The CCM Validation System (CCMVS)

November 29, 2004

Lawrence E. Bassham III

National Institute of Standards and Technology

Information Technology Laboratory

Computer Security Division

TABLE OF CONTENTS

1 Introduction

This document, *The CCM Validation System (CCMVS)* specifies the procedures involved in validating implementations of the CCM Mode of Operation as specified in SP 800-38C, *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality* [1]. The CCMVS is designed to perform automated testing on Implementations Under Test (IUTs). This document provides the basic design and configuration of the CCMVS.

This document defines the purpose, the design philosophy, and the high-level description of the validation process for CCM. The requirements and administrative procedures to be followed by those seeking formal validation of an implementation of CCM are presented. The requirements described include a specification of the data communicated between the IUT and the CCMVS, the details of the tests that the IUT must pass for formal validation, and general instruction for interfacing with the CCMVS. Additionally, an appendix is also provided containing samples of input and output files for the CCMVS.

2 Scope

This document specifies the tests required to validate IUTs for conformance to CCM specified in [1]. When applied to an IUT, the CCMVS provides testing to determine the correctness of the implementation of CCM. The CCMVS is composed of five separate tests – four to test various aspects involved in Encryption-Generation process and one to test the Decryption-Verification process. In addition to performing the tests specified in CCMVS, the IUT must undergo testing of the underlying encryption algorithm, namely AES, implementation via the appropriate validation suite (AESVS).

3 Conformance

The successful completion of the tests contained within the CCMVS and the AESVS is required to be validated as conforming to the CCM standard. Testing for the cryptographic module in which the CCM is implemented is defined in FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*.[2]

4 Definitions and Abbreviations

4.1 Definitions

DEFINITION	**MEANING**
Advanced Encryption Standard	The algorithm specified in FIPS 197, *Advanced Encryption Standard (AES)*

CMT laboratory	Cryptographic Module Testing laboratory that operates the CCMVS

4.2 Abbreviations

ABBREVIATION	MEANING
AES	Advanced Encryption Standard specified in FIPS 197
AESVS	Advanced Encryption Standard Validation System
FIPS	Federal Information Processing Standard
CCM	CCM Mode of Operation specified in SP 800-38C
IUT	Implementation Under Test

5 Design Philosophy Of CCM Validation System

The CCMVS is designed to test conformance to the CCM specification rather than provide a measure of a product's security. The validation tests are designed to assist in the detection of accidental implementation errors, and are not designed to detect intentional attempts to misrepresent conformance. Thus, validation should not be interpreted as an evaluation or endorsement of overall product security.

The CCMVS has the following design philosophy:

1. The CCMVS is designed to allow the testing of an IUT at locations remote to the CCMVS. The CCMVS and the IUT communicate data via *REQUEST* and *RESPONSE* files. The CCMVS also generates *SAMPLE* files to provide the IUT with a sample of what the *RESPONSE* file should look like.

2. The testing performed within the CCMVS utilizes statistical sampling (i.e., only a small number of the possible cases are tested); hence, the successful validation of a device does not imply 100% conformance with the standard.

6 CCMVS Test

The CCMVS tests the implementation of CCM for its conformance to the CCM standard. The testing for CCM consists of five tests. These tests are:

- Variable Associated Data Test;
- Variable Payload Test;

- Variable Nonce Test;
- Variable Tag Test; and
- Decryption-Verification Process Test.

6.1 Configuration Information

To initiate the validation process of the CCMVS, a vendor submits an application to an accredited laboratory requesting the validation of its implementation of CCM. The vendor's implementation is referred to as the Implementation Under Test (IUT). The request for validation includes background information describing the IUT along with information needed by the CCMVS to perform the specific tests. More specifically, the request for validation includes:

1. Vendor Name;
2. Product Name;
3. Product Version;
4. Implementation in software, firmware, or hardware;
5. Processor and Operating System with which the IUT was tested if the IUT is implemented in software or firmware;
6. Brief description of the IUT or the product/product family in which the IUT is implemented by the vendor (2-3 sentences); and
7. Configuration information for the CCM tests, including:
   a) Which AES key sizes are supported: 128, 192, and/or 256;
   b) Specify a minimum (greater than or equal to zero bytes) and maximum (less than or equal to 32 bytes) associated data length. Additionally, can the implementation handle an associated data length of 2^16 bytes;
   c) Specify a minimum (greater than or equal to zero bytes) and maximum (less than or equal to 32 bytes) payload length;
   d) Specify the nonce lengths supported: 7, 8, 9, 10, 11, 12, and/or 13; and
   e) Specify the tag lengths supported: 4, 6, 8, 10, 12, 14, and/or 16.

6.2 The Variable Associated Data Test

For each associated data length supported the Variable Associated Data Test provides a 10 sets of associated data and payload to the IUT. The IUT generates a ciphertext as specified by CCM using the data provided. The CCMVS verifies the correctness of the ciphertext produced by the IUT.

The CCMVS:

A. Creates a *REQUEST* file (Filename: VADT{KeySize}.req) containing:

   1. The Product Name;
   2. The algorithm being tested; and
   3. The keys, nonce, associated data, and payload values to be used as input to the CCM algorithm.

   Note: The CMT laboratory sends the *REQUEST* file to the IUT.

B. Creates a *FAX* file (Filename: VADT{KeySize}.fax) containing:

   1. The information from the *REQUEST* file; and
   2. The CT generated by the CCM algorithm.

   Note: The CMT laboratory retains the *FAX* file.

The IUT:

A. Generates the requested CTs using the data specified in the *REQUEST* file.

B. Creates a *RESPONSE* file (Filename: VADT{KeySize}.rsp) containing:

   1. The information from the *REQUEST* file; and
   2. The CT generated by the CCM algorithm.

   Note: The IUT sends the *RESPONSE* file to the CMT laboratory for processing by the CCMVS.

The CCMVS:

A. Compares the contents of the *RESPONSE* file with the contents of the *FAX* file.

B. If all values match, records PASS for this test; otherwise, records FAIL.

6.3 The Variable Payload Test

For each payload length supported the Variable Payload Test provides a 10 sets of associated data and payload to the IUT. The IUT generates a ciphertext as specified by CCM using the data provided. The CCMVS verifies the correctness of the ciphertext produced by the IUT.

The CCMVS:

A. Creates a *REQUEST* file (Filename: VPT{KeySize}.req) containing:

1. The Product Name;
2. The algorithm being tested; and
3. The keys, nonce, associated data, and payload values to be used as input to the CCM algorithm.

Note: The CMT laboratory sends the *REQUEST* file to the IUT.

B. Creates a *FAX* file (Filename: VPT{KeySize}.fax) containing:

3. The information from the *REQUEST* file; and
4. The CT generated by the CCM algorithm.

Note: The CMT laboratory retains the *FAX* file.

The IUT:

A. Generates the requested CTs using the data specified in the *REQUEST* file.

B. Creates a *RESPONSE* file (Filename: VPT{KeySize}.rsp) containing:

3. The information from the *REQUEST* file; and
4. The CT generated by the CCM algorithm.

Note: The IUT sends the *RESPONSE* file to the CMT laboratory for processing by the CCMVS.

The CCMVS:

A. Compares the contents of the *RESPONSE* file with the contents of the *FAX* file.

C. B. If all values match, records PASS for this test; otherwise, records FAIL.

6.4 The Variable Nonce Test

For each nonce length supported the Variable Nonce Test provides a 10 sets of associated data and payload to the IUT. The IUT generates a ciphertext as specified by CCM using the data provided. The CCMVS verifies the correctness of the ciphertext produced by the IUT.

The CCMVS:

A. Creates a *REQUEST* file (Filename: VNT{KeySize}.req) containing:

1. The Product Name;
2. The algorithm being tested; and
3. The keys, nonce, associated data, and payload values to be used as input to the CCM algorithm.

Note: The CMT laboratory sends the *REQUEST* file to the IUT.

B. Creates a *FAX* file (Filename: VNT{KeySize}.fax) containing:

5. The information from the *REQUEST* file; and

6. The CT generated by the CCM algorithm.

Note: The CMT laboratory retains the *FAX* file.

The IUT:

A. Generates the requested CTs using the data specified in the *REQUEST* file.

B. Creates a *RESPONSE* file (Filename: VNT{KeySize}.rsp) containing:

5. The information from the *REQUEST* file; and

6. The CT generated by the CCM algorithm.

Note: The IUT sends the *RESPONSE* file to the CMT laboratory for processing by the CCMVS.

The CCMVS:

A. Compares the contents of the *RESPONSE* file with the contents of the *FAX* file.

D. B. If all values match, records PASS for this test; otherwise, records FAIL.

6.5 The Variable Tag Test

For each tag length supported the Variable Tag Test provides a 10 sets of associated data and payload to the IUT. The IUT generates a ciphertext as specified by CCM using the data provided. The CCMVS verifies the correctness of the ciphertext produced by the IUT.

The CCMVS:

A. Creates a *REQUEST* file (Filename: VTT{KeySize}.req) containing:

1. The Product Name;

2. The algorithm being tested; and

3. The keys, nonce, associated data, and payload values to be used as input to the CCM algorithm.

Note: The CMT laboratory sends the *REQUEST* file to the IUT.

B. Creates a *FAX* file (Filename: VTT{KeySize}.fax) containing:

7. The information from the *REQUEST* file; and

8. The CT generated by the CCM algorithm.

Note: The CMT laboratory retains the *FAX* file.

The IUT:

A. Generates the requested CTs using the data specified in the *REQUEST* file.

B. Creates a *RESPONSE* file (Filename: VTT{KeySize}.rsp) containing:

7. The information from the *REQUEST* file; and

8. The CT generated by the CCM algorithm.

Note: The IUT sends the *RESPONSE* file to the CMT laboratory for processing by the CCMVS.

The CCMVS:

A. Compares the contents of the *RESPONSE* file with the contents of the *FAX* file.

E. B. If all values match, records PASS for this test; otherwise, records FAIL.

6.6 The Decryption-Verification Process Test

For each combination of associated data length, payload length, nonce length, and tag length provided as input, 15 sets of input plus ciphertext are supplied to the IUT. The IUT uses the data provided to determine if the ciphertext passes or fails the verification process.

The CCMVS:

A. Creates a *REQUEST* file (Filename: DVPT{KeySize}.req) containing:

1. The Product Name;

2. The algorithm being tested; and

3. The keys, nonce, associated data, payload, and ciphertext values to be used as input to the decryption-verification process of the CCM algorithm.

Note: The CMT laboratory sends the *REQUEST* file to the IUT.

B. Alter some of the ciphertext produced to ensure the decryption-verification process fails

C. Creates a *FAX* file (Filename: DVPT{KeySize}.fax) containing:

9. The information from the *REQUEST* file; and

10. An indication of whether or not the ciphertext passes to decryption-verification process.

Note: The CMT laboratory retains the *FAX* file.

The IUT:

A. Performs the decryption-verification process to determine whether the data sets verify correctly or not.

B. Creates a *RESPONSE* file (Filename: DVPT{KeySize}.rsp) containing:

9. The information from the *REQUEST* file; and

10. Whether or not the decryption-verification processed passed or failed.

Note: The IUT sends the *RESPONSE* file to the CMT laboratory for processing by the CCMVS.

The CCMVS:

A. Compares the contents of the *RESPONSE* file with the contents of the *FAX* file.

B. If all values match, records PASS for this test; otherwise, records FAIL.

Appendix A References

[1] *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*, Special Publication 800-38C, National Institute of Standards and Technology, May 2004.

[2] *Security Requirements for Cryptographic Modules*, FIPS Publication 140-2, National Institute of Standards and Technology, May 2001.

Appendix B Examples of *REQUEST*, *FAX*, *RESPONSE*, and *SAMPLE* Files

The following are partial examples of *REQUEST*, *FAX*, *RESPONSE*, and *SAMPLE* files for the HMACVS. Length values are in bytes.

B.1 Example of the *REQUEST* File

B.1.1 VADT128.req

```
#  CAVS 4.0
#  "CCM-VADT" information for "CCMTest"
#  AES Keylen: 128
#  Generated on Wed Nov 24 08:34:25 2004

Plen = 32
Nlen = 13
Tlen = 16

[Alen = 0]

Key = 3a69391c2cc4d3904f1ebf26c2683506
Nonce = cf0ad6e883abf8b2d4efc8b5b6

Count = 0
Adata = 00
Payload = 917a5ec58cb4728595fcb1c813f0d1b69b9c3d620940c5a9d053945e8ec963a4

Count = 1
Adata = 00
Payload = 103095480010215bda8ae2d096423a8b5d4d39704be878c0736a44a52377ff0b

Count = 2
Adata = 00
Payload = fffc4c32ef9d52a73cf7c50b197d1e807868812d2e4efb7c51f60885e56b58ca

Count = 3
Adata = 00
Payload = cefa677c99e02638c48be10986e438260df5541e7ae6136d2e2c654e44fdf6d1

Count = 4
Adata = 00
Payload = 17a4bbebee6108c275e85b499e75d8a83e9d8c486c28f344291ebd1a4724d1a7

Count = 5
Adata = 00
Payload = 98d296e5594651ae4dbd365977f7993ce89a18cf4876ce0cb20dc91cc553bd2f

Count = 6
Adata = 00
Payload = b852b3f1468c95dd13b5af0f384c14a17ecbe67f2b2dc6101cac901914cf45de
```

```
Count = 7
Adata = 00
Payload = c8e6e21a5c852dff9c37010444569e7c30df5e6b1e2795dfb4c9bb83c5e3cd71

Count = 8
Adata = 00
Payload = e4fa287a65b389f45fc68e6e947cab9eb35c9869d6a1f8fb4fec3916a437bbaa

Count = 9
Adata = 00
Payload = 2ebe78389e2b362e71d50f5eed781f86add57099a2aa1b5a57e1b02a7908d81e

[Alen = 1]

Key = 991cdc7221f2516b66cffbeea0167e99
Nonce = de5b5934915b4cbd13c389e248

Count = 10
Adata = 18
Payload = d85edbe823829f45506cce383d93ce1a2d3f97986b9d72643113002ac7d17fc6

Count = 11
Adata = d1
Payload = 3e4fad4df06ef0e833ad6057eea34490d097dfa1419efcf19804cac88eedea11

Count = 12
Adata = 87
Payload = 17587c4a63fe2a9d942c95b76a788e7b526517327f2c17723cbc524481ff9785
.
.
.
```

B.1.2 VPT128.req

```
#  CAVS 4.0
#  "CCM-VPT" information for "CCMTest"
#  AES Keylen: 128
#  Generated on Wed Nov 24 08:34:25 2004

Alen = 32
Nlen = 13
Tlen = 16

[Plen = 0]

Key = 3b50f8faf23e2ca176861bb9b95ef743
Nonce = ed57fb55a604a682d882320bf4

Count = 0
Adata = 982f43ecf4c6c0eec312ed7735da8136cbe53ac0531a71d619e6f1eb5cde09e1
Payload = 00
```

```
Count = 1
Adata = 13a1583ce3a6238b2788bb5074100fcfcad5ad6bd16b2a7762d8c44a49474691
Payload = 00

Count = 2
Adata = 7dd458a0fa4783d969f6c468057c604f646da57162827ee25bf646619d2fda23
Payload = 00

Count = 3
Adata = 2d12985b3d81ac3997dba57899d7ec2e14d0012da2c96d273aaff81601dd1bda
Payload = 00

Count = 4
Adata = 65f2ccedef6582db35a7bd6717abf53a7070777a987b0be42e84d41b1470773f
Payload = 00

Count = 5
Adata = 6b3d82f686042a40193035be076ea23e759dea24c4eb93b2c23b028621cb9164
Payload = 00

Count = 6
Adata = 08b3e0c0189542bfeedd47557b8b811cffac553a1f24ac3f37aaea4cf114247a
Payload = 00

Count = 7
Adata = 3070f4d07395fe870dca974f3de0a28da5855c9b0603401a4b2b288ac98bb418
Payload = 00

Count = 8
Adata = 0f58577c96dcbdae0c909e586e8e7987e17542ef99bb65e0f9450975fb35910f
Payload = 00

Count = 9
Adata = 7c6b2f5cd7153d4eea5e1eb6d570a429a8b4e96ede42ee90279c82316b9b6621
Payload = 00

[Plen = 1]

Key = 906de38ddeb0dd9a0783b75346c919d3
Nonce = 55e6fa59963fd2610c75aba802

Count = 10
Adata = 049542cf5c4357730ca618b5f039de1fbdf0a351e48509f4b90c9ef0d4ce5fdf
Payload = 1d

Count = 11
Adata = ecb995aa1ab070191336cc7bc6ce2e18f093577490d661189c090b95f2db52c7
Payload = 53

Count = 12
Adata = 7f37a73db7c790f76c3bb838c041e04e13c713a86cc82c461a66986e9b3a5da1
Payload = e2
.
.
```

.

B.1.3 VNT128.req

```
#  CAVS 4.0
#  "CCM-VNT" information for "CCMTest"
#  AES Keylen: 128
#  Generated on Wed Nov 24 08:34:25 2004

Alen = 32
Plen = 32
Tlen = 16

[Nlen = 7]

Key = b5d475ca8fa03e21b10ad13a3359a3c2

Count = 0
Nonce = 1043f6e725a430
Adata = cae697678007b0e6df925083d399d080a21ac867c18282a9ec6faf8575ba582b
Payload = 468e9d6bfc8b8749cd172eb7a1836bb5c4ff85034868af94a561d240a3a58db9

Count = 1
Nonce = 38701f7ec8a60b
Adata = 39bc5f205308e974bae3690516e4664dc67fd77324348b1f0a06c88c952f33df
Payload = 57d6471b58e424a8842d29400aef26be6b78c1868cec23680a43f1c8cd917efc

Count = 2
Nonce = 0f0a17e0e52720
Adata = 38900130497e0fbcc6e38f7243d1d7a1e4ac505f72e82772ad144571e4188226
Payload = 29af8e8bfbe23afa91b1574600afba43d8fd94acf8c8e9c5a714443ee0b8a85b

Count = 3
Nonce = ce4f81bad699ba
Adata = 9d11cacfdf4582f0e442ab564c740f764f88bfe8af86abb2eb406fc9b6f070d5
Payload = 1de4f0d6745f39040c6cd04673f24ee1a68b3361d337d0e9635164c838c2854c

Count = 4
Nonce = efb94af83d32f4
Adata = a393ab976d8cf849c673b11b9b4e4fec628d1a3bad48548bffc8b40cde491677
Payload = 2fd7758d5dd0423c4c530b2dd5e50f34cd15736e2d0c8977706651dd3d4040d5

Count = 5
Nonce = 334ed91288b8a1
Adata = 6e8e63320d14e7a301a62e20df50a0b983520e4f6024a3b114b718053ffe286a
Payload = 529225e2f9ba970f2949d1f021d02f3a5349d65518faff5fa39d937433bdf92d

Count = 6
Nonce = 36ecfaf09a2a3b
Adata = 6d2341d9272cc5b1ba638771a4667fc43846496889de262789634409723c3fc8
Payload = d1ccc6c6f021f2ff4c3c55f8373676ae0e0b2e2218efaf53b2e6c469a98f5b33

Count = 7
```

```
Nonce = 0c9760b8c7c9e2
Adata = 1f2464acec51654d5d4ad81ac2efae90bc2daab250c819f03b57bd4d85900ac1
Payload = 260c8c25facfc52d0a6ad3abd76cd4d60dde7c20abd65d65654965694721a881

Count = 8
Nonce = d0e02180b21820
Adata = cc4ecc728dc47882627514dffae26f2b3de449368ce6b9d04a50ccdb9b466fa4
Payload = 174614cab67c7ababd1fae0f2fb270967592fea55ce338ae5eca021322dcea3c

Count = 9
Nonce = 9bded2301657ec
Adata = 3ed0303a478ea02519a7efaa6f31e93b87c8c6f98e334677594500c15500f69d
Payload = 5284abb125644384159bcc9afaac929f26b701e0019367fff11efbea7dd11d0d

[Nlen = 8]

Key = a786a0e068284c657d3b60873cce7bf9

Count = 10
Nonce = e0c18e4579c654b8
Adata = cf8b52f552dd0715752943428e3b32474dd71aa04cf990dfe761ed4f4e4ffcd6
Payload = e298d9dda8337cd65b82999fdab62a9e03032a32cc5b4a978f7ce60aa62c372d

Count = 11
Nonce = 7cfa21baf2ae0064
Adata = 607e6078ad86c0342265a73346d8edbfc52cc01d665b3ccb3d793b05224e6f8d
Payload = 4a877916930913240ee9c17261837edc804804022364e504769fd68a12814e08

Count = 12
Nonce = 88ef34e67d239ed7
Adata = fc772d83491023a61a37228ef6260edc0d1cb972cba610d5ad1d92d554700771
Payload = a11914ec3b3c22a4b0421adce25df6fbafc0b15d0a60fc4151f733e3da4f8fe5
.
.
.
```

B.1.4 VTT128.req

```
#  CAVS 4.0
#  "CCM-VTT" information for "CCMTest"
#  AES Keylen: 128
#  Generated on Wed Nov 24 08:34:25 2004

Alen = 32
Plen = 32
Nlen = 13

[Tlen = 4]

Key = 53337ec79c834b67eb4b18d6580fe271
Nonce = fe7fc25381853f73a3dc4195fd

Count = 0
```

```
Adata = 2ebd783e78d9778deba0047d947a3bce0344d368524545ee646331956b96fe37
Payload = 2e1d19794e21235ce4dfa8d2b41d24f9b110ccbe662a184f94337fd41d9b815a

Count = 1
Adata = 650240396020f52e8bcbb8d9efb012ed82c2b8a2b382bb10447effdc5818ee17
Payload = c97a7bef210d2ecdde0fbe9a41cd14291be034ff3501c3bff01ec6e629adadb8

Count = 2
Adata = e89cf1d3fcc2a394727394f7ec5d0b339397123d59d8d79a82e75271625228e4
Payload = 93708b1417a7df704793e927dfcf6851acc6ab4e9e754aaa1f731544a32e4ab0

Count = 3
Adata = bdf7699e91744b32638d8d0a4bd111c965b706396bdf16a6899ce1856cb0ab5a
Payload = fa53a930f1ddff9badf60ea04b5584c58bccba8d311e39efab127e07f3c5fa0c

Count = 4
Adata = 29993f9dfd24cf9b3b04a1115a667eb20fb968861562813e2ab129c55a146717
Payload = 1880f3cb1c4c49d70a8da1bdd107ff7c49c88bad715af25cfb3d0a160a94b543

Count = 5
Adata = 6d32b52598e63704108781e37c6b9d774a998a90a4e5d6539f5d6fcab6e4b6a0
Payload = e291f955b993a3919b6dd4f7bc538cda32d1abe7079daa088d8f8989f1ee087a

Count = 6
Adata = 43c12c69a5c7d57a8efaa8fb5ed0932f1ebd8c4905a72f7f4199a961f4bbd469
Payload = 40a18e849ed06ceca0586399208327c388dea0fd2c3ce25cddfe5fdbba925bfe

Count = 7
Adata = 04a6a955e47347b45e7ef57cd101184df0321fadb768134ca5806f8c257f3340
Payload = 4b6e3114d294cc5df1910a40af5bdc7b28b2cff8ecf88f45a242aa44f1af9724

Count = 8
Adata = 93ed1bcd3200511eaaa48b43fd9c0acb9876ba41e3c9659917bc25cf50c71fca
Payload = 8c0dd2d73975892342ce603c5f816700c28805509cde971fe23459c851e68aa5

Count = 9
Adata = ecdb6b90d650b01681dca5b08a79eac9c4791ddbd2c808d5f57118bf226311a0
Payload = 9084317bdc6f47f95e306e88ed125564e1e0314425a56b3c8eb695e26bf2a3b0

[Tlen = 6]

Key = aeee456645d8bba9cb95d7a629bbe24c
Nonce = ce6a7d04e1e2445a13ed80cf7e

Count = 10
Adata = 532d985f25f4d149e6763e68928edf0e4ba9fab5aacd102e53db0ffbcc11c9f9
Payload = 4862f5c9168331791c72a3a35db40f0d546768ec397739b281154327a46567bb

Count = 11
Adata = 44aec5efd2f367f731b7b672ca0d90929758d68a93f87b4f6f29da9b87274d38
Payload = 048cad0bd929bd647796e3ec36985f307ccfe1758e3bfa56a5ffd1af456417ba

Count = 12
Adata = 3b6160807a6e1ce3c85ff881992631713a2f8c31c08cedeb3f5026f63c380da0
```

```
Payload = 1a0704aefda0b567ae373172571f10517f942bcedb440d9a670ea435b6093c0d
.
.
.
```

B.1.5 DVPT128.req

```
#  CAVS 4.0
#  "CCM-DVPT" information for "CCMTest"
#  AES Keylen: 128
#  Generated on Wed Nov 24 08:34:25 2004


[Alen = 0, Plen = 0, Nlen = 7, Tlen = 4]

Key = 4061d001230e05ea0da0a06207cc1461

Count = 0
Nonce = 75d339b2b513b7
Adata = 00
Payload = 00
CT = 0873b54b

Count = 1
Nonce = f8d178dcd9d6ad
Adata = 00
Payload = 00
CT = a39e84cb

Count = 2
Nonce = ab0d73d07ddc7d
Adata = 00
Payload = 00
CT = 3cc18c74

Count = 3
Nonce = 541b37bf0061c2
Adata = 00
Payload = 00
CT = 9524b42e

Count = 4
Nonce = f88dcd04ac3baa
Adata = 00
Payload = 00
CT = 8f573cfa

Count = 5
Nonce = 90301838c40872
Adata = 00
Payload = 00
CT = 38884289
```

```
Count = 6
Nonce = 994c32701485c8
Adata = 00
Payload = 00
CT = b19068a7

Count = 7
Nonce = 784f85a53138d0
Adata = 00
Payload = 00
CT = c65c90b2

Count = 8
Nonce = 02653684462e5c
Adata = 00
Payload = 00
CT = de73bfe1

Count = 9
Nonce = 3a76ba3462b709
Adata = 00
Payload = 00
CT = 552ad388

Count = 10
Nonce = 6e0dec05c6d179
Adata = 00
Payload = 00
CT = bd33919f

Count = 11
Nonce = e785e8b8529315
Adata = 00
Payload = 00
CT = b378237a

Count = 12
Nonce = 1533f8fce57847
Adata = 00
Payload = 00
CT = 4c4cd8bc

Count = 13
Nonce = 6edf9602f991c1
Adata = 00
Payload = 00
CT = e01f2179

Count = 14
Nonce = 7ff3fc66892c8c
Adata = 00
Payload = 00
CT = 706f0f3a
```

```
[Alen = 0, Plen = 0, Nlen = 7, Tlen = 16]

Key = 4e3d964a651fbbbcb1987c3355cfb533

Count = 15
Nonce = 75d339b2b513b7
Adata = 00
Payload = 00
CT = b8ef11d1fc6c2a272f97d94d178f07f5

Count = 16
Nonce = f8d178dcd9d6ad
Adata = 00
Payload = 00
CT = f89ef45bed5e21b90a356ee52fc5c3e2

Count = 17
Nonce = ab0d73d07ddc7d
Adata = 00
Payload = 00
CT = 8b37616684c6aec924ef3b5eb6b0e4d0
.
.
.
```

B.2 Example of the *FAX* File

B.2.1 VADT128.fax

```
#  CAVS 4.0
#  "CCM-VADT" information for "CCMTest"
#  AES Keylen: 128
#  Generated on Wed Nov 24 08:34:26 2004

Plen = 32
Nlen = 13
Tlen = 16

[Alen = 0]

Key = 3a69391c2cc4d3904f1ebf26c2683506
Nonce = cf0ad6e883abf8b2d4efc8b5b6

Count = 0
Adata = 00
Payload = 917a5ec58cb4728595fcb1c813f0d1b69b9c3d620940c5a9d053945e8ec963a4
CT =
b170fbca7eb5432ff288400fffe2ea0b12e4da091c511add73bf6d7d8ecadf2ce96298c77e6f49
17c8c13b60a0e48837

Count = 1
Adata = 00
Payload = 103095480010215bda8ae2d096423a8b5d4d39704be878c0736a44a52377ff0b
```

```
CT =
303a3047f21110f1bdfe13177a500136d435de1b5ef9a7b4d086bd8623744383025e8f532ff3a5
32fa93be19c35a19c2

Count = 2
Adata = 00
Payload = fffc4c32ef9d52a73cf7c50b197d1e807868812d2e4efb7c51f60885e56b58ca
CT =
dff6e93d1d9c630d5b8334ccf56f253df11066463b5f2408f21af1a6e568e442c9304c858cd7c8
1fefeea8b6e8153846

Count = 3
Adata = 00
Payload = cefa677c99e02638c48be10986e438260df5541e7ae6136d2e2c654e44fdf6d1
CT =
eef0c2736be11792a3ff10ce6af6039b848db3756ff7cc198dc09c6d44fe4a5907f5036101e990
e3ee3ef686320129d7

Count = 4
Adata = 00
Payload = 17a4bbebee6108c275e85b499e75d8a83e9d8c486c28f344291ebd1a4724d1a7
CT =
37ae1ee41c603968129caa8e7267e315b7e56b2379392c308af2443947276d2f7b979667651910
90d81d5eb51f4449e8

Count = 5
Adata = 00
Payload = 98d296e5594651ae4dbd365977f7993ce89a18cf4876ce0cb20dc91cc553bd2f
CT =
b8d833eaab4760042ac9c79e9be5a28161e2ffa45d67117811e1303fc55001a740e5af0d93274b
3d1ad1bbf5b82dc311

Count = 6
Adata = 00
Payload = b852b3f1468c95dd13b5af0f384c14a17ecbe67f2b2dc6101cac901914cf45de
CT =
985816feb48da47774c15ec8d45e2f1cf7b301143e3c1964bf40693a14ccf95615add8dba7fe9e
1c7d771cf7ff1cf857

Count = 7
Adata = 00
Payload = c8e6e21a5c852dff9c37010444569e7c30df5e6b1e2795dfb4c9bb83c5e3cd71
CT =
e8ec4715ae841c55fb43f0c3a844a5c1b9a7b9000b364aab172542a0c5e071f9e062bf8f11dbcb
9f269a5ca4c86fbac6

Count = 8
Adata = 00
Payload = e4fa287a65b389f45fc68e6e947cab9eb35c9869d6a1f8fb4fec3916a437bbaa
CT =
c4f08d7597b2b85e38b27fa9786e90233a247f02c3b0278fec00c035a4340722bbabff68cc2a43
45c847dc82a8685cc5

Count = 9
```

```
Adata = 00
Payload = 2ebe78389e2b362e71d50f5eed781f86add57099a2aa1b5a57e1b02a7908d81e
CT =
0eb4dd376c2a078416a1fe99016a243b24ad97f2b7bbc42ef40d4909790b6496870fbb6fbec1c0
a5329ba3e7c263785b

[Alen = 1]

Key = 991cdc7221f2516b66cffbeea0167e99
Nonce = de5b5934915b4cbd13c389e248

Count = 10
Adata = 18
Payload = d85edbe823829f45506cce383d93ce1a2d3f97986b9d72643113002ac7d17fc6
CT =
b4ac2eb21efc98c40987137375e8bda24aab6d5f9c4c3a19b15397b7e037f244fd4a44f2a0945f
507a3448225286b5f4

Count = 11
Adata = d1
Payload = 3e4fad4df06ef0e833ad6057eea34490d097dfa1419efcf19804cac88eedea11
CT =
52bd5817cd10f7696a46bd1ca6d83728b7032566b64fb48c18445d55a90b6793da7fa025028243
56638efe094fcf295a

Count = 12
Adata = 87
Payload = 17587c4a63fe2a9d942c95b76a788e7b526517327f2c17723cbc524481ff9785
CT =
7baa89105e802d1ccdc748fc2203fdc335f1edf588fd5f0fbcfcc5d9a6191a071c2a7dc1a21e86
d1a1276dd809ac6d9a
.
.
.
```

B.2.2 VPT128.fax

```
#  CAVS 4.0
#  "CCM-VPT" information for "CCMTest"
#  AES Keylen: 128
#  Generated on Wed Nov 24 08:34:26 2004

Alen = 32
Nlen = 13
Tlen = 16

[Plen = 0]

Key = 3b50f8faf23e2ca176861bb9b95ef743
Nonce = ed57fb55a604a682d882320bf4

Count = 0
Adata = 982f43ecf4c6c0eec312ed7735da8136cbe53ac0531a71d619e6f1eb5cde09e1
```

```
Payload = 00
CT = d295bed6c7a08db6ec6c2a3fd398cc3d

Count = 1
Adata = 13a1583ce3a6238b2788bb5074100fcfcad5ad6bd16b2a7762d8c44a49474691
Payload = 00
CT = e6a06eaad0f0352615db9c36442da666

Count = 2
Adata = 7dd458a0fa4783d969f6c468057c604f646da57162827ee25bf646619d2fda23
Payload = 00
CT = e631f737892cb7ff43c2e07dc00dca3e

Count = 3
Adata = 2d12985b3d81ac3997dba57899d7ec2e14d0012da2c96d273aaff81601dd1bda
Payload = 00
CT = 60692e28e2eeacbb5002a056c60532e6

Count = 4
Adata = 65f2ccedef6582db35a7bd6717abf53a7070777a987b0be42e84d41b1470773f
Payload = 00
CT = c7cacfa0ef0ad5a377cb25eb609790ca

Count = 5
Adata = 6b3d82f686042a40193035be076ea23e759dea24c4eb93b2c23b028621cb9164
Payload = 00
CT = 345e53484805cf5ecbd9ede80d553881

Count = 6
Adata = 08b3e0c0189542bfeedd47557b8b811cffac553a1f24ac3f37aaea4cf114247a
Payload = 00
CT = 22cfef8e0045eb84c7aec1301697691e

Count = 7
Adata = 3070f4d07395fe870dca974f3de0a28da5855c9b0603401a4b2b288ac98bb418
Payload = 00
CT = a839dec61d5b0bb34548f115ecd93cd3

Count = 8
Adata = 0f58577c96dcbdae0c909e586e8e7987e17542ef99bb65e0f9450975fb35910f
Payload = 00
CT = b651a9464a65855ff6388c42df9b2fa6

Count = 9
Adata = 7c6b2f5cd7153d4eea5e1eb6d570a429a8b4e96ede42ee90279c82316b9b6621
Payload = 00
CT = 6bc04e4555def061cbdbbc2066e01563

[Plen = 1]

Key = 906de38ddeb0dd9a0783b75346c919d3
Nonce = 55e6fa59963fd2610c75aba802

Count = 10
```

```
Adata = 049542cf5c4357730ca618b5f039de1fbdf0a351e48509f4b90c9ef0d4ce5fdf
Payload = 1d
CT = 473d92383f279c184baf9d00c7c14e0a01

Count = 11
Adata = ecb995aa1ab070191336cc7bc6ce2e18f093577490d661189c090b95f2db52c7
Payload = 53
CT = 0916781fffaaf9b4a035494c979de24613

Count = 12
Adata = 7f37a73db7c790f76c3bb838c041e04e13c713a86cc82c461a66986e9b3a5da1
Payload = e2
CT = b8a3669045ff8554e1ccdc8cf5eb44456a
.
.
.
```

B.2.3 VNT128.fax

```
#  CAVS 4.0
#  "CCM-VNT" information for "CCMTest"
#  AES Keylen: 128
#  Generated on Wed Nov 24 08:34:26 2004

Alen = 32
Plen = 32
Tlen = 16

[Nlen = 7]

Key = b5d475ca8fa03e21b10ad13a3359a3c2

Count = 0
Nonce = 1043f6e725a430
Adata = cae697678007b0e6df925083d399d080a21ac867c18282a9ec6faf8575ba582b
Payload = 468e9d6bfc8b8749cd172eb7a1836bb5c4ff85034868af94a561d240a3a58db9
CT =
15dd22a1639506ae193a55076eed92338f1f25f6472961571fa1fd19f73d571f668aa5ba6da170
2a21092b2d6eff8bdc

Count = 1
Nonce = 38701f7ec8a60b
Adata = 39bc5f205308e974bae3690516e4664dc67fd77324348b1f0a06c88c952f33df
Payload = 57d6471b58e424a8842d29400aef26be6b78c1868cec23680a43f1c8cd917efc
CT =
2e9d442432db86b6cb60a7f08258cb522ebcbf3bda26a4482d31bffbb7baf075646b62bd67947a
4c4a03fd559706941d

Count = 2
Nonce = 0f0a17e0e52720
Adata = 38900130497e0fbcc6e38f7243d1d7a1e4ac505f72e82772ad144571e4188226
Payload = 29af8e8bfbe23afa91b1574600afba43d8fd94acf8c8e9c5a714443ee0b8a85b
```

```
CT =
f71f4ece06749ac55a52e8fac7c15350174ef91913709c53688e0408b8f0b1d753f3424171c727
a75e44bd19d2701603

Count = 3
Nonce = ce4f81bad699ba
Adata = 9d11cacfdf4582f0e442ab564c740f764f88bfe8af86abb2eb406fc9b6f070d5
Payload = 1de4f0d6745f39040c6cd04673f24ee1a68b3361d337d0e9635164c838c2854c
CT =
f4293cfb2a8a6b3315eeb20bfe6b8fda24dd1403cc8cd4c3a492961e7bbf8e521397d97def40ed
3756fc88368a795f2a

Count = 4
Nonce = efb94af83d32f4
Adata = a393ab976d8cf849c673b11b9b4e4fec628d1a3bad48548bffc8b40cde491677
Payload = 2fd7758d5dd0423c4c530b2dd5e50f34cd15736e2d0c8977706651dd3d4040d5
CT =
8f7123aec1eb3fe0103864a4fdb6cc7326a1b0db74350b848788f84d004563c899c801207fa118
11a062e6e4b2593295

Count = 5
Nonce = 334ed91288b8a1
Adata = 6e8e63320d14e7a301a62e20df50a0b983520e4f6024a3b114b718053ffe286a
Payload = 529225e2f9ba970f2949d1f021d02f3a5349d65518faff5fa39d937433bdf92d
CT =
9f943ff99ccbf08373cd1455aca3136090490d7a7f53570d120f31699bf705a683478b3d33bdc8
28afd4f257486cef6d

Count = 6
Nonce = 36ecfaf09a2a3b
Adata = 6d2341d9272cc5b1ba638771a4667fc43846496889de262789634409723c3fc8
Payload = d1ccc6c6f021f2ff4c3c55f8373676ae0e0b2e2218efaf53b2e6c469a98f5b33
CT =
395e37878321382b037389cb16e57ea89af9ce37219efae30e34328f6098a46e8a6ea44c559473
9dd39ebfb581ffb492

Count = 7
Nonce = 0c9760b8c7c9e2
Adata = 1f2464acec51654d5d4ad81ac2efae90bc2daab250c819f03b57bd4d85900ac1
Payload = 260c8c25facfc52d0a6ad3abd76cd4d60dde7c20abd65d65654965694721a881
CT =
a1926e6258e13d3a1704d0a4ac9543cb0e4bb832b05374d3aec6d5c55dbeb35699f04689856c75
71d6d9fa9839592399

Count = 8
Nonce = d0e02180b21820
Adata = cc4ecc728dc47882627514dffae26f2b3de449368ce6b9d04a50ccdb9b466fa4
Payload = 174614cab67c7ababd1fae0f2fb270967592fea55ce338ae5eca021322dcea3c
CT =
53dce3228f113a0ba586077fce901bcc48e55e4e51161fbadb9388ec40bf319644ad9ccae47d81
ddfecbb7bbdc0559a0

Count = 9
Nonce = 9bded2301657ec
```

```
Adata = 3ed0303a478ea02519a7efaa6f31e93b87c8c6f98e334677594500c15500f69d
Payload = 5284abb125644384159bcc9afaac929f26b701e0019367fff11efbea7dd11d0d
CT =
9f93cbee05fc53234692cc719c2f2cc0ae5b1c68af4e63ea2cb53eb29502e6b6736370c982d131
310cc06decf5b6bac0

[Nlen = 8]

Key = a786a0e068284c657d3b60873cce7bf9

Count = 10
Nonce = e0c18e4579c654b8
Adata = cf8b52f552dd0715752943428e3b32474dd71aa04cf990dfe761ed4f4e4ffcd6
Payload = e298d9dda8337cd65b82999fdab62a9e03032a32cc5b4a978f7ce60aa62c372d
CT =
0aacfb362248f6b086048c963266e28fa82623926966d19c3404e66486e0987463889e1e77dc3c
01eb9c06ca58bf66ad

Count = 11
Nonce = 7cfa21baf2ae0064
Adata = 607e6078ad86c0342265a73346d8edbfc52cc01d665b3ccb3d793b05224e6f8d
Payload = 4a877916930913240ee9c17261837edc804804022364e504769fd68a12814e08
CT =
dc4809613a7fbe5992e4f4701403bf4c024247bcd27ea3a0aaf6deb9f3ffe585f461843b8f6068
79ab546dbedc184bce

Count = 12
Nonce = 88ef34e67d239ed7
Adata = fc772d83491023a61a37228ef6260edc0d1cb972cba610d5ad1d92d554700771
Payload = a11914ec3b3c22a4b0421adce25df6fbafc0b15d0a60fc4151f733e3da4f8fe5
CT =
703d61c75e922461967f320354f39903c110881f7ab4677d1c80d6ebdee2f1ef829998e37e464d
ec6e4f349b95e8e6f5
.
.
.
```

B.2.4 VTT128.fax

```
#  CAVS 4.0
#  "CCM-VTT" information for "CCMTest"
#  AES Keylen: 128
#  Generated on Wed Nov 24 08:34:26 2004

Alen = 32
Plen = 32
Nlen = 13

[Tlen = 4]

Key = 53337ec79c834b67eb4b18d6580fe271
Nonce = fe7fc25381853f73a3dc4195fd
```

```
Count = 0
Adata = 2ebd783e78d9778deba0047d947a3bce0344d368524545ee646331956b96fe37
Payload = 2e1d19794e21235ce4dfa8d2b41d24f9b110ccbe662a184f94337fd41d9b815a
CT = ddbf06693ff501aaec29a93fcc5ddd27c343b9337a94eab5734417a4972b11a971597802

Count = 1
Adata = 650240396020f52e8bcbb8d9efb012ed82c2b8a2b382bb10447effdc5818ee17
Payload = c97a7bef210d2ecdde0fbe9a41cd14291be034ff3501c3bff01ec6e629adadb8
CT = 3ad864ff50d90c3bd6f9bf77398dedf769b3417229bf31451769ae96a31d3d4bcd6f7020

Count = 2
Adata = e89cf1d3fcc2a394727394f7ec5d0b339397123d59d8d79a82e75271625228e4
Payload = 93708b1417a7df704793e927dfcf6851acc6ab4e9e754aaa1f731544a32e4ab0
CT = 60d294046673fd864f65e8caa78f918fde95dec382cbb850f8047d34299eda43c1ea5ac2

Count = 3
Adata = bdf7699e91744b32638d8d0a4bd111c965b706396bdf16a6899ce1856cb0ab5a
Payload = fa53a930f1ddff9badf60ea04b5584c58bccba8d311e39efab127e07f3c5fa0c
CT = 09f1b6208009dd6da5000f4d33157d1bf99fcf002da0cb154c65167779756aff94ded012

Count = 4
Adata = 29993f9dfd24cf9b3b04a1115a667eb20fb968861562813e2ab129c55a146717
Payload = 1880f3cb1c4c49d70a8da1bdd107ff7c49c88bad715af25cfb3d0a160a94b543
CT = eb22ecdb6d986b21027ba050a94706a23b9bfe206de400a61c4a6266802425b0a24534cf

Count = 5
Adata = 6d32b52598e63704108781e37c6b9d774a998a90a4e5d6539f5d6fcab6e4b6a0
Payload = e291f955b993a3919b6dd4f7bc538cda32d1abe7079daa088d8f8989f1ee087a
CT = 1133e645c8478167939bd51ac41375044082de6a1b2358f26af8e1f97b5e98890c8bb074

Count = 6
Adata = 43c12c69a5c7d57a8efaa8fb5ed0932f1ebd8c4905a72f7f4199a961f4bbd469
Payload = 40a18e849ed06ceca0586399208327c388dea0fd2c3ce25cddfe5fdbba925bfe
CT = b3039194ef044e1aa8ae627458c3de1dfa8dd570308210a63a8937ab3022cb0d5ff80129

Count = 7
Adata = 04a6a955e47347b45e7ef57cd101184df0321fadb768134ca5806f8c257f3340
Payload = 4b6e3114d294cc5df1910a40af5bdc7b28b2cff8ecf88f45a242aa44f1af9724
CT = b8cc2e04a340eeabf9670badd71b25a55ae1ba75f0467dbf4535c2347b1f07d7a6285f76

Count = 8
Adata = 93ed1bcd3200511eaaa48b43fd9c0acb9876ba41e3c9659917bc25cf50c71fca
Payload = 8c0dd2d73975892342ce603c5f816700c28805509cde971fe23459c851e68aa5
CT = 7fafcdc748a1abd54a3861d127c19edeb0db70dd806065e5054331b8db561a568f2a76d1

Count = 9
Adata = ecdb6b90d650b01681dca5b08a79eac9c4791ddbd2c808d5f57118bf226311a0
Payload = 9084317bdc6f47f95e306e88ed125564e1e0314425a56b3c8eb695e26bf2a3b0
CT = 63262e6badbb650f56c66f659552acba93b344c9391b99c669c1fd92e14233430709e0cd

[Tlen = 6]

Key = aeee456645d8bba9cb95d7a629bbe24c
Nonce = ce6a7d04e1e2445a13ed80cf7e
```

```
Count = 10
Adata = 532d985f25f4d149e6763e68928edf0e4ba9fab5aacd102e53db0ffbcc11c9f9
Payload = 4862f5c9168331791c72a3a35db40f0d546768ec397739b281154327a46567bb
CT =
07b42bcd3b1f5571f39e524f6900b2f0cd72ac9a69557d1c7ea1b7b0ed06260e40566257447c

Count = 11
Adata = 44aec5efd2f367f731b7b672ca0d90929758d68a93f87b4f6f29da9b87274d38
Payload = 048cad0bd929bd647796e3ec36985f307ccfe1758e3bfa56a5ffd1af456417ba
CT =
4b5a730ff4b5d96c987a1200022ce2cde5da2503de19bef85a4b25380c07560f1cc4865f4033

Count = 12
Adata = 3b6160807a6e1ce3c85ff881992631713a2f8c31c08cedeb3f5026f63c380da0
Payload = 1a0704aefda0b567ae373172571f10517f942bcedb440d9a670ea435b6093c0d
CT =
55d1daaad03cd16f41dbc09e63abadace681efb88b66493498ba50a2ff6a7db8b2a9c10eec48
.
.
.
```

B.2.5 DVPT128.fax

```
#  CAVS 4.0
#  "CCM-DVPT" information for "CCMTest"
#  AES Keylen: 128
#  Generated on Wed Nov 24 08:34:26 2004


[Alen = 0, Plen = 0, Nlen = 7, Tlen = 4]

Key = 4061d001230e05ea0da0a06207cc1461

Count = 0
Nonce = 75d339b2b513b7
Adata = 00
Payload = 00
CT = 0873b54b
Result = Pass

Count = 1
Nonce = f8d178dcd9d6ad
Adata = 00
Payload = 00
CT = a39e84cb
Result = Pass

Count = 2
Nonce = ab0d73d07ddc7d
Adata = 00
Payload = 00
```

```
CT = 3cc18c74
Result = Fail

Count = 3
Nonce = 541b37bf0061c2
Adata = 00
Payload = 00
CT = 9524b42e
Result = Fail

Count = 4
Nonce = f88dcd04ac3baa
Adata = 00
Payload = 00
CT = 8f573cfa
Result = Pass

Count = 5
Nonce = 90301838c40872
Adata = 00
Payload = 00
CT = 38884289
Result = Fail

Count = 6
Nonce = 994c32701485c8
Adata = 00
Payload = 00
CT = b19068a7
Result = Pass

Count = 7
Nonce = 784f85a53138d0
Adata = 00
Payload = 00
CT = c65c90b2
Result = Fail

Count = 8
Nonce = 02653684462e5c
Adata = 00
Payload = 00
CT = de73bfe1
Result = Fail

Count = 9
Nonce = 3a76ba3462b709
Adata = 00
Payload = 00
CT = 552ad388
Result = Fail

Count = 10
Nonce = 6e0dec05c6d179
```

```
Adata = 00
Payload = 00
CT = bd33919f
Result = Fail

Count = 11
Nonce = e785e8b8529315
Adata = 00
Payload = 00
CT = b378237a
Result = Pass

Count = 12
Nonce = 1533f8fce57847
Adata = 00
Payload = 00
CT = 4c4cd8bc
Result = Fail

Count = 13
Nonce = 6edf9602f991c1
Adata = 00
Payload = 00
CT = e01f2179
Result = Fail

Count = 14
Nonce = 7ff3fc66892c8c
Adata = 00
Payload = 00
CT = 706f0f3a
Result = Fail

[Alen = 0, Plen = 0, Nlen = 7, Tlen = 16]

Key = 4e3d964a651fbbbcb1987c3355cfb533

Count = 15
Nonce = 75d339b2b513b7
Adata = 00
Payload = 00
CT = b8ef11d1fc6c2a272f97d94d178f07f5
Result = Pass

Count = 16
Nonce = f8d178dcd9d6ad
Adata = 00
Payload = 00
CT = f89ef45bed5e21b90a356ee52fc5c3e2
Result = Pass

Count = 17
Nonce = ab0d73d07ddc7d
Adata = 00
```

```
Payload = 00
CT = 8b37616684c6aec924ef3b5eb6b0e4d0
Result = Fail
.
.
.
```

B.3 Example of the *RESPONSE* File

B.3.1 VADT128.rsp

```
#  CAVS 4.0
#  "CCM-VADT" information for "CCMTest"
#  AES Keylen: 128

Plen = 32
Nlen = 13
Tlen = 16

[Alen = 0]

Key = 3a69391c2cc4d3904f1ebf26c2683506
Nonce = cf0ad6e883abf8b2d4efc8b5b6

Count = 0
Adata = 00
Payload = 917a5ec58cb4728595fcb1c813f0d1b69b9c3d620940c5a9d053945e8ec963a4
CT =
b170fbca7eb5432ff288400fffe2ea0b12e4da091c511add73bf6d7d8ecadf2ce96298c77e6f49
17c8c13b60a0e48837

Count = 1
Adata = 00
Payload = 103095480010215bda8ae2d096423a8b5d4d39704be878c0736a44a52377ff0b
CT =
303a3047f21110f1bdfe13177a500136d435de1b5ef9a7b4d086bd8623744383025e8f532ff3a5
32fa93be19c35a19c2

Count = 2
Adata = 00
Payload = fffc4c32ef9d52a73cf7c50b197d1e807868812d2e4efb7c51f60885e56b58ca
CT =
dff6e93d1d9c630d5b8334ccf56f253df11066463b5f2408f21af1a6e568e442c9304c858cd7c8
1fefeea8b6e8153846

Count = 3
Adata = 00
Payload = cefa677c99e02638c48be10986e438260df5541e7ae6136d2e2c654e44fdf6d1
CT =
eef0c2736be11792a3ff10ce6af6039b848db3756ff7cc198dc09c6d44fe4a5907f5036101e990
e3ee3ef686320129d7

Count = 4
```

```
Adata = 00
Payload = 17a4bbebee6108c275e85b499e75d8a83e9d8c486c28f344291ebd1a4724d1a7
CT =
37ae1ee41c603968129caa8e7267e315b7e56b2379392c308af2443947276d2f7b979667651910
90d81d5eb51f4449e8

Count = 5
Adata = 00
Payload = 98d296e5594651ae4dbd365977f7993ce89a18cf4876ce0cb20dc91cc553bd2f
CT =
b8d833eaab4760042ac9c79e9be5a28161e2ffa45d67117811e1303fc55001a740e5af0d93274b
3d1ad1bbf5b82dc311

Count = 6
Adata = 00
Payload = b852b3f1468c95dd13b5af0f384c14a17ecbe67f2b2dc6101cac901914cf45de
CT =
985816feb48da47774c15ec8d45e2f1cf7b301143e3c1964bf40693a14ccf95615add8dba7fe9e
1c7d771cf7ff1cf857

Count = 7
Adata = 00
Payload = c8e6e21a5c852dff9c37010444569e7c30df5e6b1e2795dfb4c9bb83c5e3cd71
CT =
e8ec4715ae841c55fb43f0c3a844a5c1b9a7b9000b364aab172542a0c5e071f9e062bf8f11dbcb
9f269a5ca4c86fbac6

Count = 8
Adata = 00
Payload = e4fa287a65b389f45fc68e6e947cab9eb35c9869d6a1f8fb4fec3916a437bbaa
CT =
c4f08d7597b2b85e38b27fa9786e90233a247f02c3b0278fec00c035a4340722bbabff68cc2a43
45c847dc82a8685cc5

Count = 9
Adata = 00
Payload = 2ebe78389e2b362e71d50f5eed781f86add57099a2aa1b5a57e1b02a7908d81e
CT =
0eb4dd376c2a078416a1fe99016a243b24ad97f2b7bbc42ef40d4909790b6496870fbb6fbec1c0
a5329ba3e7c263785b

[Alen = 1]

Key = 991cdc7221f2516b66cffbeea0167e99
Nonce = de5b5934915b4cbd13c389e248

Count = 10
Adata = 18
Payload = d85edbe823829f45506cce383d93ce1a2d3f97986b9d72643113002ac7d17fc6
CT =
b4ac2eb21efc98c40987137375e8bda24aab6d5f9c4c3a19b15397b7e037f244fd4a44f2a0945f
507a3448225286b5f4

Count = 11
```

```
Adata = d1
Payload = 3e4fad4df06ef0e833ad6057eea34490d097dfa1419efcf19804cac88eedea11
CT =
52bd5817cd10f7696a46bd1ca6d83728b7032566b64fb48c18445d55a90b6793da7fa025028243
56638efe094fcf295a

Count = 12
Adata = 87
Payload = 17587c4a63fe2a9d942c95b76a788e7b526517327f2c17723cbc524481ff9785
CT =
7baa89105e802d1ccdc748fc2203fdc335f1edf588fd5f0fbcfcc5d9a6191a071c2a7dc1a21e86
d1a1276dd809ac6d9a
.
.
.
```

B.3.2 VPT128.rsp

```
#  CAVS 4.0
#  "CCM-VPT" information for "CCMTest"
#  AES Keylen: 128

Alen = 32
Nlen = 13
Tlen = 16

[Plen = 0]

Key = 3b50f8faf23e2ca176861bb9b95ef743
Nonce = ed57fb55a604a682d882320bf4

Count = 0
Adata = 982f43ecf4c6c0eec312ed7735da8136cbe53ac0531a71d619e6f1eb5cde09e1
Payload = 00
CT = d295bed6c7a08db6ec6c2a3fd398cc3d

Count = 1
Adata = 13a1583ce3a6238b2788bb5074100fcfcad5ad6bd16b2a7762d8c44a49474691
Payload = 00
CT = e6a06eaad0f0352615db9c36442da666

Count = 2
Adata = 7dd458a0fa4783d969f6c468057c604f646da57162827ee25bf646619d2fda23
Payload = 00
CT = e631f737892cb7ff43c2e07dc00dca3e

Count = 3
Adata = 2d12985b3d81ac3997dba57899d7ec2e14d0012da2c96d273aaff81601dd1bda
Payload = 00
CT = 60692e28e2eeacbb5002a056c60532e6

Count = 4
Adata = 65f2ccedef6582db35a7bd6717abf53a7070777a987b0be42e84d41b1470773f
```

```
Payload = 00
CT = c7cacfa0ef0ad5a377cb25eb609790ca

Count = 5
Adata = 6b3d82f686042a40193035be076ea23e759dea24c4eb93b2c23b028621cb9164
Payload = 00
CT = 345e53484805cf5ecbd9ede80d553881

Count = 6
Adata = 08b3e0c0189542bfeedd47557b8b811cffac553a1f24ac3f37aaea4cf114247a
Payload = 00
CT = 22cfef8e0045eb84c7aec1301697691e

Count = 7
Adata = 3070f4d07395fe870dca974f3de0a28da5855c9b0603401a4b2b288ac98bb418
Payload = 00
CT = a839dec61d5b0bb34548f115ecd93cd3

Count = 8
Adata = 0f58577c96dcbdae0c909e586e8e7987e17542ef99bb65e0f9450975fb35910f
Payload = 00
CT = b651a9464a65855ff6388c42df9b2fa6

Count = 9
Adata = 7c6b2f5cd7153d4eea5e1eb6d570a429a8b4e96ede42ee90279c82316b9b6621
Payload = 00
CT = 6bc04e4555def061cbdbbc2066e01563

[Plen = 1]

Key = 906de38ddeb0dd9a0783b75346c919d3
Nonce = 55e6fa59963fd2610c75aba802

Count = 10
Adata = 049542cf5c4357730ca618b5f039de1fbdf0a351e48509f4b90c9ef0d4ce5fdf
Payload = 1d
CT = 473d92383f279c184baf9d00c7c14e0a01

Count = 11
Adata = ecb995aa1ab070191336cc7bc6ce2e18f093577490d661189c090b95f2db52c7
Payload = 53
CT = 0916781fffaaf9b4a035494c979de24613

Count = 12
Adata = 7f37a73db7c790f76c3bb838c041e04e13c713a86cc82c461a66986e9b3a5da1
Payload = e2
CT = b8a3669045ff8554e1ccdc8cf5eb44456a
.
.
.
```

B.3.3 VNT128.rsp

```
#  CAVS 4.0
#  "CCM-VNT" information for "CCMTest"
#  AES Keylen: 128

Alen = 32
Plen = 32
Tlen = 16

[Nlen = 7]

Key = b5d475ca8fa03e21b10ad13a3359a3c2

Count = 0
Nonce = 1043f6e725a430
Adata = cae697678007b0e6df925083d399d080a21ac867c18282a9ec6faf8575ba582b
Payload = 468e9d6bfc8b8749cd172eb7a1836bb5c4ff85034868af94a561d240a3a58db9
CT =
15dd22a1639506ae193a55076eed92338f1f25f6472961571fa1fd19f73d571f668aa5ba6da170
2a21092b2d6eff8bdc

Count = 1
Nonce = 38701f7ec8a60b
Adata = 39bc5f205308e974bae3690516e4664dc67fd77324348b1f0a06c88c952f33df
Payload = 57d6471b58e424a8842d29400aef26be6b78c1868cec23680a43f1c8cd917efc
CT =
2e9d442432db86b6cb60a7f08258cb522ebcbf3bda26a4482d31bffbb7baf075646b62bd67947a
4c4a03fd559706941d

Count = 2
Nonce = 0f0a17e0e52720
Adata = 38900130497e0fbcc6e38f7243d1d7a1e4ac505f72e82772ad144571e4188226
Payload = 29af8e8bfbe23afa91b1574600afba43d8fd94acf8c8e9c5a714443ee0b8a85b
CT =
f71f4ece06749ac55a52e8fac7c15350174ef91913709c53688e0408b8f0b1d753f3424171c727
a75e44bd19d2701603

Count = 3
Nonce = ce4f81bad699ba
Adata = 9d11cacfdf4582f0e442ab564c740f764f88bfe8af86abb2eb406fc9b6f070d5
Payload = 1de4f0d6745f39040c6cd04673f24ee1a68b3361d337d0e9635164c838c2854c
CT =
f4293cfb2a8a6b3315eeb20bfe6b8fda24dd1403cc8cd4c3a492961e7bbf8e521397d97def40ed
3756fc88368a795f2a

Count = 4
Nonce = efb94af83d32f4
Adata = a393ab976d8cf849c673b11b9b4e4fec628d1a3bad48548bffc8b40cde491677
Payload = 2fd7758d5dd0423c4c530b2dd5e50f34cd15736e2d0c8977706651dd3d4040d5
CT =
8f7123aec1eb3fe0103864a4fdb6cc7326a1b0db74350b848788f84d004563c899c801207fa118
11a062e6e4b2593295
```

```
Count = 5
Nonce = 334ed91288b8a1
Adata = 6e8e63320d14e7a301a62e20df50a0b983520e4f6024a3b114b718053ffe286a
Payload = 529225e2f9ba970f2949d1f021d02f3a5349d65518faff5fa39d937433bdf92d
CT =
9f943ff99ccbf08373cd1455aca3136090490d7a7f53570d120f31699bf705a683478b3d33bdc8
28afd4f257486cef6d

Count = 6
Nonce = 36ecfaf09a2a3b
Adata = 6d2341d9272cc5b1ba638771a4667fc43846496889de262789634409723c3fc8
Payload = d1ccc6c6f021f2ff4c3c55f8373676ae0e0b2e2218efaf53b2e6c469a98f5b33
CT =
395e37878321382b037389cb16e57ea89af9ce37219efae30e34328f6098a46e8a6ea44c559473
9dd39ebfb581ffb492

Count = 7
Nonce = 0c9760b8c7c9e2
Adata = 1f2464acec51654d5d4ad81ac2efae90bc2daab250c819f03b57bd4d85900ac1
Payload = 260c8c25facfc52d0a6ad3abd76cd4d60dde7c20abd65d65654965694721a881
CT =
a1926e6258e13d3a1704d0a4ac9543cb0e4bb832b05374d3aec6d5c55dbeb35699f04689856c75
71d6d9fa9839592399

Count = 8
Nonce = d0e02180b21820
Adata = cc4ecc728dc47882627514dffae26f2b3de449368ce6b9d04a50ccdb9b466fa4
Payload = 174614cab67c7ababd1fae0f2fb270967592fea55ce338ae5eca021322dcea3c
CT =
53dce3228f113a0ba586077fce901bcc48e55e4e51161fbadb9388ec40bf319644ad9ccae47d81
ddfecbb7bbdc0559a0

Count = 9
Nonce = 9bded2301657ec
Adata = 3ed0303a478ea02519a7efaa6f31e93b87c8c6f98e334677594500c15500f69d
Payload = 5284abb125644384159bcc9afaac929f26b701e0019367fff11efbea7dd11d0d
CT =
9f93cbee05fc53234692cc719c2f2cc0ae5b1c68af4e63ea2cb53eb29502e6b6736370c982d131
310cc06decf5b6bac0

[Nlen = 8]

Key = a786a0e068284c657d3b60873cce7bf9

Count = 10
Nonce = e0c18e4579c654b8
Adata = cf8b52f552dd0715752943428e3b32474dd71aa04cf990dfe761ed4f4e4ffcd6
Payload = e298d9dda8337cd65b82999fdab62a9e03032a32cc5b4a978f7ce60aa62c372d
CT =
0aacfb362248f6b086048c963266e28fa82623926966d19c3404e66486e0987463889e1e77dc3c
01eb9c06ca58bf66ad

Count = 11
```

```
Nonce = 7cfa21baf2ae0064
Adata = 607e6078ad86c0342265a73346d8edbfc52cc01d665b3ccb3d793b05224e6f8d
Payload = 4a877916930913240ee9c17261837edc804804022364e504769fd68a12814e08
CT =
dc4809613a7fbe5992e4f4701403bf4c024247bcd27ea3a0aaf6deb9f3ffe585f461843b8f6068
79ab546dbedc184bce

Count = 12
Nonce = 88ef34e67d239ed7
Adata = fc772d83491023a61a37228ef6260edc0d1cb972cba610d5ad1d92d554700771
Payload = a11914ec3b3c22a4b0421adce25df6fbafc0b15d0a60fc4151f733e3da4f8fe5
CT =
703d61c75e922461967f320354f39903c110881f7ab4677d1c80d6ebdee2f1ef829998e37e464d
ec6e4f349b95e8e6f5
.
.
.
```

B.3.4 VTT128.rsp

```
#  CAVS 4.0
#  "CCM-VTT" information for "CCMTest"
#  AES Keylen: 128

Alen = 32
Plen = 32
Nlen = 13

[Tlen = 4]

Key = 53337ec79c834b67eb4b18d6580fe271
Nonce = fe7fc25381853f73a3dc4195fd

Count = 0
Adata = 2ebd783e78d9778deba0047d947a3bce0344d368524545ee646331956b96fe37
Payload = 2e1d19794e21235ce4dfa8d2b41d24f9b110ccbe662a184f94337fd41d9b815a
CT = ddbf06693ff501aaec29a93fcc5ddd27c343b9337a94eab5734417a4972b11a971597802

Count = 1
Adata = 650240396020f52e8bcbb8d9efb012ed82c2b8a2b382bb10447effdc5818ee17
Payload = c97a7bef210d2ecdde0fbe9a41cd14291be034ff3501c3bff01ec6e629adadb8
CT = 3ad864ff50d90c3bd6f9bf77398dedf769b3417229bf31451769ae96a31d3d4bcd6f7020

Count = 2
Adata = e89cf1d3fcc2a394727394f7ec5d0b339397123d59d8d79a82e75271625228e4
Payload = 93708b1417a7df704793e927dfcf6851acc6ab4e9e754aaa1f731544a32e4ab0
CT = 60d294046673fd864f65e8caa78f918fde95dec382cbb850f8047d34299eda43c1ea5ac2

Count = 3
Adata = bdf7699e91744b32638d8d0a4bd111c965b706396bdf16a6899ce1856cb0ab5a
Payload = fa53a930f1ddff9badf60ea04b5584c58bccba8d311e39efab127e07f3c5fa0c
CT = 09f1b6208009dd6da5000f4d33157d1bf99fcf002da0cb154c65167779756aff94ded012
```

```
Count = 4
Adata = 29993f9dfd24cf9b3b04a1115a667eb20fb968861562813e2ab129c55a146717
Payload = 1880f3cb1c4c49d70a8da1bdd107ff7c49c88bad715af25cfb3d0a160a94b543
CT = eb22ecdb6d986b21027ba050a94706a23b9bfe206de400a61c4a6266802425b0a24534cf

Count = 5
Adata = 6d32b52598e63704108781e37c6b9d774a998a90a4e5d6539f5d6fcab6e4b6a0
Payload = e291f955b993a3919b6dd4f7bc538cda32d1abe7079daa088d8f8989f1ee087a
CT = 1133e645c8478167939bd51ac41375044082de6a1b2358f26af8e1f97b5e98890c8bb074

Count = 6
Adata = 43c12c69a5c7d57a8efaa8fb5ed0932f1ebd8c4905a72f7f4199a961f4bbd469
Payload = 40a18e849ed06ceca0586399208327c388dea0fd2c3ce25cddfe5fdbba925bfe
CT = b3039194ef044e1aa8ae627458c3de1dfa8dd570308210a63a8937ab3022cb0d5ff80129

Count = 7
Adata = 04a6a955e47347b45e7ef57cd101184df0321fadb768134ca5806f8c257f3340
Payload = 4b6e3114d294cc5df1910a40af5bdc7b28b2cff8ecf88f45a242aa44f1af9724
CT = b8cc2e04a340eeabf9670badd71b25a55ae1ba75f0467dbf4535c2347b1f07d7a6285f76

Count = 8
Adata = 93ed1bcd3200511eaaa48b43fd9c0acb9876ba41e3c9659917bc25cf50c71fca
Payload = 8c0dd2d73975892342ce603c5f816700c28805509cde971fe23459c851e68aa5
CT = 7fafcdc748a1abd54a3861d127c19edeb0db70dd806065e5054331b8db561a568f2a76d1

Count = 9
Adata = ecdb6b90d650b01681dca5b08a79eac9c4791ddbd2c808d5f57118bf226311a0
Payload = 9084317bdc6f47f95e306e88ed125564e1e0314425a56b3c8eb695e26bf2a3b0
CT = 63262e6badbb650f56c66f659552acba93b344c9391b99c669c1fd92e14233430709e0cd

[Tlen = 6]

Key = aeee456645d8bba9cb95d7a629bbe24c
Nonce = ce6a7d04e1e2445a13ed80cf7e

Count = 10
Adata = 532d985f25f4d149e6763e68928edf0e4ba9fab5aacd102e53db0ffbcc11c9f9
Payload = 4862f5c9168331791c72a3a35db40f0d546768ec397739b281154327a46567bb
CT =
07b42bcd3b1f5571f39e524f6900b2f0cd72ac9a69557d1c7ea1b7b0ed06260e40566257447c

Count = 11
Adata = 44aec5efd2f367f731b7b672ca0d90929758d68a93f87b4f6f29da9b87274d38
Payload = 048cad0bd929bd647796e3ec36985f307ccfe1758e3bfa56a5ffd1af456417ba
CT =
4b5a730ff4b5d96c987a1200022ce2cde5da2503de19bef85a4b25380c07560f1cc4865f4033

Count = 12
Adata = 3b6160807a6e1ce3c85ff881992631713a2f8c31c08cedeb3f5026f63c380da0
Payload = 1a0704aefda0b567ae373172571f10517f942bcedb440d9a670ea435b6093c0d
CT =
55d1daaad03cd16f41dbc09e63abadace681efb88b66493498ba50a2ff6a7db8b2a9c10eec48
.
.
```

.

B.3.5 DVPT128.rsp

```
#  CAVS 4.0
#  "CCM-DVPT" information for "CCMTest"
#  AES Keylen: 128


[Alen = 0, Plen = 0, Nlen = 7, Tlen = 4]

Key = 4061d001230e05ea0da0a06207cc1461

Count = 0
Nonce = 75d339b2b513b7
Adata = 00
Payload = 00
CT = 0873b54b
Result = Pass

Count = 1
Nonce = f8d178dcd9d6ad
Adata = 00
Payload = 00
CT = a39e84cb
Result = Pass

Count = 2
Nonce = ab0d73d07ddc7d
Adata = 00
Payload = 00
CT = 3cc18c74
Result = Fail

Count = 3
Nonce = 541b37bf0061c2
Adata = 00
Payload = 00
CT = 9524b42e
Result = Fail

Count = 4
Nonce = f88dcd04ac3baa
Adata = 00
Payload = 00
CT = 8f573cfa
Result = Pass

Count = 5
Nonce = 90301838c40872
Adata = 00
Payload = 00
CT = 38884289
```

```
Result = Fail

Count = 6
Nonce = 994c32701485c8
Adata = 00
Payload = 00
CT = b19068a7
Result = Pass

Count = 7
Nonce = 784f85a53138d0
Adata = 00
Payload = 00
CT = c65c90b2
Result = Fail

Count = 8
Nonce = 02653684462e5c
Adata = 00
Payload = 00
CT = de73bfe1
Result = Fail

Count = 9
Nonce = 3a76ba3462b709
Adata = 00
Payload = 00
CT = 552ad388
Result = Fail

Count = 10
Nonce = 6e0dec05c6d179
Adata = 00
Payload = 00
CT = bd33919f
Result = Fail

Count = 11
Nonce = e785e8b8529315
Adata = 00
Payload = 00
CT = b378237a
Result = Pass

Count = 12
Nonce = 1533f8fce57847
Adata = 00
Payload = 00
CT = 4c4cd8bc
Result = Fail

Count = 13
Nonce = 6edf9602f991c1
Adata = 00
```

```
Payload = 00
CT = e01f2179
Result = Fail

Count = 14
Nonce = 7ff3fc66892c8c
Adata = 00
Payload = 00
CT = 706f0f3a
Result = Fail

[Alen = 0, Plen = 0, Nlen = 7, Tlen = 16]

Key = 4e3d964a651fbbbcb1987c3355cfb533

Count = 15
Nonce = 75d339b2b513b7
Adata = 00
Payload = 00
CT = b8ef11d1fc6c2a272f97d94d178f07f5
Result = Pass

Count = 16
Nonce = f8d178dcd9d6ad
Adata = 00
Payload = 00
CT = f89ef45bed5e21b90a356ee52fc5c3e2
Result = Pass

Count = 17
Nonce = ab0d73d07ddc7d
Adata = 00
Payload = 00
CT = 8b37616684c6aec924ef3b5eb6b0e4d0
Result = Fail
.
.
.
```

B.4 Example of the *SAMPLE* File

B.4.1 VADT128.sam

```
#  CAVS 4.0
#  "CCM-VADT" information for "CCMTest"
#  AES Keylen: 128
#  Generated on Wed Nov 24 08:34:26 2004

Plen = 32
Nlen = 13
Tlen = 16

[Alen = 0]
```

```
Key = 3a69391c2cc4d3904f1ebf26c2683506
Nonce = cf0ad6e883abf8b2d4efc8b5b6

Count = 0
Adata = 00
Payload = 917a5ec58cb4728595fcb1c813f0d1b69b9c3d620940c5a9d053945e8ec963a4
CT = ?

Count = 1
Adata = 00
Payload = 103095480010215bda8ae2d096423a8b5d4d39704be878c0736a44a52377ff0b
CT = ?

Count = 2
Adata = 00
Payload = fffc4c32ef9d52a73cf7c50b197d1e807868812d2e4efb7c51f60885e56b58ca
CT = ?

Count = 3
Adata = 00
Payload = cefa677c99e02638c48be10986e438260df5541e7ae6136d2e2c654e44fdf6d1
CT = ?

Count = 4
Adata = 00
Payload = 17a4bbebee6108c275e85b499e75d8a83e9d8c486c28f344291ebd1a4724d1a7
CT = ?

Count = 5
Adata = 00
Payload = 98d296e5594651ae4dbd365977f7993ce89a18cf4876ce0cb20dc91cc553bd2f
CT = ?

Count = 6
Adata = 00
Payload = b852b3f1468c95dd13b5af0f384c14a17ecbe67f2b2dc6101cac901914cf45de
CT = ?

Count = 7
Adata = 00
Payload = c8e6e21a5c852dff9c37010444569e7c30df5e6b1e2795dfb4c9bb83c5e3cd71
CT = ?

Count = 8
Adata = 00
Payload = e4fa287a65b389f45fc68e6e947cab9eb35c9869d6a1f8fb4fec3916a437bbaa
CT = ?

Count = 9
Adata = 00
Payload = 2ebe78389e2b362e71d50f5eed781f86add57099a2aa1b5a57e1b02a7908d81e
CT = ?
```

```
[Alen = 1]

Key = 991cdc7221f2516b66cffbeea0167e99
Nonce = de5b5934915b4cbd13c389e248

Count = 10
Adata = 18
Payload = d85edbe823829f45506cce383d93ce1a2d3f97986b9d72643113002ac7d17fc6
CT = ?

Count = 11
Adata = d1
Payload = 3e4fad4df06ef0e833ad6057eea34490d097dfa1419efcf19804cac88eedea11
CT = ?

Count = 12
Adata = 87
Payload = 17587c4a63fe2a9d942c95b76a788e7b526517327f2c17723cbc524481ff9785
CT = ?
.
.
.
```

B.4.2 VPT128.sam

```
#  CAVS 4.0
#  "CCM-VPT" information for "CCMTest"
#  AES Keylen: 128
#  Generated on Wed Nov 24 08:34:26 2004

Alen = 32
Nlen = 13
Tlen = 16

[Plen = 0]

Key = 3b50f8faf23e2ca176861bb9b95ef743
Nonce = ed57fb55a604a682d882320bf4

Count = 0
Adata = 982f43ecf4c6c0eec312ed7735da8136cbe53ac0531a71d619e6f1eb5cde09e1
Payload = 00
CT = ?

Count = 1
Adata = 13a1583ce3a6238b2788bb5074100fcfcad5ad6bd16b2a7762d8c44a49474691
Payload = 00
CT = ?

Count = 2
Adata = 7dd458a0fa4783d969f6c468057c604f646da57162827ee25bf646619d2fda23
Payload = 00
CT = ?
```

```
Count = 3
Adata = 2d12985b3d81ac3997dba57899d7ec2e14d0012da2c96d273aaff81601dd1bda
Payload = 00
CT = ?

Count = 4
Adata = 65f2ccedef6582db35a7bd6717abf53a7070777a987b0be42e84d41b1470773f
Payload = 00
CT = ?

Count = 5
Adata = 6b3d82f686042a40193035be076ea23e759dea24c4eb93b2c23b028621cb9164
Payload = 00
CT = ?

Count = 6
Adata = 08b3e0c0189542bfeedd47557b8b811cffac553a1f24ac3f37aaea4cf114247a
Payload = 00
CT = ?

Count = 7
Adata = 3070f4d07395fe870dca974f3de0a28da5855c9b0603401a4b2b288ac98bb418
Payload = 00
CT = ?

Count = 8
Adata = 0f58577c96dcbdae0c909e586e8e7987e17542ef99bb65e0f9450975fb35910f
Payload = 00
CT = ?

Count = 9
Adata = 7c6b2f5cd7153d4eea5e1eb6d570a429a8b4e96ede42ee90279c82316b9b6621
Payload = 00
CT = ?

[Plen = 1]

Key = 906de38ddeb0dd9a0783b75346c919d3
Nonce = 55e6fa59963fd2610c75aba802

Count = 10
Adata = 049542cf5c4357730ca618b5f039de1fbdf0a351e48509f4b90c9ef0d4ce5fdf
Payload = 1d
CT = ?

Count = 11
Adata = ecb995aa1ab070191336cc7bc6ce2e18f093577490d661189c090b95f2db52c7
Payload = 53
CT = ?

Count = 12
Adata = 7f37a73db7c790f76c3bb838c041e04e13c713a86cc82c461a66986e9b3a5da1
Payload = e2
```

```
CT = ?
.
.
.
```

B.4.3 VNT128.sam

```
#  CAVS 4.0
#  "CCM-VNT" information for "CCMTest"
#  AES Keylen: 128
#  Generated on Wed Nov 24 08:34:26 2004

Alen = 32
Plen = 32
Tlen = 16

[Nlen = 7]

Key = b5d475ca8fa03e21b10ad13a3359a3c2

Count = 0
Nonce = 1043f6e725a430
Adata = cae697678007b0e6df925083d399d080a21ac867c18282a9ec6faf8575ba582b
Payload = 468e9d6bfc8b8749cd172eb7a1836bb5c4ff85034868af94a561d240a3a58db9
CT = ?

Count = 1
Nonce = 38701f7ec8a60b
Adata = 39bc5f205308e974bae3690516e4664dc67fd77324348b1f0a06c88c952f33df
Payload = 57d6471b58e424a8842d29400aef26be6b78c1868cec23680a43f1c8cd917efc
CT = ?

Count = 2
Nonce = 0f0a17e0e52720
Adata = 38900130497e0fbcc6e38f7243d1d7a1e4ac505f72e82772ad144571e4188226
Payload = 29af8e8bfbe23afa91b1574600afba43d8fd94acf8c8e9c5a714443ee0b8a85b
CT = ?

Count = 3
Nonce = ce4f81bad699ba
Adata = 9d11cacfdf4582f0e442ab564c740f764f88bfe8af86abb2eb406fc9b6f070d5
Payload = 1de4f0d6745f39040c6cd04673f24ee1a68b3361d337d0e9635164c838c2854c
CT = ?

Count = 4
Nonce = efb94af83d32f4
Adata = a393ab976d8cf849c673b11b9b4e4fec628d1a3bad48548bffc8b40cde491677
Payload = 2fd7758d5dd0423c4c530b2dd5e50f34cd15736e2d0c8977706651dd3d4040d5
CT = ?

Count = 5
Nonce = 334ed91288b8a1
Adata = 6e8e63320d14e7a301a62e20df50a0b983520e4f6024a3b114b718053ffe286a
```

```
Payload = 529225e2f9ba970f2949d1f021d02f3a5349d65518faff5fa39d937433bdf92d
CT = ?

Count = 6
Nonce = 36ecfaf09a2a3b
Adata = 6d2341d9272cc5b1ba638771a4667fc43846496889de262789634409723c3fc8
Payload = d1ccc6c6f021f2ff4c3c55f8373676ae0e0b2e2218efaf53b2e6c469a98f5b33
CT = ?

Count = 7
Nonce = 0c9760b8c7c9e2
Adata = 1f2464acec51654d5d4ad81ac2efae90bc2daab250c819f03b57bd4d85900ac1
Payload = 260c8c25facfc52d0a6ad3abd76cd4d60dde7c20abd65d65654965694721a881
CT = ?

Count = 8
Nonce = d0e02180b21820
Adata = cc4ecc728dc47882627514dffae26f2b3de449368ce6b9d04a50ccdb9b466fa4
Payload = 174614cab67c7ababd1fae0f2fb270967592fea55ce338ae5eca021322dcea3c
CT = ?

Count = 9
Nonce = 9bded2301657ec
Adata = 3ed0303a478ea02519a7efaa6f31e93b87c8c6f98e334677594500c15500f69d
Payload = 5284abb125644384159bcc9afaac929f26b701e0019367fff11efbea7dd11d0d
CT = ?

[Nlen = 8]

Key = a786a0e068284c657d3b60873cce7bf9

Count = 10
Nonce = e0c18e4579c654b8
Adata = cf8b52f552dd0715752943428e3b32474dd71aa04cf990dfe761ed4f4e4ffcd6
Payload = e298d9dda8337cd65b82999fdab62a9e03032a32cc5b4a978f7ce60aa62c372d
CT = ?

Count = 11
Nonce = 7cfa21baf2ae0064
Adata = 607e6078ad86c0342265a73346d8edbfc52cc01d665b3ccb3d793b05224e6f8d
Payload = 4a877916930913240ee9c17261837edc804804022364e504769fd68a12814e08
CT = ?

Count = 12
Nonce = 88ef34e67d239ed7
Adata = fc772d83491023a61a37228ef6260edc0d1cb972cba610d5ad1d92d554700771
Payload = a11914ec3b3c22a4b0421adce25df6fbafc0b15d0a60fc4151f733e3da4f8fe5
CT = ?
.
.
.
```

B.4.4 VTT128.sam

```
#  CAVS 4.0
#  "CCM-VTT" information for "CCMTest"
#  AES Keylen: 128
#  Generated on Wed Nov 24 08:34:26 2004

Alen = 32
Plen = 32
Nlen = 13

[Tlen = 4]

Key = 53337ec79c834b67eb4b18d6580fe271
Nonce = fe7fc25381853f73a3dc4195fd

Count = 0
Adata = 2ebd783e78d9778deba0047d947a3bce0344d368524545ee646331956b96fe37
Payload = 2e1d19794e21235ce4dfa8d2b41d24f9b110ccbe662a184f94337fd41d9b815a
CT = ?

Count = 1
Adata = 650240396020f52e8bcbb8d9efb012ed82c2b8a2b382bb10447effdc5818ee17
Payload = c97a7bef210d2ecdde0fbe9a41cd14291be034ff3501c3bff01ec6e629adadb8
CT = ?

Count = 2
Adata = e89cf1d3fcc2a394727394f7ec5d0b339397123d59d8d79a82e75271625228e4
Payload = 93708b1417a7df704793e927dfcf6851acc6ab4e9e754aaa1f731544a32e4ab0
CT = ?

Count = 3
Adata = bdf7699e91744b32638d8d0a4bd111c965b706396bdf16a6899ce1856cb0ab5a
Payload = fa53a930f1ddff9badf60ea04b5584c58bccba8d311e39efab127e07f3c5fa0c
CT = ?

Count = 4
Adata = 29993f9dfd24cf9b3b04a1115a667eb20fb968861562813e2ab129c55a146717
Payload = 1880f3cb1c4c49d70a8da1bdd107ff7c49c88bad715af25cfb3d0a160a94b543
CT = ?

Count = 5
Adata = 6d32b52598e63704108781e37c6b9d774a998a90a4e5d6539f5d6fcab6e4b6a0
Payload = e291f955b993a3919b6dd4f7bc538cda32d1abe7079daa088d8f8989f1ee087a
CT = ?

Count = 6
Adata = 43c12c69a5c7d57a8efaa8fb5ed0932f1ebd8c4905a72f7f4199a961f4bbd469
Payload = 40a18e849ed06ceca0586399208327c388dea0fd2c3ce25cddfe5fdbba925bfe
CT = ?

Count = 7
Adata = 04a6a955e47347b45e7ef57cd101184df0321fadb768134ca5806f8c257f3340
```

```
Payload = 4b6e3114d294cc5df1910a40af5bdc7b28b2cff8ecf88f45a242aa44f1af9724
CT = ?

Count = 8
Adata = 93ed1bcd3200511eaaa48b43fd9c0acb9876ba41e3c9659917bc25cf50c71fca
Payload = 8c0dd2d73975892342ce603c5f816700c28805509cde971fe23459c851e68aa5
CT = ?

Count = 9
Adata = ecdb6b90d650b01681dca5b08a79eac9c4791ddbd2c808d5f57118bf226311a0
Payload = 9084317bdc6f47f95e306e88ed125564e1e0314425a56b3c8eb695e26bf2a3b0
CT = ?

[Tlen = 6]

Key = aeee456645d8bba9cb95d7a629bbe24c
Nonce = ce6a7d04e1e2445a13ed80cf7e

Count = 10
Adata = 532d985f25f4d149e6763e68928edf0e4ba9fab5aacd102e53db0ffbcc11c9f9
Payload = 4862f5c9168331791c72a3a35db40f0d546768ec397739b281154327a46567bb
CT = ?

Count = 11
Adata = 44aec5efd2f367f731b7b672ca0d90929758d68a93f87b4f6f29da9b87274d38
Payload = 048cad0bd929bd647796e3ec36985f307ccfe1758e3bfa56a5ffd1af456417ba
CT = ?

Count = 12
Adata = 3b6160807a6e1ce3c85ff881992631713a2f8c31c08cedeb3f5026f63c380da0
Payload = 1a0704aefda0b567ae373172571f10517f942bcedb440d9a670ea435b6093c0d
CT = ?
.
.
.
```

B.4.5 DVPT128.sam

```
#  CAVS 4.0
#  "CCM-DVPT" information for "CCMTest"
#  AES Keylen: 128
#  Generated on Wed Nov 24 08:34:26 2004


[Alen = 0, Plen = 0, Nlen = 7, Tlen = 4]

Key = 4061d001230e05ea0da0a06207cc1461

Count = 0
Nonce = 75d339b2b513b7
Adata = 00
Payload = 00
CT = 0873b54b
```

```
Result = ?

Count = 1
Nonce = f8d178dcd9d6ad
Adata = 00
Payload = 00
CT = a39e84cb
Result = ?

Count = 2
Nonce = ab0d73d07ddc7d
Adata = 00
Payload = 00
CT = 3cc18c74
Result = ?

Count = 3
Nonce = 541b37bf0061c2
Adata = 00
Payload = 00
CT = 9524b42e
Result = ?

Count = 4
Nonce = f88dcd04ac3baa
Adata = 00
Payload = 00
CT = 8f573cfa
Result = ?

Count = 5
Nonce = 90301838c40872
Adata = 00
Payload = 00
CT = 38884289
Result = ?

Count = 6
Nonce = 994c32701485c8
Adata = 00
Payload = 00
CT = b19068a7
Result = ?

Count = 7
Nonce = 784f85a53138d0
Adata = 00
Payload = 00
CT = c65c90b2
Result = ?

Count = 8
Nonce = 02653684462e5c
Adata = 00
```

```
Payload = 00
CT = de73bfe1
Result = ?

Count = 9
Nonce = 3a76ba3462b709
Adata = 00
Payload = 00
CT = 552ad388
Result = ?

Count = 10
Nonce = 6e0dec05c6d179
Adata = 00
Payload = 00
CT = bd33919f
Result = ?

Count = 11
Nonce = e785e8b8529315
Adata = 00
Payload = 00
CT = b378237a
Result = ?

Count = 12
Nonce = 1533f8fce57847
Adata = 00
Payload = 00
CT = 4c4cd8bc
Result = ?

Count = 13
Nonce = 6edf9602f991c1
Adata = 00
Payload = 00
CT = e01f2179
Result = ?

Count = 14
Nonce = 7ff3fc66892c8c
Adata = 00
Payload = 00
CT = 706f0f3a
Result = ?

[Alen = 0, Plen = 0, Nlen = 7, Tlen = 16]

Key = 4e3d964a651fbbbcb1987c3355cfb533

Count = 15
Nonce = 75d339b2b513b7
Adata = 00
Payload = 00
```

```
CT = b8ef11d1fc6c2a272f97d94d178f07f5
Result = ?

Count = 16
Nonce = f8d178dcd9d6ad
Adata = 00
Payload = 00
CT = f89ef45bed5e21b90a356ee52fc5c3e2
Result = ?

Count = 17
Nonce = ab0d73d07ddc7d
Adata = 00
Payload = 00
CT = 8b37616684c6aec924ef3b5eb6b0e4d0
Result = ?
.
.
.
```