Como descodificar o certificado DOCSIS para o modem colou o diagnóstico do estado

Índice

Introdução

Este documento descreve as etapas para descodificar o certificado DOCSIS para diagnosticar porque o Modems a cabo colou no estado do reject(pk) ou do w-reject(pk) no cable modem termination system (CMTS).

Informações de Apoio

Em diversos casos, o Modems termina acima no estado do reject(pk). Pode ser causado por circunstâncias específicas, por exemplo no certificado CM, o expedidor CM não combina o nome do sujeito de CA.

Por exemplo:

```
SLOT 5/0: May 10 10:13:48.272 CET: Got Issuer 0^A^A1^K0 ^F^CU^D^F^S^BTW1^\0^Z^F^CU^D
^S^SHitron Technologies1^O0
^F^CU^D^K^S^FDOCSIS1C0A^F^CU^D^C^S:Hitron Technologies Cable Modem Root Certificate Authority
from Certificate.
SLOT 5/0: May 10 10:13:48.272 CET: Got a new Invalid CM cert from a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.272 CET: CA Cert Subject does not match CM Cert Issuer
SLOT 5/0: May 10 10:13:48.272 CET: BPI+ CM Cert Dump:

SLOT 5/0: May 10 10:13:48.272 CET: Failed CM Issuer not found. CMTS sent AUTH reject.
SLOT 5/0: May 10 10:13:48.272 CET: Sending KEK REJECT.  Reason Code:6 Reason:16
SLOT 5/0: May 10 10:13:48.272 CET: BPI Authorization Reject Packet: a84e.3fdd.84c4
```

Esta saída não mostra claramente a causa de raiz do problema.

Este artigo pode ser usado para produzir um certificado legível (de que pode ser aberto pelo OpenSSL ou pelo KeyChain no Mac), a fim identificar a má combinação.

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Privacidade da linha base (BPI) no DOCSIS
- Cable modem termination system (CMTS)

  Dica: A fim obter a melhor compreensão da privacidade da linha base no DOCSIS, recomenda-se atravessar a privacidade da linha de base do DOCSIS 1.0 no artigo de Cisco CMTS.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

Descodifique o procedimento

A tarefa 1. recolhe os logs

No CMTS, a fim obter a cópia parcial da memória de HEX do certificado, você precisa de permitir os logs. Datilografe estes comandos.

```
debug cable mac-address <cm mac> ver
debug cable privacy
debug cable privacy tlvs
debug cable privacy auth-req
debug cable privacy auth-rep
debug cable privacy auth-rej
debug cable privacy auth-info
debug cable privacy ca-cert
debug cable bpi
```

O telnet à placa de linha e recolhe os logs da **PLACA DE LINHA no** CMTS.

```
CMTS#telnet 127.0.0.XY
Trying 127.0.0.XY ... Open

clc_X_Y>en
clc_X_Y#
clc_X_Y#show log
```

Você pode obter uma saída similar a esta.

```
SLOT 5/0: May 10 10:13:48.260 CET: BPI+ Manufacturer Cert Dump: a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.260 CET: CA Certificate Dump:
SLOT 5/0: May 10 10:13:48.260 CET: 0x0000: 30 82 03 22 30 82 02 0A A0 03 02 01 02 02 10 43
SLOT 5/0: May 10 10:13:48.260 CET: 0x0010: 64 B5 50 E8 ED 7E E5 57 14 5A C0 A2 67 52 EC 30
SLOT 5/0: May 10 10:13:48.260 CET: 0x0020: 0D 06 09 2A 86 48 86 F7 0D 01 01 05 05 00 30 6F
SLOT 5/0: May 10 10:13:48.260 CET: 0x0030: 31 0B 30 09 06 03 55 04 06 13 02 42 45 31 1F 30
SLOT 5/0: May 10 10:13:48.260 CET: 0x0040: 1D 06 03 55 04 0A 13 16 74 43 6F 6D 4C 61 62 73
```

SLOT 5/0: May 10 10:13:48.260 CET: 0x0050: 20 2D 20 45 75 72 6F 2D 44 4F 43 53 49 53 31 15
SLOT 5/0: May 10 10:13:48.260 CET: 0x0060: 30 13 06 03 55 04 0B 13 0C 43 61 62 6C 65 20 4D
SLOT 5/0: May 10 10:13:48.260 CET: 0x0070: 6F 64 65 6D 73 31 28 30 26 06 03 55 04 03 13 1F
SLOT 5/0: May 10 10:13:48.260 CET: 0x0080: 45 75 72 6F 2D 44 4F 43 53 49 53 20 43 61 62 6C
SLOT 5/0: May 10 10:13:48.260 CET: 0x0090: 65 20 4D 6F 64 65 6D 20 52 6F 6F 74 20 43 41 30
SLOT 5/0: May 10 10:13:48.260 CET: 0x00A0: 1E 17 0D 30 34 30 38 31 33 30 30 30 30 30 30 5A
SLOT 5/0: May 10 10:13:48.260 CET: 0x00B0: 17 0D 32 34 30 38 31 32 32 33 35 39 35 39 5A 30
SLOT 5/0: May 10 10:13:48.260 CET: 0x00C0: 81 86 31 0B 30 09 06 03 55 04 06 13 02 54 57 31
SLOT 5/0: May 10 10:13:48.260 CET: 0x00D0: 1C 30 1A 06 03 55 04 0A 13 13 48 69 74 72 6F 6E
SLOT 5/0: May 10 10:13:48.260 CET: 0x00E0: 20 54 65 63 68 6E 6F 6C 6F 67 69 65 73 31 14 30
SLOT 5/0: May 10 10:13:48.260 CET: 0x00F0: 12 06 03 55 04 0B 13 0B 45 75 72 6F 2D 44 4F 43
SLOT 5/0: May 10 10:13:48.260 CET: 0x0100: 53 49 53 31 43 30 41 06 03 55 04 03 13 3A 48 69
SLOT 5/0: May 10 10:13:48.260 CET: 0x0110: 74 72 6F 6E 20 54 65 63 68 6E 6F 6C 6F 67 69 65
SLOT 5/0: May 10 10:13:48.260 CET: 0x0120: 73 20 43 61 62 6C 65 20 4D 6F 64 65 6D 20 52 6F
SLOT 5/0: May 10 10:13:48.260 CET: 0x0130: 6F 74 20 43 65 72 74 69 66 69 63 61 74 65 20 41
SLOT 5/0: May 10 10:13:48.260 CET: 0x0140: 75 74 68 6F 72 69 74 79 30 81 9F 30 0D 06 09 2A
SLOT 5/0: May 10 10:13:48.260 CET: 0x0150: 86 48 86 F7 0D 01 01 01 05 00 03 81 8D 00 30 81
SLOT 5/0: May 10 10:13:48.260 CET: 0x0160: 89 02 81 81 00 B8 47 DA 9D F1 F6 30 1B 8E 79 BE
SLOT 5/0: May 10 10:13:48.260 CET: 0x0170: BE 10 C3 2D 9F 7D D6 C7 B2 50 16 AB 85 5C 1C 8C
SLOT 5/0: May 10 10:13:48.260 CET: 0x0180: 9E 6B F7 15 60 B2 53 F4 2F 6D 49 0C 2C 3E 76 88
SLOT 5/0: May 10 10:13:48.260 CET: 0x0190: 8A 8A 23 6B 25 47 61 AE B9 DF A8 A7 8C 4D 51 FB
SLOT 5/0: May 10 10:13:48.260 CET: 0x01A0: E6 C2 0F D9 C7 27 DD F7 D8 CC F0 D8 70 F8 75 75
SLOT 5/0: May 10 10:13:48.260 CET: 0x01B0: F3 D8 B7 80 C2 36 B0 53 02 A4 E9 84 02 5F 66 AE
SLOT 5/0: May 10 10:13:48.260 CET: 0x01C0: E7 59 9A 17 4A A0 B1 B4 BA F3 3B 63 C4 75 05 11
SLOT 5/0: May 10 10:13:48.260 CET: 0x01D0: 40 F1 EB B3 C8 A0 E8 AD 6E 1B 59 CC 41 20 F8 94
SLOT 5/0: May 10 10:13:48.260 CET: 0x01E0: B3 94 23 A2 99 02 03 01 00 01 A3 26 30 24 30 12
SLOT 5/0: May 10 10:13:48.260 CET: 0x01F0: 06 03 55 1D 13 01 01 FF 04 08 30 06 01 01 FF 02
SLOT 5/0: May 10 10:13:48.264 CET: 0x0200: 01 00 30 0E 06 03 55 1D 0F 01 01 FF 04 04 03 02
SLOT 5/0: May 10 10:13:48.264 CET: 0x0210: 01 06 30 0D 06 09 2A 86 48 86 F7 0D 01 01 05 05
SLOT 5/0: May 10 10:13:48.264 CET: 0x0220: 00 03 82 01 01 00 09 DB 24 B9 46 76 D7 D0 9F 70
SLOT 5/0: May 10 10:13:48.264 CET: 0x0230: 86 59 ED 7F 9B AC 96 FD AE 19 DD B3 51 3B A5 C0
SLOT 5/0: May 10 10:13:48.264 CET: 0x0240: 98 DA 80 2B 53 26 42 FA 6A 11 9F 6D 16 6F 76 F8
SLOT 5/0: May 10 10:13:48.264 CET: 0x0250: 9A F3 81 53 E8 DB EF 22 DF AC 3F 57 78 0E 70 78
SLOT 5/0: May 10 10:13:48.264 CET: 0x0260: 07 30 1D FF 19 70 34 E5 7A 52 47 99 B0 EE 7F EA
SLOT 5/0: May 10 10:13:48.264 CET: 0x0270: 23 99 DF CB 72 FF 0D BE AB 68 20 9F 16 C0 7C 69
SLOT 5/0: May 10 10:13:48.264 CET: 0x0280: 88 2D 00 6A AF 4B FF 93 A5 07 D3 F2 A8 F9 5B C4
SLOT 5/0: May 10 10:13:48.264 CET: 0x0290: DD 9F BF 49 36 C4 12 8A 64 C8 35 41 BB E2 B9 9B
SLOT 5/0: May 10 10:13:48.264 CET: 0x02A0: 52 45 67 38 DC 92 55 E3 33 A4 70 68 FC E7 6E 54
SLOT 5/0: May 10 10:13:48.264 CET: 0x02B0: 96 CA 89 B4 65 8B 2C AA 58 24 FC 4D 68 D7 84 4E
SLOT 5/0: May 10 10:13:48.264 CET: 0x02C0: 36 3B B3 CA 9A 42 13 B1 FF 8C 66 D8 52 10 56 74
SLOT 5/0: May 10 10:13:48.264 CET: 0x02D0: C7 DD 58 C3 EE 9D E3 65 E6 C1 5D B9 75 C2 A8 C9
SLOT 5/0: May 10 10:13:48.264 CET: 0x02E0: 54 5B A1 85 38 3B E1 E1 DC 55 5D 3E DD 90 ED F8
SLOT 5/0: May 10 10:13:48.264 CET: 0x02F0: 3A B0 68 93 E9 4A C2 D4 7F DC 90 E3 86 E2 CF C3
SLOT 5/0: May 10 10:13:48.264 CET: 0x0300: F2 A3 92 84 B3 A3 9A F8 71 30 F8 24 71 C2 07 BD
SLOT 5/0: May 10 10:13:48.264 CET: 0x0310: E8 6C 3C F7 FC 82 08 86 84 84 1B C4 D8 97 D3 50
SLOT 5/0: May 10 10:13:48.264 CET: 0x0320: 59 72 2D D5 4C 0B
SLOT 5/0: May 10 10:13:48.264 CET: Found existing manufacturer certificate for a84e.3fdd.84c4 with subject cn=Hitron Technologies Cable Modem Root Certificate Authority,ou=Euro-DOCSIS,o=Hitron Technologies,c=TW
SLOT 5/0: May 10 10:13:48.264 CET: BPI: setting a84e.3fdd.84c4 caidx:3

SLOT 5/0: May 10 10:13:48.264 CET: Mfg serial no. from a84e.3fdd.84c4 certificate: 4364B550E8ED7EE557145AC0A26752EC
SLOT 5/0: May 10 10:13:48.264 CET: Finger print of a84e.3fdd.84c4 manufacturer certificate matched.
SLOT 5/0: May 10 10:13:48.264 CET: cr10k_clc_snmp_bpiplus_broadcast_cert() CA idx:3 state:Chained rowStatus:Active prov:0 len:1078 idx:3 state:Chained rowState:Active prov:0 learn:1 idx:3
SLOT 5/0: May 10 10:13:48.268 CET: BPI: Sent CA Cert to RP successfully.
SLOT 5/0: May 10 10:13:48.268 CET: Success in validating AUTH Info message from a84e.3fdd.84c4.
SLOT 5/0: May 10 10:13:48.268 CET: CMTS Received AUTH REQ from a84e.3fdd.84c4.
SLOT 5/0: May 10 10:13:48.268 CET: BPI Authorization Request Packet: a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.268 CET: BPKM Attributes: a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.268 CET: Found COMPOUND CM Identification (length = 173):

```
SLOT 5/0: May 10 10:13:48.268 CET:  Found Serial Number (length = 12):
SLOT 5/0: May 10 10:13:48.268 CET:     32353331 36433030  38303433
SLOT 5/0: May 10 10:13:48.268 CET:  Found Manufacturer ID (length = 3):
SLOT 5/0: May 10 10:13:48.268 CET:     0050F1
SLOT 5/0: May 10 10:13:48.268 CET:  Found MAC Address (length = 6):
SLOT 5/0: May 10 10:13:48.268 CET:     A84E3FDD 84C4
SLOT 5/0: May 10 10:13:48.268 CET:  Found RSA Public Key (length = 140):
SLOT 5/0: May 10 10:13:48.268 CET:     30818902 818100B0  D4F2B649 87FCE340
SLOT 5/0: May 10 10:13:48.268 CET:     B21FB1E0 8CFE04DD  DB3D05D5 34170886
SLOT 5/0: May 10 10:13:48.268 CET:     7623EE25 4E4A61FC  6D134830 55F402CF
SLOT 5/0: May 10 10:13:48.268 CET:     89B11B34 867B3EF7  D9FE6CBE 8B4C251F
SLOT 5/0: May 10 10:13:48.268 CET:     DA5A2E47 D65C2120  8EFC72E2 238D5443
SLOT 5/0: May 10 10:13:48.268 CET:     786F151A A7FE6C21  371957DD 3FEB8435
SLOT 5/0: May 10 10:13:48.268 CET:     8AA1B7A2 181DAF7A  4F7DD4E9 128D953C
SLOT 5/0: May 10 10:13:48.268 CET:     146B77F4 51A9F868  5D1A253F A9590AC0
SLOT 5/0: May 10 10:13:48.268 CET:     F69D24DF 2B84C102  03010001
SLOT 5/0: May 10 10:13:48.268 CET:  Found CM Certificate (length = 652):
SLOT 5/0: May 10 10:13:48.268 CET:     30820288 308201F1  A0030201 02020C41
SLOT 5/0: May 10 10:13:48.268 CET:     38344533 46444438  34433430 0D06092A
SLOT 5/0: May 10 10:13:48.268 CET:     864886F7 0D010105  05003081 81310B30
SLOT 5/0: May 10 10:13:48.268 CET:     09060355 04061302  5457311C 301A0603
SLOT 5/0: May 10 10:13:48.268 CET:     55040A13 13486974  726F6E20 54656368
SLOT 5/0: May 10 10:13:48.268 CET:     6E6F6C6F 67696573  310F300D 06035504
SLOT 5/0: May 10 10:13:48.268 CET:     0B130644 4F435349  53314330 41060355
SLOT 5/0: May 10 10:13:48.268 CET:     0403133A 48697472  6F6E2054 6563686E
SLOT 5/0: May 10 10:13:48.268 CET:     6F6C6F67 69657320  4361626C 65204D6F
SLOT 5/0: May 10 10:13:48.268 CET:     64656D20 526F6F74  20436572 74696669
SLOT 5/0: May 10 10:13:48.268 CET:     63617465 20417574  686F7269 7479301E
SLOT 5/0: May 10 10:13:48.268 CET:     170D3137 30313031  30303030 30305A17
SLOT 5/0: May 10 10:13:48.268 CET:     0D333631 32323832  33353935 395A3081
SLOT 5/0: May 10 10:13:48.268 CET:     86310B30 09060355  04061302 5457311C
SLOT 5/0: May 10 10:13:48.268 CET:     301A0603 55040A13  13486974 726F6E20
SLOT 5/0: May 10 10:13:48.268 CET:     54656368 6E6F6C6F  67696573 313D303B
SLOT 5/0: May 10 10:13:48.268 CET:     06035504 0B13344E  6F2E2034 302C2057
SLOT 5/0: May 10 10:13:48.268 CET:     752D6B75 6E672035  74682052 642E2C20
SLOT 5/0: May 10 10:13:48.268 CET:     57752D6B 752C2054  61697065 69204873
SLOT 5/0: May 10 10:13:48.268 CET:     69656E2C 20546169  77616E31 1A301806
SLOT 5/0: May 10 10:13:48.268 CET:     03550403 13114138  3A34453A 33463A44
SLOT 5/0: May 10 10:13:48.268 CET:     443A3834 3A433430  819F300D 06092A86
SLOT 5/0: May 10 10:13:48.268 CET:     4886F70D 01010105  0003818D 00308189
SLOT 5/0: May 10 10:13:48.268 CET:     02818100 B0D4F2B6  4987FCE3 40B21FB1
SLOT 5/0: May 10 10:13:48.268 CET:     E08CFE04 DDDB3D05  D5341708 867623EE
SLOT 5/0: May 10 10:13:48.268 CET:     254E4A61 FC6D1348  3055F402 CF89B11B
SLOT 5/0: May 10 10:13:48.268 CET:     34867B3E F7D9FE6C  BE8B4C25 1FDA5A2E
SLOT 5/0: May 10 10:13:48.268 CET:     47D65C21 208EFC72  E2238D54 43786F15
SLOT 5/0: May 10 10:13:48.268 CET:     1AA7FE6C 21371957  DD3FEB84 358AA1B7
SLOT 5/0: May 10 10:13:48.268 CET:     A2181DAF 7A4F7DD4  E9128D95 3C146B77
SLOT 5/0: May 10 10:13:48.268 CET:     F451A9F8 685D1A25  3FA9590A C0F69D24
SLOT 5/0: May 10 10:13:48.268 CET:     DF2B84C1 02030100  01300D06 092A8648
SLOT 5/0: May 10 10:13:48.268 CET:     86F70D01 01050500  03818100 08DFC2DA
SLOT 5/0: May 10 10:13:48.268 CET:     8C3ECCDA 98289410  E1B8657A 9A3F220D
SLOT 5/0: May 10 10:13:48.268 CET:     AE368029 0E89923F  0DF09E06 8142BAB7
SLOT 5/0: May 10 10:13:48.268 CET:     E8A6D5B3 6D7604FF  6A07A8B8 409D0B0B
SLOT 5/0: May 10 10:13:48.268 CET:     6D568AF4 F9395199  AB54126C E9C22F1B
SLOT 5/0: May 10 10:13:48.268 CET:     6390543A 3B67EFB8  FCF0E755 F642E1E0
SLOT 5/0: May 10 10:13:48.268 CET:     273A3853 F4DDBFF1  391E63CE 8BB7BBC0
SLOT 5/0: May 10 10:13:48.268 CET:     8AFC59FC 767C3FA5  A5EB255C 8878F4AB
SLOT 5/0: May 10 10:13:48.272 CET:     63665AA9 CDCF779A  3DFE0C4C
SLOT 5/0: May 10 10:13:48.272 CET:  Found COMPOUND SA Capabilities (length = 13):
SLOT 5/0: May 10 10:13:48.272 CET:  Found Crypto Suite List (length = 6):
SLOT 5/0: May 10 10:13:48.272 CET:     01000200 0300
SLOT 5/0: May 10 10:13:48.272 CET:  Found BPI Version (length = 1):
SLOT 5/0: May 10 10:13:48.272 CET:     01
SLOT 5/0: May 10 10:13:48.272 CET:  Found SAID (length = 2):
```

```
SLOT 5/0: May 10 10:13:48.272 CET:     0000
SLOT 5/0: May 10 10:13:48.272 CET: END BPKM Attributes: a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.272 CET: Get a CM Certificate.
SLOT 5/0: May 10 10:13:48.272 CET: Cable5/0/12: Auth-Req contains 1 SID(s).
SLOT 5/0: May 10 10:13:48.272 CET: Cable5/0/12: AuthReq with NULL SAID - D3.0 modem.
SLOT 5/0: May 10 10:13:48.272 CET: EAE_BPI_REQ:  DISABLE a84e.3fdd.84c4 - OK
SLOT 5/0: May 10 10:13:48.272 CET: BPI_AES:  Encryption priority is: aes128-des56-des40.
SLOT 5/0: May 10 10:13:48.272 CET: BPI_AES:  AES is a candidate.
SLOT 5/0: May 10 10:13:48.272 CET: BPI Crypto Algorithm: sid:0 cfg_mod:1, cm_cap:0x7, assigned:3
aes_support:1
SLOT 5/0: May 10 10:13:48.272 CET: CMTS generated AUTH_KEY.
SLOT 5/0: May 10 10:13:48.272 CET: CMTS received 0 as primary SAID - D3.0
SLOT 5/0: May 10 10:13:48.272 CET:  CM state:2050 MAC:a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.272 CET: Parsed/Matched MAC Address:a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.272 CET: Got Issuer 0^A^A1^K0 ^F^CU^D^F^S^BTW1^\0^Z^F^CU^D
^S^SHitron Technologies1^O0
^F^CU^D^K^S^FDOCSIS1C0A^F^CU^D^C^S:Hitron Technologies Cable Modem Root Certificate Authority
from Certificate.
SLOT 5/0: May 10 10:13:48.272 CET: Got a new Invalid CM cert from a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.272 CET: CA Cert Subject does not match CM Cert Issuer
```

Você pode ver naqueles logs, isso lá é duas cópias parciais da memória de HEX separadas.

1. Cópia parcial da memória de HEX para o certificado de CA. Começa com uma linha na **descarga** corajosa do **certificado de CA:** .
2. Cópia parcial da memória de HEX para o certificado CM. Começa com uma linha no **certificado encontrado** corajoso **CM (comprimento = 652):**.

A tarefa 2. Sanitize os Certificados

Para que a descarga do certificado seja processada corretamente, você precisa de remover toda a informação extra e de manter somente os valores da cópia parcial da memória de HEX.

> Nota: O caso (superior e inferior) e os espaços na descarga do certificado são irrelevantes para este processo.

> Dica: Um rápido e uma maneira fácil remover toda a linha encabeçamentos (número de slot, timestamp, etc.) são guardar a chave ALT em um editor de texto, como sublime ou Notepad++.

Um exemplo da descarga do certificado de CA.

```
SLOT 5/0: May 10 10:13:48.260 CET: BPI+ Manufacturer Cert Dump: a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.260 CET: CA Certificate Dump:
SLOT 5/0: May 10 10:13:48.260 CET: 0x0000: 30 82 03 22 30 82 02 0A A0 03 02 01 02 02 10 43
SLOT 5/0: May 10 10:13:48.260 CET: 0x0010: 64 B5 50 E8 ED 7E E5 57 14 5A C0 A2 67 52 EC 30
SLOT 5/0: May 10 10:13:48.260 CET: 0x0020: 0D 06 09 2A 86 48 86 F7 0D 01 01 05 05 00 30 6F
SLOT 5/0: May 10 10:13:48.260 CET: 0x0030: 31 0B 30 09 06 03 55 04 06 13 02 42 45 31 1F 30
SLOT 5/0: May 10 10:13:48.260 CET: 0x0040: 1D 06 03 55 04 0A 13 16 74 43 6F 6D 4C 61 62 73
SLOT 5/0: May 10 10:13:48.260 CET: 0x0050: 20 2D 20 45 75 72 6F 2D 44 4F 43 53 49 53 31 15
SLOT 5/0: May 10 10:13:48.260 CET: 0x0060: 30 13 06 03 55 04 0B 13 0C 43 61 62 6C 65 20 4D
SLOT 5/0: May 10 10:13:48.260 CET: 0x0070: 6F 64 65 6D 73 31 28 30 26 06 03 55 04 03 13 1F
SLOT 5/0: May 10 10:13:48.260 CET: 0x0080: 45 75 72 6F 2D 44 4F 43 53 49 53 20 43 61 62 6C
SLOT 5/0: May 10 10:13:48.260 CET: 0x0090: 65 20 4D 6F 64 65 6D 20 52 6F 6F 74 20 43 41 30
SLOT 5/0: May 10 10:13:48.260 CET: 0x00A0: 1E 17 0D 30 34 30 38 31 33 30 30 30 30 30 30 5A
SLOT 5/0: May 10 10:13:48.260 CET: 0x00B0: 17 0D 32 34 30 38 31 32 32 33 35 39 35 39 5A 30
SLOT 5/0: May 10 10:13:48.260 CET: 0x00C0: 81 86 31 0B 30 09 06 03 55 04 06 13 02 54 57 31
```

SLOT 5/0: May 10 10:13:48.260 CET: 0x00D0: 1C 30 1A 06 03 55 04 0A 13 13 48 69 74 72 6F 6E
SLOT 5/0: May 10 10:13:48.260 CET: 0x00E0: 20 54 65 63 68 6E 6F 6C 6F 67 69 65 73 31 14 30
SLOT 5/0: May 10 10:13:48.260 CET: 0x00F0: 12 06 03 55 04 0B 13 0B 45 75 72 6F 2D 44 4F 43
SLOT 5/0: May 10 10:13:48.260 CET: 0x0100: 53 49 53 31 43 30 41 06 03 55 04 03 13 3A 48 69
SLOT 5/0: May 10 10:13:48.260 CET: 0x0110: 74 72 6F 6E 20 54 65 63 68 6E 6F 6C 6F 67 69 65
SLOT 5/0: May 10 10:13:48.260 CET: 0x0120: 73 20 43 61 62 6C 65 20 4D 6F 64 65 6D 20 52 6F
SLOT 5/0: May 10 10:13:48.260 CET: 0x0130: 6F 74 20 43 65 72 74 69 66 69 63 61 74 65 20 41
SLOT 5/0: May 10 10:13:48.260 CET: 0x0140: 75 74 68 6F 72 69 74 79 30 81 9F 30 0D 06 09 2A
SLOT 5/0: May 10 10:13:48.260 CET: 0x0150: 86 48 86 F7 0D 01 01 01 05 00 03 81 8D 00 30 81
SLOT 5/0: May 10 10:13:48.260 CET: 0x0160: 89 02 81 81 00 B8 47 DA 9D F1 F6 30 1B 8E 79 BE
SLOT 5/0: May 10 10:13:48.260 CET: 0x0170: BE 10 C3 2D 9F 7D D6 C7 B2 50 16 AB 85 5C 1C 8C
SLOT 5/0: May 10 10:13:48.260 CET: 0x0180: 9E 6B F7 15 60 B2 53 F4 2F 6D 49 0C 2C 3E 76 88
SLOT 5/0: May 10 10:13:48.260 CET: 0x0190: 8A 8A 23 6B 25 47 61 AE B9 DF A8 A7 8C 4D 51 FB
SLOT 5/0: May 10 10:13:48.260 CET: 0x01A0: E6 C2 0F D9 C7 27 DD F7 D8 CC F0 D8 70 F8 75 75
SLOT 5/0: May 10 10:13:48.260 CET: 0x01B0: F3 D8 B7 80 C2 36 B0 53 02 A4 E9 84 02 5F 66 AE
SLOT 5/0: May 10 10:13:48.260 CET: 0x01C0: E7 59 9A 17 4A A0 B1 B4 BA F3 3B 63 C4 75 05 11
SLOT 5/0: May 10 10:13:48.260 CET: 0x01D0: 40 F1 EB B3 C8 A0 E8 AD 6E 1B 59 CC 41 20 F8 94
SLOT 5/0: May 10 10:13:48.260 CET: 0x01E0: B3 94 23 A2 99 02 03 01 00 01 A3 26 30 24 30 12
SLOT 5/0: May 10 10:13:48.260 CET: 0x01F0: 06 03 55 1D 13 01 01 FF 04 08 30 06 01 01 FF 02
SLOT 5/0: May 10 10:13:48.264 CET: 0x0200: 01 00 30 0E 06 03 55 1D 0F 01 01 FF 04 04 03 02
SLOT 5/0: May 10 10:13:48.264 CET: 0x0210: 01 06 30 0D 06 09 2A 86 48 86 F7 0D 01 01 05 05
SLOT 5/0: May 10 10:13:48.264 CET: 0x0220: 00 03 82 01 01 00 09 DB 24 B9 46 76 D7 D0 9F 70
SLOT 5/0: May 10 10:13:48.264 CET: 0x0230: 86 59 ED 7F 9B AC 96 FD AE 19 DD B3 51 3B A5 C0
SLOT 5/0: May 10 10:13:48.264 CET: 0x0240: 98 DA 80 2B 53 26 42 FA 6A 11 9F 6D 16 6F 76 F8
SLOT 5/0: May 10 10:13:48.264 CET: 0x0250: 9A F3 81 53 E8 DB EF 22 DF AC 3F 57 78 0E 70 78
SLOT 5/0: May 10 10:13:48.264 CET: 0x0260: 07 30 1D FF 19 70 34 E5 7A 52 47 99 B0 EE 7F EA
SLOT 5/0: May 10 10:13:48.264 CET: 0x0270: 23 99 DF CB 72 FF 0D BE AB 68 20 9F 16 C0 7C 69
SLOT 5/0: May 10 10:13:48.264 CET: 0x0280: 88 2D 00 6A AF 4B FF 93 A5 07 D3 F2 A8 F9 5B C4
SLOT 5/0: May 10 10:13:48.264 CET: 0x0290: DD 9F BF 49 36 C4 12 8A 64 C8 35 41 BB E2 B9 9B
SLOT 5/0: May 10 10:13:48.264 CET: 0x02A0: 52 45 67 38 DC 92 55 E3 33 A4 70 68 FC E7 6E 54
SLOT 5/0: May 10 10:13:48.264 CET: 0x02B0: 96 CA 89 B4 65 8B 2C AA 58 24 FC 4D 68 D7 84 4E
SLOT 5/0: May 10 10:13:48.264 CET: 0x02C0: 36 3B B3 CA 9A 42 13 B1 FF 8C 66 D8 52 10 56 74
SLOT 5/0: May 10 10:13:48.264 CET: 0x02D0: C7 DD 58 C3 EE 9D E3 65 E6 C1 5D B9 75 C2 A8 C9
SLOT 5/0: May 10 10:13:48.264 CET: 0x02E0: 54 5B A1 85 38 3B E1 E1 DC 55 5D 3E DD 90 ED F8
SLOT 5/0: May 10 10:13:48.264 CET: 0x02F0: 3A B0 68 93 E9 4A C2 D4 7F DC 90 E3 86 E2 CF C3
SLOT 5/0: May 10 10:13:48.264 CET: 0x0300: F2 A3 92 84 B3 A3 9A F8 71 30 F8 24 71 C2 07 BD
SLOT 5/0: May 10 10:13:48.264 CET: 0x0310: E8 6C 3C F7 FC 82 08 86 84 84 1B C4 D8 97 D3 50
SLOT 5/0: May 10 10:13:48.264 CET: 0x0320: 59 72 2D D5 4C 0B
SLOT 5/0: May 10 10:13:48.264 CET: Found existing manufacturer certificate for a84e.3fdd.84c4 with subject cn=Hitron Technologies Cable Modem Root Certificate Authority,ou=Euro-DOCSIS,o=Hitron Technologies,c=TW
SLOT 5/0: May 10 10:13:48.264 CET: BPI: setting a84e.3fdd.84c4 caidx:3

SLOT 5/0: May 10 10:13:48.264 CET: Mfg serial no. from a84e.3fdd.84c4 certificate: 4364B550E8ED7EE557145AC0A26752EC
SLOT 5/0: May 10 10:13:48.264 CET: Finger print of a84e.3fdd.84c4 manufacturer certificate matched.
SLOT 5/0: May 10 10:13:48.264 CET: cr10k_clc_snmp_bpiplus_broadcast_cert() CA idx:3 state:Chained rowStatus:Active prov:0 len:1078 idx:3 state:Chained rowState:Active prov:0 learn:1 idx:3
SLOT 5/0: May 10 10:13:48.268 CET: BPI: Sent CA Cert to RP successfully.
SLOT 5/0: May 10 10:13:48.268 CET: Success in validating AUTH Info message from a84e.3fdd.84c4.
SLOT 5/0: May 10 10:13:48.268 CET: CMTS Received AUTH REQ from a84e.3fdd.84c4.
SLOT 5/0: May 10 10:13:48.268 CET: BPI Authorization Request Packet: a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.268 CET: BPKM Attributes: a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.268 CET: Found COMPOUND CM Identification (length = 173):
SLOT 5/0: May 10 10:13:48.268 CET: Found Serial Number (length = 12):
SLOT 5/0: May 10 10:13:48.268 CET: 32353331 36433030 38303433
SLOT 5/0: May 10 10:13:48.268 CET: Found Manufacturer ID (length = 3):
SLOT 5/0: May 10 10:13:48.268 CET: 0050F1
SLOT 5/0: May 10 10:13:48.268 CET: Found MAC Address (length = 6):
SLOT 5/0: May 10 10:13:48.268 CET: A84E3FDD 84C4
SLOT 5/0: May 10 10:13:48.268 CET: Found RSA Public Key (length = 140):
SLOT 5/0: May 10 10:13:48.268 CET: 30818902 818100B0 D4F2B649 87FCE340

```
SLOT 5/0: May 10 10:13:48.268 CET:     B21FB1E0 8CFE04DD  DB3D05D5 34170886
SLOT 5/0: May 10 10:13:48.268 CET:     7623EE25 4E4A61FC  6D134830 55F402CF
SLOT 5/0: May 10 10:13:48.268 CET:     89B11B34 867B3EF7  D9FE6CBE 8B4C251F
SLOT 5/0: May 10 10:13:48.268 CET:     DA5A2E47 D65C2120  8EFC72E2 238D5443
SLOT 5/0: May 10 10:13:48.268 CET:     786F151A A7FE6C21  371957DD 3FEB8435
SLOT 5/0: May 10 10:13:48.268 CET:     8AA1B7A2 181DAF7A  4F7DD4E9 128D953C
SLOT 5/0: May 10 10:13:48.268 CET:     146B77F4 51A9F868  5D1A253F A9590AC0
SLOT 5/0: May 10 10:13:48.268 CET:     F69D24DF 2B84C102  03010001
SLOT 5/0: May 10 10:13:48.268 CET:  Found CM Certificate (length = 652):
SLOT 5/0: May 10 10:13:48.268 CET:     30820288 308201F1  A0030201 02020C41
SLOT 5/0: May 10 10:13:48.268 CET:     38344533 46444438  34433430 0D06092A
SLOT 5/0: May 10 10:13:48.268 CET:     864886F7 0D010105  05003081 81310B30
SLOT 5/0: May 10 10:13:48.268 CET:     09060355 04061302  5457311C 301A0603
SLOT 5/0: May 10 10:13:48.268 CET:     55040A13 13486974  726F6E20 54656368
SLOT 5/0: May 10 10:13:48.268 CET:     6E6F6C6F 67696573  310F300D 06035504
SLOT 5/0: May 10 10:13:48.268 CET:     0B130644 4F435349  53314330 41060355
SLOT 5/0: May 10 10:13:48.268 CET:     0403133A 48697472  6F6E2054 6563686E
SLOT 5/0: May 10 10:13:48.268 CET:     6F6C6F67 69657320  4361626C 65204D6F
SLOT 5/0: May 10 10:13:48.268 CET:     64656D20 526F6F74  20436572 74696669
SLOT 5/0: May 10 10:13:48.268 CET:     63617465 20417574  686F7269 7479301E
SLOT 5/0: May 10 10:13:48.268 CET:     170D3137 30313031  30303030 30305A17
SLOT 5/0: May 10 10:13:48.268 CET:     0D333631 32323832  33353935 395A3081
SLOT 5/0: May 10 10:13:48.268 CET:     86310B30 09060355  04061302 5457311C
SLOT 5/0: May 10 10:13:48.268 CET:     301A0603 55040A13  13486974 726F6E20
SLOT 5/0: May 10 10:13:48.268 CET:     54656368 6E6F6C6F  67696573 313D303B
SLOT 5/0: May 10 10:13:48.268 CET:     06035504 0B13344E  6F2E2034 302C2057
SLOT 5/0: May 10 10:13:48.268 CET:     752D6B75 6E672035  74682052 642E2C20
SLOT 5/0: May 10 10:13:48.268 CET:     57752D6B 752C2054  61697065 69204873
SLOT 5/0: May 10 10:13:48.268 CET:     69656E2C 20546169  77616E31 1A301806
SLOT 5/0: May 10 10:13:48.268 CET:     03550403 13114138  3A34453A 33463A44
SLOT 5/0: May 10 10:13:48.268 CET:     443A3834 3A433430  819F300D 06092A86
SLOT 5/0: May 10 10:13:48.268 CET:     4886F70D 01010105  0003818D 00308189
SLOT 5/0: May 10 10:13:48.268 CET:     02818100 B0D4F2B6  4987FCE3 40B21FB1
SLOT 5/0: May 10 10:13:48.268 CET:     E08CFE04 DDDB3D05  D5341708 867623EE
SLOT 5/0: May 10 10:13:48.268 CET:     254E4A61 FC6D1348  3055F402 CF89B11B
SLOT 5/0: May 10 10:13:48.268 CET:     34867B3E F7D9FE6C  BE8B4C25 1FDA5A2E
SLOT 5/0: May 10 10:13:48.268 CET:     47D65C21 208EFC72  E2238D54 43786F15
SLOT 5/0: May 10 10:13:48.268 CET:     1AA7FE6C 21371957  DD3FEB84 358AA1B7
SLOT 5/0: May 10 10:13:48.268 CET:     A2181DAF 7A4F7DD4  E9128D95 3C146B77
SLOT 5/0: May 10 10:13:48.268 CET:     F451A9F8 685D1A25  3FA9590A C0F69D24
SLOT 5/0: May 10 10:13:48.268 CET:     DF2B84C1 02030100  01300D06 092A8648
SLOT 5/0: May 10 10:13:48.268 CET:     86F70D01 01050500  03818100 08DFC2DA
SLOT 5/0: May 10 10:13:48.268 CET:     8C3ECCDA 98289410  E1B8657A 9A3F220D
SLOT 5/0: May 10 10:13:48.268 CET:     AE368029 0E89923F  0DF09E06 8142BAB7
SLOT 5/0: May 10 10:13:48.268 CET:     E8A6D5B3 6D7604FF  6A07A8B8 409D0B0B
SLOT 5/0: May 10 10:13:48.268 CET:     6D568AF4 F9395199  AB54126C E9C22F1B
SLOT 5/0: May 10 10:13:48.268 CET:     6390543A 3B67EFB8  FCF0E755 F642E1E0
SLOT 5/0: May 10 10:13:48.268 CET:     273A3853 F4DDBFF1  391E63CE 8BB7BBC0
SLOT 5/0: May 10 10:13:48.268 CET:     8AFC59FC 767C3FA5  A5EB255C 8878F4AB
SLOT 5/0: May 10 10:13:48.272 CET:     63665AA9 CDCF779A  3DFE0C4C
SLOT 5/0: May 10 10:13:48.272 CET:  Found COMPOUND SA Capabilities (length = 13):
SLOT 5/0: May 10 10:13:48.272 CET:  Found Crypto Suite List (length = 6):
SLOT 5/0: May 10 10:13:48.272 CET:     01000200 0300
SLOT 5/0: May 10 10:13:48.272 CET:  Found BPI Version (length = 1):
SLOT 5/0: May 10 10:13:48.272 CET:     01
SLOT 5/0: May 10 10:13:48.272 CET:  Found SAID (length = 2):
SLOT 5/0: May 10 10:13:48.272 CET:     0000
SLOT 5/0: May 10 10:13:48.272 CET: END BPKM Attributes: a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.272 CET: Get a CM Certificate.
SLOT 5/0: May 10 10:13:48.272 CET: Cable5/0/12: Auth-Req contains 1 SID(s).
SLOT 5/0: May 10 10:13:48.272 CET: Cable5/0/12: AuthReq with NULL SAID - D3.0 modem.
SLOT 5/0: May 10 10:13:48.272 CET: EAE_BPI_REQ:  DISABLE a84e.3fdd.84c4 - OK
SLOT 5/0: May 10 10:13:48.272 CET: BPI_AES:  Encryption priority is: aes128-des56-des40.
SLOT 5/0: May 10 10:13:48.272 CET: BPI_AES:  AES is a candidate.
```

```
SLOT 5/0: May 10 10:13:48.272 CET: BPI Crypto Algorithm: sid:0 cfg_mod:1, cm_cap:0x7, assigned:3
aes_support:1
SLOT 5/0: May 10 10:13:48.272 CET: CMTS generated AUTH_KEY.
SLOT 5/0: May 10 10:13:48.272 CET: CMTS received 0 as primary SAID - D3.0
SLOT 5/0: May 10 10:13:48.272 CET:  CM state:2050 MAC:a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.272 CET: Parsed/Matched MAC Address:a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.272 CET: Got Issuer 0^A^A1^K0 ^F^CU^D^F^S^BTW1^\0^Z^F^CU^D
^S^SHitron Technologies1^O0
^F^CU^D^K^S^FDOCSIS1C0A^F^CU^D^C^S:Hitron Technologies Cable Modem Root Certificate Authority
from Certificate.
SLOT 5/0: May 10 10:13:48.272 CET: Got a new Invalid CM cert from a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.272 CET: CA Cert Subject does not match CM Cert Issuer
```

Salvar este arquivo com um nome **cacert.txt.**

Um exemplo da descarga do certificado CM.

```
SLOT 5/0: May 10 10:13:48.260 CET: BPI+ Manufacturer Cert Dump: a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.260 CET: CA Certificate Dump:
SLOT 5/0: May 10 10:13:48.260 CET: 0x0000: 30 82 03 22 30 82 02 0A A0 03 02 01 02 02 10 43
SLOT 5/0: May 10 10:13:48.260 CET: 0x0010: 64 B5 50 E8 ED 7E E5 57 14 5A C0 A2 67 52 EC 30
SLOT 5/0: May 10 10:13:48.260 CET: 0x0020: 0D 06 09 2A 86 48 86 F7 0D 01 01 05 05 00 30 6F
SLOT 5/0: May 10 10:13:48.260 CET: 0x0030: 31 0B 30 09 06 03 55 04 06 13 02 42 45 31 1F 30
SLOT 5/0: May 10 10:13:48.260 CET: 0x0040: 1D 06 03 55 04 0A 13 16 74 43 6F 6D 4C 61 62 73
SLOT 5/0: May 10 10:13:48.260 CET: 0x0050: 20 2D 20 45 75 72 6F 2D 44 4F 43 53 49 53 31 15
SLOT 5/0: May 10 10:13:48.260 CET: 0x0060: 30 13 06 03 55 04 0B 13 0C 43 61 62 6C 65 20 4D
SLOT 5/0: May 10 10:13:48.260 CET: 0x0070: 6F 64 65 6D 73 31 28 30 26 06 03 55 04 03 13 1F
SLOT 5/0: May 10 10:13:48.260 CET: 0x0080: 45 75 72 6F 2D 44 4F 43 53 49 53 20 43 61 62 6C
SLOT 5/0: May 10 10:13:48.260 CET: 0x0090: 65 20 4D 6F 64 65 6D 20 52 6F 6F 74 20 43 41 30
SLOT 5/0: May 10 10:13:48.260 CET: 0x00A0: 1E 17 0D 30 34 30 38 31 33 30 30 30 30 30 30 5A
SLOT 5/0: May 10 10:13:48.260 CET: 0x00B0: 17 0D 32 34 30 38 31 32 32 33 35 39 35 39 5A 30
SLOT 5/0: May 10 10:13:48.260 CET: 0x00C0: 81 86 31 0B 30 09 06 03 55 04 06 13 02 54 57 31
SLOT 5/0: May 10 10:13:48.260 CET: 0x00D0: 1C 30 1A 06 03 55 04 0A 13 13 48 69 74 72 6F 6E
SLOT 5/0: May 10 10:13:48.260 CET: 0x00E0: 20 54 65 63 68 6E 6F 6C 6F 67 69 65 73 31 14 30
SLOT 5/0: May 10 10:13:48.260 CET: 0x00F0: 12 06 03 55 04 0B 13 0B 45 75 72 6F 2D 44 4F 43
SLOT 5/0: May 10 10:13:48.260 CET: 0x0100: 53 49 53 31 43 30 41 06 03 55 04 03 13 3A 48 69
SLOT 5/0: May 10 10:13:48.260 CET: 0x0110: 74 72 6F 6E 20 54 65 63 68 6E 6F 6C 6F 67 69 65
SLOT 5/0: May 10 10:13:48.260 CET: 0x0120: 73 20 43 61 62 6C 65 20 4D 6F 64 65 6D 20 52 6F
SLOT 5/0: May 10 10:13:48.260 CET: 0x0130: 6F 74 20 43 65 72 74 69 66 69 63 61 74 65 20 41
SLOT 5/0: May 10 10:13:48.260 CET: 0x0140: 75 74 68 6F 72 69 74 79 30 81 9F 30 0D 06 09 2A
SLOT 5/0: May 10 10:13:48.260 CET: 0x0150: 86 48 86 F7 0D 01 01 01 05 00 03 81 8D 00 30 81
SLOT 5/0: May 10 10:13:48.260 CET: 0x0160: 89 02 81 81 00 B8 47 DA 9D F1 F6 30 1B 8E 79 BE
SLOT 5/0: May 10 10:13:48.260 CET: 0x0170: BE 10 C3 2D 9F 7D D6 C7 B2 50 16 AB 85 5C 1C 8C
SLOT 5/0: May 10 10:13:48.260 CET: 0x0180: 9E 6B F7 15 60 B2 53 F4 2F 6D 49 0C 2C 3E 76 88
SLOT 5/0: May 10 10:13:48.260 CET: 0x0190: 8A 8A 23 6B 25 47 61 AE B9 DF A8 A7 8C 4D 51 FB
SLOT 5/0: May 10 10:13:48.260 CET: 0x01A0: E6 C2 0F D9 C7 27 DD F7 D8 CC F0 D8 70 F8 75 75
SLOT 5/0: May 10 10:13:48.260 CET: 0x01B0: F3 D8 B7 80 C2 36 B0 53 02 A4 E9 84 02 5F 66 AE
SLOT 5/0: May 10 10:13:48.260 CET: 0x01C0: E7 59 9A 17 4A A0 B1 B4 BA F3 3B 63 C4 75 05 11
SLOT 5/0: May 10 10:13:48.260 CET: 0x01D0: 40 F1 EB B3 C8 A0 E8 AD 6E 1B 59 CC 41 20 F8 94
SLOT 5/0: May 10 10:13:48.260 CET: 0x01E0: B3 94 23 A2 99 02 03 01 00 01 A3 26 30 24 30 12
SLOT 5/0: May 10 10:13:48.260 CET: 0x01F0: 06 03 55 1D 13 01 01 FF 04 08 30 06 01 01 FF 02
SLOT 5/0: May 10 10:13:48.264 CET: 0x0200: 01 00 30 0E 06 03 55 1D 0F 01 01 FF 04 04 03 02
SLOT 5/0: May 10 10:13:48.264 CET: 0x0210: 01 06 30 0D 06 09 2A 86 48 86 F7 0D 01 01 05 05
SLOT 5/0: May 10 10:13:48.264 CET: 0x0220: 00 03 82 01 01 00 09 DB 24 B9 46 76 D7 D0 9F 70
SLOT 5/0: May 10 10:13:48.264 CET: 0x0230: 86 59 ED 7F 9B AC 96 FD AE 19 DD B3 51 3B A5 C0
SLOT 5/0: May 10 10:13:48.264 CET: 0x0240: 98 DA 80 2B 53 26 42 FA 6A 11 9F 6D 16 6F 76 F8
SLOT 5/0: May 10 10:13:48.264 CET: 0x0250: 9A F3 81 53 E8 DB EF 22 DF AC 3F 57 78 0E 70 78
SLOT 5/0: May 10 10:13:48.264 CET: 0x0260: 07 30 1D FF 19 70 34 E5 7A 52 47 99 B0 EE 7F EA
SLOT 5/0: May 10 10:13:48.264 CET: 0x0270: 23 99 DF CB 72 FF 0D BE AB 68 20 9F 16 C0 7C 69
SLOT 5/0: May 10 10:13:48.264 CET: 0x0280: 88 2D 00 6A AF 4B FF 93 A5 07 D3 F2 A8 F9 5B C4
SLOT 5/0: May 10 10:13:48.264 CET: 0x0290: DD 9F BF 49 36 C4 12 8A 64 C8 35 41 BB E2 B9 9B
SLOT 5/0: May 10 10:13:48.264 CET: 0x02A0: 52 45 67 38 DC 92 55 E3 33 A4 70 68 FC E7 6E 54
SLOT 5/0: May 10 10:13:48.264 CET: 0x02B0: 96 CA 89 B4 65 8B 2C AA 58 24 FC 4D 68 D7 84 4E
SLOT 5/0: May 10 10:13:48.264 CET: 0x02C0: 36 3B B3 CA 9A 42 13 B1 FF 8C 66 D8 52 10 56 74
```

SLOT 5/0: May 10 10:13:48.264 CET: 0x02D0: C7 DD 58 C3 EE 9D E3 65 E6 C1 5D B9 75 C2 A8 C9
SLOT 5/0: May 10 10:13:48.264 CET: 0x02E0: 54 5B A1 85 38 3B E1 E1 DC 55 5D 3E DD 90 ED F8
SLOT 5/0: May 10 10:13:48.264 CET: 0x02F0: 3A B0 68 93 E9 4A C2 D4 7F DC 90 E3 86 E2 CF C3
SLOT 5/0: May 10 10:13:48.264 CET: 0x0300: F2 A3 92 84 B3 A3 9A F8 71 30 F8 24 71 C2 07 BD
SLOT 5/0: May 10 10:13:48.264 CET: 0x0310: E8 6C 3C F7 FC 82 08 86 84 84 1B C4 D8 97 D3 50
SLOT 5/0: May 10 10:13:48.264 CET: 0x0320: 59 72 2D D5 4C 0B
SLOT 5/0: May 10 10:13:48.264 CET: Found existing manufacturer certificate for a84e.3fdd.84c4 with subject cn=Hitron Technologies Cable Modem Root Certificate Authority,ou=Euro-DOCSIS,o=Hitron Technologies,c=TW
SLOT 5/0: May 10 10:13:48.264 CET: BPI: setting a84e.3fdd.84c4 caidx:3

SLOT 5/0: May 10 10:13:48.264 CET: Mfg serial no. from a84e.3fdd.84c4 certificate: 4364B550E8ED7EE557145AC0A26752EC
SLOT 5/0: May 10 10:13:48.264 CET: Finger print of a84e.3fdd.84c4 manufacturer certificate matched.
SLOT 5/0: May 10 10:13:48.264 CET: cr10k_clc_snmp_bpiplus_broadcast_cert() CA idx:3 state:Chained rowStatus:Active prov:0 len:1078 idx:3 state:Chained rowState:Active prov:0 learn:1 idx:3
SLOT 5/0: May 10 10:13:48.268 CET: BPI: Sent CA Cert to RP successfully.
SLOT 5/0: May 10 10:13:48.268 CET: Success in validating AUTH Info message from a84e.3fdd.84c4.
SLOT 5/0: May 10 10:13:48.268 CET: CMTS Received AUTH REQ from a84e.3fdd.84c4.
SLOT 5/0: May 10 10:13:48.268 CET: BPI Authorization Request Packet: a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.268 CET: BPKM Attributes: a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.268 CET: Found COMPOUND CM Identification (length = 173):
SLOT 5/0: May 10 10:13:48.268 CET: Found Serial Number (length = 12):
SLOT 5/0: May 10 10:13:48.268 CET: 32353331 36433030 38303433
SLOT 5/0: May 10 10:13:48.268 CET: Found Manufacturer ID (length = 3):
SLOT 5/0: May 10 10:13:48.268 CET: 0050F1
SLOT 5/0: May 10 10:13:48.268 CET: Found MAC Address (length = 6):
SLOT 5/0: May 10 10:13:48.268 CET: A84E3FDD 84C4
SLOT 5/0: May 10 10:13:48.268 CET: Found RSA Public Key (length = 140):
SLOT 5/0: May 10 10:13:48.268 CET: 30818902 818100B0 D4F2B649 87FCE340
SLOT 5/0: May 10 10:13:48.268 CET: B21FB1E0 8CFE04DD DB3D05D5 34170886
SLOT 5/0: May 10 10:13:48.268 CET: 7623EE25 4E4A61FC 6D134830 55F402CF
SLOT 5/0: May 10 10:13:48.268 CET: 89B11B34 867B3EF7 D9FE6CBE 8B4C251F
SLOT 5/0: May 10 10:13:48.268 CET: DA5A2E47 D65C2120 8EFC72E2 238D5443
SLOT 5/0: May 10 10:13:48.268 CET: 786F151A A7FE6C21 371957DD 3FEB8435
SLOT 5/0: May 10 10:13:48.268 CET: 8AA1B7A2 181DAF7A 4F7DD4E9 128D953C
SLOT 5/0: May 10 10:13:48.268 CET: 146B77F4 51A9F868 5D1A253F A9590AC0
SLOT 5/0: May 10 10:13:48.268 CET: F69D24DF 2B84C102 03010001
SLOT 5/0: May 10 10:13:48.268 CET: Found CM Certificate (length = 652):
SLOT 5/0: May 10 10:13:48.268 CET: 30820288 308201F1 A0030201 02020C41
SLOT 5/0: May 10 10:13:48.268 CET: 38344533 46444438 34433430 0D06092A
SLOT 5/0: May 10 10:13:48.268 CET: 864886F7 0D010105 05003081 81310B30
SLOT 5/0: May 10 10:13:48.268 CET: 09060355 04061302 5457311C 301A0603
SLOT 5/0: May 10 10:13:48.268 CET: 55040A13 13486974 726F6E20 54656368
SLOT 5/0: May 10 10:13:48.268 CET: 6E6F6C6F 67696573 310F300D 06035504
SLOT 5/0: May 10 10:13:48.268 CET: 0B130644 4F435349 53314330 41060355
SLOT 5/0: May 10 10:13:48.268 CET: 0403133A 48697472 6F6E2054 6563686E
SLOT 5/0: May 10 10:13:48.268 CET: 6F6C6F67 69657320 4361626C 65204D6F
SLOT 5/0: May 10 10:13:48.268 CET: 64656D20 526F6F74 20436572 74696669
SLOT 5/0: May 10 10:13:48.268 CET: 63617465 20417574 686F7269 7479301E
SLOT 5/0: May 10 10:13:48.268 CET: 170D3137 30313031 30303030 30305A17
SLOT 5/0: May 10 10:13:48.268 CET: 0D333631 32323832 33353935 395A3081
SLOT 5/0: May 10 10:13:48.268 CET: 86310B30 09060355 04061302 5457311C
SLOT 5/0: May 10 10:13:48.268 CET: 301A0603 55040A13 13486974 726F6E20
SLOT 5/0: May 10 10:13:48.268 CET: 54656368 6E6F6C6F 67696573 313D303B
SLOT 5/0: May 10 10:13:48.268 CET: 06035504 0B13344E 6F2E2034 302C2057
SLOT 5/0: May 10 10:13:48.268 CET: 752D6B75 6E672035 74682052 642E2C20
SLOT 5/0: May 10 10:13:48.268 CET: 57752D6B 752C2054 61697065 69204873
SLOT 5/0: May 10 10:13:48.268 CET: 69656E2C 20546169 77616E31 1A301806
SLOT 5/0: May 10 10:13:48.268 CET: 03550403 13114138 3A34453A 33463A44
SLOT 5/0: May 10 10:13:48.268 CET: 443A3834 3A433430 819F300D 06092A86
SLOT 5/0: May 10 10:13:48.268 CET: 4886F70D 01010105 0003818D 00308189

```
SLOT 5/0: May 10 10:13:48.268 CET:     02818100 B0D4F2B6  4987FCE3 40B21FB1
SLOT 5/0: May 10 10:13:48.268 CET:     E08CFE04 DDDB3D05  D5341708 867623EE
SLOT 5/0: May 10 10:13:48.268 CET:     254E4A61 FC6D1348  3055F402 CF89B11B
SLOT 5/0: May 10 10:13:48.268 CET:     34867B3E F7D9FE6C  BE8B4C25 1FDA5A2E
SLOT 5/0: May 10 10:13:48.268 CET:     47D65C21 208EFC72  E2238D54 43786F15
SLOT 5/0: May 10 10:13:48.268 CET:     1AA7FE6C 21371957  DD3FEB84 358AA1B7
SLOT 5/0: May 10 10:13:48.268 CET:     A2181DAF 7A4F7DD4  E9128D95 3C146B77
SLOT 5/0: May 10 10:13:48.268 CET:     F451A9F8 685D1A25  3FA9590A C0F69D24
SLOT 5/0: May 10 10:13:48.268 CET:     DF2B84C1 02030100  01300D06 092A8648
SLOT 5/0: May 10 10:13:48.268 CET:     86F70D01 01050500  03818100 08DFC2DA
SLOT 5/0: May 10 10:13:48.268 CET:     8C3ECCDA 98289410  E1B8657A 9A3F220D
SLOT 5/0: May 10 10:13:48.268 CET:     AE368029 0E89923F  0DF09E06 8142BAB7
SLOT 5/0: May 10 10:13:48.268 CET:     E8A6D5B3 6D7604FF  6A07A8B8 409D0B0B
SLOT 5/0: May 10 10:13:48.268 CET:     6D568AF4 F9395199  AB54126C E9C22F1B
SLOT 5/0: May 10 10:13:48.268 CET:     6390543A 3B67EFB8  FCF0E755 F642E1E0
SLOT 5/0: May 10 10:13:48.268 CET:     273A3853 F4DDBFF1  391E63CE 8BB7BBC0
SLOT 5/0: May 10 10:13:48.268 CET:     8AFC59FC 767C3FA5  A5EB255C 8878F4AB
SLOT 5/0: May 10 10:13:48.272 CET:     63665AA9 CDCF779A  3DFE0C4C
SLOT 5/0: May 10 10:13:48.272 CET:  Found COMPOUND SA Capabilities (length = 13):
SLOT 5/0: May 10 10:13:48.272 CET:  Found Crypto Suite List (length = 6):
SLOT 5/0: May 10 10:13:48.272 CET:     01000200 0300
SLOT 5/0: May 10 10:13:48.272 CET:  Found BPI Version (length = 1):
SLOT 5/0: May 10 10:13:48.272 CET:     01
SLOT 5/0: May 10 10:13:48.272 CET:  Found SAID (length = 2):
SLOT 5/0: May 10 10:13:48.272 CET:     0000
SLOT 5/0: May 10 10:13:48.272 CET: END BPKM Attributes: a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.272 CET: Get a CM Certificate.
SLOT 5/0: May 10 10:13:48.272 CET: Cable5/0/12: Auth-Req contains 1 SID(s).
SLOT 5/0: May 10 10:13:48.272 CET: Cable5/0/12: AuthReq with NULL SAID - D3.0 modem.
SLOT 5/0: May 10 10:13:48.272 CET: EAE_BPI_REQ:  DISABLE a84e.3fdd.84c4 - OK
SLOT 5/0: May 10 10:13:48.272 CET: BPI_AES:  Encryption priority is: aes128-des56-des40.
SLOT 5/0: May 10 10:13:48.272 CET: BPI_AES:  AES is a candidate.
SLOT 5/0: May 10 10:13:48.272 CET: BPI Crypto Algorithm: sid:0 cfg_mod:1, cm_cap:0x7, assigned:3
aes_support:1
SLOT 5/0: May 10 10:13:48.272 CET: CMTS generated AUTH_KEY.
SLOT 5/0: May 10 10:13:48.272 CET: CMTS received 0 as primary SAID - D3.0
SLOT 5/0: May 10 10:13:48.272 CET:  CM state:2050 MAC:a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.272 CET: Parsed/Matched MAC Address:a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.272 CET: Got Issuer 0^A^A1^K0 ^F^CU^D^F^S^BTW1^\0^Z^F^CU^D
^S^SHitron Technologies1^O0
^F^CU^D^K^S^FDOCSIS1C0A^F^CU^D^C^S:Hitron Technologies Cable Modem Root Certificate Authority
from Certificate.
SLOT 5/0: May 10 10:13:48.272 CET: Got a new Invalid CM cert from a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.272 CET: CA Cert Subject does not match CM Cert Issuer
```

Salvar este filewith um nome **cmcert.txt.**

A tarefa 3. prepara o arquivo para a utilidade do xxd

XXD é uma utilidade de Linux/Mac que reserve converter e vice-versa uma cópia parcial da memória de HEX em um arquivo binário. XXD precisa os dados encantar de ter uma linha específica encabeçamento a fim trabalhar. Use o seguinte script do pitão que adiciona o encabeçamento necessário:

```
SLOT 5/0: May 10 10:13:48.260 CET: BPI+ Manufacturer Cert Dump: a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.260 CET: CA Certificate Dump:
SLOT 5/0: May 10 10:13:48.260 CET: 0x0000: 30 82 03 22 30 82 02 0A A0 03 02 01 02 02 10 43
SLOT 5/0: May 10 10:13:48.260 CET: 0x0010: 64 B5 50 E8 ED 7E E5 57 14 5A C0 A2 67 52 EC 30
SLOT 5/0: May 10 10:13:48.260 CET: 0x0020: 0D 06 09 2A 86 48 86 F7 0D 01 01 05 05 00 30 6F
SLOT 5/0: May 10 10:13:48.260 CET: 0x0030: 31 0B 30 09 06 03 55 04 06 13 02 42 45 31 1F 30
```

SLOT 5/0: May 10 10:13:48.260 CET: 0x0040: 1D 06 03 55 04 0A 13 16 74 43 6F 6D 4C 61 62 73
SLOT 5/0: May 10 10:13:48.260 CET: 0x0050: 20 2D 20 45 75 72 6F 2D 44 4F 43 53 49 53 31 15
SLOT 5/0: May 10 10:13:48.260 CET: 0x0060: 30 13 06 03 55 04 0B 13 0C 43 61 62 6C 65 20 4D
SLOT 5/0: May 10 10:13:48.260 CET: 0x0070: 6F 64 65 6D 73 31 28 30 26 06 03 55 04 03 13 1F
SLOT 5/0: May 10 10:13:48.260 CET: 0x0080: 45 75 72 6F 2D 44 4F 43 53 49 53 20 43 61 62 6C
SLOT 5/0: May 10 10:13:48.260 CET: 0x0090: 65 20 4D 6F 64 65 6D 20 52 6F 6F 74 20 43 41 30
SLOT 5/0: May 10 10:13:48.260 CET: 0x00A0: 1E 17 0D 30 34 30 38 31 33 30 30 30 30 30 30 5A
SLOT 5/0: May 10 10:13:48.260 CET: 0x00B0: 17 0D 32 34 30 38 31 32 32 33 35 39 35 39 5A 30
SLOT 5/0: May 10 10:13:48.260 CET: 0x00C0: 81 86 31 0B 30 09 06 03 55 04 06 13 02 54 57 31
SLOT 5/0: May 10 10:13:48.260 CET: 0x00D0: 1C 30 1A 06 03 55 04 0A 13 13 48 69 74 72 6F 6E
SLOT 5/0: May 10 10:13:48.260 CET: 0x00E0: 20 54 65 63 68 6E 6F 6C 6F 67 69 65 73 31 14 30
SLOT 5/0: May 10 10:13:48.260 CET: 0x00F0: 12 06 03 55 04 0B 13 0B 45 75 72 6F 2D 44 4F 43
SLOT 5/0: May 10 10:13:48.260 CET: 0x0100: 53 49 53 31 43 30 41 06 03 55 04 03 13 3A 48 69
SLOT 5/0: May 10 10:13:48.260 CET: 0x0110: 74 72 6F 6E 20 54 65 63 68 6E 6F 6C 6F 67 69 65
SLOT 5/0: May 10 10:13:48.260 CET: 0x0120: 73 20 43 61 62 6C 65 20 4D 6F 64 65 6D 20 52 6F
SLOT 5/0: May 10 10:13:48.260 CET: 0x0130: 6F 74 20 43 65 72 74 69 66 69 63 61 74 65 20 41
SLOT 5/0: May 10 10:13:48.260 CET: 0x0140: 75 74 68 6F 72 69 74 79 30 81 9F 30 0D 06 09 2A
SLOT 5/0: May 10 10:13:48.260 CET: 0x0150: 86 48 86 F7 0D 01 01 01 05 00 03 81 8D 00 30 81
SLOT 5/0: May 10 10:13:48.260 CET: 0x0160: 89 02 81 81 00 B8 47 DA 9D F1 F6 30 1B 8E 79 BE
SLOT 5/0: May 10 10:13:48.260 CET: 0x0170: BE 10 C3 2D 9F 7D D6 C7 B2 50 16 AB 85 5C 1C 8C
SLOT 5/0: May 10 10:13:48.260 CET: 0x0180: 9E 6B F7 15 60 B2 53 F4 2F 6D 49 0C 2C 3E 76 88
SLOT 5/0: May 10 10:13:48.260 CET: 0x0190: 8A 8A 23 6B 25 47 61 AE B9 DF A8 A7 8C 4D 51 FB
SLOT 5/0: May 10 10:13:48.260 CET: 0x01A0: E6 C2 0F D9 C7 27 DD F7 D8 CC F0 D8 70 F8 75 75
SLOT 5/0: May 10 10:13:48.260 CET: 0x01B0: F3 D8 B7 80 C2 36 B0 53 02 A4 E9 84 02 5F 66 AE
SLOT 5/0: May 10 10:13:48.260 CET: 0x01C0: E7 59 9A 17 4A A0 B1 B4 BA F3 3B 63 C4 75 05 11
SLOT 5/0: May 10 10:13:48.260 CET: 0x01D0: 40 F1 EB B3 C8 A0 E8 AD 6E 1B 59 CC 41 20 F8 94
SLOT 5/0: May 10 10:13:48.260 CET: 0x01E0: B3 94 23 A2 99 02 03 01 00 01 A3 26 30 24 30 12
SLOT 5/0: May 10 10:13:48.260 CET: 0x01F0: 06 03 55 1D 13 01 01 FF 04 08 30 06 01 01 FF 02
SLOT 5/0: May 10 10:13:48.264 CET: 0x0200: 01 00 30 0E 06 03 55 1D 0F 01 01 FF 04 04 03 02
SLOT 5/0: May 10 10:13:48.264 CET: 0x0210: 01 06 30 0D 06 09 2A 86 48 86 F7 0D 01 01 05 05
SLOT 5/0: May 10 10:13:48.264 CET: 0x0220: 00 03 82 01 01 00 09 DB 24 B9 46 76 D7 D0 9F 70
SLOT 5/0: May 10 10:13:48.264 CET: 0x0230: 86 59 ED 7F 9B AC 96 FD AE 19 DD B3 51 3B A5 C0
SLOT 5/0: May 10 10:13:48.264 CET: 0x0240: 98 DA 80 2B 53 26 42 FA 6A 11 9F 6D 16 6F 76 F8
SLOT 5/0: May 10 10:13:48.264 CET: 0x0250: 9A F3 81 53 E8 DB EF 22 DF AC 3F 57 78 0E 70 78
SLOT 5/0: May 10 10:13:48.264 CET: 0x0260: 07 30 1D FF 19 70 34 E5 7A 52 47 99 B0 EE 7F EA
SLOT 5/0: May 10 10:13:48.264 CET: 0x0270: 23 99 DF CB 72 FF 0D BE AB 68 20 9F 16 C0 7C 69
SLOT 5/0: May 10 10:13:48.264 CET: 0x0280: 88 2D 00 6A AF 4B FF 93 A5 07 D3 F2 A8 F9 5B C4
SLOT 5/0: May 10 10:13:48.264 CET: 0x0290: DD 9F BF 49 36 C4 12 8A 64 C8 35 41 BB E2 B9 9B
SLOT 5/0: May 10 10:13:48.264 CET: 0x02A0: 52 45 67 38 DC 92 55 E3 33 A4 70 68 FC E7 6E 54
SLOT 5/0: May 10 10:13:48.264 CET: 0x02B0: 96 CA 89 B4 65 8B 2C AA 58 24 FC 4D 68 D7 84 4E
SLOT 5/0: May 10 10:13:48.264 CET: 0x02C0: 36 3B B3 CA 9A 42 13 B1 FF 8C 66 D8 52 10 56 74
SLOT 5/0: May 10 10:13:48.264 CET: 0x02D0: C7 DD 58 C3 EE 9D E3 65 E6 C1 5D B9 75 C2 A8 C9
SLOT 5/0: May 10 10:13:48.264 CET: 0x02E0: 54 5B A1 85 38 3B E1 E1 DC 55 5D 3E DD 90 ED F8
SLOT 5/0: May 10 10:13:48.264 CET: 0x02F0: 3A B0 68 93 E9 4A C2 D4 7F DC 90 E3 86 E2 CF C3
SLOT 5/0: May 10 10:13:48.264 CET: 0x0300: F2 A3 92 84 B3 A3 9A F8 71 30 F8 24 71 C2 07 BD
SLOT 5/0: May 10 10:13:48.264 CET: 0x0310: E8 6C 3C F7 FC 82 08 86 84 84 1B C4 D8 97 D3 50
SLOT 5/0: May 10 10:13:48.264 CET: 0x0320: 59 72 2D D5 4C 0B
SLOT 5/0: May 10 10:13:48.264 CET: Found existing manufacturer certificate for a84e.3fdd.84c4 with subject cn=Hitron Technologies Cable Modem Root Certificate Authority,ou=Euro-DOCSIS,o=Hitron Technologies,c=TW
SLOT 5/0: May 10 10:13:48.264 CET: BPI: setting a84e.3fdd.84c4 caidx:3

SLOT 5/0: May 10 10:13:48.264 CET: Mfg serial no. from a84e.3fdd.84c4 certificate: 4364B550E8ED7EE557145AC0A26752EC
SLOT 5/0: May 10 10:13:48.264 CET: Finger print of a84e.3fdd.84c4 manufacturer certificate matched.
SLOT 5/0: May 10 10:13:48.264 CET: cr10k_clc_snmp_bpiplus_broadcast_cert() CA idx:3 state:Chained rowStatus:Active prov:0 len:1078 idx:3 state:Chained rowState:Active prov:0 learn:1 idx:3
SLOT 5/0: May 10 10:13:48.268 CET: BPI: Sent CA Cert to RP successfully.
SLOT 5/0: May 10 10:13:48.268 CET: Success in validating AUTH Info message from a84e.3fdd.84c4.
SLOT 5/0: May 10 10:13:48.268 CET: CMTS Received AUTH REQ from a84e.3fdd.84c4.
SLOT 5/0: May 10 10:13:48.268 CET: BPI Authorization Request Packet: a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.268 CET: BPKM Attributes: a84e.3fdd.84c4

```
SLOT 5/0: May 10 10:13:48.268 CET:  Found COMPOUND CM Identification (length = 173):
SLOT 5/0: May 10 10:13:48.268 CET:  Found Serial Number (length = 12):
SLOT 5/0: May 10 10:13:48.268 CET:     32353331 36433030  38303433
SLOT 5/0: May 10 10:13:48.268 CET:  Found Manufacturer ID (length = 3):
SLOT 5/0: May 10 10:13:48.268 CET:     0050F1
SLOT 5/0: May 10 10:13:48.268 CET:  Found MAC Address (length = 6):
SLOT 5/0: May 10 10:13:48.268 CET:     A84E3FDD 84C4
SLOT 5/0: May 10 10:13:48.268 CET:  Found RSA Public Key (length = 140):
SLOT 5/0: May 10 10:13:48.268 CET:     30818902 818100B0  D4F2B649 87FCE340
SLOT 5/0: May 10 10:13:48.268 CET:     B21FB1E0 8CFE04DD  DB3D05D5 34170886
SLOT 5/0: May 10 10:13:48.268 CET:     7623EE25 4E4A61FC  6D134830 55F402CF
SLOT 5/0: May 10 10:13:48.268 CET:     89B11B34 867B3EF7  D9FE6CBE 8B4C251F
SLOT 5/0: May 10 10:13:48.268 CET:     DA5A2E47 D65C2120  8EFC72E2 238D5443
SLOT 5/0: May 10 10:13:48.268 CET:     786F151A A7FE6C21  371957DD 3FEB8435
SLOT 5/0: May 10 10:13:48.268 CET:     8AA1B7A2 181DAF7A  4F7DD4E9 128D953C
SLOT 5/0: May 10 10:13:48.268 CET:     146B77F4 51A9F868  5D1A253F A9590AC0
SLOT 5/0: May 10 10:13:48.268 CET:     F69D24DF 2B84C102  03010001
SLOT 5/0: May 10 10:13:48.268 CET:  Found CM Certificate (length = 652):
SLOT 5/0: May 10 10:13:48.268 CET:     30820288 308201F1  A0030201 02020C41
SLOT 5/0: May 10 10:13:48.268 CET:     38344533 46444438  34433430 0D06092A
SLOT 5/0: May 10 10:13:48.268 CET:     864886F7 0D010105  05003081 81310B30
SLOT 5/0: May 10 10:13:48.268 CET:     09060355 04061302  5457311C 301A0603
SLOT 5/0: May 10 10:13:48.268 CET:     55040A13 13486974  726F6E20 54656368
SLOT 5/0: May 10 10:13:48.268 CET:     6E6F6C6F 67696573  310F300D 06035504
SLOT 5/0: May 10 10:13:48.268 CET:     0B130644 4F435349  53314330 41060355
SLOT 5/0: May 10 10:13:48.268 CET:     0403133A 48697472  6F6E2054 6563686E
SLOT 5/0: May 10 10:13:48.268 CET:     6F6C6F67 69657320  4361626C 65204D6F
SLOT 5/0: May 10 10:13:48.268 CET:     64656D20 526F6F74  20436572 74696669
SLOT 5/0: May 10 10:13:48.268 CET:     63617465 20417574  686F7269 7479301E
SLOT 5/0: May 10 10:13:48.268 CET:     170D3137 30313031  30303030 30305A17
SLOT 5/0: May 10 10:13:48.268 CET:     0D333631 32323832  33353935 395A3081
SLOT 5/0: May 10 10:13:48.268 CET:     86310B30 09060355  04061302 5457311C
SLOT 5/0: May 10 10:13:48.268 CET:     301A0603 55040A13  13486974 726F6E20
SLOT 5/0: May 10 10:13:48.268 CET:     54656368 6E6F6C6F  67696573 313D303B
SLOT 5/0: May 10 10:13:48.268 CET:     06035504 0B13344E  6F2E2034 302C2057
SLOT 5/0: May 10 10:13:48.268 CET:     752D6B75 6E672035  74682052 642E2C20
SLOT 5/0: May 10 10:13:48.268 CET:     57752D6B 752C2054  61697065 69204873
SLOT 5/0: May 10 10:13:48.268 CET:     69656E2C 20546169  77616E31 1A301806
SLOT 5/0: May 10 10:13:48.268 CET:     03550403 13114138  3A34453A 33463A44
SLOT 5/0: May 10 10:13:48.268 CET:     443A3834 3A433430  819F300D 06092A86
SLOT 5/0: May 10 10:13:48.268 CET:     4886F70D 01010105  0003818D 00308189
SLOT 5/0: May 10 10:13:48.268 CET:     02818100 B0D4F2B6  4987FCE3 40B21FB1
SLOT 5/0: May 10 10:13:48.268 CET:     E08CFE04 DDDB3D05  D5341708 867623EE
SLOT 5/0: May 10 10:13:48.268 CET:     254E4A61 FC6D1348  3055F402 CF89B11B
SLOT 5/0: May 10 10:13:48.268 CET:     34867B3E F7D9FE6C  BE8B4C25 1FDA5A2E
SLOT 5/0: May 10 10:13:48.268 CET:     47D65C21 208EFC72  E2238D54 43786F15
SLOT 5/0: May 10 10:13:48.268 CET:     1AA7FE6C 21371957  DD3FEB84 358AA1B7
SLOT 5/0: May 10 10:13:48.268 CET:     A2181DAF 7A4F7DD4  E9128D95 3C146B77
SLOT 5/0: May 10 10:13:48.268 CET:     F451A9F8 685D1A25  3FA9590A C0F69D24
SLOT 5/0: May 10 10:13:48.268 CET:     DF2B84C1 02030100  01300D06 092A8648
SLOT 5/0: May 10 10:13:48.268 CET:     86F70D01 01050500  03818100 08DFC2DA
SLOT 5/0: May 10 10:13:48.268 CET:     8C3ECCDA 98289410  E1B8657A 9A3F220D
SLOT 5/0: May 10 10:13:48.268 CET:     AE368029 0E89923F  0DF09E06 8142BAB7
SLOT 5/0: May 10 10:13:48.268 CET:     E8A6D5B3 6D7604FF  6A07A8B8 409D0B0B
SLOT 5/0: May 10 10:13:48.268 CET:     6D568AF4 F9395199  AB54126C E9C22F1B
SLOT 5/0: May 10 10:13:48.268 CET:     6390543A 3B67EFB8  FCF0E755 F642E1E0
SLOT 5/0: May 10 10:13:48.268 CET:     273A3853 F4DDBFF1  391E63CE 8BB7BBC0
SLOT 5/0: May 10 10:13:48.268 CET:     8AFC59FC 767C3FA5  A5EB255C 8878F4AB
SLOT 5/0: May 10 10:13:48.272 CET:     63665AA9 CDCF779A  3DFE0C4C
SLOT 5/0: May 10 10:13:48.272 CET:  Found COMPOUND SA Capabilities (length = 13):
SLOT 5/0: May 10 10:13:48.272 CET:  Found Crypto Suite List (length = 6):
SLOT 5/0: May 10 10:13:48.272 CET:     01000200 0300
SLOT 5/0: May 10 10:13:48.272 CET:  Found BPI Version (length = 1):
SLOT 5/0: May 10 10:13:48.272 CET:     01
```

```
SLOT 5/0: May 10 10:13:48.272 CET:  Found SAID (length = 2):
SLOT 5/0: May 10 10:13:48.272 CET:     0000
SLOT 5/0: May 10 10:13:48.272 CET: END BPKM Attributes: a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.272 CET: Get a CM Certificate.
SLOT 5/0: May 10 10:13:48.272 CET: Cable5/0/12: Auth-Req contains 1 SID(s).
SLOT 5/0: May 10 10:13:48.272 CET: Cable5/0/12: AuthReq with NULL SAID - D3.0 modem.
SLOT 5/0: May 10 10:13:48.272 CET: EAE_BPI_REQ:  DISABLE a84e.3fdd.84c4 - OK
SLOT 5/0: May 10 10:13:48.272 CET: BPI_AES:  Encryption priority is: aes128-des56-des40.
SLOT 5/0: May 10 10:13:48.272 CET: BPI_AES:  AES is a candidate.
SLOT 5/0: May 10 10:13:48.272 CET: BPI Crypto Algorithm: sid:0 cfg_mod:1, cm_cap:0x7, assigned:3
aes_support:1
SLOT 5/0: May 10 10:13:48.272 CET: CMTS generated AUTH_KEY.
SLOT 5/0: May 10 10:13:48.272 CET: CMTS received 0 as primary SAID - D3.0
SLOT 5/0: May 10 10:13:48.272 CET:  CM state:2050 MAC:a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.272 CET: Parsed/Matched MAC Address:a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.272 CET: Got Issuer 0^A^A1^K0 ^F^CU^D^F^S^BTW1^\0^Z^F^CU^D
^S^SHitron Technologies1^O0
^F^CU^D^K^S^FDOCSIS1C0A^F^CU^D^C^S:Hitron Technologies Cable Modem Root Certificate Authority
from Certificate.
SLOT 5/0: May 10 10:13:48.272 CET: Got a new Invalid CM cert from a84e.3fdd.84c4
SLOT 5/0: May 10 10:13:48.272 CET: CA Cert Subject does not match CM Cert Issuer
```

Certificados do converso da tarefa 4. de Hexdump ao formato binário

Execute este comando converter o certificado de CA.

```
python3.5 addoffset.py cacert.txt | xxd -r > cacert.crt
```

Execute este comando converter o certificado CM.

```
python3.5 addoffset.py cmcert.txt | xxd -r > cmcert.crt
```

Estes arquivos gerados CRT agora podem ser verificados para ver se há toda a má combinação.

Certificados da revisão da tarefa 5.

A fim ler os arquivos usam-se com utilidade do OpenSSL ou do Keychain.

Um exemplo com utilidade do OpenSSL para o certificado de CA.

```
TVANEGRO-M-N1QP:Desktop tvanegro$ openssl x509 -inform der -in cacert.crt -noout -text
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
43:64:b5:50:e8:ed:7e:e5:57:14:5a:c0:a2:67:52:ec
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=BE, O=tComLabs - Euro-DOCSIS, OU=Cable Modems, CN=Euro-DOCSIS Cable Modem Root CA
Validity
Not Before: Aug 13 00:00:00 2004 GMT
Not After : Aug 12 23:59:59 2024 GMT
Subject: C=TW, O=Hitron Technologies, OU=Euro-DOCSIS, CN=Hitron Technologies Cable Modem Root
Certificate Authority
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:b8:47:da:9d:f1:f6:30:1b:8e:79:be:be:10:c3:
2d:9f:7d:d6:c7:b2:50:16:ab:85:5c:1c:8c:9e:6b:
f7:15:60:b2:53:f4:2f:6d:49:0c:2c:3e:76:88:8a:
8a:23:6b:25:47:61:ae:b9:df:a8:a7:8c:4d:51:fb:
e6:c2:0f:d9:c7:27:dd:f7:d8:cc:f0:d8:70:f8:75:
```

```
75:f3:d8:b7:80:c2:36:b0:53:02:a4:e9:84:02:5f:
66:ae:e7:59:9a:17:4a:a0:b1:b4:ba:f3:3b:63:c4:
75:05:11:40:f1:eb:b3:c8:a0:e8:ad:6e:1b:59:cc:
41:20:f8:94:b3:94:23:a2:99
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints: critical
CA:TRUE, pathlen:0
X509v3 Key Usage: critical
Certificate Sign, CRL Sign
Signature Algorithm: sha1WithRSAEncryption
09:db:24:b9:46:76:d7:d0:9f:70:86:59:ed:7f:9b:ac:96:fd:
ae:19:dd:b3:51:3b:a5:c0:98:da:80:2b:53:26:42:fa:6a:11:
9f:6d:16:6f:76:f8:9a:f3:81:53:e8:db:ef:22:df:ac:3f:57:
78:0e:70:78:07:30:1d:ff:19:70:34:e5:7a:52:47:99:b0:ee:
7f:ea:23:99:df:cb:72:ff:0d:be:ab:68:20:9f:16:c0:7c:69:
88:2d:00:6a:af:4b:ff:93:a5:07:d3:f2:a8:f9:5b:c4:dd:9f:
bf:49:36:c4:12:8a:64:c8:35:41:bb:e2:b9:9b:52:45:67:38:
dc:92:55:e3:33:a4:70:68:fc:e7:6e:54:96:ca:89:b4:65:8b:
2c:aa:58:24:fc:4d:68:d7:84:4e:36:3b:b3:ca:9a:42:13:b1:
ff:8c:66:d8:52:10:56:74:c7:dd:58:c3:ee:9d:e3:65:e6:c1:
5d:b9:75:c2:a8:c9:54:5b:a1:85:38:3b:e1:e1:dc:55:5d:3e:
dd:90:ed:f8:3a:b0:68:93:e9:4a:c2:d4:7f:dc:90:e3:86:e2:
cf:c3:f2:a3:92:84:b3:a3:9a:f8:71:30:f8:24:71:c2:07:bd:
e8:6c:3c:f7:fc:82:08:86:84:84:1b:c4:d8:97:d3:50:59:72:
2d:d5:4c:0b
```

Um exemplo com utilidade do OpenSSL para o certificado CM.

```
TVANEGRO-M-N1QP:Desktop tvanegro$ openssl x509 -inform der -in cmcert.crt -noout -text
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
41:38:34:45:33:46:44:44:38:34:43:34
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=TW, O=Hitron Technologies, OU=DOCSIS, CN=Hitron Technologies Cable Modem Root
Certificate Authority
Validity
Not Before: Jan 1 00:00:00 2017 GMT
Not After : Dec 28 23:59:59 2036 GMT
Subject: C=TW, O=Hitron Technologies, OU=No. 40, Wu-kung 5th Rd., Wu-ku, Taipei Hsien, Taiwan,
CN=A8:4E:3F:DD:84:C4
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:b0:d4:f2:b6:49:87:fc:e3:40:b2:1f:b1:e0:8c:
fe:04:dd:db:3d:05:d5:34:17:08:86:76:23:ee:25:
4e:4a:61:fc:6d:13:48:30:55:f4:02:cf:89:b1:1b:
34:86:7b:3e:f7:d9:fe:6c:be:8b:4c:25:1f:da:5a:
2e:47:d6:5c:21:20:8e:fc:72:e2:23:8d:54:43:78:
6f:15:1a:a7:fe:6c:21:37:19:57:dd:3f:eb:84:35:
8a:a1:b7:a2:18:1d:af:7a:4f:7d:d4:e9:12:8d:95:
3c:14:6b:77:f4:51:a9:f8:68:5d:1a:25:3f:a9:59:
0a:c0:f6:9d:24:df:2b:84:c1
Exponent: 65537 (0x10001)
Signature Algorithm: sha1WithRSAEncryption
08:df:c2:da:8c:3e:cc:da:98:28:94:10:e1:b8:65:7a:9a:3f:
22:0d:ae:36:80:29:0e:89:92:3f:0d:f0:9e:06:81:42:ba:b7:
e8:a6:d5:b3:6d:76:04:ff:6a:07:a8:b8:40:9d:0b:0b:6d:56:
8a:f4:f9:39:51:99:ab:54:12:6c:e9:c2:2f:1b:63:90:54:3a:
3b:67:ef:b8:fc:f0:e7:55:f6:42:e1:e0:27:3a:38:53:f4:dd:
bf:f1:39:1e:63:ce:8b:b7:bb:c0:8a:fc:59:fc:76:7c:3f:a5:
```

```
a5:eb:25:5c:88:78:f4:ab:63:66:5a:a9:cd:cf:77:9a:3d:fe:
0c:4c
```

Você pode ver que o campo **OU= (unidade organizacional)** não combina. No exemplo, você vê o **DOCSIS** e o Euro-**DOCSIS.** Aquela é a razão pela qual o CMTS rejeita o certificado.

Você pode usar a ferramenta de Keychain no Mac OS para ver os Certificados.