF 03 81
    23 0E 44 56 23 E1 83 9A 0E E4 8A D7 10 93 F4 01
    B8 EA AD 40 3E 24 C4 CC E7 32 1D 81 18 CD 35 5D
    8E 42 43 69 F6 1E 4A 7A 8C 64 F5 1E 6A 8D A7 E1
```

```
62 03 B4 57 66 E6 EA EA 78 CF BC AF 40 0C F2 AA
3B 82 B5 AC 80 FB 34 0A 3C 5B DC 6A 63 54 EC 34
65 D7 97 84 0D F5 24 54 39 42 33 80 70 BC B6 C2
B2 8D 8E E3 55 89 37 74 BB 1C 92 63 31 8D 26 F9
3D 4E 81 E9 B0 F9 32 87 4F 80 D6 25 50 73 D2 B1
F5 38 72 63 29 2D BC 10 89 07 5F D0 BA 52 AF 07


>>> DHPH
>>> Signature_A
[CI+][CC] HOST DEVCERT: 1068 bytes
30 82 04 28 30 82 03 10 A0 03 02 01 02 02 0E 4E
05 00 00 00 2C C1 76 D3 34 75 A2 02 B7 30 0D 06
09 2A 86 48 86 F7 0D 01 01 0A 30 00 30 81 A6 31
0B 30 09 06 03 55 04 06 13 02 43 4E 31 12 30 10
06 03 55 04 08 13 09 48 4F 4E 47 20 4B 4F 4E 47
31 12 30 10 06 03 55 04 07 13 09 48 4F 4E 47 20
4B 4F 4E 47 31 24 30 22 06 03 55 04 0A 13 1B 4C
4F 53 41 4E 47 20 45 4E 4D 41 52 20 28 48 2E 4B
2E 29 20 4C 69 6D 69 74 65 64 31 13 30 11 06 03
55 04 0B 13 0A 50 72 6F 64 75 63 74 69 6F 6E 31
34 30 32 06 03 55 04 03 13 2B 43 49 20 50 6C 75
73 20 52 4F 54 20 66 6F 72 20 4C 4F 53 41 4E 47
20 45 4E 4D 41 52 20 28 48 2E 4B 2E 29 20 4C 69
6D 69 74 65 64 30 1E 17 0D 31 33 30 36 31 39 31
```

```
38 30 38 35 37 5A 17 0D 36 33 30 36 31 39 31 38

30 38 35 37 5A 30 81 9E 31 0B 30 09 06 03 55 04

06 13 02 43 4E 31 12 30 10 06 03 55 04 08 13 09

48 4F 4E 47 20 4B 4F 4E 47 31 12 30 10 06 03 55

04 07 13 09 48 4F 4E 47 20 4B 4F 4E 47 31 24 30

22 06 03 55 04 0A 13 1B 4C 4F 53 41 4E 47 20 45

4E 4D 41 52 20 28 48 2E 4B 2E 29 20 4C 69 6D 69

74 65 64 31 13 30 11 06 03 55 04 0B 13 0A 50 72

6F 64 75 63 74 69 6F 6E 31 11 30 0F 06 03 55 04

0B 13 08 4C 4D 32 36 6D 33 30 38 31 19 30 17 06

03 55 04 03 13 10 30 30 32 32 35 46 44 33 44 31

31 33 36 43 37 37 30 82 01 22 30 0D 06 09 2A 86

48 86 F7 0D 01 01 01 05 00 03 82 01 0F 00 30 82

01 0A 02 82 01 01 00 A1 EF 90 CC 01 FE 36 43 F0

2F F4 6C 10 84 02 23 F8 DE 91 70 93 16 AE 94 E1

9A 93 5B AD 4B 60 30 93 81 E1 85 B8 C0 74 11 C3

BB A2 A2 E2 F9 53 2C E5 67 DB 08 A4 06 99 4E 10

1C B6 ED FA FC 47 AD 99 1C 49 13 EF 3A CB 24 02

83 DE D9 56 76 EB 1A 9A 00 08 9C 22 67 22 0A 8E

22 5B 99 E0 42 D0 86 FC 21 76 18 BC F3 59 53 F8

BC C1 73 01 14 F4 31 CC 96 BC 49 3C E5 D3 51 9B

B7 A1 61 FC 12 9B 72 A8 A9 C4 C9 4A 60 B6 1B C2

AA E6 3B 37 61 E8 4B C5 D0 AE 8C 99 13 07 7A 41

3B 34 A8 2C B3 A1 2D 4F 1A 88 B9 27 E9 39 AB D7

8C 34 15 0A B2 A2 5B 3F 23 5D FC 85 B2 02 CE 8F
```

```
14 71 D4 4E 8B 4B EF 07 DE 14 14 60 1E E7 B4 91

5A BE A8 7C 29 56 91 16 A2 A2 BB 3D C0 18 95 15

35 44 28 74 3A 94 97 E0 F8 4F 50 95 4C 48 A6 48

65 FD AF DA BF 72 F1 D2 C6 B8 F0 C2 C2 21 4E F8

F5 9E F7 5C 6C 47 A5 02 03 01 00 01 A3 5A 30 58

30 1F 06 03 55 1D 23 04 18 30 16 80 14 BB C4 3D

61 B1 E5 60 EE E2 7F 1F C6 DB 44 22 0A 25 18 C7

0C 30 0C 06 03 55 1D 13 01 01 FF 04 02 30 00 30

0E 06 03 55 1D 0F 01 01 FF 04 04 03 02 07 80 30

17 06 08 2B 06 01 05 05 07 01 19 01 01 FF 04 08

30 06 02 01 01 02 01 00 30 0D 06 09 2A 86 48 86

F7 0D 01 01 0A 30 00 03 82 01 01 00 37 C4 CF 62

E6 DB BD 0C 93 97 91 85 6D 58 80 40 D9 26 74 72

03 0B 87 6C A2 75 2F F4 B3 59 58 BC 65 59 FE 8C

3E 18 0A 80 C6 09 F5 B7 C1 59 30 18 59 CA D3 75

79 06 1B 6F 25 E1 1A 5C 9B 59 99 F4 79 B7 9D 30

8D D3 9D 5A BA 1C A9 5D CF 1F 1C C3 EE 39 7E 6D

83 70 5F 03 F5 22 34 6E 11 BD EC 8C E5 F2 A4 0D

D4 BC 16 31 AD 64 69 2B EE CD 13 50 62 88 41 68

42 09 B1 DC A0 62 F6 21 BA 9C E5 E0 E9 C1 6C AA

F3 50 9C 0B E1 CC FB 5C FB B9 C0 44 A1 2D 58 0D

20 5C 57 2B 63 60 36 76 9A 70 14 B6 53 0F 9C 1D

34 16 14 37 4C 2D 8D A3 1F 8F 47 BF CB D7 7F 41

FC 5B 8B 82 C8 E3 C6 38 7A 99 86 6D 83 3A D3 69
```

```
50 D0 2E F0 EE 54 3A 41 62 F4 66 B7 50 61 69 63

A2 54 94 0E F3 26 DD 2B 4D AA 1B F5 16 32 0E BE

3B 54 05 46 27 C7 22 63 B0 7E B6 44 D2 64 CB 3D

AA 2B FA AC 8C A8 B4 43 E3 44 AA 71

>>> Host_dev_cert

[CI+][CC] HOST BRANDCERT: 1067 bytes

30 82 04 27 30 82 03 0F A0 03 02 01 02 02 0E 22

B0 00 00 00 2C 3B EF B3 50 7D 30 BF F0 30 0D 06

09 2A 86 48 86 F7 0D 01 01 0A 30 00 30 81 91 31

0B 30 09 06 03 55 04 06 13 02 55 4B 31 0F 30 0D

06 03 55 04 08 13 06 4C 6F 6E 64 6F 6E 31 0F 30

0D 06 03 55 04 07 13 06 4C 6F 6E 64 6F 6E 31 14

30 12 06 03 55 04 0A 13 0B 43 49 20 50 6C 75 73

20 4C 4C 50 31 0F 30 0D 06 03 55 04 0B 13 06 45

75 72 6F 70 65 31 13 30 11 06 03 55 04 0B 13 0A

50 72 6F 64 75 63 74 69 6F 6E 31 24 30 22 06 03

55 04 03 13 1B 43 49 20 50 6C 75 73 20 52 6F 6F

74 20 43 41 20 63 65 72 74 69 66 69 63 61 74 65

30 1E 17 0D 31 31 30 33 32 39 30 38 31 30 34 39

5A 17 0D 39 39 31 32 33 31 32 33 35 39 35 39 5A

30 81 A6 31 0B 30 09 06 03 55 04 06 13 02 43 4E

31 12 30 10 06 03 55 04 08 13 09 48 4F 4E 47 20

4B 4F 4E 47 31 12 30 10 06 03 55 04 07 13 09 48

4F 4E 47 20 4B 4F 4E 47 31 24 30 22 06 03 55 04

0A 13 1B 4C 4F 53 41 4E 47 20 45 4E 4D 41 52 20
```

```
28 48 2E 4B 2E 29 20 4C 69 6D 69 74 65 64 31 13

30 11 06 03 55 04 0B 13 0A 50 72 6F 64 75 63 74

69 6F 6E 31 34 30 32 06 03 55 04 03 13 2B 43 49

20 50 6C 75 73 20 52 4F 54 20 66 6F 72 20 4C 4F

53 41 4E 47 20 45 4E 4D 41 52 20 28 48 2E 4B 2E

29 20 4C 69 6D 69 74 65 64 30 82 01 22 30 0D 06

09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82 01 0F

00 30 82 01 0A 02 82 01 01 00 EA 61 5D 2B 07 FF

32 87 20 7A C7 EE 94 60 4B E2 CD B3 B0 0C E9 4C

72 84 6A BA AD 0A F8 2E CD A0 49 42 09 15 40 68

90 E7 F6 B5 17 6B 24 2B 0E 48 DF 7A D5 4C F1 6F

20 13 2C AA F0 16 8A 70 76 AF A4 6A E3 71 0D E7

15 11 F7 6A 5F AC E5 A3 0A E7 16 54 B7 28 F4 68

9E 6D DC 50 F8 96 A8 F9 6B 56 C4 9C 15 75 B6 B5

E5 BA B5 52 25 D9 3F D2 EF 67 CB 18 9B 52 8D A0

E1 FE AD 9A 0A 5C 49 0E 52 E7 17 FF 4C 67 89 CF

60 F2 CF 47 E7 5F 43 00 E8 E7 7F 25 D3 10 A5 B0

46 8E 96 13 BF 15 43 37 14 85 73 FD 2A 7E 92 B0

0C 31 7E 60 C8 F1 88 97 42 26 5D F2 8D 6A 26 22

7F F9 84 7D CB B0 2E 4C 89 AC 6A 69 FA C6 B1 21

02 40 A6 2C 1A D0 A0 27 E5 60 90 F4 26 31 94 26

A5 32 5D 50 7C EB 72 D4 1B 19 93 51 35 B1 64 A5

C7 25 2F C6 CF 7E C7 26 B5 BC 99 F7 A5 AA 2C EA

1F 74 77 37 6F AA 88 C3 96 1B 02 03 01 00 01 A3
```

```
66 30 64 30 1F 06 03 55 1D 23 04 18 30 16 80 14

27 C8 75 CE BD 7D 44 74 B1 7B 6B 9D 49 A1 C2 79

80 D8 2E 3F 30 12 06 03 55 1D 13 01 01 FF 04 08

30 06 01 01 FF 02 01 00 30 0E 06 03 55 1D 0F 01

01 FF 04 04 03 02 02 04 30 1D 06 03 55 1D 0E 04

16 04 14 BB C4 3D 61 B1 E5 60 EE E2 7F 1F C6 DB

44 22 0A 25 18 C7 0C 30 0D 06 09 2A 86 48 86 F7

0D 01 01 0A 30 00 03 82 01 01 00 0E 95 CC 90 78

E2 07 C0 D3 94 0E E8 C9 53 1D 95 9E CF FA D0 E4

F3 05 8F EA C0 63 07 D8 7D 99 B7 2B 78 AC F5 13

5B 80 8A 5F D9 77 FF 0B 50 BB C1 74 BA B8 76 3D

72 5F 46 01 C7 D0 9D 6C AD A6 69 B7 35 05 18 66

16 CD FB 1F E4 01 97 B7 FB D8 B4 7E A1 11 B9 1E

E4 EB 2F 2C 32 B8 9B 4D FC B8 D4 70 0B E5 36 3B

6F 02 9C 1E 53 18 51 33 8E 46 94 39 55 D7 56 E5

03 8C 0F 42 C7 7F 90 F0 AD 26 6D A5 20 6B FF 43

87 01 BE 52 F4 69 8B DA A7 E0 FF AC C2 09 1A 65

BF 1C 68 B4 4B F1 43 10 37 63 5B C0 07 0E DB 2D

C8 41 23 F4 A4 4A 8A B1 0E E7 31 2F 83 ED 7F A3

96 03 4E 09 36 BA 2F 33 00 3E E6 CC AD A0 AF C8

8B C0 F2 B3 0B EC 40 A3 3C 96 DD 28 F8 5E A5 09

FD 50 44 AE 72 86 B0 1B A0 24 29 CF 28 E2 65 03

34 1D F7 5B C5 18 00 7B B7 CE B9 69 E9 AB 33 5B

2F 1A 7D B6 A9 EC 71 1D 2B D9 39

>>> Host_brand_cert
>>> [CI+][CC] CC Data Cnf: DHPH + Signature_A + Host_dev_cert + Host_brand_cert

LIST
Subtitle Generic Status Reporting
Bottom Press Ok or Exit to quit
[65340 ms] TX: 01 00 A0 0B 01 90 02 00 07 9F 88 02 02 01 01

[65549 ms] TX: 01 80 A0 82 0A 70 01 90 02 00 05 9F 90 04 82 0A 65 01 04 0D 01 00 2E B0 C2 E8 BC E4 F8 D9 CC
38 C2 20 BD 14 B0 2B 68 8A 52 D0 73 2D 8F 53 C8 F3 BB 91 4A 26 49 80 0C D8 CB 47 C3 C
[110119 ms] RX: 01 00 80 02 01 80

[110222 ms] TX: 01 00 81 01 01

[110329 ms] RX: 01 80 A0 82 0A 57 01 90 02 00 05 9F 90 03 82 0A 4C 01 04 0E 01 00 97 40 6D 8D A9 B2 95 A9 FD
1E 21 D3 EE 37 FB 52 F9 68 9B B4 45 37 D1 E4 B9 D2 FF 9B C0 64 19 88 02 37 A2 BC 90 06 89 C0 91 0D 57 C7
28 2D FC DC 10 EE 95 50 62 87 97 53 CA 85 B2 8C B2 4B 44 D0 A2 80 97 C7 FD 3E 6D AC 9F 13 9A 99 44 E4 2A
2D E1 7A FC 8B C3 F4 DB E8 2D 5F EC 62 08 37 B5 BD DC F6 0A 8F 8C CD 25 6C 58 9A (Omit~)

[110365 ms] RX: 01 00 51 FA B0 6B 0E 79 2A 35 A2 F6 D3 D8 60 57 33 D7 0B B3 67 BD 1A 83 F9 2B 64 17 9A 27
C9 FF D8 D7 1A F2 23 67 91 0A 8F 84 3B A6 8B 72 09 B7 81 DF 05 E7 B7 67 B7 49 39 BE E7 1C 1C 8B 28 68 13
2E 2D E9 BA E1 CB EF 3A 0C BD 53 F1 14 13 A2 B0 37 FF 34 BD 6F 75 BB 2D A5 68 E2 F7 07 2C D9 09 ED 60
FE AF 82 50 C5 DA 7E B3 7C 46 5F D3 9F 84 62 7A 19 99 BC 84 D1 D8 E7 2C D3 B9 09 46 9C (Omit~)

<<< [CI+][CC] CC Data Req

    <<< DHPM

    <<< Signature B

    [CI+][CC] Signature_B:

    4B E9 31 B7 11 60 7F E2 61 56 7A B3 35 8F B3 1C

    1E C6 CC 45 9C D5 1B CE E4 8E B0 C9 8E 95 31 8B

    F4 E2 ED BB 9C 24 6D 28 A7 77 2D D4 74 0A D5 FF

    E2 D4 E1 25 FD 8E F2 B4 4C 40 68 1B 3F 0E D9 65

    93 1C BA 30 F6 CD AE 5A B7 3E 8D 2E 66 02 B3 FB

    8D A7 A5 18 A3 E1 6F 97 6B 80 F3 AD 51 CF E8 1A

    C9 80 80 8B B7 01 01 C9 A1 A6 88 20 62 8C 01 7E

    73 1E 74 83 2D 88 2C DB CF BA 7F C3 BB 6E ED BF

    CF 97 D2 5D E4 93 0D 66 AD ED 45 0E 39 ED 02 46
    2B AB A5 11 C5 92 7A 32 4A 66 28 05 35 6E B5 B5

    37 F8 38 61 09 5F 10 62 E6 1A E3 13 9C A0 94 82

    3A 8B 85 01 8E 9A EB C6 59 58 30 42 83 A0 5A 2A

    DE 12 3D 0C 66 95 76 BD EA 89 FE B4 48 B7 A4 2A

    54 FD 62 2D 65 3F 33 E5 F6 E9 78 BC DE BB 28 66

    9B DA C6 08 DA CE 80 A7 70 CF 87 94 01 18 78 4E

    D7 3C 70 72 3D 09 01 F8 75 3D B0 FE 62 11 46 A0



    <<< CICAM Device Certificate

    <<< CICAM Brand Certificate

From Date: 2009/4/23
To Date    : 2099/12/31
Now Date : 2014/10/24 32:51:20
[CI+][X.509] Verify Certificate Pass!

From Date: 2009/9/16
To Date    : 2059/9/16
Now Date : 2014/10/24 32:51:20
[CI+][X.509] Verify Certificate Pass!

>>> [CI+][CC] CC Data Cnf: Status: 0

    [CI+][CC] CICAM ID:

    FC 84 16 3F 79 E1 5F 0A

    [CI+][CC] Host ID:

    00 22 5F D3 D1 13 6C 77

    [CI+][CC] DHSK:

    46 57 35 23 44 5D 20 9D 49 94 AD 28 EF F9 8D 86

    B5 D7 E3 3C 67 4B AD 7D E0 0F 3C C0 18 AB 9A 0F

    31 38 73 73 45 27 31 FA 48 86 E6 23 2C 32 51 B2
    04 12 50 F1 89 B0 90 C0 B0 2B 73 35 46 ED 9D 71

    A8 6B BE 1E 48 FD 7C 89 9F A8 51 EA D1 F5 1E 8B

    B0 01 E7 BA AA 8C 4C 11 D9 67 D3 85 07 02 B4 F1

    9B 1A C4 E0 F7 FC 4A B5 CB DF 3C 7D 52 E0 05 B1

    39 EE 93 72 F3 B4 C9 A5 65 81 07 E0 9E E8 54 63

    BE 2F 6F 0B FF 99 25 97 6E 7C AF 8D E6 C0 A9 CE

    DC 04 CD D9 74 2F 57 B5 EF 5A 0D F3 DF 79 D0 54

    F7 F6 84 FB D5 E3 9F 1E 4D F6 BB F5 88 5C A5 11

    3C 73 8E 9B 12 22 8C 05 AB F7 37 CA 30 49 54 3F

    2E 82 CC AB 52 D2 BE 2B 49 CE BF 2F 0E 12 E1 84

    28 64 7A B5 D0 99 D8 CF 5B F8 E4 CC CA 3D 42 2F

    7E 5F 38 86 FC D9 08 94 D2 C7 4D 19 58 3C 1B EC

    0F 42 04 1A 87 36 05 40 77 EA 75 E0 D1 FB DB C2



    [CI+][CC] AKH: 1

    02 13 6C AF 24 E9 A7 2A 96 A8 F3 C8 62 0A 05 9A

    6E 90 CC B2 BD ED 55 56 78 1C EA 34 4F C5 FF 8B



[111495 ms] TX: 01 00 A0 0F 01 90 02 00 05 9F 90 04 06 01 01 1E 00 01 00

[145801 ms] RX: 01 00 80 02 01 80

[145904 ms] TX: 01 00 81 01 01

[146006 ms] RX: 01 00 A0 0D 01 90 02 00 05 9F 90 03 04 01 00 01 16 80 02 01 00

<<< [CI+][CC] CC Data Req

    [CI+][CC] Get AKH:-01

    02 13 6C AF 24 E9 A7 2A 96 A8 F3 C8 62 0A 05 9A
    6E 90 CC B2 BD ED 55 56 78 1C EA 34 4F C5 FF 8B


    >>> AKH

>>> [CI+][CC] CC Data Cnf: AKH

[146130 ms] TX: 01 00 A0 2E 01 90 02 00 05 9F 90 04 25 01 01 16 00 20 02 13 6C AF 24 E9 A7 2A 96 A8 F3 C8 62
0A 05 9A 6E 90 CC B2 BD ED 55 56 78 1C EA 34 4F C5 FF 8B

[146544 ms] RX: 01 00 80 02 01 80

[146647 ms] TX: 01 00 81 01 01

[146749 ms] RX: 01 00 A0 24 01 90 02 00 05 9F 90 03 1B 01 02 06 00 08 FC 84 16 3F 79 E1 5F 0A 15 00 08 DA D8
BC 9D E2 7D 7C D1 02 05 14 80 02 01 00

<<< [CI+][CC] CC Data Req

    <<< CICAM ID

    [CI+][CC]    Cert CICAM ID:

    FC 84 16 3F 79 E1 5F 0A

    [CI+][CC]    Received CICAM ID:

    FC 84 16 3F 79 E1 5F 0A

    <<< CICAM Ns_module

    [CI+][CC] Ns_Module:

    DA D8 BC 9D E2 7D 7C D1

    [CI+][CC] HOST ID:

    00 22 5F D3 D1 13 6C 77

    [CI+][CC] Ns_Host:

    C8 B6 36 3C 47 70 F0 20

>>> [CI+][CC] CC Data Cnf: Host_ID + Ns_Host

    [CI+][CC] DHSK LSB 128 bits:
```

```
0F 42 04 1A 87 36 05 40 77 EA 75 E0 D1 FB DB C2


[CI+][CC] Current AKH:

02 13 6C AF 24 E9 A7 2A 96 A8 F3 C8 62 0A 05 9A

6E 90 CC B2 BD ED 55 56 78 1C EA 34 4F C5 FF 8B


[CI+][CC] Ns_Host:

C8 B6 36 3C 47 70 F0 20

[CI+][CC] Ns_Module:

DA D8 BC 9D E2 7D 7C D1

[CI+][CC] Hash Input:

0F 42 04 1A 87 36 05 40 77 EA 75 E0 D1 FB DB C2

02 13 6C AF 24 E9 A7 2A 96 A8 F3 C8 62 0A 05 9A

6E 90 CC B2 BD ED 55 56 78 1C EA 34 4F C5 FF 8B

C8 B6 36 3C 47 70 F0 20 DA D8 BC 9D E2 7D 7C D1


[CI+][CC] Ks:

30 D7 A9 E9 C9 C4 30 A1 0D 9D C3 D2 52 1B 91 7F

6D A5 DB 24 31 E7 06 A2 B3 A5 E5 2D FD 67 0C 90


[CI+][CC] Km:

EF 85 9C E5 20 FE 49 A5 18 20 DB 98 1A FB BD D0

36 8C 5D A4 20 80 84 A6 BB D9 9B 9E 32 E6 57 4F


[CI+][CC] SEK:
    EF 85 9C E5 20 FE 49 A5 18 20 DB 98 1A FB BD D0


    [CI+][CC] SAK:

    36 8C 5D A4 20 80 84 A6 BB D9 9B 9E 32 E6 57 4F


[146977 ms] TX: 01 00 A0 21 01 90 02 00 05 9F 90 04 18 01 02 05 00 08 00 22 5F D3 D1 13 6C 77 14 00 08 C8 B6
36 3C 47 70 F0 20

[147388 ms] RX: 01 00 80 02 01 80

[147491 ms] TX: 01 00 81 01 01

[147594 ms] RX: 01 00 A0 09 01 90 02 00 05 9F 90 05 00 80 02 01 00

<<< [CI+][CC] CC Sync Req

>>> [CI+][CC] CC Sync Cnf

[147704 ms] TX: 01 00 A0 0A 01 90 02 00 05 9F 90 06 01 00

[148109 ms] RX: 01 00 80 02 01 80

[148212 ms] TX: 01 00 81 01 01

[148314 ms] RX: 01 00 A0 31 01 90 02 00 05 9F 90 07 28 00 00 00 01 01 00 00 10 A8 E7 F9 65 25 53 2F F9 3B 84
72 34 93 92 96 A7 B6 3B F7 A0 00 CA 7C C2 20 E3 25 1E 50 8E 44 DB 80 02 01 00

<<< [CI+][CC] CC SAC Data Req

    [CI+][CC] SAC Data: message_counter = 1

    [CI+][CC] SAC Data: protocol_version = 0x00

    [CI+][CC] SAC Data: authentication_cipher_flag = 0x00

    [CI+][CC] SAC Data: payload_encryption_flag = 0x01

    [CI+][CC] SAC Data: encryption_cipher_flag = 0x00

    [CI+][CC] SAC Data: length_payload = 0x10

    [CI+][CC] AES128_CBC_DECRYPT Input:
```

```
    A8 E7 F9 65 25 53 2F F9 3B 84 72 34 93 92 96 A7

    B6 3B F7 A0 00 CA 7C C2 20 E3 25 1E 50 8E 44 DB



    [CI+][CC] SIV:

    F7 70 B0 36 03 61 F7 96 65 74 8A 26 EA 4E 85 41



CC SAC Data: AES128 CBC CRYPT OK!!!

AES128_CBC_DECRYPT Output:

    01 00 01 1D 80 00 00 00 00 00 00 00 00 00 00 00

    A8 91 33 11 EF 81 FA 17 0D E2 39 DE 99 84 79 37



    [CI+][CC] SAC Packet:

    04 00 00 00 01 01 00 00 10 01 00 01 1D 80 00 00

    00 00 00 00 00 00 00 00 00

    [CI+][CC] CC Rcv Msg:

    01 00 01 1D 80 00 00 00 00 00 00 00 00 00 00 00



    >>> URI Version 1

    [CI+][CC] CC Send Msg:

    01 01 1D 00 20 00 00 00 00 00 00 00 00 00 00 00

    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

    00 00 00 00 01

    [CI+][CC] SAC Packet:

    04 00 00 00 01 01 00 00 30 01 01 1D 00 20 00 00

    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 01 80 00

    00 00 00 00 00 00 00 00 00

    [CI+][CC] Auth:

    34 97 1F 70 11 EE EE 18 B8 EA 70 EB 31 48 11 65



    [CI+][CC] AES128_CBC_ENCRYPT Input:

    01 01 1D 00 20 00 00 00 00 00 00 00 00 00 00 00

    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

    00 00 00 00 01 80 00 00 00 00 00 00 00 00 00 00

    34 97 1F 70 11 EE EE 18 B8 EA 70 EB 31 48 11 65



    [CI+][CC] SIV:

    F7 70 B0 36 03 61 F7 96 65 74 8A 26 EA 4E 85 41



CC SAC Data: AES128 CBC CRYPT OK!!!

AES128_CBC_ENCRYPT Output:

    F3 FF BA E2 9F 4A E0 F2 C7 E7 EF 10 2D 6C 49 94

    83 7A 3D 5B AF 77 66 D7 36 F6 60 61 EB 6E 9D 81

    25 D5 47 15 4E D0 10 9A C9 25 F3 8B 3E F8 5D 07

    21 97 87 B8 9E 97 17 59 BD C5 66 94 36 01 F1 F5



>>> [CI+][CC] CC SAC Data Cnf

[148602 ms] TX: 01 00 A0 51 01 90 02 00 05 9F 90 08 48 00 00 00 01 01 00 00 30 F3 FF BA E2 9F 4A E0 F2 C7 E7
EF 10 2D 6C 49 94 83 7A 3D 5B AF 77 66 D7 36 F6 60 61 EB 6E 9D 81 25 D5 47 15 4E D0 10 9A C9 25 F3 8B 3E
F8 5D 07 21 97 87 B8 9E 97 17 59 BD C5 66 94 36 01 F1 F5
```

```
[149025 ms] RX: 01 00 80 02 01 80

[149128 ms] TX: 01 00 81 01 01

[149230 ms] RX: 01 00 A0 61 01 90 02 00 05 9F 90 07 58 00 00 00 02 01 00 00 40 91 F5 55 82 37 77 D4 3D 08 B0
C5 89 55 CD 42 9A 8A 29 A7 56 5A 84 10 C2 CF FC A2 42 AE F0 88 9D 33 4C D6 FF 81 51 CE B2 39 F9 3D 8D 23
2E 4B D7 BE 31 88 D0 00 65 F9 E6 5C 68 6C 0C 34 05 97 35 C7 4D A6 07 2C DD 6F B6 95 46 78 9B 18 F4 3B 4D
80 02 01 00

<<< [CI+][CC] CC SAC Data Req

        [CI+][CC] SAC Data: message_counter = 2

        [CI+][CC] SAC Data: protocol_version = 0x00

        [CI+][CC] SAC Data: authentication_cipher_flag = 0x00

        [CI+][CC] SAC Data: payload_encryption_flag = 0x01

        [CI+][CC] SAC Data: encryption_cipher_flag = 0x00

        [CI+][CC] SAC Data: length_payload = 0x40

        [CI+][CC] AES128_CBC_DECRYPT Input:

        91 F5 55 82 37 77 D4 3D 08 B0 C5 89 55 CD 42 9A

        8A 29 A7 56 5A 84 10 C2 CF FC A2 42 AE F0 88 9D

        33 4C D6 FF 81 51 CE B2 39 F9 3D 8D 23 2E 4B D7

        BE 31 88 D0 00 65 F9 E6 5C 68 6C 0C 34 05 97 35

        C7 4D A6 07 2C DD 6F B6 95 46 78 9B 18 F4 3B 4D



        [CI+][CC] SIV:

        F7 70 B0 36 03 61 F7 96 65 74 8A 26 EA 4E 85 41



CC SAC Data: AES128 CBC CRYPT OK!!!

AES128_CBC_DECRYPT Output:

        01 03 06 00 08 FC 84 16 3F 79 E1 5F 0A 0C 00 20
```

```
    21 62 84 51 24 9C C0 9C 53 72 73 99 BD 4F F6 EE
    A9 12 63 A1 24 BC 8C 73 44 F1 8D B2 3D C4 BB BF
    1C 00 01 01 02 05 1E 80 00 00 00 00 00 00 00 00
    F4 44 08 EA 76 B6 39 EC 63 7B 91 5C C4 49 9B B4

    [CI+][CC] SAC Packet:
    04 00 00 00 02 01 00 00 40 01 03 06 00 08 FC 84
    16 3F 79 E1 5F 0A 0C 00 20 21 62 84 51 24 9C C0
    9C 53 72 73 99 BD 4F F6 EE A9 12 63 A1 24 BC 8C
    73 44 F1 8D B2 3D C4 BB BF 1C 00 01 01 02 05 1E
    80 00 00 00 00 00 00 00 00
    [CI+][CC] CC Rcv Msg:
    01 03 06 00 08 FC 84 16 3F 79 E1 5F 0A 0C 00 20
    21 62 84 51 24 9C C0 9C 53 72 73 99 BD 4F F6 EE
    A9 12 63 A1 24 BC 8C 73 44 F1 8D B2 3D C4 BB BF
    1C 00 01 01 02 05 1E 80 00 00 00 00 00 00 00 00

    <<< CICAM ID
    <<< Kp
    [CI+][CC] Kp:
    21 62 84 51 24 9C C0 9C 53 72 73 99 BD 4F F6 EE
    A9 12 63 A1 24 BC 8C 73 44 F1 8D B2 3D C4 BB BF

    <<< Key Register: Odd Key
CC_AUTH_HOST_ID_REQ.
```

```
CC_AUTH_STATUS_REQ.

        >>> Host_ID

        >>> Status: 0

        [CI+][CC] CC Send Msg:

        01 02 05 00 08 00 22 5F D3 D1 13 6C 77 1E 00 01

        00

        [CI+][CC] SAC Packet:

        04 00 00 00 02 01 00 00 20 01 02 05 00 08 00 22

        5F D3 D1 13 6C 77 1E 00 01 00 80 00 00 00 00 00

        00 00 00 00 00 00 00 00 00

        [CI+][CC] Auth:

        65 78 DC 1E 94 2C 68 75 D2 AA AD 44 40 E1 7D BA


        [CI+][CC] AES128_CBC_ENCRYPT Input:

        01 02 05 00 08 00 22 5F D3 D1 13 6C 77 1E 00 01

        00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00

        65 78 DC 1E 94 2C 68 75 D2 AA AD 44 40 E1 7D BA


        [CI+][CC] SIV:

        F7 70 B0 36 03 61 F7 96 65 74 8A 26 EA 4E 85 41


CC SAC Data: AES128 CBC CRYPT OK!!!

AES128_CBC_ENCRYPT Output:

        AB 2B 70 21 13 C1 05 90 88 2F F9 91 7B 1F BF 59
        D4 4C 07 F4 B3 DB 6E A3 5F B1 5E C2 75 87 ED 53

        2B 53 49 29 E4 F4 11 8D C3 CD 19 C5 F8 B5 27 9E



>>> [CI+][CC] CC SAC Data Cnf

[CI+][CC] CICAM Brand ID = 0x0000

[149589 ms] TX: 01 00 A0 41 01 90 02 00 05 9F 90 08 38 00 00 00 02 01 00 00 20 AB 2B 70 21 13 C1 05 90 88 2F
F9 91 7B 1F BF 59 D4 4C 07 F4 B3 DB 6E A3 5F B1 5E C2 75 87 ED 53 2B 53 49 29 E4 F4 11 8D C3 CD 19 C5 F8
B5 27 9E

[150008 ms] RX: 01 00 80 02 01 80

[150111 ms] TX: 01 00 81 01 01

[150213 ms] RX: 01 00 A0 21 01 90 02 00 05 9F 90 09 18 00 00 00 03 01 00 00 00 5A 20 A8 05 03 13 46 D9 A9 11
0C 23 A8 BE 98 F3 80 02 01 00

<<< [CI+][CC] CC SAC SYNC Req

        [CI+][CC] SAC Data: message_counter = 3

        [CI+][CC] SAC Data: protocol_version = 0x00

        [CI+][CC] SAC Data: authentication_cipher_flag = 0x00

        [CI+][CC] SAC Data: payload_encryption_flag = 0x01

        [CI+][CC] SAC Data: encryption_cipher_flag = 0x00

        [CI+][CC] SAC Data: length_payload = 0x00

        [CI+][CC] AES128_CBC_DECRYPT Input:

        5A 20 A8 05 03 13 46 D9 A9 11 0C 23 A8 BE 98 F3



        [CI+][CC] SIV:

        F7 70 B0 36 03 61 F7 96 65 74 8A 26 EA 4E 85 41



CC SAC Data: AES128 CBC CRYPT OK!!!
```

```
AES128_CBC_DECRYPT Output:

    1D 23 3E 86 1F 3F 0F 9D 33 49 4C 3B 34 4B FC AB



    [CI+][CC] SAC Packet:

    04 00 00 00 03 01 00 00 00

    [CI+][CC] CC Rcv Msg:

    No Data.

    >>> Status: 0

    [CI+][CC] CC Send Msg:

    00

    [CI+][CC] SAC Packet:

    04 00 00 00 03 01 00 00 10 00 80 00 00 00 00 00

    00 00 00 00 00 00 00 00 00

    [CI+][CC] Auth:

    61 D3 A8 D4 52 21 F0 AF D2 8F 32 57 35 C2 D3 54



    [CI+][CC] AES128_CBC_ENCRYPT Input:

    00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00

    61 D3 A8 D4 52 21 F0 AF D2 8F 32 57 35 C2 D3 54



    [CI+][CC] SIV:

    F7 70 B0 36 03 61 F7 96 65 74 8A 26 EA 4E 85 41



CC SAC Data: AES128 CBC CRYPT OK!!!

AES128_CBC_ENCRYPT Output:
    A9 7A 1A CA 4F 18 FE 95 94 23 03 DF 97 A5 75 20

    5F D6 24 56 38 E6 D4 7D FC C8 4C 07 78 AB CC 3B



>>> [CI+][CC] CC SAC Sync Cnf

    [CI+][CC] Scramble Mode: 0x02

    [CI+][CC] Km:

    BC 1C E9 57 74 F5 13 83 87 98 8A CC 1A DA B0 A8

    B8 A0 26 1E C3 7B 1A F3 58 0B 74 FB FA 85 BD 42



    [CI+][CC] AES CCK:

    BC 1C E9 57 74 F5 13 83 87 98 8A CC 1A DA B0 A8



    [CI+][CC] AES CIV:

    B8 A0 26 1E C3 7B 1A F3 58 0B 74 FB FA 85 BD 42



[CI+][CC] [0]Connect DSCMB Fid : 31 | Pid : 49

[CI+][CC] [1]Connect DSCMB Fid : 30 | Pid : 49

[CI+][CC] [2]Connect DSCMB Fid : 29 | Pid : 52

[CI+][HSS] Do HSS Check...

[CI+][HSS] MDrv_CI_HSS_SetSunningStatus: 0

[CI+][HSS] HSS In-active! (TS ID(0001) | Service ID(0002)) | 1 | 0

[CI+][HSS] HSS In-active should sent PMT again

[CI+][HSS] MDrv_CI_HSS_GetSunningStatus: 0

[CI+][HSS] MDrv_CI_HSS_GetSunningStatus: 0
```

```
[150506 ms] TX: 01 00 A0 31 01 90 02 00 05 9F 90 10 28 00 00 00 03 01 00 00 10 A9 7A 1A CA 4F 18 FE 95 94 23
03 DF 97 A5 75 20 5F D6 24 56 38 E6 D4 7D FC C8 4C 07 78 AB CC 3B

[150721 ms] TX: 01 00 A0 2B 01 90 02 00 08 9F 80 32 22 03 00 02 C1 F0 00 01 E0 31 F0 09 01 09 06 10 00 E1 7A
FF FA 04 E0 34 F0 09 01 09 06 10 00 E1 7B FF FA

[152334 ms] RX: 01 00 80 02 01 80

[152437 ms] TX: 01 00 81 01 01

[152539 ms] RX: 01 00 A0 41 01 90 02 00 05 9F 90 07 38 00 00 00 04 01 00 00 20 27 E3 E4 2F 62 66 29 01 72 E7 A9
29 40 21 62 C4 BE 31 43 96 8E 44 62 E6 98 A7 BB 7B 64 CE 4D 44 05 15 68 BB 60 F7 F9 42 D5 68 3F C5 5F EB
2B 1B 80 02 01 00

<<< [CI+][CC] CC SAC Data Req

    [CI+][CC] SAC Data: message_counter = 4

    [CI+][CC] SAC Data: protocol_version = 0x00

    [CI+][CC] SAC Data: authentication_cipher_flag = 0x00

    [CI+][CC] SAC Data: payload_encryption_flag = 0x01

    [CI+][CC] SAC Data: encryption_cipher_flag = 0x00

    [CI+][CC] SAC Data: length_payload = 0x20

    [CI+][CC] AES128_CBC_DECRYPT Input:

    27 E3 E4 2F 62 66 29 01 72 E7 A9 29 40 21 62 C4

    BE 31 43 96 8E 44 62 E6 98 A7 BB 7B 64 CE 4D 44

    05 15 68 BB 60 F7 F9 42 D5 68 3F C5 5F EB 2B 1B



    [CI+][CC] SIV:

    F7 70 B0 36 03 61 F7 96 65 74 8A 26 EA 4E 85 41



CC SAC Data: AES128 CBC CRYPT OK!!!

AES128_CBC_DECRYPT Output:

    01 02 19 00 08 01 30 00 00 00 00 00 00 1A 00 02
```

```
00 02 01 1B 80 00 00 00 00 00 00 00 00 00 00 00

07 DC EF 87 1E 40 85 ED B1 A2 87 AE 55 9F EA 3B



[CI+][CC] SAC Packet:

04 00 00 00 04 01 00 00 20 01 02 19 00 08 01 30

00 00 00 00 00 00 1A 00 02 00 02 01 1B 80 00 00

00 00 00 00 00 00 00 00 00

[CI+][CC] CC Rcv Msg:

01 02 19 00 08 01 30 00 00 00 00 00 00 1A 00 02

00 02 01 1B 80 00 00 00 00 00 00 00 00 00 00 00



<<< URI Message

URI Message:

01 30 00 00 00 00 00 00

[CI+][CC] URI Message: protocol_version: 01

[CI+][CC] URI Message: aps_copy_control_info: 00

[CI+][CC] URI Message: emi_copy_control_info: 03

[CI+][CC] URI Message: ict_copy_control_info: 00

[CI+][CC] URI Message: rct_copy_control_info: 00

[CI+][CC] URI Message: rl_copy_control_info:    00

<<< Program Number: 0x0002

>>> URI Confirmation

[CI+][CC] CC Send Msg:

01 01 1B 00 20 81 80 42 B0 A8 EF 9D A7 07 73 45
```

```
    AF A9 F7 D8 7A CD C6 28 5D C8 41 2C 68 1B BD F6
    16 A8 FF 34 40
    [CI+][CC] SAC Packet:
    04 00 00 00 04 01 00 00 30 01 01 1B 00 20 81 80
    42 B0 A8 EF 9D A7 07 73 45 AF A9 F7 D8 7A CD C6
    28 5D C8 41 2C 68 1B BD F6 16 A8 FF 34 40 80 00
    00 00 00 00 00 00 00 00 00
    [CI+][CC] Auth:
    51 77 F0 9E 8E E7 31 DC A4 BE 0D 04 8C 4D EE CE

    [CI+][CC] AES128_CBC_ENCRYPT Input:
    01 01 1B 00 20 81 80 42 B0 A8 EF 9D A7 07 73 45
    AF A9 F7 D8 7A CD C6 28 5D C8 41 2C 68 1B BD F6
    16 A8 FF 34 40 80 00 00 00 00 00 00 00 00 00 00
    51 77 F0 9E 8E E7 31 DC A4 BE 0D 04 8C 4D EE CE

    [CI+][CC] SIV:
    F7 70 B0 36 03 61 F7 96 65 74 8A 26 EA 4E 85 41

CC SAC Data: AES128 CBC CRYPT OK!!!
AES128_CBC_ENCRYPT Output:
    3B BA 7F 1D 41 3D 31 D8 13 C4 04 59 C7 A8 D9 7A
    BC 5D 4E 51 F4 EC 0C AD 2F 5B BA 56 50 0D 41 C7
    C9 5C B6 FE 3C 9C 31 8C 8D 24 62 B8 48 2F 97 2B
    B1 F9 D7 13 79 69 0B 48 D1 9D 49 8F 81 5F E0 B7
```

```
>>> [CI+][CC] CC SAC Data Cnf

[CI+] URI Copy Never....
[152965 ms] TX: 01 00 A0 51 01 90 02 00 05 9F 90 08 48 00 00 00 04 01 00 00 30 3B BA 7F 1D 41 3D 31 D8 13 C4
04 59 C7 A8 D9 7A BC 5D 4E 51 F4 EC 0C AD 2F 5B BA 56 50 0D 41 C7 C9 5C B6 FE 3C 9C 31 8C 8D 24 62 B8
48 2F 97 2B B1 F9 D7 13 79 69 0B 48 D1 9D 49 8F 81 5F E0 B7

[153389 ms] RX: 01 00 80 02 01 80

[153492 ms] TX: 01 00 81 01 01

[153595 ms] RX: 01 00 A0 41 01 90 02 00 05 9F 90 07 38 00 00 00 05 01 00 00 20 46 53 25 DE B9 BB 0D 3C B9 81
66 66 32 D4 CB 1F 1A 22 DB F9 0A 6E 1D C4 49 28 14 12 B8 DD 31 D0 E1 7A 89 B1 C5 B0 16 4D 9B 10 A7 19 8C
C2 C7 AE 80 02 01 00

<<< [CI+][CC] CC SAC Data Req

      [CI+][CC] SAC Data: message_counter = 5

      [CI+][CC] SAC Data: protocol_version = 0x00

      [CI+][CC] SAC Data: authentication_cipher_flag = 0x00

      [CI+][CC] SAC Data: payload_encryption_flag = 0x01

      [CI+][CC] SAC Data: encryption_cipher_flag = 0x00

      [CI+][CC] SAC Data: length_payload = 0x20

      [CI+][CC] AES128_CBC_DECRYPT Input:

      46 53 25 DE B9 BB 0D 3C B9 81 66 66 32 D4 CB 1F

      1A 22 DB F9 0A 6E 1D C4 49 28 14 12 B8 DD 31 D0

      E1 7A 89 B1 C5 B0 16 4D 9B 10 A7 19 8C C2 C7 AE



      [CI+][CC] SIV:

      F7 70 B0 36 03 61 F7 96 65 74 8A 26 EA 4E 85 41



CC SAC Data: AES128 CBC CRYPT OK!!!
```

```
AES128_CBC_DECRYPT Output:

    01 02 19 00 08 01 00 00 00 00 00 00 00 1A 00 02

    00 02 01 1B 80 00 00 00 00 00 00 00 00 00 00 00

    F3 49 F2 BD 74 C2 9F 89 14 97 93 B0 DF 19 A3 73



    [CI+][CC] SAC Packet:

    04 00 00 00 05 01 00 00 20 01 02 19 00 08 01 00

    00 00 00 00 00 00 1A 00 02 00 02 01 1B 80 00 00

    00 00 00 00 00 00 00 00 00

    [CI+][CC] CC Rcv Msg:

    01 02 19 00 08 01 00 00 00 00 00 00 00 1A 00 02

    00 02 01 1B 80 00 00 00 00 00 00 00 00 00 00 00



    <<< URI Message

    URI Message:

    01 00 00 00 00 00 00 00

    [CI+][CC] URI Message: protocol_version: 01

    [CI+][CC] URI Message: aps_copy_control_info: 00

    [CI+][CC] URI Message: emi_copy_control_info: 00

    [CI+][CC] URI Message: ict_copy_control_info: 00

    [CI+][CC] URI Message: rct_copy_control_info: 00

    [CI+][CC] URI Message: rl_copy_control_info:    00

    <<< Program Number: 0x0002

    >>> URI Confirmation
    [CI+][CC] CC Send Msg:
    01 01 1B 00 20 65 78 7D 96 C5 3D 26 16 89 FD C5
    3A 8F E6 62 58 D2 28 B3 19 E3 62 5B BD 41 35 DD
    09 22 F8 9E 14
    [CI+][CC] SAC Packet:
    04 00 00 00 05 01 00 00 30 01 01 1B 00 20 65 78
    7D 96 C5 3D 26 16 89 FD C5 3A 8F E6 62 58 D2 28
    B3 19 E3 62 5B BD 41 35 DD 09 22 F8 9E 14 80 00
    00 00 00 00 00 00 00 00 00
    [CI+][CC] Auth:
    61 F1 C5 FB 36 11 E5 37 09 1D 43 38 A6 73 3B 45


    [CI+][CC] AES128_CBC_ENCRYPT Input:
    01 01 1B 00 20 65 78 7D 96 C5 3D 26 16 89 FD C5
    3A 8F E6 62 58 D2 28 B3 19 E3 62 5B BD 41 35 DD
    09 22 F8 9E 14 80 00 00 00 00 00 00 00 00 00 00
    61 F1 C5 FB 36 11 E5 37 09 1D 43 38 A6 73 3B 45


    [CI+][CC] SIV:
    F7 70 B0 36 03 61 F7 96 65 74 8A 26 EA 4E 85 41


CC SAC Data: AES128 CBC CRYPT OK!!!
AES128_CBC_ENCRYPT Output:
    2E 21 D3 B1 F6 DC 66 3A A9 A9 DA 1E 3C C7 CE 0F
    32 7D F4 EE BA AD 94 DE 5F 06 0A 64 3C 3F 5A 61
    21 5E E6 F2 8E 4A 4F 7C 5C E0 DE AE E9 37 21 76

    99 AD 90 86 46 22 F7 A5 0E 3E DD 71 A4 06 78 C3



>>> [CI+][CC] CC SAC Data Cnf

[CI+] URI Copy Freely....
[153942 ms] TX: 01 00 A0 51 01 90 02 00 05 9F 90 08 48 00 00 00 05 01 00 00 30 2E 21 D3 B1 F6 DC 66 3A A9 A9 DA 1E 3C C7 CE 0F 32 7D F4 EE BA AD 94 DE 5F 06 0A 64 3C 3F 5A 61 21 5E E6 F2 8E 4A 4F 7C 5C E0 DE AE E9 37 21 76 99 AD 90 86 46 22 F7 A5 0E 3E DD 71 A4 06 78 C3
```

时间和 key 都正常，就出现以上正常的解密了，

CODE 相关设置：

首先根据需要打开相关的宏

```
#if ((ENABLE_DTV) && (!BLOADER))
#define ENABLE_CI                          ENABLE
#define ENABLE_CI_PLUS               ENABLE// DISABLE  //
#else // #if (ENABLE_DTV)
#define ENABLE_CI                          DISABLE
#define ENABLE_CI_PLUS                     DISABLE
#endif
```

其次就是相关的 KEY 了

普通的 CI 打开红就可以了，注意

```
        case CI_EVENT_CC_CREDENTIALS_LOAD:
          {
          #if (ENABLE_UPGRADE_CIPLUSKEY_BY_USB)
              BOOLEAN bValidkey = FALSE;

              bValidkey = Mapp_check_valid_key();
              if(bValidkey == TRUE)
              {
                  U16 u16CredentialsLength = 0;
                  U8 u8aTempBuf[2] = { 0x00 };
                  msAPI_Flash_Read(   CIPLUS_KEY_BANK*FLASH_BLOCK_SIZE   +   12,   2, u8aTempBuf );//0X72000+12
                  u16CredentialsLength = (U16)u8aTempBuf[0] << 8 | (U16)u8aTempBuf[1];
                  printf("\n## Valid ci+ key len=%x",u16CredentialsLength);
                  msAPI_Flash_Read(    CIPLUS_KEY_BANK*FLASH_BLOCK_SIZE    +    12, (U32)u16CredentialsLength, msAPI_CI_CC_GetCredentialsBufferAddr() );
              }
              else
              {
                  U8* ciBuf;
```

```
                    U16 i;
                    printf("\n## invalid ci+ key!");
                    ciBuf = msAPI_CI_CC_GetCredentialsBufferAddr();
                    for(i=0;i<0x1362;i++)
                    {
                        ciBuf[i] = Default_CIPlus_KEY[12+i];
                    }
                }
            #else
                U8 u8aTempBuf[2] = { 0x00 };
                U16 u16CredentialsLength = 0;

                msAPI_Flash_Read( CIPLUS_KEY_BANK*FLASH_BLOCK_SIZE + 12， 2， u8aTempBuf );
                u16CredentialsLength = (U16)u8aTempBuf[0] << 8 | (U16)u8aTempBuf[1];

                msAPI_Flash_Read(CIPLUS_KEY_BANK*FLASH_BLOCK_SIZE + 12， (U32)u16CredentialsLength， msAPI_CI_CC_GetCredentialsBufferAddr() );
            #endif
            }
            break;
```

这个地址，这地址关系的 CI 的存储和读取，建议采用动态地址，也可以使用静态地址，但一定要正确，不确定的情况下先打印出来。

如果是 CI+的相对稍微复杂点

 首先客户的 KEY 是否是外部加密的，如果是外部加密的需要添加

格式：（此为 N022 的 key 的密码，不同的客户不一样）

```
  static U8 gu8aAesXcbcKey[16] =
{
    0x19， 0x28， 0x58， 0x92， 0x49， 0x39， 0x82， 0x39， 0x66， 0x83， 0x59， 0x82， 0x39， 0x68， 0x76， 0x21
};
static U8 gu8aAesCbcKey[16] =
{
    0x0F， 0x1E， 0x2D， 0x3C， 0x4B， 0x5A， 0x69， 0x78， 0x8A， 0x9C， 0xA5， 0xB4， 0xC3， 0xD2， 0xE1， 0xF0
};
static U8 gu8aAesCbcIV[16] =
{
    0x00， 0x17， 0x22， 0x38， 0x44， 0x55， 0x6C， 0x77， 0x88， 0x99， 0xAB， 0xBB， 0xCC， 0xDF， 0xEE， 0xFF
};
```

关键位置：

 CI 的初始化，初始化会影响到是否能正确去识别 ci 卡和解码，还有切台等响应速度。

```
 #if ENABLE_CI
static void MApp_Init_CI(void)
{
    msAPI_CI_SetPMTBufAddr(_PA2VA((CI_PMT_BUFFER_MEMORY_TYPE & MIU1) ? (CI_PMT_BUFFER_ADR | MIU_INTERVAL) : (CI_PMT_BUFFER_ADR)));
    msAPI_CI_SetMMIBufAddr(_PA2VA((MMI_TEXTSTRING_MEMORY_TYPE & MIU1) ? (MMI_TEXTSTRING_ADR | MIU_INTERVAL) : (MMI_TEXTSTRING_ADR)));
#if (ENABLE_CI_PLUS)
```

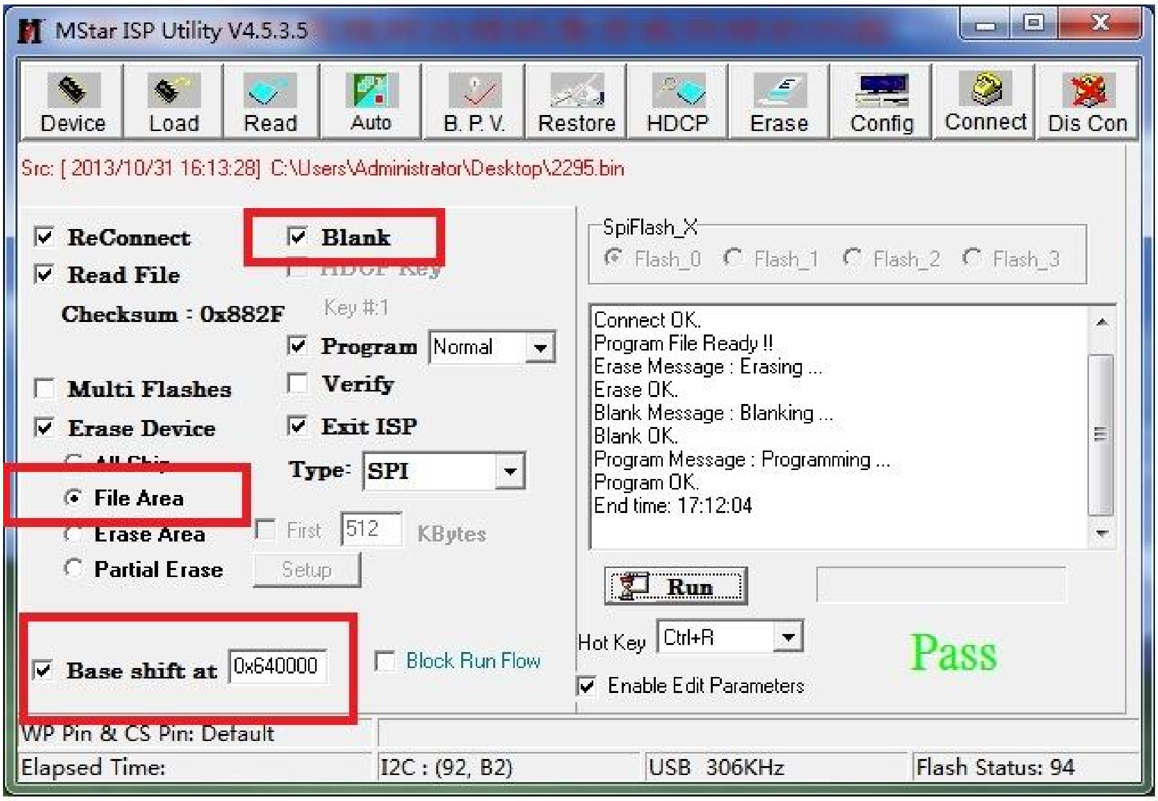
```
    msAPI_CI_Initial( TRUE );   // TRUE: CI+ Supported
#else
    msAPI_CI_Initial( FALSE );  // FALSE: CI VI Only
#endif
    msAPI_CI_InstallCallback_CI_Event(MApp_CI_Event_Cb);
#if (ENABLE_CI_PLUS)
    /* Set up CI+ Credentials Setting.
       If using default CI+ Test Keys, please keep marking line.
       If using outside (from Flash) CI+ Production Keys, please unmark this line.
    */
#if  1//ENABLE_UPGRADE_CIPLUSKEY_BY_USB
    msAPI_CI_CC_SetCredentialsType(TRUE, TRUE);//CI+必须打开这里，否则影响到解码//影响到 KEY 的导入的，上面打印 NG 就是和此处有关。
#endif
msAPI_CI_CC_SetDescryptKeyForEncryptedCredentials(gu8aAesXcbcKey, gu8aAesCbcKey,gu8aAesCbcIV);//caimingan add for CI_PLUS//此为密码的调用
#endif
  //  msAPI_CI_Set_TXRX_Interval(70,70,1);
    msAPI_CI_Set_TXRX_Interval(100,100,1);//此为通讯时序
   // msAPI_CI_Set_TXRX_Interval(70,70,1);
    //msAPI_CI_Set_TXRX_Interval(0,5,1);
    //msAPI_CI_Set_TXRX_Interval(120,120,1);

    /* For CI/CI+ Debuging. */
    //msAPI_CI_SetDebugLevel(EN_CI_FUNCTION_DEFAULT, 1);
    //msAPI_CI_SetDebugLevel(EN_CI_FUNCTION_HSS, 1);
   // msAPI_CI_SetDebugLevel(EN_CI_FUNCTION_CC, 4);
}
#endif
```

如果以上过程都设置 OK 基本上解码就 OK 了

外部 CI+key 的烧录：

烧录 CI+ KEY 操作说明

和烧主程序是一样的，有两个地方要注意，设置如下：



Src: [2013/10/31 16:13:28] C:\Users\Administrator\Desktop\2295.bin

☑ ReConnect
☑ Read File
Checksum : 0x882F
☑ Blank
☐ HDCP Key
Key #:1
☑ Program Normal
☐ Multi Flashes
☐ Verify
☑ Erase Device
☑ Exit ISP
○ All Chip
● File Area
○ Erase Area
○ Partial Erase
Type: SPI
☐ First 512 KBytes
Setup
☑ Base shift at 0x640000
☐ Block Run Flow

SpiFlash_X: ● Flash_0 ○ Flash_1 ○ Flash_2 ○ Flash_3

```
Connect OK.
Program File Ready !!
Erase Message : Erasing ...
Erase OK.
Blank Message : Blanking ...
Blank OK.
Program Message : Programming ...
Program OK.
End time: 17:12:04
```

Hot Key Ctrl+R
☑ Enable Edit Parameters

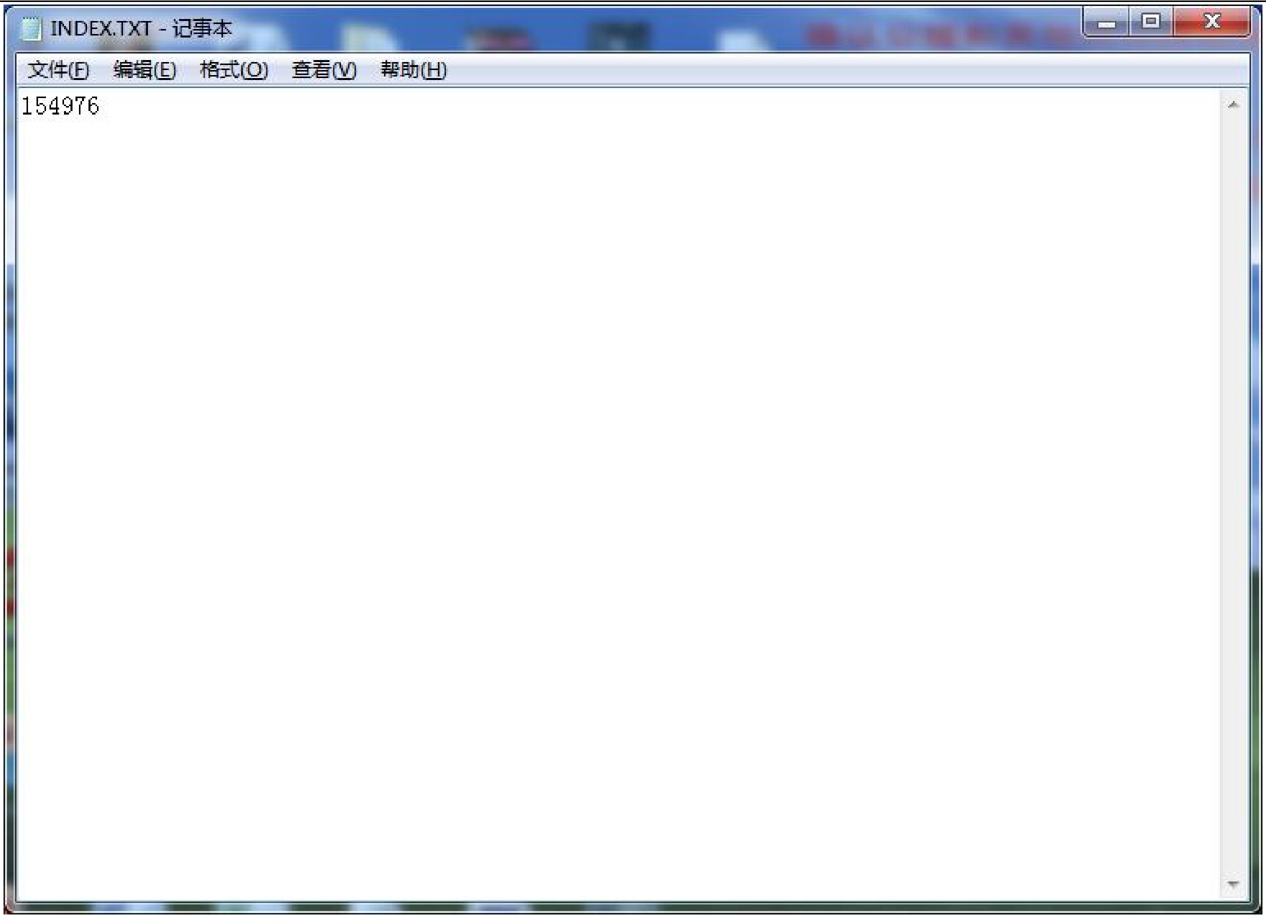
WP Pin & CS Pin: Default
Elapsed Time: | I2C : (92, B2) | USB 306KHz | Flash Status: 94

注意事项：

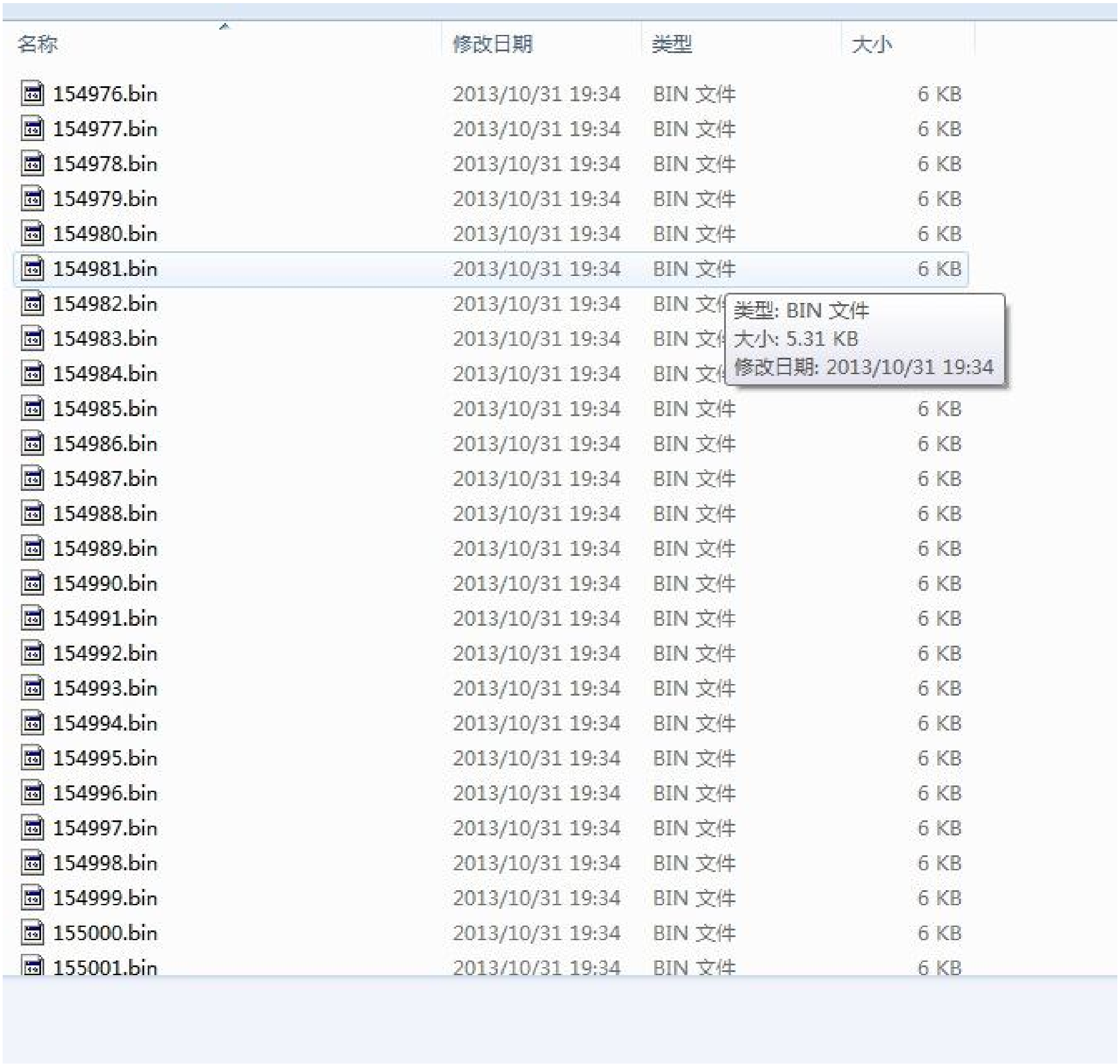
1. CI+ 的功能必须要烧录 CI+ KEY，并且必须要和主程序搭配才能用，但并不是所有的其他程序都可以用，必须是指定的主程序，即使烧到别的程序上也没有作用。
2. 必须先烧主程序，再烧 KEY，如果这个板子中间烧过别的程序，因为别的程序可能太大，地址已经超过这个偏移地址，会覆盖掉 KEY，必须重烧主程序和 KEY。

方法二

1、将 CI+KEY 的所有 bin 文件拷如 U 盘的根目录下，新建一个 INDEX.TXT 文档，将文档的里的数字写为要烧的 KEY 的（例如要顺序烧录如图所示的文档，INDEX.TXT 写为 154976）



```
154976
```



名称	修改日期	类型	大小
154976.bin	2013/10/31 19:34	BIN 文件	6 KB
154977.bin	2013/10/31 19:34	BIN 文件	6 KB
154978.bin	2013/10/31 19:34	BIN 文件	6 KB
154979.bin	2013/10/31 19:34	BIN 文件	6 KB
154980.bin	2013/10/31 19:34	BIN 文件	6 KB
154981.bin	2013/10/31 19:34	BIN 文件	6 KB
154982.bin	2013/10/31 19:34	BIN 文	
154983.bin	2013/10/31 19:34	BIN 文	
154984.bin	2013/10/31 19:34	BIN 文	
154985.bin	2013/10/31 19:34	BIN 文件	6 KB
154986.bin	2013/10/31 19:34	BIN 文件	6 KB
154987.bin	2013/10/31 19:34	BIN 文件	6 KB
154988.bin	2013/10/31 19:34	BIN 文件	6 KB
154989.bin	2013/10/31 19:34	BIN 文件	6 KB
154990.bin	2013/10/31 19:34	BIN 文件	6 KB
154991.bin	2013/10/31 19:34	BIN 文件	6 KB
154992.bin	2013/10/31 19:34	BIN 文件	6 KB
154993.bin	2013/10/31 19:34	BIN 文件	6 KB
154994.bin	2013/10/31 19:34	BIN 文件	6 KB
154995.bin	2013/10/31 19:34	BIN 文件	6 KB
154996.bin	2013/10/31 19:34	BIN 文件	6 KB
154997.bin	2013/10/31 19:34	BIN 文件	6 KB
154998.bin	2013/10/31 19:34	BIN 文件	6 KB
154999.bin	2013/10/31 19:34	BIN 文件	6 KB
155000.bin	2013/10/31 19:34	BIN 文件	6 KB
155001.bin	2013/10/31 19:34	BIN 文件	6 KB

类型: BIN 文件
大小: 5.31 KB
修改日期: 2013/10/31 19:34

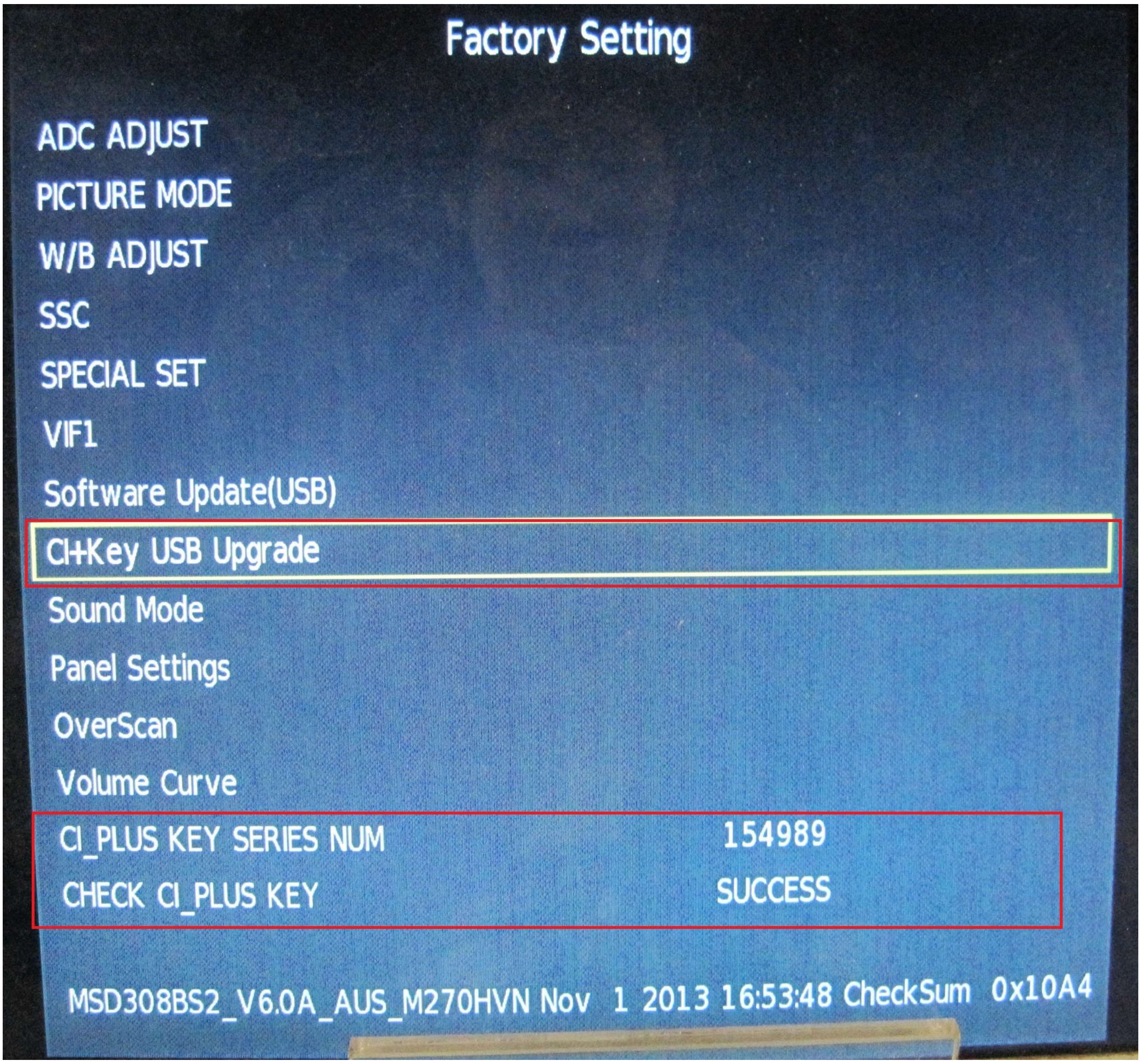
2、

2、按 source+7411 或者 AT035 遥控的 F1 按键，或者进工厂菜单选择升级选项,烧完看见等闪烁一下，工厂菜单的下图所示会

刷新为对应 KEY 的 INDEX.。

升级完成后会删除 U 盘的文件。

升级成功如下图所示。、:



CI_PLUS KEY SERIES NUM 154989

CHECK CI_PLUS KEY SUCCESS

MSD308BS2_V6.0A_AUS_M270HVN Nov 1 2013 16:53:48 CheckSum 0x10A4

以上的地址和方式不是固定的，需要根据不同需要进行变化。

CODE 部分识别 CI 是否烧录成功的一些重要位置：

```
  #if CIPLUS_KEY_INFO_ENABLE
extern BOOLEAN MDrv_UsbDeviceConnect(void);
extern BOOLEAN MDrv_UsbDeviceConnect_Port2(void);
#define CIPLUS_KEY_ORIGINAL_SIZE    5442//5458  //CI PLUS KEY offer by different customer, the size is different, you need to change according to the key  一定要根据客户的 key 大小来变化，必须对应
#define CIPLUS_KEYSIZE  (CIPLUS_KEY_ORIGINAL_SIZE -4)   //The last 4 BYTE is CRC value
U32 Mapp_Get_Ciplus_crc(void)//获取 key 的相关的信息
{
    U8 u8aTempBuf[4] = { 0x00 };
    U32 u32CRC = 0;
//CRC
    msAPI_Flash_Read( CIPLUS_KEY_BANK*FLASH_BLOCK_SIZE + CIPLUS_KEYSIZE, 4, u8aTempBuf );//caimingan changge
    u32CRC = (U32)u8aTempBuf[0] << 24 | (U32)u8aTempBuf[1]<<16 |(U32)u8aTempBuf[2]<<8 |(U32)u8aTempBuf[3];
    printf("~CRC32: 0x%X\r\n", u32CRC);
    return u32CRC;
```

```
}
//series No.
U32 Mapp_Get_Ciplus_SeriesNo(void)//获取 KEY 的编号
{
    U8 u8aTempBuf[4] = { 0x00 };
    U32 u32SeriesNo = 0;
    msAPI_Flash_Read( CIPLUS_KEY_BANK*FLASH_BLOCK_SIZE, 4, u8aTempBuf );
    u32SeriesNo = (U32)u8aTempBuf[0] << 24 | (U32)u8aTempBuf[1]<<16 |(U32)u8aTempBuf[2]<<8
|(U32)u8aTempBuf[3];
    printf("~series No: %ld\r\n", u32SeriesNo);

    return u32SeriesNo;
}
unsigned long crc32_encode(const unsigned char *octets, int len)
{
  unsigned long crc = 0xFFFFFFFF;
  unsigned long temp;
  int j;

  while (len--)
  {
    temp = (unsigned long)((crc & 0xFF) ^ *octets++);
    for (j = 0; j < 8; j++)
    {
      if (temp & 0x1)
        temp = (temp >> 1) ^ 0xEDB88320;
      else
        temp >>= 1;
    }
    crc = (crc >> 8) ^ temp;
  }
  return crc ^ 0xFFFFFFFF;
}

U32 MApp_LoadCIPlusKey(void)//lode KEY 进行比对
{
    U8 u8aTempBuf[CIPLUS_KEYSIZE] = { 0x00 };
    U32 u32Cacu_CRC = 0;
    U32 u32SeriesNo = 0;
       msAPI_MIU_Copy(FLASH_BLOCK_SIZE*CIPLUS_KEY_BANK,((CIPLUST_KEY_BUFFER_MEMORY_TYPE &
MIU1) ? (CIPLUST_KEY_BUFFER_ADR | MIU_INTERVAL) :
(CIPLUST_KEY_BUFFER_ADR)),(U32)CIPLUST_KEY_BUFFER_LEN,MIU_FLASH2SDRAM);
    memcpy(u8aTempBuf, (U8*)_PA2VA((U32)(DRAM_GEN_DB_START((CIPLUST_KEY_BUFFER_MEMORY_TYPE &
MIU1) ? (CIPLUST_KEY_BUFFER_ADR | MIU_INTERVAL) : (CIPLUST_KEY_BUFFER_ADR)))), CIPLUS_KEYSIZE);
    u32SeriesNo = (U32)u8aTempBuf[0] << 24 | (U32)u8aTempBuf[1]<<16 |(U32)u8aTempBuf[2]<<8
|(U32)u8aTempBuf[3];
    u32Cacu_CRC = ~crc32_encode(u8aTempBuf, CIPLUS_KEYSIZE);
    printf("~Caculate CRC : 0x%lx\r\n", u32Cacu_CRC);
    return u32Cacu_CRC;
}
#endif //CIPLUS_KEY_INFO_ENABLE
```

工厂菜单 CI_PLUS KEY 的相关信息选项，就是跟以上函数判断

分别为序列号以及读取 CI_PLUS KEY 的状态（FALSE 或者 SUCCESSS）

CI KEY U 盘烧录，为了方便客户烧录，做了将所有 KEY 按 CI 的序列号进行烧录，每烧录完成一个对应的 INDEX 加 1，删除原有的 KEY。

主要调用函数

```
  BOOLEAN MApp_WriteCIPlusKeyPlus(void)
{
    U32 KeyLen;
    U8 u8KeyFileName[40] ;//= "CIPLUSKEY.bin";
    U32 u32FileIndex;
      #if ((BOARD_TYPE_SEL ==BOARD_TYPE_P75_309BS2_V60A)||(BOARD_TYPE_SEL==BOARD_TYPE_P40_309BS2_V30A))
    while(!MDrv_UsbDeviceConnect_Port2())
    #else
    while (!MDrv_UsbDeviceConnect())
     #endif
    {
        EE_LOAD(printf("init USB fail\n"));
        return FALSE;
    }

    U8 u8PortEnStatus = MDrv_USBGetPortEnableStatus();
       #if ((BOARD_TYPE_SEL ==BOARD_TYPE_309B_V30)||(BOARD_TYPE_SEL ==BOARD_TYPE_P75_309BS2_V60A)||(BOARD_TYPE_SEL==BOARD_TYPE_P40_309BS2_V30A))
    if((u8PortEnStatus & BIT1) == BIT1)
    {
        MApp_UsbSaveData_SetPort(BIT1);
    }
    else if((u8PortEnStatus & BIT0) == BIT0)
    {
        MApp_UsbSaveData_SetPort(BIT0);
    }
    #else
    if((u8PortEnStatus & BIT0) == BIT0)
    {
        MApp_UsbSaveData_SetPort(BIT0);
    }
    else if((u8PortEnStatus & BIT1) == BIT1)
    {
        MApp_UsbSaveData_SetPort(BIT1);
    }
    #endif

    else
    {
        EE_LOAD(printf("Error> Unknown USB port\n"));
        return FALSE;
    }

    if (!MApp_UsbSaveData_InitFileSystem())
    {
        MApp_UsbSaveData_Exit();
        EE_LOAD(printf("Exit"));
        return FALSE;
    }
    memset(u8KeyFileName,0,sizeof(u8KeyFileName));
    if(!MApp_UsbSaveData_GetKeyFileNamePlus(u8KeyFileName,&u32FileIndex))
        return FALSE;
    puts((char *)u8KeyFileName);
    printf("fileindex = %ld",u32FileIndex);
    U8 u8HandleNo;

    if (MApp_UsbSaveData_SearchFileInRoot((U8 *)u8KeyFileName, &g_fileEntry))
    {
        u8HandleNo = msAPI_FCtrl_FileOpen(&g_fileEntry, OPEN_MODE_FOR_READ);

              if(u8HandleNo != FCTRL_INVALID_FILE_HANDLE)
              {
                EE_LOAD(printf("current file is exist\r\n"));
                   KeyLen = msAPI_FCtrl_FileLength(u8HandleNo);
                  msAPI_FCtrl_FileRead(u8HandleNo,    ((CIPLUST_KEY_BUFFER_MEMORY_TYPE    &
MIU1) ? (CIPLUST_KEY_BUFFER_ADR| MIU_INTERVAL) : (CIPLUST_KEY_BUFFER_ADR)), KeyLen);

                  EE_LOAD( printf("Close file: msAPI_FCtrl_FileClose\n") );
                  msAPI_FCtrl_FileClose(u8HandleNo);

              }
              else
              {
                  EE_LOAD(printf("Open file fail\n"));
                return FALSE;
              }
    }
    else
    {
        EE_LOAD(printf("database file is not exist\r\n"));
        return FALSE;
    }

    //store to flash immediately
    MApp_DB_SaveCIPlusKey((S32)KeyLen);
    if(!MApp_UsbSaveData_SetKeyFileNamePlus(&u32FileIndex))
        return FALSE;
    if (MApp_UsbSaveData_SearchFileInRoot((U8 *)u8KeyFileName, &g_fileEntry))
            msAPI_FCtrl_FileDelete(&g_fileEntry);

    while(msAPI_MIU_QuickDataBaseCheck() != TRUE);
    MApp_CheckFlash();
          LED_RED_ON();
            LED_GREEN_OFF();
    MsOS_DelayTask(200);
            LED_GREEN_ON();
            LED_RED_OFF();
    //msAPI_BLoader_Reboot();
    return TRUE;
}


#if ENABLE_CI_PLUS_KEY_BY_USB
void MApp_DB_SaveCIPlusKey(S32 KeyLen)
{
    msAPI_MIU_StoreDataBase2Flash(CIPLUS_KEY_BANK, ((CIPLUST_KEY_BUFFER_MEMORY_TYPE  &  MIU1)  ?
(CIPLUST_KEY_BUFFER_ADR | MIU_INTERVAL) : (CIPLUST_KEY_BUFFER_ADR)), KeyLen, TRUE);
}

void MApp_DB_ReadCIPlusKey(void)
{
    BOOL bXCopyFWStatus= MApi_BDMA_XCopyGetFWStatus();
    MApi_BDMA_XCopySetFWStatus(0);//caucy.niu 090921 for hisense DB Save in flash
       msAPI_MIU_Copy(SYSTEM_BANK_SIZE*CIPLUS_KEY_BANK,((CIPLUST_KEY_BUFFER_MEMORY_TYPE       &
MIU1)          ?           (CIPLUST_KEY_BUFFER_ADR             |           MIU_INTERVAL)           :
(CIPLUST_KEY_BUFFER_ADR)),(U32)CIPLUST_KEY_BUFFER_LEN,MIU_FLASH2SDRAM);
        MApi_BDMA_XCopySetFWStatus(bXCopyFWStatus);//caucy.niu 090921 for hisense DB Save in flash

}

#endif

#if ENABLE_CI_PLUS_KEY_BY_USB
BOOLEAN MApp_UsbSaveData_GetKeyFileNamePlus(U8* u8KeyFileName,U32* u32FileIndex)
{
    FileEntry fileEntrytemp;
    U8 u8HandleNo;
    U8 u8FileName[40] = "index.txt";
    U16 u16FileName[20];
    U32 AddressOffSet = 1;
    U8 i = 0,j = 0;
    U16 Index = 0x31;
    U8 u8KeyLength = 0;

    *u32FileIndex = 0;
    if(!MApp_UsbSaveData_SearchFileInRoot((U8 *)u8FileName, &fileEntrytemp))
    {
        printf("\r\n there is not index file plus\n");
        ASCIItoUnicode2((S8*)u8FileName, strlen((char *)u8FileName));
        memset(u16FileName, 0, sizeof(u16FileName));
        memcpy(u16FileName, u8FileName, sizeof(u16FileName));
        u8HandleNo      =       MApp_UsbSaveData_OpenNewFileForWrite((U16       *)u16FileName,
UnicodeLen((S8*)u16FileName));
        if(u8HandleNo != FCTRL_INVALID_FILE_HANDLE)
        {
            msAPI_MIU_Copy((_VA2PA((U32)(&Index))), ((CIPLUST_KEY_BUFFER_MEMORY_TYPE & MIU1) ?
(CIPLUST_KEY_BUFFER_ADR|   MIU_INTERVAL)   :   (CIPLUST_KEY_BUFFER_ADR)),   (U32)(sizeof(U8)),
MIU_SDRAM2SDRAM);
            msAPI_FCtrl_FileWrite(u8HandleNo,((CIPLUST_KEY_BUFFER_MEMORY_TYPE   &   MIU1)   ?
(CIPLUST_KEY_BUFFER_ADR| MIU_INTERVAL) : (CIPLUST_KEY_BUFFER_ADR)),(U32)(sizeof(U8)));
         }
        else
            return false;
    }
    else
    {
        printf("\r\n exist index file open for read\n");
        u8HandleNo = msAPI_FCtrl_FileOpen(&fileEntrytemp, OPEN_MODE_FOR_READ);
    }

     i = msAPI_FCtrl_FileLength(u8HandleNo);

     msAPI_FCtrl_FileRead(u8HandleNo,((CIPLUST_KEY_BUFFER_MEMORY_TYPE      &      MIU1)      ?
(CIPLUST_KEY_BUFFER_ADR| MIU_INTERVAL) : (CIPLUST_KEY_BUFFER_ADR)), (U32)(i));
     msAPI_FCtrl_FileClose(u8HandleNo);
     msAPI_MIU_Copy(((CIPLUST_KEY_BUFFER_MEMORY_TYPE   &   MIU1)   ?   (CIPLUST_KEY_BUFFER_ADR|
MIU_INTERVAL)     :     (CIPLUST_KEY_BUFFER_ADR)),(_VA2PA((U32)(u8KeyFileName))),     (U32)(i),
MIU_SDRAM2SDRAM);

     for(j=0;j<i;j++)
        {
            *u32FileIndex +=((u8KeyFileName[i-j-1]-0x30)*AddressOffSet);
            AddressOffSet *=10;
        }

    U32 u32Temp;

    u32Temp = *u32FileIndex ;
    while(u32Temp)
    {
        u32Temp /= 10;
        u8KeyLength++;
    }
    u32Temp = *u32FileIndex ;
    for(i=1;i<=u8KeyLength;i++)
    {
        u8KeyFileName[u8KeyLength-i]=(u32Temp%10 + 0x30);
        u32Temp /=10;
    }
     u8KeyFileName[u8KeyLength] = ’.’;
     u8KeyLength++;
        u8KeyFileName[u8KeyLength] = ’b’;
     u8KeyLength++;
        u8KeyFileName[u8KeyLength] = ’i’;
     u8KeyLength++;
        u8KeyFileName[u8KeyLength] = ’n’;
      *u32FileIndex= *u32FileIndex+1;
    return TRUE;
}
#endif
```

如何生成 CI_PLUS KEY 的 BIN 档文件

1. 准备资料：

工作前需要客户提供购买的 KEY 原始文件，以及附带文件，以 M013 客户为例，客户提供了俩个文件夹“Batch-20110309-10000bin.rar”和“other file needed”，附带文件夹中必须包含三个文件“cert.der”，“ciplus_root.crt” 和“license_constants_prod_host_manufacturers.txt”，其中前俩个是客户信息，相同客户的这俩个文件可能会相同，第三个文件是本次购买 KEY 的详细信息，其中有一些数组，下面会讲到怎样的用法。

2. 将我们自己修改后的“polarssl.rar”文件解压到 Z 盘，打开 SOURCE INSIGHT 工程，打开 SECURE.C 文件，将_u8agDH_p【】，_u8agDH_g[],_u8agDH_q[],U8 _u8agSIV[],U8 _u8agPRNGSeed[],U8 _gu8aSLK[],U8 _gu8Aclk[],这几个文件的内容修改成“license_constants_prod_host_manufacturers.txt”文件中对应数组的内容。注意_gu8aAesXcbcKey[16]，U8 _gu8aAesCbcKey[16] 和 U8 _gu8aAesCbcIV[16]这三个数组，是我们为客户添加的加密措施，不同客户这几个数组可以不同，但是长度一定要相同，现在的内容格式是数组前面几个值与客户名称 ASCII 码一致。
3. 进入 Z 盘，进入“polarssl”第一层目录，运行“make clean”和”make”命令，在\programs\ciplus 目录下生成 SECURE 文件。并将 KEY 原始文件附带文件夹中“cert.der”， “ciplus_root.crt”复制到此文件夹下。在此路径下新建文件夹并命名为 key,将 KEY 原始文件拷贝到 key 文件夹。
4. 在此路径下运行“./tt.sh 1 10”，其中后面这俩个参数分辨是生成 BIN 的起始序号，和生成个数。
5. 命令运行后，将会生成 3 个新文件夹，keyto ,keybin,keybin2,同时原有 key 文件夹内容复制到 keyto 文件，keybin 生成了与原有 KEY 名称一样的 BIN 档，keybin2 将生成按照我们命名方式的 BIN 文件。

   针对圣亚客户，我们只需要客户提供按照客户提供的 license_constants_prod_host_manufacturers.txt 文件生成 SECURE 文件给客户既可。

   tt.sh，是我们自己制作的批处理文件，以乐新客户使用为准。

   具体的客户那些文件就不上传了。

Peixl 干扰问题

此问题我们做过如下实验：首先在非 DTV/C/S 下关闭

TS CLK,导入了你客户调节后的寄存器，去掉电容，用频谱仪分析干扰等。综合最近的一系列反馈和我们所做的实验总结如下：

有电容时 插卡 信号源用码流电脑播放 0x100B56 0x100B58 的值写成 0000 画面无马赛克 ，写成 0F01 有你提到的马赛克

有电容时 无卡 信号源用码流电脑播放 0x100B56 0x100B58 的值写成 0000 或者 0F01 正常

无电容时 插卡 信号源用码流电脑播放 0x100B56 0x100B58 的值写成 0000 有马赛克，0F01 正常

无电容时 无卡 信号源用码流电脑播放 0x100B56 0x100B58 的值成 0000 或者 0F01 正常

有电容时 插卡 信号源用实地信号 0x100B56 0x100B58 的值写成 0000 画面有马赛克 ，写成 0F01 无马赛克

有电容时 无卡 信号源用实地信号 0x100B56 0x100B58 的值写成 0000 有马赛克，0F01 正常

无电容时 插卡 信号源用实地信号 0x100B56 0x100B58 的值写成 0000 或者 0F01 正常 ，但根据你客户反馈写成 0F01 能解决 piexl 问题，此后测试你客户又发现有。

无电容时 无卡 信号源用实地信号 0x100B56 0x100B58 的值写成 0000 或者 0F01 正常

计划周六去你们那边用实地信号和码流电脑综合调试一下，得出结论。

客户反映有 PEIXL 问题，具体的画面没看到过也无从得知，做了如下措施客户反馈解决。

检测 CI 卡时判断是否写入相关寄存器

```
插卡是          MDrv_Write2Byte(0x100B56, 0x0F01);//
                MDrv_Write2Byte(0x100B58, 0x0F01);//
拔卡            MDrv_Write2Byte(0x100B56, 0x0000);//
                MDrv_Write2Byte(0x100B58, 0x0000);//
```

所有相关寄存器：

TS CLK 的调整方法(8 Bit Address)：

BK1033_00 低 8 位。

默认值是 0x13，输出幅度大约是 7.2MHz 调整得越大，输出的 TS CLK 幅度越低，例如输入 0x16，输出幅度大约是 6.26MHz.

计算公式是：ts_clk=288/(2*(0x16+1))=6.26MHz

TS Phase 的调整方法(8 Bit Address)：

内置 Demod:

0x103300[12] = 1，0x10330a[12:8]，从 0~31 一个个去 try，看哪个值 OK. (phase 值)

外挂 demod 或者插了 CI 卡：

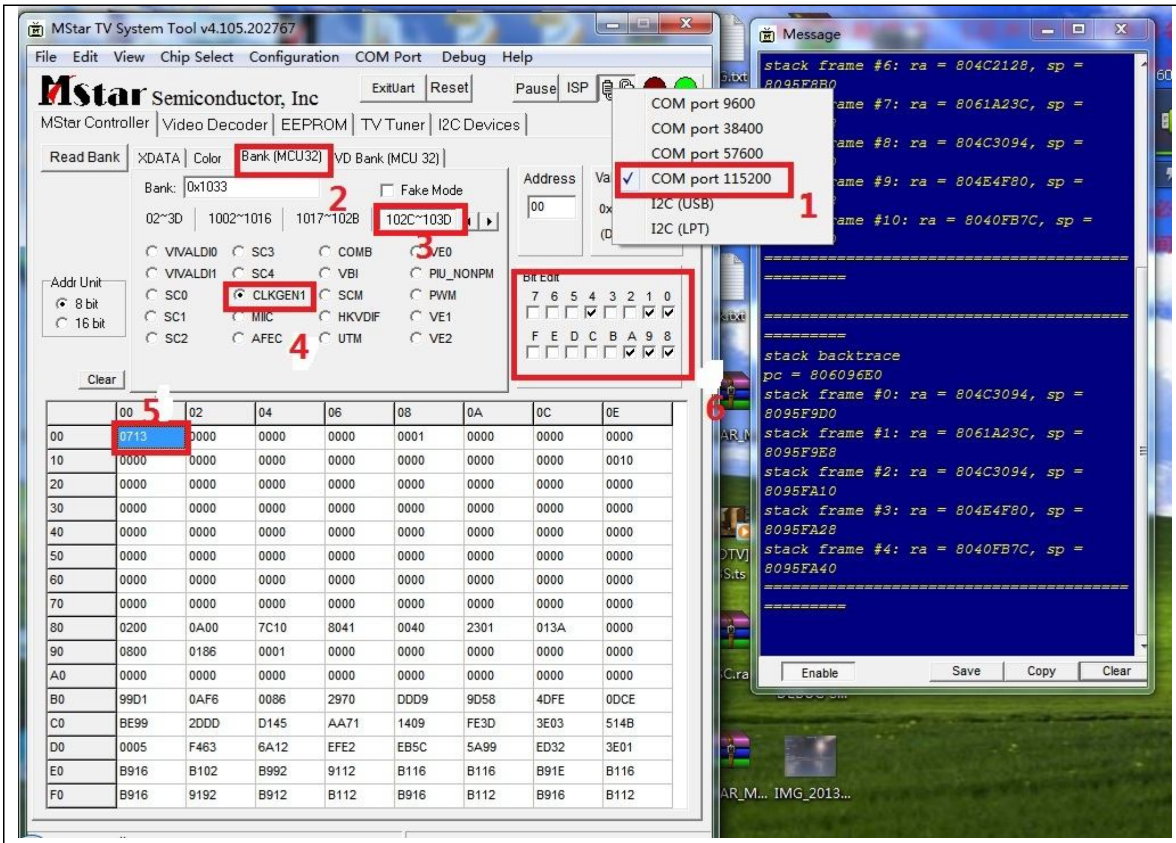
0x100B56[0] = 1，0x100B56[11:8]，從 0 ~15 一個個試,何者 OK. (phase 值)

TS1 的 Drving 的调整方法(16 Bit Address)

101E09[10 : 0]

PCM 的 Drving 的调整方法(16 Bit Address)

101E08[15:8]


MStar TV System Tool v4.105.202767
File Edit View Chip Select Configuration COM Port Debug Help
MStar Semiconductor, Inc
ExitUart Reset Pause ISP
MStar Controller | Video Decoder | EEPROM | TV Tuner | I2C Devices
Read Bank | XDATA | Color | Bank (MCU32) | VD Bank (MCU 32)
COM port 9600
COM port 38400
COM port 57600
✓ COM port 115200
I2C (USB)
I2C (LPT)
1
2
3
4
5
6
Address
Clear
Bit Edit
Message
Enable Save Copy Clear

Bank: 0x1033 □ Fake Mode

02~3D | 1002~1016 | 1017~102B | 102C~103D

Address: 00

○ VIVALDI0	○ SC3	○ COMB	○ VE0
○ VIVALDI1	○ SC4	○ VBI	○ PIU_NONPM
○ SC0	● CLKGEN1	○ SCM	○ PWM
○ SC1	○ MIIC	○ HKVDIF	○ VE1
○ SC2	○ AFEC	○ UTM	○ VE2

Addr Unit: ● 8 bit ○ 16 bit

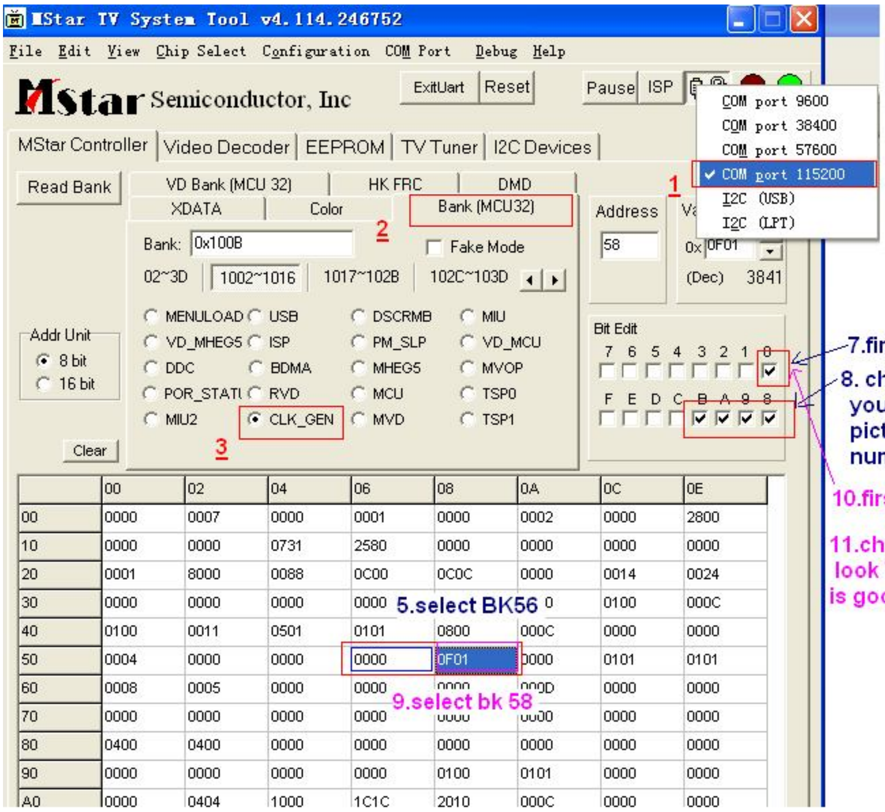
Bit Edit

7	6	5	4	3	2	1	0
□	□	□	☑	□	□	☑	☑

F	E	D	C	B	A	9	8
□	□	□	□	□	☑	☑	☑

	00	02	04	06	08	0A	0C	0E
00	0713	0000	0000	0000	0001	0000	0000	0000
10	0000	0000	0000	0000	0000	0000	0000	0010
20	0000	0000	0000	0000	0000	0000	0000	0000
30	0000	0000	0000	0000	0000	0000	0000	0000
40	0000	0000	0000	0000	0000	0000	0000	0000
50	0000	0000	0000	0000	0000	0000	0000	0000
60	0000	0000	0000	0000	0000	0000	0000	0000
70	0000	0000	0000	0000	0000	0000	0000	0000
80	0200	0A00	7C10	8041	0040	2301	013A	0000
90	0800	0186	0001	0000	0000	0000	0000	0000
A0	0000	0000	0000	0000	0000	0000	0000	0000
B0	99D1	0AF6	0086	2970	DDD9	9D58	4DFE	0DCE
C0	BE99	2DDD	D145	AA71	1409	FE3D	3E03	514B
D0	0005	F463	6A12	EFE2	EB5C	5A99	ED32	3E01
E0	B916	B102	B992	9112	B116	B116	B91E	B116
F0	B916	9192	B912	B112	B916	B112	B916	B112

```
stack frame #6: ra = 804C2128, sp =
8095F8B0
ame #7: ra = 8061A23C, sp =
ame #8: ra = 804C3094, sp =
ame #9: ra = 804E4F80, sp =
ame #10: ra = 8040FB7C, sp =
==================================================
==========

==================================================
==========
stack backtrace
pc = 806096E0
stack frame #0: ra = 804C3094, sp =
8095F9D0
stack frame #1: ra = 8061A23C, sp =
8095F9E8
stack frame #2: ra = 804C3094, sp =
8095FA10
stack frame #3: ra = 804E4F80, sp =
8095FA28
stack frame #4: ra = 8040FB7C, sp =
8095FA40
==================================================
==========
```


MStar TV System Tool v4.114.246752
File Edit View Chip Select Configuration COM Port Debug Help
MStar Semiconductor, Inc
ExitUart Reset Pause ISP
MStar Controller | Video Decoder | EEPROM | TV Tuner | I2C Devices
Read Bank | VD Bank (MCU 32) | HK FRC | DMD | XDATA | Color | Bank (MCU32)
COM port 9600
COM port 38400
COM port 57600
✓ COM port 115200
I2C (USB)
I2C (LPT)
1
2
3
Address
Clear
Bit Edit

Bank: 0x100B □ Fake Mode

02~3D | 1002~1016 | 1017~102B | 102C~103D

Address: 58 0x 0F01 (Dec) 3841

○ MENULOAD	○ USB	○ DSCRMB	○ MIU
○ VD_MHEG5	○ ISP	○ PM_SLP	○ VD_MCU
○ DDC	○ BDMA	○ MHEG5	○ MVOP
○ POR_STATU	○ RVD	○ MCU	○ TSP0
○ MIU2	● CLK_GEN	○ MVD	○ TSP1

Addr Unit: ● 8 bit ○ 16 bit

Bit Edit

7	6	5	4	3	2	1	0
□	□	□	□	□	□	□	☑

F	E	D	C	B	A	9	8
□	□	□	□	☑	☑	☑	☑

	00	02	04	06	08	0A	0C	0E
00	0000	0007	0000	0001	0000	0002	0000	2800
10	0000	0000	0731	2580	0000	0000	0000	0000
20	0001	8000	0088	0C00	0C0C	0000	0014	0024
30	0000	0000	0000	0000	[illegible]	[illegible]	0100	000C
40	0100	0011	0501	0101	0800	000C	0000	0000
50	0004	0000	0000	0000	0F01	0000	0101	0101
60	0008	0005	0000	0000	0000	000D	0000	0000
70	0000	0000	0000	0000	0000	0000	0000	0000
80	0400	0400	0000	0000	0000	0000	0000	0000
90	0000	0000	0000	0000	0100	0101	0000	0000
A0	0000	0404	1000	1C1C	2010	000C	0000	0000

5.select BK56

9.select bk 58

7.first set bit0 ->1 like picture

8. chang bit[8 11] , like picture you need look TV picture ,if picture is good ,you save this num.

10.first set bit0 ->1

11.chang bit [8 11], you need look TV PICTURE, if picture is good ,you save this num

蔡敏淦
2013-12-05

深圳市鼎科实业有限公司 **程 序 文 件**		文件编号	RD-TBC
		版　　本	A/0
		制定日期	2012-7-30
文件名称	**调试报告**	页　　码	共　页，第　页

审核及见意：