Supplement to ANSI X9.24-3-2017

Test Vectors —

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

This page intentionally left blank

Contents **Page**

1 Scope

This document is a supplement to ANSI X9.24-3-2017 and describes a set of test vectors that can be used to support validation of an implementation of the AES DUKPT algorithm on a transaction-originating SCD or a receiving SCD. AES DUKPT is used to derive transaction key(s) from an initial terminal DUKPT key based on the transaction number. Keys that can be derived include symmetric encryption/decryption keys, authentication keys, and HMAC (keyed hash message authentication code) keys. AES DUKPT supports the derivation of AES-128, AES-192, AES-256, double length TDEA, and triple length TDEA keys from AES-128, AES-192, and AES-256 initial keys.

While the included set of test vectors is fairly broad and representative of most use cases of the algorithm, this set of test vectors is not designed to be inclusive of all possible test cases and edge cases when implementing the AES DUKPT algorithm. Care must be taken by implementers of the AES DUKPT algorithm to consider all use cases for which they plan to use the algorithm to ensure they have developed a set of tests that cover their use cases.

2 Test Vectors

2.1 General

The following test vectors are provided for validating that an implementation correctly implements the algorithm described in the main body of the standard. The counter values are chosen to cover the first eight transactions, the first “skipped bit” near transaction 131072, a transaction chosen at random from the middle of the space (8675309), the last five transaction counters, and the DUKPT update key encryption key (counter = 0xFFFFFFFF).

The following important use cases are explicitly covered:

- Generating 128-bit AES keys from an 128-bit AES BDK/Initial Key
- Generating 128-bit AES keys from a 256-bit AES BDK/Initial Key
- Generating 256-bit AES keys from a 256-bit AES BDK/Initial Key
- Generating 2-key TDEA keys from an 128-bit AES BDK/Initial Key
- Generating 3-key TDEA keys from an 128-bit AES BDK/Initial Key

Examples of the calculation of AES PIN Blocks (Format 4) are also given.

Lastly, a trace of all the internal calculations for the derivation of the first eight transaction counters is given, both for the host and terminal sides of the algorithm. The inputs and outputs of each function from the pseudocode, as well as the values of all internal variables are given. This is done to aid in debugging implementations of this standard, to make it easy to spot where a given implementation diverges from correct behavior.

For more complex debugging and validation, it is recommended that the python code be used to generate additional test vectors and traces. The file is located at http://x9.org/standards/x9-24-part-3-test-vectors/.

2.2 Test Vectors for Various Transaction Keys

Test Vectors for generating KeyType._AES256 from KeyType._AES256 Base Derivation Key

```
BDK-128:
FEDCBA98 76543210 F1F1F1F1 F1F1F1F1

BDK-256:
FEDCBA98 76543210 F1F1F1F1 F1F1F1F1 FEDCBA98 76543210 F1F1F1F1 F1F1F1F1

InitialKeyID:
12345678 90123456

Derivation Data:
01018001 00020080 12345678 90123456

Initial Key:
1273671E A26AC29A FA4D1084 127652A1
```

Test Vectors for generating KeyType._AES128 from KeyType._AES128 Base Derivation Key

```
Initial Key:
1273671E A26AC29A FA4D1084 127652A1


Counter:  1    ( 0x1 )

Derivation Key:
4F21B565 BAD9835E 112B6465 635EAE44
PIN Encryption Derivation Data:
01011000 00020080 90123456 00000001
PIN Encryption Key:
AF8CB133 A78F8DC2 D1359F18 527593FB
MAC Derivation Data:
01012000 00020080 90123456 00000001
Message Authentication, Generation:
A2DC23DE 6FDE0824 A2BC321E 08E4B8B7
Encryption Derivation Data:
01013000 00020080 90123456 00000001
Data Encryption, Encrypt:
A35C412E FD41FDB9 8B69797C 02DCD08F

Counter:  2    ( 0x2 )

Derivation Key:
2F34D68D E10F68D3 8091A73B 9E7C437C
PIN Encryption Derivation Data:
01011000 00020080 90123456 00000002
PIN Encryption Key:
D30BDC73 EC9714B0 00BEC66B DB7B6D09
MAC Derivation Data:
01012000 00020080 90123456 00000002
```

```
Message Authentication, Generation:
484C3B06 E8562704 528CD5B4 6FB12FB6
Encryption Derivation Data:
01013000 00020080 90123456 00000002
Data Encryption, Encrypt:
D639514A A33AC43A D9229E43 3D6D4E5B

Counter:  3    (  0x3  )

Derivation Key:
031504E5 30365CF8 12642385 40518318
PIN Encryption Derivation Data:
01011000 00020080 90123456 00000003
PIN Encryption Key:
7D69F01F 3B45449F 62C7816E CE723268
MAC Derivation Data:
01012000 00020080 90123456 00000003
Message Authentication, Generation:
A5DF7D9D 800CA769 766F0C77 CA4E6E6C
Encryption Derivation Data:
01013000 00020080 90123456 00000003
Data Encryption, Encrypt:
EF17F6AB 45B4820C 93A3DCB2 1BC491AD

Counter:  4    (  0x4  )

Derivation Key:
0EEFC7AD A628BA68 878DA916 5A8A1887
PIN Encryption Derivation Data:
01011000 00020080 90123456 00000004
PIN Encryption Key:
91A05883 18EC2673 214271F7 0137896E
MAC Derivation Data:
01012000 00020080 90123456 00000004
Message Authentication, Generation:
E6E46796 47D8A905 7C1FC155 37CB4C4E
Encryption Derivation Data:
01013000 00020080 90123456 00000004
Data Encryption, Encrypt:
B3BD44C0 8BB6BA27 C3BB4711 D7D70387

Counter:  5    (  0x5  )

Derivation Key:
C2A7AC32 8A5DA2D6 002D6246 5BFC028B
PIN Encryption Derivation Data:
01011000 00020080 90123456 00000005
PIN Encryption Key:
35A43BC9 EFEB09C7 56204B57 E3FB7D4D
MAC Derivation Data:
01012000 00020080 90123456 00000005
Message Authentication, Generation:
0588185F E1FF8C7E 22FAD78C 1C61F065
Encryption Derivation Data:
01013000 00020080 90123456 00000005
```

```
Data Encryption, Encrypt:
CA02DF6F 30B39E14 BD0B4A30 E460920F

Counter:   6     (  0x6  )

Derivation Key:
D30F7D93 51DA5844 8A2F5E92 B4EE3B7D
PIN Encryption Derivation Data:
01011000 00020080 90123456 00000006
PIN Encryption Key:
02DCC6CD 1201A3A2 CA709955 9C862123
MAC Derivation Data:
01012000 00020080 90123456 00000006
Message Authentication, Generation:
7B60F72A 5639C0EE 7EB2100F A80BB793
Encryption Derivation Data:
01013000 00020080 90123456 00000006
Data Encryption, Encrypt:
C9B8A7C4 E486180B 22291151 64F0B293

Counter:   7     (  0x7  )

Derivation Key:
A8253CEE D9AC042C 54F75D35 C8352278
PIN Encryption Derivation Data:
01011000 00020080 90123456 00000007
PIN Encryption Key:
6ECF912F 3B18CA11 A7A27BB6 0705FD09
MAC Derivation Data:
01012000 00020080 90123456 00000007
Message Authentication, Generation:
BAA08CA2 63C69525 BC6B1BA8 F4275D69
Encryption Derivation Data:
01013000 00020080 90123456 00000007
Data Encryption, Encrypt:
0FA8F1F0 A2DD7B10 05A862D7 7CDED698

Counter:   8     (  0x8  )

Derivation Key:
718EE6CF 0B27E53D 5F7AF99C 4D8146A2
PIN Encryption Derivation Data:
01011000 00020080 90123456 00000008
PIN Encryption Key:
4D9DF3FB EE3448FC 3E676D04 320A90F5
MAC Derivation Data:
01012000 00020080 90123456 00000008
Message Authentication, Generation:
6FD572E5 D59E6188 75F19348 4F9178FB
Encryption Derivation Data:
01013000 00020080 90123456 00000008
Data Encryption, Encrypt:
650F3420 4ABD4E57 764D61AC 3D266FB1

Counter:   131070     (  0x1fffe  )
```

```
Derivation Key:
E21E8C8D 347F8561 A2BE752D AA85A111
PIN Encryption Derivation Data:
01011000 00020080 90123456 0001FFFE
PIN Encryption Key:
DDF7E08A 84B5478C 498D007C 743BF762
MAC Derivation Data:
01012000 00020080 90123456 0001FFFE
Message Authentication, Generation:
6D7623AD 652734B8 FAE1B6E0 93EACE3D
Encryption Derivation Data:
01013000 00020080 90123456 0001FFFE
Data Encryption, Encrypt:
8E4E5D5E 0F01C54F 01F4ACA1 C8F8EDCE

Counter:  131071    (  0x1ffff  )

Derivation Key:
1FE36898 8089CDD7 6DA18A34 58E113BA
PIN Encryption Derivation Data:
01011000 00020080 90123456 0001FFFF
PIN Encryption Key:
73BA667D 6368A208 6E72576D F41A4037
MAC Derivation Data:
01012000 00020080 90123456 0001FFFF
Message Authentication, Generation:
8B543DCF 4A31EA3A B47DAD16 B8ABD404
Encryption Derivation Data:
01013000 00020080 90123456 0001FFFF
Data Encryption, Encrypt:
D18ACA30 B4D63DB6 1CE474D3 F57733D3

Counter:  131072    (  0x20000  )

Derivation Key:
F7AE9025 468A25D3 7B7249CF FED224C8
PIN Encryption Derivation Data:
01011000 00020080 90123456 00020000
PIN Encryption Key:
AB828BE7 B58C7EC5 D5ED0D5D 320A0C9D
MAC Derivation Data:
01012000 00020080 90123456 00020000
Message Authentication, Generation:
0B59D3D7 D93028D9 7135FB89 5CACE24E
Encryption Derivation Data:
01013000 00020080 90123456 00020000
Data Encryption, Encrypt:
13361208 97575531 8FE7AE28 C9616014

Counter:  131073    (  0x20001  )

Derivation Key:
692C8EA4 01364513 5B364971 31DF9D2C
PIN Encryption Derivation Data:
```

```
01011000 00020080 90123456 00020001
PIN Encryption Key:
8AC85C93 EED24605 4ADC3104 479115A6
MAC Derivation Data:
01012000 00020080 90123456 00020001
Message Authentication, Generation:
EF7C9461 E2AFED2A 8012CC63 01CFEEBE
Encryption Derivation Data:
01013000 00020080 90123456 00020001
Data Encryption, Encrypt:
B93B4BF0 D52163B3 CF9312F8 E55629A3

Counter:   8675309    (  0x845fed  )

Derivation Key:
549067A1 706E6D06 B9713360 48936D5D
PIN Encryption Derivation Data:
01011000 00020080 90123456 00845FED
PIN Encryption Key:
D1DDA386 AA4A556A F0119FDC B5D132C6
MAC Derivation Data:
01012000 00020080 90123456 00845FED
Message Authentication, Generation:
89365C79 70950CAC 0A6261FF C7DB26C6
Encryption Derivation Data:
01013000 00020080 90123456 00845FED
Data Encryption, Encrypt:
B1E4D900 6A87DD08 D87F11A1 24D35517

Counter:   4294844416    (  0xfffe2000  )

Derivation Key:
48E585B6 94EB0B18 D5C35443 E163C0BA
PIN Encryption Derivation Data:
01011000 00020080 90123456 FFFE2000
PIN Encryption Key:
4C9EF39E EFA1A868 7FF42AFC F37DC079
MAC Derivation Data:
01012000 00020080 90123456 FFFE2000
Message Authentication, Generation:
A20520D4 1C2F6501 49505181 F8AADB0A
Encryption Derivation Data:
01013000 00020080 90123456 FFFE2000
Data Encryption, Encrypt:
6E48CE0A CFD3CD56 16548DC2 E769252E

Counter:   4294852608    (  0xfffe4000  )

Derivation Key:
396C2C7C A1EA701C 03B86B7D 41F0C562
PIN Encryption Derivation Data:
01011000 00020080 90123456 FFFE4000
PIN Encryption Key:
6239A27F 572DEDB1 7BCA1AC4 13EF9FE9
MAC Derivation Data:
```

```
01012000 00020080 90123456 FFFE4000
Message Authentication, Generation:
87C593AD B0ABBE48 F9A52D76 6369196F
Encryption Derivation Data:
01013000 00020080 90123456 FFFE4000
Data Encryption, Encrypt:
4FD5DE33 5840FD8F CD527BF7 B0BC6898

Counter:   4294868992    (  0xfffe8000  )

Derivation Key:
0387625F 189B58AE 03EF0E8C CA41105E
PIN Encryption Derivation Data:
01011000 00020080 90123456 FFFE8000
PIN Encryption Key:
F10C1404 137A8071 8FCCE8BD 90FF9F67
MAC Derivation Data:
01012000 00020080 90123456 FFFE8000
Message Authentication, Generation:
1A88A6E0 BCE9079A FE5E12C0 1F37E891
Encryption Derivation Data:
01013000 00020080 90123456 FFFE8000
Data Encryption, Encrypt:
A71075F9 37FC2632 968F826C 74425E08

Counter:   4294901760    (  0xffff0000  )

Derivation Key:
F6BA5938 9BD14A98 55BE9727 E7C52E3C
PIN Encryption Derivation Data:
01011000 00020080 90123456 FFFF0000
PIN Encryption Key:
27EFAC1D 15863258 8F4AC69E 45C247C4
MAC Derivation Data:
01012000 00020080 90123456 FFFF0000
Message Authentication, Generation:
AE558BAB C206D303 FDF68B11 81F228C6
Encryption Derivation Data:
01013000 00020080 90123456 FFFF0000
Data Encryption, Encrypt:
08878BFC C45CA5AE F6A1AB40 BAC882B5

DUKPT Update Key (counter =   0xffffffff  )

Derivation Key:
36C6EBBC C0536FC9 1C1D5066 0D4F82AE
Derivation Data:
01010002 00020080 90123456 FFFFFFFF
Key Encryption Key:
9A9770AE E1ACD1B1 3473D046 3A1883B9

Test Vectors for generating    KeyType._AES128    from    KeyType._AES256    Base
Derivation Key

Initial Key:
```

```
CE9CE0C1 01D1138F 97FB6CAD 4DF045A7 083D4EAE 2D35A317 89D01CCF 0949550F


Counter:  1    (  0x1  )

Derivation Key:
54AC2B32 B145EA4A 554CB8BC 44B17467 063A7998 56B1CCC2 A138D36E 8DBF78B3
PIN Encryption Derivation Data:
01011000 00020080 90123456 00000001
PIN Encryption Key:
09C9C432 966811D6 B2C3336B AC1B1202
MAC Derivation Data:
01012000 00020080 90123456 00000001
Message Authentication, Generation:
F04A1FAB D4176E15 490CEC82 E217A96D
Encryption Derivation Data:
01013000 00020080 90123456 00000001
Data Encryption, Encrypt:
616D59AE 91F8CC70 16F89FDA 29605FA4

Counter:  2    (  0x2  )

Derivation Key:
5DD5A025 3842BBBE 1D7C0DA2 7021412C 6F1FAB53 FB928DEA E56DA060 90A9DE97
PIN Encryption Derivation Data:
01011000 00020080 90123456 00000002
PIN Encryption Key:
D632226A 80795D13 A80AFE66 A3E97B01
MAC Derivation Data:
01012000 00020080 90123456 00000002
Message Authentication, Generation:
DD99D77B 4E2AB538 B26BB6A8 B3FB0BE3
Encryption Derivation Data:
01013000 00020080 90123456 00000002
Data Encryption, Encrypt:
07B79D9B FF3633C0 7A9FDDF1 32070B30

Counter:  3    (  0x3  )

Derivation Key:
8EEEF7C4 64AE415B B1D73FAE D21993CD 669F7999 092A579E C6DD3CC6 80C65171
PIN Encryption Derivation Data:
01011000 00020080 90123456 00000003
PIN Encryption Key:
C2CBD3D7 66B16F9F 82F4EE3F 74478918
MAC Derivation Data:
01012000 00020080 90123456 00000003
Message Authentication, Generation:
5A742A4A 0403B3D7 BB30842D AFBB5972
Encryption Derivation Data:
01013000 00020080 90123456 00000003
Data Encryption, Encrypt:
706E4E62 9E466BED 956548E7 B0D90C3D

Counter:  4    (  0x4  )
```

```
Derivation Key:
C18CBED5 70B3B89E CADA7CEC 9C224CD5 A86ECF3D E377D3EF AB720F8C 4D76B9D0
PIN Encryption Derivation Data:
01011000 00020080 90123456 00000004
PIN Encryption Key:
58A3779C 1E24B3ED AF068609 E7E56D59
MAC Derivation Data:
01012000 00020080 90123456 00000004
Message Authentication, Generation:
C531F7E0 8514858C 445D5F54 BFE7DA8E
Encryption Derivation Data:
01013000 00020080 90123456 00000004
Data Encryption, Encrypt:
CF3A4D9C A7E962E4 023A84A2 FE47DC80

Counter:  5    (  0x5  )

Derivation Key:
6B3C3C93 307151C2 5DC23094 56F01C5C 3108DAD5 71C32189 9A9B7E0C 009FD2EB
PIN Encryption Derivation Data:
01011000 00020080 90123456 00000005
PIN Encryption Key:
97504C8B B0FD4D4A 88D60514 3BF00025
MAC Derivation Data:
01012000 00020080 90123456 00000005
Message Authentication, Generation:
E2E25AA7 FE6E5DD6 042C632A 5DFED945
Encryption Derivation Data:
01013000 00020080 90123456 00000005
Data Encryption, Encrypt:
94C28455 AEAD9705 55F32629 8557FA81

Counter:  6    (  0x6  )

Derivation Key:
B8BB61AE 3E2D5CD8 C699E0C5 78FB2C7B 89B0C0CF 02DBAB60 864D8049 C986C844
PIN Encryption Derivation Data:
01011000 00020080 90123456 00000006
PIN Encryption Key:
BF281141 609E6CAE 7DF10DFA 47A8D03D
MAC Derivation Data:
01012000 00020080 90123456 00000006
Message Authentication, Generation:
07B21592 9C5DB426 2DECEE4A 0336DD4F
Encryption Derivation Data:
01013000 00020080 90123456 00000006
Data Encryption, Encrypt:
408D3B9A 7D1AF109 E2F68951 4BF79AC7

Counter:  7    (  0x7  )

Derivation Key:
88D0ACA2 87B3066F 5DE0C933 96337D4C 2DA8D92C 1F720A57 6D62CEB4 C979E01E
PIN Encryption Derivation Data:
```

```
01011000 00020080 90123456 00000007
PIN Encryption Key:
B7C6BB18 7134E9D4 29C3E8B7 CCBD8477
MAC Derivation Data:
01012000 00020080 90123456 00000007
Message Authentication, Generation:
3AC9CC51 59F96E10 FCC5EB64 015AC76A
Encryption Derivation Data:
01013000 00020080 90123456 00000007
Data Encryption, Encrypt:
DC2915BF 421D617E 7725E63A 7DACB18D

Counter:   8     (  0x8  )

Derivation Key:
20A796D5 077D51B8 E7613893 A4F095B1 34E02917 DC84BD39 1F3661D0 873FF308
PIN Encryption Derivation Data:
01011000 00020080 90123456 00000008
PIN Encryption Key:
53C1C60A 65532313 141A102A D720E967
MAC Derivation Data:
01012000 00020080 90123456 00000008
Message Authentication, Generation:
6E94A928 3EA9AEB7 EAA77C3F F55FF2D1
Encryption Derivation Data:
01013000 00020080 90123456 00000008
Data Encryption, Encrypt:
8950DD50 C254C60E 26737CA9 229F0F18

Counter:   131070    (  0x1fffe  )

Derivation Key:
A289508C BF122845 2CD86AB7 7B15CB35 577AC828 C18BB666 81E5A16D 6C9CCED3
PIN Encryption Derivation Data:
01011000 00020080 90123456 0001FFFE
PIN Encryption Key:
96E2B96B AB214582 AFE9E9AD 7078EFFE
MAC Derivation Data:
01012000 00020080 90123456 0001FFFE
Message Authentication, Generation:
50D3DC88 D381EAC3 EA9597F1 4ED0B310
Encryption Derivation Data:
01013000 00020080 90123456 0001FFFE
Data Encryption, Encrypt:
4093FA44 A14F1142 6FE40EF3 BF701B28

Counter:   131071    (  0x1ffff  )

Derivation Key:
7C1F24BC 33C5B146 E1D30151 26F4AC2E 0C48AC08 0DC92341 37B82890 E8E91FB8
PIN Encryption Derivation Data:
01011000 00020080 90123456 0001FFFF
PIN Encryption Key:
B02966FC B8EB55F8 1256D1D9 5ADBDF71
MAC Derivation Data:
```

```
01012000 00020080 90123456 0001FFFF
Message Authentication, Generation:
474B9E9D 0457F19D 0B23E3AD A422B8C2
Encryption Derivation Data:
01013000 00020080 90123456 0001FFFF
Data Encryption, Encrypt:
9B1E5F83 41C8678F 28C5C095 39A6A814

Counter:  131072    (  0x20000  )

Derivation Key:
D62DDA94 A47D7DA5 D763443B 4ECB15EA 8DD62E0E 4F915958 BA459591 F8312E37
PIN Encryption Derivation Data:
01011000 00020080 90123456 00020000
PIN Encryption Key:
5F1B560F 963161FD 42BC0869 E72911DF
MAC Derivation Data:
01012000 00020080 90123456 00020000
Message Authentication, Generation:
C62B97CA 93BC80F4 7DF02D87 9ADE361C
Encryption Derivation Data:
01013000 00020080 90123456 00020000
Data Encryption, Encrypt:
CA331440 0D2679DE F6CA986D E6097A5E

Counter:  131073    (  0x20001  )

Derivation Key:
44110A11 02748D4A 3AC326F5 3D8CAC65 0212590C A7126D54 546DDE0F 20E89CEE
PIN Encryption Derivation Data:
01011000 00020080 90123456 00020001
PIN Encryption Key:
8D156B5E FC1131F1 5BA335C4 F9F85FA0
MAC Derivation Data:
01012000 00020080 90123456 00020001
Message Authentication, Generation:
627AB254 566D7E99 2421C44A 17484C2D
Encryption Derivation Data:
01013000 00020080 90123456 00020001
Data Encryption, Encrypt:
943CF9BD D0EAFE80 599080CF AD376777

Counter:  8675309    (  0x845fed  )

Derivation Key:
C6070328 5DEAFA0A 8BA260D6 702C3776 286B63B0 497FE8D5 BD11813C ABE90354
PIN Encryption Derivation Data:
01011000 00020080 90123456 00845FED
PIN Encryption Key:
774E7049 F709BAA4 800B8BC3 CBA59590
MAC Derivation Data:
01012000 00020080 90123456 00845FED
Message Authentication, Generation:
DD30C7F6 4123F516 09798E97 F6BA7A21
Encryption Derivation Data:
```

```
01013000 00020080 90123456 00845FED
Data Encryption, Encrypt:
BA2874A9 1A6505E3 8EBA7098 DF0D3733

Counter:   4294844416    (  0xfffe2000  )

Derivation Key:
4625EB06 E4886D4A FCC9AE37 ED4F4E4E 1653C9E6 0E3F2474 2A87A26A A96AB7A6
PIN Encryption Derivation Data:
01011000 00020080 90123456 FFFE2000
PIN Encryption Key:
894C9424 6519CAAF 3B5DC4F2 AE63CD61
MAC Derivation Data:
01012000 00020080 90123456 FFFE2000
Message Authentication, Generation:
BBE3BBBA 90D60B61 DB46F6CF EAC521D3
Encryption Derivation Data:
01013000 00020080 90123456 FFFE2000
Data Encryption, Encrypt:
7E24B09E 56F794E8 EDDBBDD3 D5870759

Counter:   4294852608    (  0xfffe4000  )

Derivation Key:
FF20E1BB 575539AC CB44E311 1BE8757F 83AE8549 A2DD71B4 41A4A424 F7FFD4B1
PIN Encryption Derivation Data:
01011000 00020080 90123456 FFFE4000
PIN Encryption Key:
244CB694 AE864209 1C600946 FC9CA669
MAC Derivation Data:
01012000 00020080 90123456 FFFE4000
Message Authentication, Generation:
8C4908F3 6E8FD107 FC529038 02A9CC32
Encryption Derivation Data:
01013000 00020080 90123456 FFFE4000
Data Encryption, Encrypt:
1972B3D1 6911DB6B E5D4B9E5 57E82C91

Counter:   4294868992    (  0xfffe8000  )

Derivation Key:
630535C9 C53E1EC6 52401693 0B56F672 8909C454 03536B41 9AEBCB25 B7351C07
PIN Encryption Derivation Data:
01011000 00020080 90123456 FFFE8000
PIN Encryption Key:
166B5F73 C318731A 4FFC41BB 3ECFF485
MAC Derivation Data:
01012000 00020080 90123456 FFFE8000
Message Authentication, Generation:
403534FA 87769D96 AD238181 D93F6FF5
Encryption Derivation Data:
01013000 00020080 90123456 FFFE8000
Data Encryption, Encrypt:
DA2F6923 5E1E2934 DE246D61 29937EAB
```

```
Counter:   4294901760    (  0xffff0000  )

Derivation Key:
6D6DB7AA AE8B3EA9 0E57A39E 4BBA71E1 73B21B44 6B30A78D 64BFC6A8 806C55EE
PIN Encryption Derivation Data:
01011000 00020080 90123456 FFFF0000
PIN Encryption Key:
27082818 8E3644D4 727126E4 D08D3FA0
MAC Derivation Data:
01012000 00020080 90123456 FFFF0000
Message Authentication, Generation:
CB9DEA55 B56ACC78 14C6533A 8DCDD96E
Encryption Derivation Data:
01013000 00020080 90123456 FFFF0000
Data Encryption, Encrypt:
E2824C64 F793CB8B 95E0A4B4 AEF4DD53

DUKPT Update Key (counter =   0xffffffff  )

Derivation Key:
39064FDC 8373D710 AFAA823E 757E5919 0C92DD8F BF86B87B 673632F4 E04C97D2
Derivation Data:
01010002 00020080 90123456 FFFFFFFF
Key Encryption Key:
90E54E4A 70160C7E 085C09D2 B241D343

Test Vectors for generating    KeyType._AES256    from    KeyType._AES256    Base
Derivation Key

Initial Key:
CE9CE0C1 01D1138F 97FB6CAD 4DF045A7 083D4EAE 2D35A317 89D01CCF 0949550F


Counter:   1    (  0x1  )

Derivation Key:
54AC2B32 B145EA4A 554CB8BC 44B17467 063A7998 56B1CCC2 A138D36E 8DBF78B3
PIN Encryption Derivation Data:
01021000 00040100 90123456 00000001
PIN Encryption Key:
8C1AB7BE E973829E 30242E0B BBDD4946 D540C98F C1B5BDCF 94790001 A23FD502
MAC Derivation Data:
01022000 00040100 90123456 00000001
Message Authentication, Generation:
61DABDF4 B340CF46 1EE860B1 D1AB5535 7142BD2D 69773068 59CF49AE FE8F1549
Encryption Derivation Data:
01023000 00040100 90123456 00000001
Data Encryption, Encrypt:
71EB36C9 A6B7F801 D1D1700C 29741FC5 A5C4E9B4 5D742DA7 AF6992B8 AA29AF58

Counter:   2    (  0x2  )

Derivation Key:
5DD5A025 3842BBBE 1D7C0DA2 7021412C 6F1FAB53 FB928DEA E56DA060 90A9DE97
PIN Encryption Derivation Data:
```

```
01021000 00040100 90123456 00000002
PIN Encryption Key:
3583D6CD 02FC3882 2CC71A8D 7678E04F 4A855633 5E6CC668 63D3DADC 5AEE2C62
MAC Derivation Data:
01022000 00040100 90123456 00000002
Message Authentication, Generation:
44173562 19B2F93C E3F26716 23DDCAB5 8A8B85AD 80662A8D 62802400 0956D426
Encryption Derivation Data:
01023000 00040100 90123456 00000002
Data Encryption, Encrypt:
D0AC9F71 F875FFFF 3A83778F 72F39EBB 0924A5A5 26617AF6 69665E0A 19725465

Counter:   3    (  0x3  )

Derivation Key:
8EEEF7C4 64AE415B B1D73FAE D21993CD 669F7999 092A579E C6DD3CC6 80C65171
PIN Encryption Derivation Data:
01021000 00040100 90123456 00000003
PIN Encryption Key:
96A1AB5D 37CB7CF8 1DDE64F6 6C46E038 9B833E7A D5F4E44C 791F04FA FDA6DA0E
MAC Derivation Data:
01022000 00040100 90123456 00000003
Message Authentication, Generation:
35BD00A4 6F2A2BD1 27F565FB F2974B73 5AE3BB70 242C0A41 5857CF69 B2C2691A
Encryption Derivation Data:
01023000 00040100 90123456 00000003
Data Encryption, Encrypt:
8E70D5DF 53F48ED2 F2A0B54F C4F45C84 4579BE96 F6F16122 2CDD5019 3E2F737F

Counter:   4    (  0x4  )

Derivation Key:
C18CBED5 70B3B89E CADA7CEC 9C224CD5 A86ECF3D E377D3EF AB720F8C 4D76B9D0
PIN Encryption Derivation Data:
01021000 00040100 90123456 00000004
PIN Encryption Key:
420AA584 BF215C47 77E93009 B56D08DE 80687021 D07ED963 49FF7137 9CE5636D
MAC Derivation Data:
01022000 00040100 90123456 00000004
Message Authentication, Generation:
D80617C3 C5869A8D CF0DA538 3D032A0D 6E6C51C0 BF649BE9 92BE84AA 191AE326
Encryption Derivation Data:
01023000 00040100 90123456 00000004
Data Encryption, Encrypt:
41D23F7D 78E22A97 8D726BC7 1D266374 263120EE 49146CE5 C1291FD0 EE7DDD31

Counter:   5    (  0x5  )

Derivation Key:
6B3C3C93 307151C2 5DC23094 56F01C5C 3108DAD5 71C32189 9A9B7E0C 009FD2EB
PIN Encryption Derivation Data:
01021000 00040100 90123456 00000005
PIN Encryption Key:
B1E9E3D9 18952E6E 5F67917F 0FE77060 F865AE27 DCAD5742 DDF90F61 453B98BA
MAC Derivation Data:
```

```
01022000 00040100 90123456 00000005
Message Authentication, Generation:
8B047E32 C476C0A0 AF90A9B8 D1C247C4 33E3D4C1 DF1C7FC5 2E8CB1DC 4C8FB275
Encryption Derivation Data:
01023000 00040100 90123456 00000005
Data Encryption, Encrypt:
813D156C 142E5BB8 F136427E BD0A1AC4 DC9B2B59 63C481F5 E0A58F4B F33BD185

Counter:  6    (  0x6  )

Derivation Key:
B8BB61AE 3E2D5CD8 C699E0C5 78FB2C7B 89B0C0CF 02DBAB60 864D8049 C986C844
PIN Encryption Derivation Data:
01021000 00040100 90123456 00000006
PIN Encryption Key:
8714EB94 E3BFD301 8EC99D04 34D9C94F 071AF2EE BF4332FB 14F51797 93AA582C
MAC Derivation Data:
01022000 00040100 90123456 00000006
Message Authentication, Generation:
A2FF6FFB 37CB8042 B8C9B2F9 4C90C83D 94DD5BEC CD9951CF AB0BE7BD 865CA403
Encryption Derivation Data:
01023000 00040100 90123456 00000006
Data Encryption, Encrypt:
F1FB0591 AA2E45E1 CE4C5D97 0C7396C4 A87E53E5 900C4A6D 95C17414 0CC0AC9C

Counter:  7    (  0x7  )

Derivation Key:
88D0ACA2 87B3066F 5DE0C933 96337D4C 2DA8D92C 1F720A57 6D62CEB4 C979E01E
PIN Encryption Derivation Data:
01021000 00040100 90123456 00000007
PIN Encryption Key:
693C893A 1E81D280 302E0A47 E7E63433 7B9A9B26 E7CC6064 D807E08F F911AFAC
MAC Derivation Data:
01022000 00040100 90123456 00000007
Message Authentication, Generation:
E8A57085 DBE804B8 C2767F9F 77D54854 861E9963 3A062C70 0B4E50A8 65153150
Encryption Derivation Data:
01023000 00040100 90123456 00000007
Data Encryption, Encrypt:
69BC5C9A FB2C93CC 30C3F752 9360B34D 7B64B720 6E0F0940 D8654378 C54824F2

Counter:  8    (  0x8  )

Derivation Key:
20A796D5 077D51B8 E7613893 A4F095B1 34E02917 DC84BD39 1F3661D0 873FF308
PIN Encryption Derivation Data:
01021000 00040100 90123456 00000008
PIN Encryption Key:
173A4528 4262A3E2 92D86D08 FD6DE916 79632144 50D1D48F 6103BD2E B08E61B5
MAC Derivation Data:
01022000 00040100 90123456 00000008
Message Authentication, Generation:
949A3FEF 12DBD273 DD25BB60 E29BBE31 3C872A9D E3BE03A7 E29626AC A0A42880
Encryption Derivation Data:
```

```
01023000 00040100 90123456 00000008
Data Encryption, Encrypt:
0BF8789A 21D06841 0A16C9F7 FCBF65A7 B4FF7320 3ADC0F1B 4B5E5BF8 050E4284

Counter:  131070    (  0x1fffe  )

Derivation Key:
A289508C BF122845 2CD86AB7 7B15CB35 577AC828 C18BB666 81E5A16D 6C9CCED3
PIN Encryption Derivation Data:
01021000 00040100 90123456 0001FFFE
PIN Encryption Key:
464EA18F EBD8E87F D2B0298D A5E1C87B 0C18C515 E671D06C 9B1D2297 EA23EB89
MAC Derivation Data:
01022000 00040100 90123456 0001FFFE
Message Authentication, Generation:
E59DE149 5A594F37 58F8741A E25CE70B F86C9946 592268FA 4BBFB229 A691E2B5
Encryption Derivation Data:
01023000 00040100 90123456 0001FFFE
Data Encryption, Encrypt:
3A86AF6C 384A6995 80E87C3F 155C1107 6A71042E B96FA1B2 75D588F4 F154A28F

Counter:  131071    (  0x1ffff  )

Derivation Key:
7C1F24BC 33C5B146 E1D30151 26F4AC2E 0C48AC08 0DC92341 37B82890 E8E91FB8
PIN Encryption Derivation Data:
01021000 00040100 90123456 0001FFFF
PIN Encryption Key:
377EE835 8754A1BB 583D06BA 85A5D8C5 F12094A4 BA08061B 4865B7AD 04617372
MAC Derivation Data:
01022000 00040100 90123456 0001FFFF
Message Authentication, Generation:
812D91F2 511E1323 8A3BC8D9 351E9712 30FC8557 5D70B522 4C8FC8AF 4A91021F
Encryption Derivation Data:
01023000 00040100 90123456 0001FFFF
Data Encryption, Encrypt:
9B140778 583AA22C 512EB898 3870B89D ED1D8C82 8436D84A 4BD0C610 02A158E6

Counter:  131072    (  0x20000  )

Derivation Key:
D62DDA94 A47D7DA5 D763443B 4ECB15EA 8DD62E0E 4F915958 BA459591 F8312E37
PIN Encryption Derivation Data:
01021000 00040100 90123456 00020000
PIN Encryption Key:
C3DE6948 5ABD2A6D DD3A3C93 B54D60B3 2E1B324D F294ACE6 FBED1AC0 1EF8FA85
MAC Derivation Data:
01022000 00040100 90123456 00020000
Message Authentication, Generation:
E0FEAA9D 225DEFD8 01A36F20 4D8C9000 112FC71C 6706988C F51F7F0C 8052CD99
Encryption Derivation Data:
01023000 00040100 90123456 00020000
Data Encryption, Encrypt:
031E6D5A FA9FD679 2FE8D9B5 5FA24502 924B0828 B5BE79FD 8A0917E4 F74D204F
```

```
Counter:  131073    ( 0x20001 )

Derivation Key:
44110A11 02748D4A 3AC326F5 3D8CAC65 0212590C A7126D54 546DDE0F 20E89CEE
PIN Encryption Derivation Data:
01021000 00040100 90123456 00020001
PIN Encryption Key:
DEB9E187 FD5702B5 91672913 3176B5C0 BB67FCDD 247F56B2 FA02AEDC 898D2EA6
MAC Derivation Data:
01022000 00040100 90123456 00020001
Message Authentication, Generation:
EA2813D9 2E47F2F6 0DF54EDA 5046B739 79477542 DE3098AD 934DBC66 8C662367
Encryption Derivation Data:
01023000 00040100 90123456 00020001
Data Encryption, Encrypt:
DC16A8D2 3BC41DB3 3153DAB4 5517F7D9 422A9B6A AC6D4DF1 88928EF2 58474F97

Counter:  8675309    ( 0x845fed )

Derivation Key:
C6070328 5DEAFA0A 8BA260D6 702C3776 286B63B0 497FE8D5 BD11813C ABE90354
PIN Encryption Derivation Data:
01021000 00040100 90123456 00845FED
PIN Encryption Key:
BE517466 FC1C9CC9 B3B138D6 162164CC A172BA2F 8DE2EF42 FCBAF832 F1456E80
MAC Derivation Data:
01022000 00040100 90123456 00845FED
Message Authentication, Generation:
7840369D C5701CC4 944F138C 110C43C1 42BDFB39 044CFD03 F723C2E2 D86FAF89
Encryption Derivation Data:
01023000 00040100 90123456 00845FED
Data Encryption, Encrypt:
B58359E2 393B2116 8C6175A4 3A4F880E F995896C D30270B0 9E3F0E69 C7EC62D7

Counter:  4294844416    ( 0xfffe2000 )

Derivation Key:
4625EB06 E4886D4A FCC9AE37 ED4F4E4E 1653C9E6 0E3F2474 2A87A26A A96AB7A6
PIN Encryption Derivation Data:
01021000 00040100 90123456 FFFE2000
PIN Encryption Key:
31F322CC 81DB4B0B 1970A6C4 CBFDF1A7 6640F478 A6E6B25C 266B6CC2 4F2975EB
MAC Derivation Data:
01022000 00040100 90123456 FFFE2000
Message Authentication, Generation:
3AB8E7E3 6650E123 7DDBE5B1 8497D09A 8F54A1D9 DEC33EA4 D9B90E5F 6A82A6C9
Encryption Derivation Data:
01023000 00040100 90123456 FFFE2000
Data Encryption, Encrypt:
10E2F8B6 9020AC12 3517428B EB31A662 DBD753A9 28AE4AD2 1C59E35B 26362794

Counter:  4294852608    ( 0xfffe4000 )

Derivation Key:
FF20E1BB 575539AC CB44E311 1BE8757F 83AE8549 A2DD71B4 41A4A424 F7FFD4B1
```

```
PIN Encryption Derivation Data:
01021000 00040100 90123456 FFFE4000
PIN Encryption Key:
F388FF9F B1D66E88 12BC67CA 5B85CE55 54063E09 A2440EC1 AF4EB433 CCFBAF35
MAC Derivation Data:
01022000 00040100 90123456 FFFE4000
Message Authentication, Generation:
E3F9FEEE 9DEDA37B E0B95883 A6F66BBE DEE8D2DE CE2C6FA7 D20CEA06 F695EC56
Encryption Derivation Data:
01023000 00040100 90123456 FFFE4000
Data Encryption, Encrypt:
98C74A38 4D046F83 7703899A AC2E803D 2427AE89 12B117B5 E2574F81 78F1D664

Counter:   4294868992    (  0xfffe8000  )

Derivation Key:
630535C9 C53E1EC6 52401693 0B56F672 8909C454 03536B41 9AEBCB25 B7351C07
PIN Encryption Derivation Data:
01021000 00040100 90123456 FFFE8000
PIN Encryption Key:
FAC4E05A 67AB1522 505CF0E9 4E5977B9 9D0E5B11 6D76ABB6 B8A64F0D 785FF6DF
MAC Derivation Data:
01022000 00040100 90123456 FFFE8000
Message Authentication, Generation:
5C9CF40C 8862D129 36488E38 B694FA95 5C6E22C3 5B0432C1 78E3C3EA 487987BB
Encryption Derivation Data:
01023000 00040100 90123456 FFFE8000
Data Encryption, Encrypt:
E21C882D B68FF2AD 4C8E0AA5 B2383F6B EC7F9A09 30D6E27A 8A34EE99 39AB4F2C

Counter:   4294901760    (  0xffff0000  )

Derivation Key:
6D6DB7AA AE8B3EA9 0E57A39E 4BBA71E1 73B21B44 6B30A78D 64BFC6A8 806C55EE
PIN Encryption Derivation Data:
01021000 00040100 90123456 FFFF0000
PIN Encryption Key:
88B82556 AEF4A681 E0687F44 3A4C4F30 5AF9203B 114470DF C77C7F08 BC43F9DA
MAC Derivation Data:
01022000 00040100 90123456 FFFF0000
Message Authentication, Generation:
7B224593 72EE2C4F AB4BB15E A869C8E5 A6CAB725 55EC1D13 EAA6A87F B516CBD1
Encryption Derivation Data:
01023000 00040100 90123456 FFFF0000
Data Encryption, Encrypt:
FA76ADC9 48472280 03867B12 FB31C6B6 C1BFB542 6E97C7B3 A86BE4F9 A78C4DA8

DUKPT Update Key (counter =   0xffffffff  )

Derivation Key:
39064FDC 8373D710 AFAA823E 757E5919 0C92DD8F BF86B87B 673632F4 E04C97D2
Derivation Data:
01020002 00040100 90123456 FFFFFFFF
Key Encryption Key:
AEFB210C 136278A1 279F7C88 15F446DB 8EBE2AA9 10B157AA 4E6484D8 DE9C4807
```

Test Vectors for generating KeyType._2TDEA from KeyType._AES128 Base Derivation Key

Initial Key:
1273671E A26AC29A FA4D1084 127652A1

Counter: 1 (0x1)

Derivation Key:
4F21B565 BAD9835E 112B6465 635EAE44
PIN Encryption Derivation Data:
01011000 00000080 90123456 00000001
PIN Encryption Key:
630C706D 9546E47D 4449313F 61C4D4AB
MAC Derivation Data:
01012000 00000080 90123456 00000001
Message Authentication, Generation:
5D8FD787 E8A796D0 7035FFCA 9B5800BB
Encryption Derivation Data:
01013000 00000080 90123456 00000001
Data Encryption, Encrypt:
BD44121C 223F8314 46A01EE3 A4CB58D2

Counter: 2 (0x2)

Derivation Key:
2F34D68D E10F68D3 8091A73B 9E7C437C
PIN Encryption Derivation Data:
01011000 00000080 90123456 00000002
PIN Encryption Key:
EC2E1FE6 0BD125A0 F90456AF 3CEEE337
MAC Derivation Data:
01012000 00000080 90123456 00000002
Message Authentication, Generation:
3062579B E8F8F021 A3FB107C 471CDF28
Encryption Derivation Data:
01013000 00000080 90123456 00000002
Data Encryption, Encrypt:
F26FD64A 387B3671 EBF356D1 225B10CD

Counter: 3 (0x3)

Derivation Key:
031504E5 30365CF8 12642385 40518318
PIN Encryption Derivation Data:
01011000 00000080 90123456 00000003
PIN Encryption Key:
ED4327CB CE6D6F2B DB48BFA1 B4F33F0A
MAC Derivation Data:
01012000 00000080 90123456 00000003
Message Authentication, Generation:
B09C2633 E0D873E5 7394BEF5 71644D57
Encryption Derivation Data:

```
01013000 00000080 90123456 00000003
Data Encryption, Encrypt:
4B6B4402 137AE95F F5B0D62B FA743F4B

Counter:  4    (  0x4  )

Derivation Key:
0EEFC7AD A628BA68 878DA916 5A8A1887
PIN Encryption Derivation Data:
01011000 00000080 90123456 00000004
PIN Encryption Key:
841088CF B718BFCA 6EEA5904 26D67C65
MAC Derivation Data:
01012000 00000080 90123456 00000004
Message Authentication, Generation:
DD5A7950 56BFAF44 0F040BFA 9F9354AB
Encryption Derivation Data:
01013000 00000080 90123456 00000004
Data Encryption, Encrypt:
C5D1D4D2 9D21D9E6 3137C38F 5CE599DA

Counter:  5    (  0x5  )

Derivation Key:
C2A7AC32 8A5DA2D6 002D6246 5BFC028B
PIN Encryption Derivation Data:
01011000 00000080 90123456 00000005
PIN Encryption Key:
14213F39 8F0A9A1C 525A7902 91909A4A
MAC Derivation Data:
01012000 00000080 90123456 00000005
Message Authentication, Generation:
36DBF68E 75923624 AFD9A3FC 99C95691
Encryption Derivation Data:
01013000 00000080 90123456 00000005
Data Encryption, Encrypt:
29878D70 A9072C3C 7B2CC064 EA07704C

Counter:  6    (  0x6  )

Derivation Key:
D30F7D93 51DA5844 8A2F5E92 B4EE3B7D
PIN Encryption Derivation Data:
01011000 00000080 90123456 00000006
PIN Encryption Key:
1305263B 441D7CC6 79E98981 99FA3073
MAC Derivation Data:
01012000 00000080 90123456 00000006
Message Authentication, Generation:
D8C9F079 394ADD8E 98EC3814 2BD9A27A
Encryption Derivation Data:
01013000 00000080 90123456 00000006
Data Encryption, Encrypt:
28475B85 AFB6A54A B76EE88A 432B8281
```

```
Counter:   7     (  0x7  )

Derivation Key:
A8253CEE D9AC042C 54F75D35 C8352278
PIN Encryption Derivation Data:
01011000 00000080 90123456 00000007
PIN Encryption Key:
89FB6F07 0CC0F64E 4EB63A80 E41CCC7D
MAC Derivation Data:
01012000 00000080 90123456 00000007
Message Authentication, Generation:
F9ACB0AF B3B19A4A 12ECE4BB AFC76EB4
Encryption Derivation Data:
01013000 00000080 90123456 00000007
Data Encryption, Encrypt:
0F835112 82253704 F2DC0866 9B5F247A

Counter:   8     (  0x8  )

Derivation Key:
718EE6CF 0B27E53D 5F7AF99C 4D8146A2
PIN Encryption Derivation Data:
01011000 00000080 90123456 00000008
PIN Encryption Key:
D58AF1FE 16236751 885C3F16 B7D86803
MAC Derivation Data:
01012000 00000080 90123456 00000008
Message Authentication, Generation:
EF9089D6 F3BFBA42 5BDC4BB9 039D4B7D
Encryption Derivation Data:
01013000 00000080 90123456 00000008
Data Encryption, Encrypt:
E9DA97A3 B8BDD99A A8B0F197 5FBB9F59

Counter:   131070     (  0x1fffe  )

Derivation Key:
E21E8C8D 347F8561 A2BE752D AA85A111
PIN Encryption Derivation Data:
01011000 00000080 90123456 0001FFFE
PIN Encryption Key:
EF78A00D 8E5C554F FA44A4D9 E9AAB341
MAC Derivation Data:
01012000 00000080 90123456 0001FFFE
Message Authentication, Generation:
06008905 436F9E32 23DD6998 BD8E0586
Encryption Derivation Data:
01013000 00000080 90123456 0001FFFE
Data Encryption, Encrypt:
22DAE483 8C95370A 2F64B0D9 824B6AB9

Counter:   131071     (  0x1ffff  )

Derivation Key:
1FE36898 8089CDD7 6DA18A34 58E113BA
```

```
PIN Encryption Derivation Data:
01011000 00000080 90123456 0001FFFF
PIN Encryption Key:
C4989C5B F624370A 78D6F9D5 2068CC29
MAC Derivation Data:
01012000 00000080 90123456 0001FFFF
Message Authentication, Generation:
0C61436D 3F6641F2 563E45DD 719658F1
Encryption Derivation Data:
01013000 00000080 90123456 0001FFFF
Data Encryption, Encrypt:
4FED7B6E 8B9D474E D4203968 9143CD89

Counter:   131072    (  0x20000  )

Derivation Key:
F7AE9025 468A25D3 7B7249CF FED224C8
PIN Encryption Derivation Data:
01011000 00000080 90123456 00020000
PIN Encryption Key:
6F6BA2A5 38C2F15A A041E8DF 83E68FF6
MAC Derivation Data:
01012000 00000080 90123456 00020000
Message Authentication, Generation:
E1C89FB1 4BD5BF55 379FE09A 8D389FFE
Encryption Derivation Data:
01013000 00000080 90123456 00020000
Data Encryption, Encrypt:
BD5EE154 97E46EEA B8D0F2F8 57A7B01E

Counter:   131073    (  0x20001  )

Derivation Key:
692C8EA4 01364513 5B364971 31DF9D2C
PIN Encryption Derivation Data:
01011000 00000080 90123456 00020001
PIN Encryption Key:
083AE338 4749FA3C 17BA7265 D07FE05E
MAC Derivation Data:
01012000 00000080 90123456 00020001
Message Authentication, Generation:
38F50B6C 914FCC1C 6BD59257 6847006B
Encryption Derivation Data:
01013000 00000080 90123456 00020001
Data Encryption, Encrypt:
F64C0766 A5F59464 2976CA79 4BA64F83

Counter:   8675309    (  0x845fed  )

Derivation Key:
549067A1 706E6D06 B9713360 48936D5D
PIN Encryption Derivation Data:
01011000 00000080 90123456 00845FED
PIN Encryption Key:
E65C585C E1C5CE8E 10CBF808 0D62A556
```

```
MAC Derivation Data:
01012000 00000080 90123456 00845FED
Message Authentication, Generation:
89B29343 844D2779 FB385EED 90E6871B
Encryption Derivation Data:
01013000 00000080 90123456 00845FED
Data Encryption, Encrypt:
D39FC396 7F97FCCD 7DB60F04 E4FE24BB

Counter:   4294844416    (  0xfffe2000  )

Derivation Key:
48E585B6 94EB0B18 D5C35443 E163C0BA
PIN Encryption Derivation Data:
01011000 00000080 90123456 FFFE2000
PIN Encryption Key:
D080E58C C6104FB8 42CD7709 9C400A0C
MAC Derivation Data:
01012000 00000080 90123456 FFFE2000
Message Authentication, Generation:
0C34EECD F23ADD46 7D6E69AC F680309A
Encryption Derivation Data:
01013000 00000080 90123456 FFFE2000
Data Encryption, Encrypt:
9AB13E0B AECFAC3D 0A1FE0FD 13F03AFC

Counter:   4294852608    (  0xfffe4000  )

Derivation Key:
396C2C7C A1EA701C 03B86B7D 41F0C562
PIN Encryption Derivation Data:
01011000 00000080 90123456 FFFE4000
PIN Encryption Key:
0AB46BDF 909B34ED 6709A246 D682EFB7
MAC Derivation Data:
01012000 00000080 90123456 FFFE4000
Message Authentication, Generation:
5D6F7B6E C536CF63 71258836 66A27FA5
Encryption Derivation Data:
01013000 00000080 90123456 FFFE4000
Data Encryption, Encrypt:
7E40A8AC B92709E7 297166ED CBF99E58

Counter:   4294868992    (  0xfffe8000  )

Derivation Key:
0387625F 189B58AE 03EF0E8C CA41105E
PIN Encryption Derivation Data:
01011000 00000080 90123456 FFFE8000
PIN Encryption Key:
E3717600 201D7D5B 40C3E8E3 0C844374
MAC Derivation Data:
01012000 00000080 90123456 FFFE8000
Message Authentication, Generation:
C4DE593A 618470E8 504D8127 39A7E8C6
```

```
Encryption Derivation Data:
01013000 00000080 90123456 FFFE8000
Data Encryption, Encrypt:
0E16D25F D9BF7870 7BA0BB5D 7CB718CA

Counter:  4294901760    (  0xffff0000  )

Derivation Key:
F6BA5938 9BD14A98 55BE9727 E7C52E3C
PIN Encryption Derivation Data:
01011000 00000080 90123456 FFFF0000
PIN Encryption Key:
95EC78F7 443D6770 2D83B56E DE6832DA
MAC Derivation Data:
01012000 00000080 90123456 FFFF0000
Message Authentication, Generation:
D7C1FCE3 E525936F 6AECD573 85F54EAA
Encryption Derivation Data:
01013000 00000080 90123456 FFFF0000
Data Encryption, Encrypt:
F72FCA40 0C51A297 8E9E01C8 B77FA5E5

DUKPT Update Key (counter =  0xffffffff  )

Derivation Key:
36C6EBBC C0536FC9 1C1D5066 0D4F82AE
Derivation Data:
01010002 00000080 90123456 FFFFFFFF
Key Encryption Key:
4744A5EC BC62B5C4 BB76FBEA E1E244A3

Test Vectors for generating    KeyType._3TDEA    from    KeyType._AES128    Base
Derivation Key

Initial Key:
1273671E A26AC29A FA4D1084 127652A1


Counter:  1    (  0x1  )

Derivation Key:
4F21B565 BAD9835E 112B6465 635EAE44
PIN Encryption Derivation Data:
01021000 000100C0 90123456 00000001
PIN Encryption Key:
EA8B3F37 EB9B1583 1167EF29 77FD8762 D9B5913F 35766F6A
MAC Derivation Data:
01022000 000100C0 90123456 00000001
Message Authentication, Generation:
2A1061A6 EAC2C14F AC3758EA 07B3648A 624B24E9 42785BF1
Encryption Derivation Data:
01023000 000100C0 90123456 00000001
Data Encryption, Encrypt:
F716DFBC 6B2D2D58 25B694EE EE181A01 3F2F1C09 380BBE0C
```

```
Counter:  2    (  0x2  )

Derivation Key:
2F34D68D E10F68D3 8091A73B 9E7C437C
PIN Encryption Derivation Data:
01021000 000100C0 90123456 00000002
PIN Encryption Key:
6D27F0B2 15342736 4EA723BF 5A97EB0D E9C68176 DB748EB3
MAC Derivation Data:
01022000 000100C0 90123456 00000002
Message Authentication, Generation:
E656A0DF 80022775 DEF85FC1 3B77C387 F74C9C59 C7BCDF2E
Encryption Derivation Data:
01023000 000100C0 90123456 00000002
Data Encryption, Encrypt:
9F4CE1AE A03614D5 8481EFFF 39CCC0B4 C3FBAE43 ACCCAC3D

Counter:  3    (  0x3  )

Derivation Key:
031504E5 30365CF8 12642385 40518318
PIN Encryption Derivation Data:
01021000 000100C0 90123456 00000003
PIN Encryption Key:
844D0D61 A5B7B564 E71DD0BF CCB453BD 8CBC9DE3 66E753EF
MAC Derivation Data:
01022000 000100C0 90123456 00000003
Message Authentication, Generation:
2B894EA9 783144A8 A2C34FBB 9B74848F 9C40F46F D4ACB68A
Encryption Derivation Data:
01023000 000100C0 90123456 00000003
Data Encryption, Encrypt:
7A03F3FD 0EA49729 9C680A20 BEADE8EA 9E08D00E 94DE31B2

Counter:  4    (  0x4  )

Derivation Key:
0EEFC7AD A628BA68 878DA916 5A8A1887
PIN Encryption Derivation Data:
01021000 000100C0 90123456 00000004
PIN Encryption Key:
FBEC56F2 6AD0F28C 6BBE5FD8 6CD785FD A43ED655 4FADB511
MAC Derivation Data:
01022000 000100C0 90123456 00000004
Message Authentication, Generation:
EEFBEE2A B22A6F78 A9EEFDA3 D1E63D10 512F8B3C CE66A710
Encryption Derivation Data:
01023000 000100C0 90123456 00000004
Data Encryption, Encrypt:
8873D10D D49B31D8 34078696 98C8E6DA AB9AA8BE F20578EE

Counter:  5    (  0x5  )

Derivation Key:
C2A7AC32 8A5DA2D6 002D6246 5BFC028B
```

```
PIN Encryption Derivation Data:
01021000 000100C0 90123456 00000005
PIN Encryption Key:
F8A23032 C56D53F0 5A3798CF ADC13859 DBE65D8B 6B34569D
MAC Derivation Data:
01022000 000100C0 90123456 00000005
Message Authentication, Generation:
73B3D815 983BABE0 CF207E5C 9A630D91 C349B145 8941259B
Encryption Derivation Data:
01023000 000100C0 90123456 00000005
Data Encryption, Encrypt:
924DEA5B 10550B2F 75CE4CB2 B6889A1D 01767035 8CB9C97E

Counter:   6    (  0x6  )

Derivation Key:
D30F7D93 51DA5844 8A2F5E92 B4EE3B7D
PIN Encryption Derivation Data:
01021000 000100C0 90123456 00000006
PIN Encryption Key:
3F298133 56A26E16 68215E4A 9E627FF7 282ACD5D B9272E2F
MAC Derivation Data:
01022000 000100C0 90123456 00000006
Message Authentication, Generation:
420D0610 A824E42D 4BB53FB7 4E6BE641 7B5E37DE 442CFCC0
Encryption Derivation Data:
01023000 000100C0 90123456 00000006
Data Encryption, Encrypt:
74A87437 1DF625E5 9BE9EB1C 0980C511 AF573CB3 862AC580

Counter:   7    (  0x7  )

Derivation Key:
A8253CEE D9AC042C 54F75D35 C8352278
PIN Encryption Derivation Data:
01021000 000100C0 90123456 00000007
PIN Encryption Key:
0199D91A DB5C53D9 3A7B39E9 6C23419C 9DA8FABF 70F11BB7
MAC Derivation Data:
01022000 000100C0 90123456 00000007
Message Authentication, Generation:
82110122 D2AF4562 C2B4C3BB 9A2E2F43 CD7CFA93 231562D4
Encryption Derivation Data:
01023000 000100C0 90123456 00000007
Data Encryption, Encrypt:
2C8CBDBE FE3A12EF 8A8D4D3F 6EB34606 39E46CB1 705889EC

Counter:   8    (  0x8  )

Derivation Key:
718EE6CF 0B27E53D 5F7AF99C 4D8146A2
PIN Encryption Derivation Data:
01021000 000100C0 90123456 00000008
PIN Encryption Key:
182FC80F 08633E60 C75CD112 C079C2FE 02E218FB 6BA5EA3B
```

```
MAC Derivation Data:
01022000 000100C0 90123456 00000008
Message Authentication, Generation:
255ED43D 7290AEF2 5FBB1D10 623E601D 77B38D04 3B700788
Encryption Derivation Data:
01023000 000100C0 90123456 00000008
Data Encryption, Encrypt:
EF31ABFD 01892366 B45CD72B 79D20CA6 9F3F8985 F477A033

Counter:  131070    ( 0x1fffe  )

Derivation Key:
E21E8C8D 347F8561 A2BE752D AA85A111
PIN Encryption Derivation Data:
01021000 000100C0 90123456 0001FFFE
PIN Encryption Key:
CF5AB7FB 78A8F110 11D44D97 5E264BF1 AAC5CF3B 0FD42B69
MAC Derivation Data:
01022000 000100C0 90123456 0001FFFE
Message Authentication, Generation:
5D33A33F E9CF0AB1 DB9D07EA AC85C2C4 4487C7DE 658DDF04
Encryption Derivation Data:
01023000 000100C0 90123456 0001FFFE
Data Encryption, Encrypt:
6744710C 3486354A 95BC33F5 3E396AD9 B08FDB97 46A9C56E

Counter:  131071    ( 0x1ffff  )

Derivation Key:
1FE36898 8089CDD7 6DA18A34 58E113BA
PIN Encryption Derivation Data:
01021000 000100C0 90123456 0001FFFF
PIN Encryption Key:
CE4363CE F9B12528 E6DF8C93 190153E6 24F1433C 8D3FDFCA
MAC Derivation Data:
01022000 000100C0 90123456 0001FFFF
Message Authentication, Generation:
4DCB86BC 1271FA16 F0F0FE11 3D9D045B 7B75F3D9 8B835BDC
Encryption Derivation Data:
01023000 000100C0 90123456 0001FFFF
Data Encryption, Encrypt:
8B3C7CD3 D3A53C36 9506F499 773E9DFD 52CB8CE9 BB59E337

Counter:  131072    ( 0x20000  )

Derivation Key:
F7AE9025 468A25D3 7B7249CF FED224C8
PIN Encryption Derivation Data:
01021000 000100C0 90123456 00020000
PIN Encryption Key:
E9CD303F B904B76C A188CCCD 992AE5D9 04CC0F0A 55899126
MAC Derivation Data:
01022000 000100C0 90123456 00020000
Message Authentication, Generation:
AA4978BF D3143B5B D51536DC D26B203A E246AF37 0511704C
```

```
Encryption Derivation Data:
01023000 000100C0 90123456 00020000
Data Encryption, Encrypt:
695D2B7C BF1C9762 0AE1EE0A F6C0AEAB 73D1A460 AE87E868

Counter:  131073    (  0x20001  )

Derivation Key:
692C8EA4 01364513 5B364971 31DF9D2C
PIN Encryption Derivation Data:
01021000 000100C0 90123456 00020001
PIN Encryption Key:
3553F72A FB072A15 D555707B 46357EEA E090138F DA5B4368
MAC Derivation Data:
01022000 000100C0 90123456 00020001
Message Authentication, Generation:
A84E9390 318358D1 B245C6C0 997D7DF4 DAAB8509 8353491F
Encryption Derivation Data:
01023000 000100C0 90123456 00020001
Data Encryption, Encrypt:
6CE0B7F1 15123807 FA8EFFC2 57402D24 FB97E40D 2EBCA56C

Counter:  8675309    (  0x845fed  )

Derivation Key:
549067A1 706E6D06 B9713360 48936D5D
PIN Encryption Derivation Data:
01021000 000100C0 90123456 00845FED
PIN Encryption Key:
33D7DFCC 09EA50C6 6CAE246C 8BC170CB AD7A6851 0643BBCB
MAC Derivation Data:
01022000 000100C0 90123456 00845FED
Message Authentication, Generation:
29F12405 4110E8E1 6DD750AF 2E2DFF55 70027C9B 6C17DCA9
Encryption Derivation Data:
01023000 000100C0 90123456 00845FED
Data Encryption, Encrypt:
65E77BDD 49CB94AB 96CAE506 90733B2C 2503EBFD 54C4A9DA

Counter:  4294844416    (  0xfffe2000  )

Derivation Key:
48E585B6 94EB0B18 D5C35443 E163C0BA
PIN Encryption Derivation Data:
01021000 000100C0 90123456 FFFE2000
PIN Encryption Key:
05F163FA 3128683B 93A5739B 4B37C712 F9C1747A EAAAE9D5
MAC Derivation Data:
01022000 000100C0 90123456 FFFE2000
Message Authentication, Generation:
0378C346 68397959 083EB6B8 2EDA76A1 7FE8C702 691541AC
Encryption Derivation Data:
01023000 000100C0 90123456 FFFE2000
Data Encryption, Encrypt:
7F61B4F4 88504F50 8A4C1995 2D2DBD3C 5715174F 65EC7348
```

```
Counter:   4294852608    (  0xfffe4000  )

Derivation Key:
396C2C7C A1EA701C 03B86B7D 41F0C562
PIN Encryption Derivation Data:
01021000 000100C0 90123456 FFFE4000
PIN Encryption Key:
5322753A 3CD9E18B 956B1857 7DACDD4C C631FFDC 5873CDC2
MAC Derivation Data:
01022000 000100C0 90123456 FFFE4000
Message Authentication, Generation:
F95DCFD6 ECB0315E DC39835A 405B0144 868F931C 7473F047
Encryption Derivation Data:
01023000 000100C0 90123456 FFFE4000
Data Encryption, Encrypt:
81F967FE AB633BC8 28D0E906 1171B6FA 7FC38949 F8903F10

Counter:   4294868992    (  0xfffe8000  )

Derivation Key:
0387625F 189B58AE 03EF0E8C CA41105E
PIN Encryption Derivation Data:
01021000 000100C0 90123456 FFFE8000
PIN Encryption Key:
A3057799 7DACC2F5 4EF95BBD 0618D8E4 9C4036C9 96B98F85
MAC Derivation Data:
01022000 000100C0 90123456 FFFE8000
Message Authentication, Generation:
3BFC9E40 8D33AC18 BA9EBDE9 6BF7EA00 1E9C2E4F 18090070
Encryption Derivation Data:
01023000 000100C0 90123456 FFFE8000
Data Encryption, Encrypt:
056F4300 1E258D78 6CE026F3 62D90A58 90697BAB 8F7F41DE

Counter:   4294901760    (  0xffff0000  )

Derivation Key:
F6BA5938 9BD14A98 55BE9727 E7C52E3C
PIN Encryption Derivation Data:
01021000 000100C0 90123456 FFFF0000
PIN Encryption Key:
9B650FCC 3E0EDF7C DDF9A57F 4515BFFD 23C7654A E06970D2
MAC Derivation Data:
01022000 000100C0 90123456 FFFF0000
Message Authentication, Generation:
A718671F 2EAEB8AF 08771236 425D1C13 EEECB649 784960DC
Encryption Derivation Data:
01023000 000100C0 90123456 FFFF0000
Data Encryption, Encrypt:
E25E3C49 5948CB16 E7412199 A0507EDA 5859904F 160DB814

DUKPT Update Key (counter =   0xffffffff  )

Derivation Key:
```

```
36C6EBBC C0536FC9 1C1D5066 0D4F82AE
Derivation Data:
01020002 000100C0 90123456 FFFFFFFF
Key Encryption Key:
AF82BE85 33CFCA52 6DA71708 667AD0BB C7A75175 04C78C8A

 All Key Usages for Transaction   1   (AES-128 under AES-128 BDK)

   Initial Key:
1273671E A26AC29A FA4D1084 127652A1

   Counter:   1     (  0x1  )

Derivation Key:
4F21B565 BAD9835E 112B6465 635EAE44
Key Encryption Key Derivation Data:
01010002 00020080 90123456 00000001
Key Encryption Key:
36A724B7 BEFA5A25 F5E7B578 2A4554A2

PIN Encryption Derivation Data:
01011000 00020080 90123456 00000001
PIN Encryption Key:
AF8CB133 A78F8DC2 D1359F18 527593FB

MAC Generation Derivation Data:
01012000 00020080 90123456 00000001
Message Auth, Generation:
A2DC23DE 6FDE0824 A2BC321E 08E4B8B7

MAC Verification Derivation Data:
01012001 00020080 90123456 00000001
Message Auth, Verification:
DBB46394 5B286C07 CD3AD82E E96FD9C9

MAC Both Ways Derivation Data:
01012002 00020080 90123456 00000001
Message Auth, Both Ways:
85675439 D18D7F11 58BD8E3E AA3D502B

DE Encrypt Derivation Data:
01013000 00020080 90123456 00000001
Data Encryption, Encrypt:
A35C412E FD41FDB9 8B69797C 02DCD08F

DE Decrypt Derivation Data:
01013001 00020080 90123456 00000001
Data Encryption, Decrypt:
16292C6E A8F64C54 20A0584B FBC577BE

DE Both Ways Derivation Data:
01013002 00020080 90123456 00000001
Data Encryption, Both Ways:
A308E080 DD15A1B7 41F1721B F67DE11C
```

```
Key Derivation Derivation Data:
01018000 00020080 90123456 00000001
Key Derivation Key:
30E54D3C 69B22501 A7FC4396 9D81D5C0

Calculation of AES PIN Block (Format 4)

PAN = 4111111111111111
PIN = 1234
Random Number = 2F69ADDE2E9E7ACE

Plaintext PIN field:
441234AA  AAAAAAAA  2F69ADDE  2E9E7ACE
Plaintext PAN field:
44111111  11111111  10000000  00000000
PIN Encryption Key:
AF8CB133 A78F8DC2 D1359F18 527593FB

Intermediate Block A:
DE84127C F6DCA7DF E47BDE89 057CB820
Intermediate Block B:
9A95036D E7CDB6CE F47BDE89 057CB820
Encrypted PIN Block:
A9121503 91AB65A6 7E52883D 81CE2D15

 All Key Usages for Transaction   2   (AES-128 under AES-128 BDK)

   Initial Key:
1273671E A26AC29A FA4D1084 127652A1

   Counter:   2    (  0x2  )

Derivation Key:
2F34D68D E10F68D3 8091A73B 9E7C437C
Key Encryption Key Derivation Data:
01010002 00020080 90123456 00000002
Key Encryption Key:
7D55435B 90FDA0E6 4B18FCF1 186C1C4E

PIN Encryption Derivation Data:
01011000 00020080 90123456 00000002
PIN Encryption Key:
D30BDC73 EC9714B0 00BEC66B DB7B6D09

MAC Generation Derivation Data:
01012000 00020080 90123456 00000002
Message Auth, Generation:
484C3B06 E8562704 528CD5B4 6FB12FB6

MAC Verification Derivation Data:
01012001 00020080 90123456 00000002
Message Auth, Verification:
6CA3F901 BBCA029A E5A6EE2F 4C70B101

MAC Both Ways Derivation Data:
```

```
01012002 00020080 90123456 00000002
Message Auth, Both Ways:
7832C83D 08539133 C8117F84 BBBF4EF6

DE Encrypt Derivation Data:
01013000 00020080 90123456 00000002
Data Encryption, Encrypt:
D639514A A33AC43A D9229E43 3D6D4E5B

DE Decrypt Derivation Data:
01013001 00020080 90123456 00000002
Data Encryption, Decrypt:
EA0174D3 54623672 5407EBF9 D4082F8A

DE Both Ways Derivation Data:
01013002 00020080 90123456 00000002
Data Encryption, Both Ways:
384DBC2D E98F6AEF A18BD7C1 B5997E3B

Key Derivation Derivation Data:
01018000 00020080 90123456 00000002
Key Derivation Key:
3D22F4D5 FE33128F 48449786 55B59C67

Calculation of AES PIN Block (Format 4)

PAN = 4111111111111111
PIN = 1234
Random Number = 2F69ADDE2E9E7ACE

Plaintext PIN field:
441234AA  AAAAAAAA  2F69ADDE  2E9E7ACE
Plaintext PAN field:
44111111  11111111  10000000  00000000
PIN Encryption Key:
D30BDC73 EC9714B0 00BEC66B DB7B6D09

Intermediate Block A:
37489F3D B975A040 CD1EEE9E 68051A44
Intermediate Block B:
73598E2C A864B151 DD1EEE9E 68051A44
Encrypted PIN Block:
52A00503 BD34BA13 83F6A7EE 9FE2547F

 All Key Usages for Transaction   3   (AES-128 under AES-128 BDK)

   Initial Key:
1273671E A26AC29A FA4D1084 127652A1

   Counter:   3     (  0x3  )

Derivation Key:
031504E5 30365CF8 12642385 40518318
Key Encryption Key Derivation Data:
01010002 00020080 90123456 00000003
```

```
Key Encryption Key:
72D6E73E BF25F9AD 1C0B3EE1 A486FEAD

PIN Encryption Derivation Data:
01011000 00020080 90123456 00000003
PIN Encryption Key:
7D69F01F 3B45449F 62C7816E CE723268

MAC Generation Derivation Data:
01012000 00020080 90123456 00000003
Message Auth, Generation:
A5DF7D9D 800CA769 766F0C77 CA4E6E6C

MAC Verification Derivation Data:
01012001 00020080 90123456 00000003
Message Auth, Verification:
BDFC0690 BF2AFAB4 6238A033 08541F99

MAC Both Ways Derivation Data:
01012002 00020080 90123456 00000003
Message Auth, Both Ways:
4DE8789D 44988C5A CAF208DA 5856D471

DE Encrypt Derivation Data:
01013000 00020080 90123456 00000003
Data Encryption, Encrypt:
EF17F6AB 45B4820C 93A3DCB2 1BC491AD

DE Decrypt Derivation Data:
01013001 00020080 90123456 00000003
Data Encryption, Decrypt:
F6815240 46D3A640 C83F238B 4161B131

DE Both Ways Derivation Data:
01013002 00020080 90123456 00000003
Data Encryption, Both Ways:
832DB864 C4B8861E C910358B 81E32DC3

Key Derivation Derivation Data:
01018000 00020080 90123456 00000003
Key Derivation Key:
ABF18287 8DE14289 44F872AC 43EDDC75

Calculation of AES PIN Block (Format 4)

PAN = 4111111111111111
PIN = 1234
Random Number = 2F69ADDE2E9E7ACE

Plaintext PIN field:
441234AA  AAAAAAAA  2F69ADDE  2E9E7ACE
Plaintext PAN field:
44111111  11111111  10000000  00000000
PIN Encryption Key:
7D69F01F 3B45449F 62C7816E CE723268
```

```
Intermediate Block A:
497BE94D 8C33CD43 12215567 50CD9EEA
Intermediate Block B:
0D6AF85C 9D22DC52 02215567 50CD9EEA
Encrypted PIN Block:
A5A27E82 B43A9A86 6A93D7AB E89CEF93

 All Key Usages for Transaction   4   (AES-128 under AES-128 BDK)

   Initial Key:
1273671E A26AC29A FA4D1084 127652A1

   Counter:   4     (  0x4  )

Derivation Key:
0EEFC7AD A628BA68 878DA916 5A8A1887
Key Encryption Key Derivation Data:
01010002 00020080 90123456 00000004
Key Encryption Key:
09204D02 45072FDF FE58B51E 717CBEFB

PIN Encryption Derivation Data:
01011000 00020080 90123456 00000004
PIN Encryption Key:
91A05883 18EC2673 214271F7 0137896E

MAC Generation Derivation Data:
01012000 00020080 90123456 00000004
Message Auth, Generation:
E6E46796 47D8A905 7C1FC155 37CB4C4E

MAC Verification Derivation Data:
01012001 00020080 90123456 00000004
Message Auth, Verification:
9B7F2A03 3461A60F 1E957522 514FC833

MAC Both Ways Derivation Data:
01012002 00020080 90123456 00000004
Message Auth, Both Ways:
B6CBFE77 AAEF6D55 86F70FE1 3FF2E7FA

DE Encrypt Derivation Data:
01013000 00020080 90123456 00000004
Data Encryption, Encrypt:
B3BD44C0 8BB6BA27 C3BB4711 D7D70387

DE Decrypt Derivation Data:
01013001 00020080 90123456 00000004
Data Encryption, Decrypt:
99BC22ED 802BB7D7 D18613C5 AD02ABAB

DE Both Ways Derivation Data:
01013002 00020080 90123456 00000004
Data Encryption, Both Ways:
```

```
151EF298 C5852964 6D9BDFF0 8906CA4B

Key Derivation Derivation Data:
01018000 00020080 90123456 00000004
Key Derivation Key:
4B6CA65C 425B1629 CDF84059 0F2F2605

Calculation of AES PIN Block (Format 4)

PAN = 4111111111111111
PIN = 1234
Random Number = 2F69ADDE2E9E7ACE

Plaintext PIN field:
441234AA  AAAAAAAA  2F69ADDE  2E9E7ACE
Plaintext PAN field:
44111111  11111111  10000000  00000000
PIN Encryption Key:
91A05883 18EC2673 214271F7 0137896E

Intermediate Block A:
A23B6265 83D22FE2 FCF077EF 17104971
Intermediate Block B:
E62A7374 92C33EF3 ECF077EF 17104971
Encrypted PIN Block:
71B3D052 86694987 77555A8B E6698E44

 All Key Usages for Transaction   5   (AES-128 under AES-128 BDK)

   Initial Key:
1273671E A26AC29A FA4D1084 127652A1

   Counter:   5    (  0x5  )

Derivation Key:
C2A7AC32 8A5DA2D6 002D6246 5BFC028B
Key Encryption Key Derivation Data:
01010002 00020080 90123456 00000005
Key Encryption Key:
507838E8 17F32B6D 75151FC9 E8EF1A80

PIN Encryption Derivation Data:
01011000 00020080 90123456 00000005
PIN Encryption Key:
35A43BC9 EFEB09C7 56204B57 E3FB7D4D

MAC Generation Derivation Data:
01012000 00020080 90123456 00000005
Message Auth, Generation:
0588185F E1FF8C7E 22FAD78C 1C61F065

MAC Verification Derivation Data:
01012001 00020080 90123456 00000005
Message Auth, Verification:
75923E65 09A80723 C60DB758 84F4C984
```

```
MAC Both Ways Derivation Data:
01012002 00020080 90123456 00000005
Message Auth, Both Ways:
082FAFAA C4780503 28DE6F37 25EFE4B4

DE Encrypt Derivation Data:
01013000 00020080 90123456 00000005
Data Encryption, Encrypt:
CA02DF6F 30B39E14 BD0B4A30 E460920F

DE Decrypt Derivation Data:
01013001 00020080 90123456 00000005
Data Encryption, Decrypt:
666F64FB A90777C1 7DF22C0B F2D1142F

DE Both Ways Derivation Data:
01013002 00020080 90123456 00000005
Data Encryption, Both Ways:
948BE71B 8C8DD813 62C88061 D462A946

Key Derivation Derivation Data:
01018000 00020080 90123456 00000005
Key Derivation Key:
E61C7FB5 44669AF1 E49D8264 FF8E3979

Calculation of AES PIN Block (Format 4)

PAN = 4111111111111111
PIN = 1234
Random Number = 2F69ADDE2E9E7ACE

Plaintext PIN field:
441234AA  AAAAAAAA  2F69ADDE  2E9E7ACE
Plaintext PAN field:
44111111  11111111  10000000  00000000
PIN Encryption Key:
35A43BC9 EFEB09C7 56204B57 E3FB7D4D

Intermediate Block A:
2C820EF7 660EFADB 0F5378DB 04509A9B
Intermediate Block B:
68931FE6 771FEBCA 1F5378DB 04509A9B
Encrypted PIN Block:
881A7F77 A2E04E5B EA985E34 2FD0B628

 All Key Usages for Transaction   6   (AES-128 under AES-128 BDK)

   Initial Key:
1273671E A26AC29A FA4D1084 127652A1

   Counter:   6    (  0x6  )

Derivation Key:
D30F7D93 51DA5844 8A2F5E92 B4EE3B7D
```

```
Key Encryption Key Derivation Data:
01010002 00020080 90123456 00000006
Key Encryption Key:
FC7AB8F7 80CE16BA 3C1C0A62 417F85B0

PIN Encryption Derivation Data:
01011000 00020080 90123456 00000006
PIN Encryption Key:
02DCC6CD 1201A3A2 CA709955 9C862123

MAC Generation Derivation Data:
01012000 00020080 90123456 00000006
Message Auth, Generation:
7B60F72A 5639C0EE 7EB2100F A80BB793

MAC Verification Derivation Data:
01012001 00020080 90123456 00000006
Message Auth, Verification:
FDB53F44 62EE4B39 EE84EF14 50A0B54B

MAC Both Ways Derivation Data:
01012002 00020080 90123456 00000006
Message Auth, Both Ways:
B53ECBED F231A94B 6303D4B3 D9F10FBB

DE Encrypt Derivation Data:
01013000 00020080 90123456 00000006
Data Encryption, Encrypt:
C9B8A7C4 E486180B 22291151 64F0B293

DE Decrypt Derivation Data:
01013001 00020080 90123456 00000006
Data Encryption, Decrypt:
4A7CD6FE 17AFD57C 9EF43CD0 11EAEE0B

DE Both Ways Derivation Data:
01013002 00020080 90123456 00000006
Data Encryption, Both Ways:
39B56DE4 583A8303 73D3110D 8C363761

Key Derivation Derivation Data:
01018000 00020080 90123456 00000006
Key Derivation Key:
CEFC0CA4 9F3B228D 56E26121 524ADD9D

Calculation of AES PIN Block (Format 4)

PAN = 4111111111111111
PIN = 1234
Random Number = 2F69ADDE2E9E7ACE

Plaintext PIN field:
441234AA  AAAAAAAA  2F69ADDE  2E9E7ACE
Plaintext PAN field:
44111111  11111111  10000000  00000000
```

```
PIN Encryption Key:
02DCC6CD 1201A3A2 CA709955 9C862123

Intermediate Block A:
A00365C3 190DB5D9 720BD6EC F00A3262
Intermediate Block B:
E41274D2 081CA4C8 620BD6EC F00A3262
Encrypted PIN Block:
BDC1C387 1AFB0B34 0AA5B5CE FD08695E

 All Key Usages for Transaction   7   (AES-128 under AES-128 BDK)

   Initial Key:
1273671E A26AC29A FA4D1084 127652A1

   Counter:   7     (  0x7  )

Derivation Key:
A8253CEE D9AC042C 54F75D35 C8352278
Key Encryption Key Derivation Data:
01010002 00020080 90123456 00000007
Key Encryption Key:
53250B59 B66E1044 5C790A9B 73772063

PIN Encryption Derivation Data:
01011000 00020080 90123456 00000007
PIN Encryption Key:
6ECF912F 3B18CA11 A7A27BB6 0705FD09

MAC Generation Derivation Data:
01012000 00020080 90123456 00000007
Message Auth, Generation:
BAA08CA2 63C69525 BC6B1BA8 F4275D69

MAC Verification Derivation Data:
01012001 00020080 90123456 00000007
Message Auth, Verification:
03130A11 AAD3F068 F8D373DD DE93E400

MAC Both Ways Derivation Data:
01012002 00020080 90123456 00000007
Message Auth, Both Ways:
E2AF0498 4705A94A B5DAF76B 3AE35FB0

DE Encrypt Derivation Data:
01013000 00020080 90123456 00000007
Data Encryption, Encrypt:
0FA8F1F0 A2DD7B10 05A862D7 7CDED698

DE Decrypt Derivation Data:
01013001 00020080 90123456 00000007
Data Encryption, Decrypt:
FFC14C40 6ED7396A 3A90A66A 0D576CB6

DE Both Ways Derivation Data:
```

```
01013002 00020080 90123456 00000007
Data Encryption, Both Ways:
80535379 3C3FF8D3 EA196A46 8BB57F6D

Key Derivation Derivation Data:
01018000 00020080 90123456 00000007
Key Derivation Key:
34E30CEB DE41AE72 8F736F1A 07DDE77A

Calculation of AES PIN Block (Format 4)

PAN = 4111111111111111
PIN = 1234
Random Number = 2F69ADDE2E9E7ACE

Plaintext PIN field:
441234AA  AAAAAAAA  2F69ADDE  2E9E7ACE
Plaintext PAN field:
44111111  11111111  10000000  00000000
PIN Encryption Key:
6ECF912F 3B18CA11 A7A27BB6 0705FD09

Intermediate Block A:
409382FC A5CE2A27 BF3005FF 9FA5D9F2
Intermediate Block B:
048293ED B4DF3B36 AF3005FF 9FA5D9F2
Encrypted PIN Block:
4A8E6B8C 7DBEE6CB A6DC774F 0CB83396

 All Key Usages for Transaction   8   (AES-128 under AES-128 BDK)

   Initial Key:
1273671E A26AC29A FA4D1084 127652A1

   Counter:   8     (  0x8  )

Derivation Key:
718EE6CF 0B27E53D 5F7AF99C 4D8146A2
Key Encryption Key Derivation Data:
01010002 00020080 90123456 00000008
Key Encryption Key:
219BBA49 C1963248 9E8C089F B22ACCBC

PIN Encryption Derivation Data:
01011000 00020080 90123456 00000008
PIN Encryption Key:
4D9DF3FB EE3448FC 3E676D04 320A90F5

MAC Generation Derivation Data:
01012000 00020080 90123456 00000008
Message Auth, Generation:
6FD572E5 D59E6188 75F19348 4F9178FB

MAC Verification Derivation Data:
01012001 00020080 90123456 00000008
```

```
Message Auth, Verification:
4CB304CF BA8A10ED 4535321F 4245E5B7

MAC Both Ways Derivation Data:
01012002 00020080 90123456 00000008
Message Auth, Both Ways:
CE29DBBF 5F39913C 5C60C511 68EA068E

DE Encrypt Derivation Data:
01013000 00020080 90123456 00000008
Data Encryption, Encrypt:
650F3420 4ABD4E57 764D61AC 3D266FB1

DE Decrypt Derivation Data:
01013001 00020080 90123456 00000008
Data Encryption, Decrypt:
4D46EE36 CCC09616 43EC89D2 51C3F107

DE Both Ways Derivation Data:
01013002 00020080 90123456 00000008
Data Encryption, Both Ways:
19F12146 0E4C73E2 1E7A61CF 02B22A04

Key Derivation Derivation Data:
01018000 00020080 90123456 00000008
Key Derivation Key:
FFBF6177 C5B969E2 73B8529F C1D5C117

Calculation of AES PIN Block (Format 4)

PAN = 4111111111111111
PIN = 1234
Random Number = 2F69ADDE2E9E7ACE

Plaintext PIN field:
441234AA  AAAAAAAA  2F69ADDE  2E9E7ACE
Plaintext PAN field:
44111111  11111111  10000000  00000000
PIN Encryption Key:
4D9DF3FB EE3448FC 3E676D04 320A90F5

Intermediate Block A:
4C6F5F4E D252AAB5 E893990D FFB0E4CF
Intermediate Block B:
087E4E5F C343BBA4 F893990D FFB0E4CF
Encrypted PIN Block:
8308BB85 7C17F390 369F761F 8EB358FA

 All Key Usages for Transaction   8675309   (AES-128 under AES-128 BDK)

   Initial Key:
1273671E A26AC29A FA4D1084 127652A1

   Counter:   8675309    (  0x845fed  )
```

```
Derivation Key:
549067A1 706E6D06 B9713360 48936D5D
Key Encryption Key Derivation Data:
01010002 00020080 90123456 00845FED
Key Encryption Key:
A8A73AF2 7612054B 6B49126C D8933A9C

PIN Encryption Derivation Data:
01011000 00020080 90123456 00845FED
PIN Encryption Key:
D1DDA386 AA4A556A F0119FDC B5D132C6

MAC Generation Derivation Data:
01012000 00020080 90123456 00845FED
Message Auth, Generation:
89365C79 70950CAC 0A6261FF C7DB26C6

MAC Verification Derivation Data:
01012001 00020080 90123456 00845FED
Message Auth, Verification:
6833594C 83A01DF3 CF6AD613 57FE4168

MAC Both Ways Derivation Data:
01012002 00020080 90123456 00845FED
Message Auth, Both Ways:
B27575B7 464E0A31 27D56820 9E0DEF7F

DE Encrypt Derivation Data:
01013000 00020080 90123456 00845FED
Data Encryption, Encrypt:
B1E4D900 6A87DD08 D87F11A1 24D35517

DE Decrypt Derivation Data:
01013001 00020080 90123456 00845FED
Data Encryption, Decrypt:
A9CE94E1 5AE2B3CD B989EE14 BB245204

DE Both Ways Derivation Data:
01013002 00020080 90123456 00845FED
Data Encryption, Both Ways:
CB68B9C5 A4F694D2 04635B0F 89C6EA5F

Key Derivation Derivation Data:
01018000 00020080 90123456 00845FED
Key Derivation Key:
CF2792DE 3EAC4433 066FD23E 5C4316FE

Calculation of AES PIN Block (Format 4)

PAN = 4111111111111111
PIN = 1234
Random Number = 2F69ADDE2E9E7ACE

Plaintext PIN field:
441234AA  AAAAAAAA  2F69ADDE  2E9E7ACE
```

```
Plaintext PAN field:
44111111  11111111  10000000  00000000
PIN Encryption Key:
D1DDA386 AA4A556A F0119FDC B5D132C6

Intermediate Block A:
822DD7E9 213A41B1 12B2020D 0D21ABD4
Intermediate Block B:
C63CC6F8 302B50A0 02B2020D 0D21ABD4
Encrypted PIN Block:
3AB5FF37 0302F730 89003AD3 6CB7E046
```

2.3 Full internal state

2.3.1 Full calculation of first eight keys (Host Algorithm)

```
Test Vectors for generating  KeyType._AES128  from  KeyType._AES128  Base
Derivation Key

Counter:  1    (  0x1  )
Host_Derive_Working_Key(BDK =  FEDCBA98  76543210  F1F1F1F1  F1F1F1F1
sessionKeyUsage =  KeyUsage._PINEncryption  sessionKeyType =  KeyType._AES128
initialKeyID =  12345678  90123456  counter =  1  )
   Derive_Initial_Key(BDK =  FEDCBA98  76543210  F1F1F1F1  F1F1F1F1  keyType =
KeyType._AES128  initialKeyID =  12345678  90123456  )
     derivationData:  01018001  00020080  12345678  90123456
       Derive_Key(derivationKey =  FEDCBA98  76543210  F1F1F1F1  F1F1F1F1  keyType =
KeyType._AES128  derivationData =  01018001  00020080  12345678  90123456  deriveType
=  KeyType._AES128  )
          AES_Encrypt_ECB(key =  FEDCBA98  76543210  F1F1F1F1  F1F1F1F1  data =
01018001  00020080  12345678  90123456  )
            result =  1273671E  A26AC29A  FA4D1084  127652A1
        derivedKey:  1273671E  A26AC29A  FA4D1084  127652A1
     initialKey:  1273671E  A26AC29A  FA4D1084  127652A1
  initialKey:  1273671E  A26AC29A  FA4D1084  127652A1
  BIT FOUND:  1
  derivationData:  01018000  00020080  90123456  00000001
    Derive_Key(derivationKey =  1273671E  A26AC29A  FA4D1084  127652A1  keyType =
KeyType._AES128  derivationData =  01018000  00020080  90123456  00000001  deriveType
=  KeyType._AES128  )
       AES_Encrypt_ECB(key =  1273671E  A26AC29A  FA4D1084  127652A1  data =  01018000
00020080  90123456  00000001  )
         result =  4F21B565  BAD9835E  112B6465  635EAE44
     derivedKey:  4F21B565  BAD9835E  112B6465  635EAE44
  derivationKey:  4F21B565  BAD9835E  112B6465  635EAE44
  FINAL DERIVATION:
  derivationData  01011000  00020080  90123456  00000001
    Derive_Key(derivationKey =  4F21B565  BAD9835E  112B6465  635EAE44  keyType =
KeyType._AES128  derivationData =  01011000  00020080  90123456  00000001  deriveType
=  KeyType._AES128  )
       AES_Encrypt_ECB(key =  4F21B565  BAD9835E  112B6465  635EAE44  data =  01011000
00020080  90123456  00000001  )
         result =  AF8CB133  A78F8DC2  D1359F18  527593FB
     derivedKey:  AF8CB133  A78F8DC2  D1359F18  527593FB
  sessionKey  AF8CB133  A78F8DC2  D1359F18  527593FB
```

```
PIN Encryption Key:                AF8CB133  A78F8DC2  D1359F18  527593FB

Counter:  2    ( 0x2 )
Host_Derive_Working_Key(BDK = FEDCBA98 76543210 F1F1F1F1 F1F1F1F1
sessionKeyUsage = KeyUsage._PINEncryption sessionKeyType = KeyType._AES128
initialKeyID = 12345678 90123456 counter = 2 )
   Derive_Initial_Key(BDK = FEDCBA98 76543210 F1F1F1F1 F1F1F1F1 keyType =
KeyType._AES128 initialKeyID = 12345678 90123456 )
     derivationData:  01018001 00020080 12345678 90123456
       Derive_Key(derivationKey = FEDCBA98 76543210 F1F1F1F1 F1F1F1F1 keyType =
KeyType._AES128 derivationData = 01018001 00020080 12345678 90123456 deriveType
= KeyType._AES128 )
          AES_Encrypt_ECB(key = FEDCBA98 76543210 F1F1F1F1 F1F1F1F1 data =
01018001 00020080 12345678 90123456 )
            result =  1273671E A26AC29A FA4D1084 127652A1
        derivedKey: 1273671E A26AC29A FA4D1084 127652A1
     initialKey:  1273671E A26AC29A FA4D1084 127652A1
  initialKey: 1273671E A26AC29A FA4D1084 127652A1
  BIT FOUND: 2
  derivationData: 01018000 00020080 90123456 00000002
    Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00000002 deriveType
= KeyType._AES128 )
       AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00000002 )
        result =  2F34D68D E10F68D3 8091A73B 9E7C437C
     derivedKey: 2F34D68D E10F68D3 8091A73B 9E7C437C
  derivationKey: 2F34D68D E10F68D3 8091A73B 9E7C437C
  FINAL DERIVATION:
  derivationData 01011000 00020080 90123456 00000002
    Derive_Key(derivationKey = 2F34D68D E10F68D3 8091A73B 9E7C437C keyType =
KeyType._AES128 derivationData = 01011000 00020080 90123456 00000002 deriveType
= KeyType._AES128 )
       AES_Encrypt_ECB(key = 2F34D68D E10F68D3 8091A73B 9E7C437C data = 01011000
00020080 90123456 00000002 )
        result =  D30BDC73 EC9714B0 00BEC66B DB7B6D09
     derivedKey: D30BDC73 EC9714B0 00BEC66B DB7B6D09
  sessionKey D30BDC73 EC9714B0 00BEC66B DB7B6D09

PIN Encryption Key:                D30BDC73  EC9714B0  00BEC66B  DB7B6D09

Counter:  3    ( 0x3 )
Host_Derive_Working_Key(BDK = FEDCBA98 76543210 F1F1F1F1 F1F1F1F1
sessionKeyUsage = KeyUsage._PINEncryption sessionKeyType = KeyType._AES128
initialKeyID = 12345678 90123456 counter = 3 )
   Derive_Initial_Key(BDK = FEDCBA98 76543210 F1F1F1F1 F1F1F1F1 keyType =
KeyType._AES128 initialKeyID = 12345678 90123456 )
     derivationData:  01018001 00020080 12345678 90123456
       Derive_Key(derivationKey = FEDCBA98 76543210 F1F1F1F1 F1F1F1F1 keyType =
KeyType._AES128 derivationData = 01018001 00020080 12345678 90123456 deriveType
= KeyType._AES128 )
          AES_Encrypt_ECB(key = FEDCBA98 76543210 F1F1F1F1 F1F1F1F1 data =
01018001 00020080 12345678 90123456 )
            result =  1273671E A26AC29A FA4D1084 127652A1
        derivedKey: 1273671E A26AC29A FA4D1084 127652A1
```

```
     initialKey:  1273671E  A26AC29A  FA4D1084  127652A1
  initialKey:  1273671E  A26AC29A  FA4D1084  127652A1
  BIT FOUND:  2
  derivationData:  01018000  00020080  90123456  00000002
    Derive_Key(derivationKey =  1273671E  A26AC29A  FA4D1084  127652A1  keyType =
KeyType._AES128  derivationData =  01018000  00020080  90123456  00000002  deriveType
=  KeyType._AES128  )
       AES_Encrypt_ECB(key =  1273671E  A26AC29A  FA4D1084  127652A1  data =  01018000
00020080  90123456  00000002  )
         result =  2F34D68D  E10F68D3  8091A73B  9E7C437C
     derivedKey:  2F34D68D  E10F68D3  8091A73B  9E7C437C
  derivationKey:  2F34D68D  E10F68D3  8091A73B  9E7C437C
  BIT FOUND:  1
  derivationData:  01018000  00020080  90123456  00000003
    Derive_Key(derivationKey =  2F34D68D  E10F68D3  8091A73B  9E7C437C  keyType =
KeyType._AES128  derivationData =  01018000  00020080  90123456  00000003  deriveType
=  KeyType._AES128  )
       AES_Encrypt_ECB(key =  2F34D68D  E10F68D3  8091A73B  9E7C437C  data =  01018000
00020080  90123456  00000003  )
         result =  031504E5  30365CF8  12642385  40518318
     derivedKey:  031504E5  30365CF8  12642385  40518318
  derivationKey:  031504E5  30365CF8  12642385  40518318
  FINAL DERIVATION:
  derivationData  01011000  00020080  90123456  00000003
    Derive_Key(derivationKey =  031504E5  30365CF8  12642385  40518318  keyType =
KeyType._AES128  derivationData =  01011000  00020080  90123456  00000003  deriveType
=  KeyType._AES128  )
       AES_Encrypt_ECB(key =  031504E5  30365CF8  12642385  40518318  data =  01011000
00020080  90123456  00000003  )
         result =  7D69F01F  3B45449F  62C7816E  CE723268
     derivedKey:  7D69F01F  3B45449F  62C7816E  CE723268
  sessionKey  7D69F01F  3B45449F  62C7816E  CE723268

PIN Encryption Key:               7D69F01F  3B45449F  62C7816E  CE723268

Counter:  4    (  0x4  )
Host_Derive_Working_Key(BDK =  FEDCBA98  76543210  F1F1F1F1  F1F1F1F1
sessionKeyUsage =  KeyUsage._PINEncryption  sessionKeyType =  KeyType._AES128
initialKeyID =  12345678  90123456  counter =  4  )
   Derive_Initial_Key(BDK =  FEDCBA98  76543210  F1F1F1F1  F1F1F1F1  keyType =
KeyType._AES128  initialKeyID =  12345678  90123456  )
     derivationData:  01018001  00020080  12345678  90123456
       Derive_Key(derivationKey =  FEDCBA98  76543210  F1F1F1F1  F1F1F1F1  keyType =
KeyType._AES128  derivationData =  01018001  00020080  12345678  90123456  deriveType
=  KeyType._AES128  )
         AES_Encrypt_ECB(key =  FEDCBA98  76543210  F1F1F1F1  F1F1F1F1  data =
01018001  00020080  12345678  90123456  )
           result =  1273671E  A26AC29A  FA4D1084  127652A1
       derivedKey:  1273671E  A26AC29A  FA4D1084  127652A1
     initialKey:  1273671E  A26AC29A  FA4D1084  127652A1
  initialKey:  1273671E  A26AC29A  FA4D1084  127652A1
  BIT FOUND:  4
  derivationData:  01018000  00020080  90123456  00000004
```

```
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00000004 deriveType
= KeyType._AES128 )
       AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00000004 )
        result =  0EEFC7AD A628BA68 878DA916 5A8A1887
     derivedKey: 0EEFC7AD A628BA68 878DA916 5A8A1887
  derivationKey: 0EEFC7AD A628BA68 878DA916 5A8A1887
  FINAL DERIVATION:
  derivationData 01011000 00020080 90123456 00000004
   Derive_Key(derivationKey = 0EEFC7AD A628BA68 878DA916 5A8A1887 keyType =
KeyType._AES128 derivationData = 01011000 00020080 90123456 00000004 deriveType
= KeyType._AES128 )
       AES_Encrypt_ECB(key = 0EEFC7AD A628BA68 878DA916 5A8A1887 data = 01011000
00020080 90123456 00000004 )
        result =  91A05883 18EC2673 214271F7 0137896E
     derivedKey: 91A05883 18EC2673 214271F7 0137896E
  sessionKey 91A05883 18EC2673 214271F7 0137896E

PIN Encryption Key:               91A05883 18EC2673 214271F7 0137896E

Counter:  5    ( 0x5 )
Host_Derive_Working_Key(BDK = FEDCBA98 76543210 F1F1F1F1 F1F1F1F1
sessionKeyUsage = KeyUsage._PINEncryption sessionKeyType = KeyType._AES128
initialKeyID = 12345678 90123456 counter = 5 )
   Derive_Initial_Key(BDK = FEDCBA98 76543210 F1F1F1F1 F1F1F1F1 keyType =
KeyType._AES128 initialKeyID = 12345678 90123456 )
     derivationData:  01018001 00020080 12345678 90123456
      Derive_Key(derivationKey = FEDCBA98 76543210 F1F1F1F1 F1F1F1F1 keyType =
KeyType._AES128 derivationData = 01018001 00020080 12345678 90123456 deriveType
= KeyType._AES128 )
         AES_Encrypt_ECB(key = FEDCBA98 76543210 F1F1F1F1 F1F1F1F1 data =
01018001 00020080 12345678 90123456 )
          result =  1273671E A26AC29A FA4D1084 127652A1
       derivedKey: 1273671E A26AC29A FA4D1084 127652A1
     initialKey:  1273671E A26AC29A FA4D1084 127652A1
  initialKey: 1273671E A26AC29A FA4D1084 127652A1
  BIT FOUND: 4
  derivationData: 01018000 00020080 90123456 00000004
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00000004 deriveType
= KeyType._AES128 )
       AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00000004 )
        result =  0EEFC7AD A628BA68 878DA916 5A8A1887
     derivedKey: 0EEFC7AD A628BA68 878DA916 5A8A1887
  derivationKey: 0EEFC7AD A628BA68 878DA916 5A8A1887
  BIT FOUND: 1
  derivationData: 01018000 00020080 90123456 00000005
   Derive_Key(derivationKey = 0EEFC7AD A628BA68 878DA916 5A8A1887 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00000005 deriveType
= KeyType._AES128 )
       AES_Encrypt_ECB(key = 0EEFC7AD A628BA68 878DA916 5A8A1887 data = 01018000
00020080 90123456 00000005 )
        result =  C2A7AC32 8A5DA2D6 002D6246 5BFC028B
```

```
     derivedKey:  C2A7AC32  8A5DA2D6  002D6246  5BFC028B
  derivationKey:  C2A7AC32  8A5DA2D6  002D6246  5BFC028B
  FINAL DERIVATION:
  derivationData  01011000  00020080  90123456  00000005
    Derive_Key(derivationKey =  C2A7AC32  8A5DA2D6  002D6246  5BFC028B  keyType =
KeyType._AES128  derivationData =  01011000  00020080  90123456  00000005  deriveType
=  KeyType._AES128  )
       AES_Encrypt_ECB(key =  C2A7AC32  8A5DA2D6  002D6246  5BFC028B  data =  01011000
00020080  90123456  00000005  )
         result =   35A43BC9  EFEB09C7  56204B57  E3FB7D4D
     derivedKey:  35A43BC9  EFEB09C7  56204B57  E3FB7D4D
  sessionKey  35A43BC9  EFEB09C7  56204B57  E3FB7D4D

PIN Encryption Key:                35A43BC9  EFEB09C7  56204B57  E3FB7D4D

Counter:   6     (  0x6  )
Host_Derive_Working_Key(BDK =  FEDCBA98  76543210  F1F1F1F1  F1F1F1F1
sessionKeyUsage =  KeyUsage._PINEncryption  sessionKeyType =  KeyType._AES128
initialKeyID =  12345678  90123456  counter =  6  )
    Derive_Initial_Key(BDK =  FEDCBA98  76543210  F1F1F1F1  F1F1F1F1  keyType =
KeyType._AES128  initialKeyID =  12345678  90123456  )
     derivationData:   01018001  00020080  12345678  90123456
       Derive_Key(derivationKey =  FEDCBA98  76543210  F1F1F1F1  F1F1F1F1  keyType =
KeyType._AES128  derivationData =  01018001  00020080  12345678  90123456  deriveType
=  KeyType._AES128  )
          AES_Encrypt_ECB(key =  FEDCBA98  76543210  F1F1F1F1  F1F1F1F1  data =
01018001  00020080  12345678  90123456  )
            result =   1273671E  A26AC29A  FA4D1084  127652A1
         derivedKey:  1273671E  A26AC29A  FA4D1084  127652A1
     initialKey:   1273671E  A26AC29A  FA4D1084  127652A1
  initialKey:  1273671E  A26AC29A  FA4D1084  127652A1
  BIT FOUND:  4
  derivationData:  01018000  00020080  90123456  00000004
    Derive_Key(derivationKey =  1273671E  A26AC29A  FA4D1084  127652A1  keyType =
KeyType._AES128  derivationData =  01018000  00020080  90123456  00000004  deriveType
=  KeyType._AES128  )
       AES_Encrypt_ECB(key =  1273671E  A26AC29A  FA4D1084  127652A1  data =  01018000
00020080  90123456  00000004  )
         result =   0EEFC7AD  A628BA68  878DA916  5A8A1887
     derivedKey:  0EEFC7AD  A628BA68  878DA916  5A8A1887
  derivationKey:  0EEFC7AD  A628BA68  878DA916  5A8A1887
  BIT FOUND:  2
  derivationData:  01018000  00020080  90123456  00000006
    Derive_Key(derivationKey =  0EEFC7AD  A628BA68  878DA916  5A8A1887  keyType =
KeyType._AES128  derivationData =  01018000  00020080  90123456  00000006  deriveType
=  KeyType._AES128  )
       AES_Encrypt_ECB(key =  0EEFC7AD  A628BA68  878DA916  5A8A1887  data =  01018000
00020080  90123456  00000006  )
         result =   D30F7D93  51DA5844  8A2F5E92  B4EE3B7D
     derivedKey:  D30F7D93  51DA5844  8A2F5E92  B4EE3B7D
  derivationKey:  D30F7D93  51DA5844  8A2F5E92  B4EE3B7D
  FINAL DERIVATION:
  derivationData  01011000  00020080  90123456  00000006
```

```
   Derive_Key(derivationKey =  D30F7D93  51DA5844  8A2F5E92  B4EE3B7D  keyType =
KeyType._AES128  derivationData =  01011000  00020080  90123456  00000006  deriveType
=  KeyType._AES128  )
       AES_Encrypt_ECB(key =  D30F7D93  51DA5844  8A2F5E92  B4EE3B7D  data =  01011000
00020080  90123456  00000006  )
        result =  02DCC6CD  1201A3A2  CA709955  9C862123
     derivedKey:  02DCC6CD  1201A3A2  CA709955  9C862123
  sessionKey  02DCC6CD  1201A3A2  CA709955  9C862123

PIN Encryption Key:                02DCC6CD  1201A3A2  CA709955  9C862123

Counter:  7    (  0x7  )
Host_Derive_Working_Key(BDK =  FEDCBA98  76543210  F1F1F1F1  F1F1F1F1
sessionKeyUsage =  KeyUsage._PINEncryption  sessionKeyType =  KeyType._AES128
initialKeyID =  12345678  90123456  counter =  7  )
   Derive_Initial_Key(BDK =  FEDCBA98  76543210  F1F1F1F1  F1F1F1F1  keyType =
KeyType._AES128  initialKeyID =  12345678  90123456  )
     derivationData:  01018001  00020080  12345678  90123456
      Derive_Key(derivationKey =  FEDCBA98  76543210  F1F1F1F1  F1F1F1F1  keyType =
KeyType._AES128  derivationData =  01018001  00020080  12345678  90123456  deriveType
=  KeyType._AES128  )
         AES_Encrypt_ECB(key =  FEDCBA98  76543210  F1F1F1F1  F1F1F1F1  data =
01018001  00020080  12345678  90123456  )
           result =  1273671E  A26AC29A  FA4D1084  127652A1
        derivedKey:  1273671E  A26AC29A  FA4D1084  127652A1
     initialKey:  1273671E  A26AC29A  FA4D1084  127652A1
  initialKey:  1273671E  A26AC29A  FA4D1084  127652A1
  BIT FOUND:  4
  derivationData:  01018000  00020080  90123456  00000004
   Derive_Key(derivationKey =  1273671E  A26AC29A  FA4D1084  127652A1  keyType =
KeyType._AES128  derivationData =  01018000  00020080  90123456  00000004  deriveType
=  KeyType._AES128  )
       AES_Encrypt_ECB(key =  1273671E  A26AC29A  FA4D1084  127652A1  data =  01018000
00020080  90123456  00000004  )
        result =  0EEFC7AD  A628BA68  878DA916  5A8A1887
     derivedKey:  0EEFC7AD  A628BA68  878DA916  5A8A1887
  derivationKey:  0EEFC7AD  A628BA68  878DA916  5A8A1887
  BIT FOUND:  2
  derivationData:  01018000  00020080  90123456  00000006
   Derive_Key(derivationKey =  0EEFC7AD  A628BA68  878DA916  5A8A1887  keyType =
KeyType._AES128  derivationData =  01018000  00020080  90123456  00000006  deriveType
=  KeyType._AES128  )
       AES_Encrypt_ECB(key =  0EEFC7AD  A628BA68  878DA916  5A8A1887  data =  01018000
00020080  90123456  00000006  )
        result =  D30F7D93  51DA5844  8A2F5E92  B4EE3B7D
     derivedKey:  D30F7D93  51DA5844  8A2F5E92  B4EE3B7D
  derivationKey:  D30F7D93  51DA5844  8A2F5E92  B4EE3B7D
  BIT FOUND:  1
  derivationData:  01018000  00020080  90123456  00000007
   Derive_Key(derivationKey =  D30F7D93  51DA5844  8A2F5E92  B4EE3B7D  keyType =
KeyType._AES128  derivationData =  01018000  00020080  90123456  00000007  deriveType
=  KeyType._AES128  )
       AES_Encrypt_ECB(key =  D30F7D93  51DA5844  8A2F5E92  B4EE3B7D  data =  01018000
00020080  90123456  00000007  )
        result =  A8253CEE  D9AC042C  54F75D35  C8352278
```

```
     derivedKey:  A8253CEE  D9AC042C  54F75D35  C8352278
  derivationKey:  A8253CEE  D9AC042C  54F75D35  C8352278
  FINAL DERIVATION:
  derivationData  01011000  00020080  90123456  00000007
    Derive_Key(derivationKey =  A8253CEE  D9AC042C  54F75D35  C8352278  keyType =
KeyType._AES128  derivationData =  01011000  00020080  90123456  00000007  deriveType
=  KeyType._AES128  )
       AES_Encrypt_ECB(key =  A8253CEE  D9AC042C  54F75D35  C8352278  data =  01011000
00020080  90123456  00000007  )
         result =   6ECF912F  3B18CA11  A7A27BB6  0705FD09
     derivedKey:  6ECF912F  3B18CA11  A7A27BB6  0705FD09
  sessionKey  6ECF912F  3B18CA11  A7A27BB6  0705FD09

PIN Encryption Key:                6ECF912F  3B18CA11  A7A27BB6  0705FD09

Counter:   8     (  0x8  )
Host_Derive_Working_Key(BDK =  FEDCBA98  76543210  F1F1F1F1  F1F1F1F1
sessionKeyUsage =  KeyUsage._PINEncryption  sessionKeyType =  KeyType._AES128
initialKeyID =  12345678  90123456  counter =  8  )
    Derive_Initial_Key(BDK =  FEDCBA98  76543210  F1F1F1F1  F1F1F1F1  keyType =
KeyType._AES128  initialKeyID =  12345678  90123456  )
     derivationData:   01018001  00020080  12345678  90123456
       Derive_Key(derivationKey =  FEDCBA98  76543210  F1F1F1F1  F1F1F1F1  keyType =
KeyType._AES128  derivationData =  01018001  00020080  12345678  90123456  deriveType
=  KeyType._AES128  )
          AES_Encrypt_ECB(key =  FEDCBA98  76543210  F1F1F1F1  F1F1F1F1  data =
01018001  00020080  12345678  90123456  )
            result =   1273671E  A26AC29A  FA4D1084  127652A1
         derivedKey:  1273671E  A26AC29A  FA4D1084  127652A1
     initialKey:   1273671E  A26AC29A  FA4D1084  127652A1
  initialKey:  1273671E  A26AC29A  FA4D1084  127652A1
  BIT FOUND:  8
  derivationData:  01018000  00020080  90123456  00000008
    Derive_Key(derivationKey =  1273671E  A26AC29A  FA4D1084  127652A1  keyType =
KeyType._AES128  derivationData =  01018000  00020080  90123456  00000008  deriveType
=  KeyType._AES128  )
       AES_Encrypt_ECB(key =  1273671E  A26AC29A  FA4D1084  127652A1  data =  01018000
00020080  90123456  00000008  )
         result =   718EE6CF  0B27E53D  5F7AF99C  4D8146A2
     derivedKey:  718EE6CF  0B27E53D  5F7AF99C  4D8146A2
  derivationKey:  718EE6CF  0B27E53D  5F7AF99C  4D8146A2
  FINAL DERIVATION:
  derivationData  01011000  00020080  90123456  00000008
    Derive_Key(derivationKey =  718EE6CF  0B27E53D  5F7AF99C  4D8146A2  keyType =
KeyType._AES128  derivationData =  01011000  00020080  90123456  00000008  deriveType
=  KeyType._AES128  )
       AES_Encrypt_ECB(key =  718EE6CF  0B27E53D  5F7AF99C  4D8146A2  data =  01011000
00020080  90123456  00000008  )
         result =   4D9DF3FB  EE3448FC  3E676D04  320A90F5
     derivedKey:  4D9DF3FB  EE3448FC  3E676D04  320A90F5
  sessionKey  4D9DF3FB  EE3448FC  3E676D04  320A90F5

PIN Encryption Key:                4D9DF3FB  EE3448FC  3E676D04  320A90F5
```

2.3.2 Full calculation of first eight keys (Terminal Algorithm)

```
Test Vectors for generating  KeyType._AES128  from  KeyType._AES128  Base
Derivation Key
Derive_Initial_Key(BDK =  FEDCBA98  76543210  F1F1F1F1  F1F1F1F1  keyType =
KeyType._AES128  initialKeyID =  12345678  90123456  )
  derivationData:  01018001  00020080  12345678  90123456
    Derive_Key(derivationKey =  FEDCBA98  76543210  F1F1F1F1  F1F1F1F1  keyType =
KeyType._AES128  derivationData =  01018001  00020080  12345678  90123456  deriveType
=  KeyType._AES128  )
       AES_Encrypt_ECB(key =  FEDCBA98  76543210  F1F1F1F1  F1F1F1F1  data =  01018001
00020080  12345678  90123456  )
         result =  1273671E  A26AC29A  FA4D1084  127652A1
     derivedKey:  1273671E  A26AC29A  FA4D1084  127652A1
  initialKey:  1273671E  A26AC29A  FA4D1084  127652A1

Initial Key:                      1273671E  A26AC29A  FA4D1084  127652A1

Load_Initial_Key(initialKey =  1273671E  A26AC29A  FA4D1084  127652A1  deriveKeyType
=  KeyType._AES128  initialKeyID =  12345678  90123456  )
  gIntermediateDerivationKeyRegister[0] <-  1273671E  A26AC29A  FA4D1084  127652A1
  gDeviceID <-  12345678  90123456
  gCounter <-  0
  gShiftRegister <-  1
  gDeriveKeyType <-  KeyType._AES128
  Update_Derivation_Keys(deriveKeyType =  KeyType._AES128  )
    gCurrentKey:  0
    baseKey:  1273671E  A26AC29A  FA4D1084  127652A1
    i:  31  gShiftRegister:  2147483648
    derivationData:  01018000  00020080  90123456  80000000
    Derive_Key(derivationKey =  1273671E  A26AC29A  FA4D1084  127652A1  keyType =
KeyType._AES128  derivationData =  01018000  00020080  90123456  80000000  deriveType
=  KeyType._AES128  )
       AES_Encrypt_ECB(key =  1273671E  A26AC29A  FA4D1084  127652A1  data =  01018000
00020080  90123456  80000000  )
         result =  9DC56486  499A2E85  7FDEFC47  40641EA8
     derivedKey:  9DC56486  499A2E85  7FDEFC47  40641EA8
    gIntermediateDerivationKeyRegister[  31  ] <-  9DC56486  499A2E85  7FDEFC47
40641EA8
    i:  30  gShiftRegister:  1073741824
    derivationData:  01018000  00020080  90123456  40000000
    Derive_Key(derivationKey =  1273671E  A26AC29A  FA4D1084  127652A1  keyType =
KeyType._AES128  derivationData =  01018000  00020080  90123456  40000000  deriveType
=  KeyType._AES128  )
       AES_Encrypt_ECB(key =  1273671E  A26AC29A  FA4D1084  127652A1  data =  01018000
00020080  90123456  40000000  )
         result =  36AF4AA9  FC1100B2  AE774210  1540340A
     derivedKey:  36AF4AA9  FC1100B2  AE774210  1540340A
    gIntermediateDerivationKeyRegister[  30  ] <-  36AF4AA9  FC1100B2  AE774210
1540340A
    i:  29  gShiftRegister:  536870912
    derivationData:  01018000  00020080  90123456  20000000
```

```
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 20000000 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 20000000 )
        result = 7CCE4E67 9F4FC347 8E3CD450 9D64A7F3
     derivedKey: 7CCE4E67 9F4FC347 8E3CD450 9D64A7F3
   gIntermediateDerivationKeyRegister[ 29 ] <- 7CCE4E67 9F4FC347 8E3CD450
9D64A7F3
   i: 28 gShiftRegister: 268435456
   derivationData: 01018000 00020080 90123456 10000000
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 10000000 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 10000000 )
        result = 69B45311 8411404D B54AE2B7 51F02F43
     derivedKey: 69B45311 8411404D B54AE2B7 51F02F43
   gIntermediateDerivationKeyRegister[ 28 ] <- 69B45311 8411404D B54AE2B7
51F02F43
   i: 27 gShiftRegister: 134217728
   derivationData: 01018000 00020080 90123456 08000000
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 08000000 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 08000000 )
        result = 97D7BB3F C342B9E9 61308BB8 B801775B
     derivedKey: 97D7BB3F C342B9E9 61308BB8 B801775B
   gIntermediateDerivationKeyRegister[ 27 ] <- 97D7BB3F C342B9E9 61308BB8
B801775B
   i: 26 gShiftRegister: 67108864
   derivationData: 01018000 00020080 90123456 04000000
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 04000000 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 04000000 )
        result = 61C70779 F920BBD3 7815C21B 5A1A7B75
     derivedKey: 61C70779 F920BBD3 7815C21B 5A1A7B75
   gIntermediateDerivationKeyRegister[ 26 ] <- 61C70779 F920BBD3 7815C21B
5A1A7B75
   i: 25 gShiftRegister: 33554432
   derivationData: 01018000 00020080 90123456 02000000
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 02000000 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 02000000 )
        result = FBDF917E 209B42F9 DB8843D1 8BEE8033
     derivedKey: FBDF917E 209B42F9 DB8843D1 8BEE8033
   gIntermediateDerivationKeyRegister[ 25 ] <- FBDF917E 209B42F9 DB8843D1
8BEE8033
   i: 24 gShiftRegister: 16777216
   derivationData: 01018000 00020080 90123456 01000000
```

```
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 01000000 deriveType
= KeyType._AES128 )
       AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 01000000 )
        result = 145E8C93 3FC0D619 00592035 CF18A5AF
     derivedKey: 145E8C93 3FC0D619 00592035 CF18A5AF
   gIntermediateDerivationKeyRegister[ 24 ] <- 145E8C93 3FC0D619 00592035
CF18A5AF
   i: 23 gShiftRegister: 8388608
   derivationData: 01018000 00020080 90123456 00800000
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00800000 deriveType
= KeyType._AES128 )
       AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00800000 )
        result = DF16D5BA C52FFA75 64D7DBD2 DE7C6CCF
     derivedKey: DF16D5BA C52FFA75 64D7DBD2 DE7C6CCF
   gIntermediateDerivationKeyRegister[ 23 ] <- DF16D5BA C52FFA75 64D7DBD2
DE7C6CCF
   i: 22 gShiftRegister: 4194304
   derivationData: 01018000 00020080 90123456 00400000
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00400000 deriveType
= KeyType._AES128 )
       AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00400000 )
        result = E5517163 6976BDC5 758A6FA4 C25F0008
     derivedKey: E5517163 6976BDC5 758A6FA4 C25F0008
   gIntermediateDerivationKeyRegister[ 22 ] <- E5517163 6976BDC5 758A6FA4
C25F0008
   i: 21 gShiftRegister: 2097152
   derivationData: 01018000 00020080 90123456 00200000
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00200000 deriveType
= KeyType._AES128 )
       AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00200000 )
        result = 988A3AB8 9B9332A1 5D0BE2C5 4C279923
     derivedKey: 988A3AB8 9B9332A1 5D0BE2C5 4C279923
   gIntermediateDerivationKeyRegister[ 21 ] <- 988A3AB8 9B9332A1 5D0BE2C5
4C279923
   i: 20 gShiftRegister: 1048576
   derivationData: 01018000 00020080 90123456 00100000
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00100000 deriveType
= KeyType._AES128 )
       AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00100000 )
        result = 5787EB83 7B6FFB3A F24759F8 625CEC19
     derivedKey: 5787EB83 7B6FFB3A F24759F8 625CEC19
   gIntermediateDerivationKeyRegister[ 20 ] <- 5787EB83 7B6FFB3A F24759F8
625CEC19
   i: 19 gShiftRegister: 524288
   derivationData: 01018000 00020080 90123456 00080000
```

```
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00080000 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00080000 )
        result =  5AAF46AA D7593E0D 224E05E1 3629ED1E
     derivedKey: 5AAF46AA D7593E0D 224E05E1 3629ED1E
   gIntermediateDerivationKeyRegister[ 19 ] <-  5AAF46AA D7593E0D 224E05E1
3629ED1E
   i: 18 gShiftRegister: 262144
   derivationData: 01018000 00020080 90123456 00040000
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00040000 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00040000 )
        result =  579594A9 86E87917 382A1815 76FA7A9A
     derivedKey: 579594A9 86E87917 382A1815 76FA7A9A
   gIntermediateDerivationKeyRegister[ 18 ] <-  579594A9 86E87917 382A1815
76FA7A9A
   i: 17 gShiftRegister: 131072
   derivationData: 01018000 00020080 90123456 00020000
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00020000 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00020000 )
        result =  F7AE9025 468A25D3 7B7249CF FED224C8
     derivedKey: F7AE9025 468A25D3 7B7249CF FED224C8
   gIntermediateDerivationKeyRegister[ 17 ] <-  F7AE9025 468A25D3 7B7249CF
FED224C8
   i: 16 gShiftRegister: 65536
   derivationData: 01018000 00020080 90123456 00010000
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00010000 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00010000 )
        result =  F4C6237D B49E28BF 96E6A18C D8CDDA00
     derivedKey: F4C6237D B49E28BF 96E6A18C D8CDDA00
   gIntermediateDerivationKeyRegister[ 16 ] <-  F4C6237D B49E28BF 96E6A18C
D8CDDA00
   i: 15 gShiftRegister: 32768
   derivationData: 01018000 00020080 90123456 00008000
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00008000 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00008000 )
        result =  9EF99A4D 5FD548A2 3D299074 047F7F6B
     derivedKey: 9EF99A4D 5FD548A2 3D299074 047F7F6B
   gIntermediateDerivationKeyRegister[ 15 ] <-  9EF99A4D 5FD548A2 3D299074
047F7F6B
   i: 14 gShiftRegister: 16384
   derivationData: 01018000 00020080 90123456 00004000
```

```
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00004000 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00004000 )
       result = 4EC5FC0C 3CD62AFF 174A37B6 FDC2B0D9
    derivedKey: 4EC5FC0C 3CD62AFF 174A37B6 FDC2B0D9
   gIntermediateDerivationKeyRegister[ 14 ] <- 4EC5FC0C 3CD62AFF 174A37B6
FDC2B0D9
   i: 13 gShiftRegister: 8192
   derivationData: 01018000 00020080 90123456 00002000
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00002000 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00002000 )
       result = 84F4CCA4 5C4F1D4E 063F1CE5 B95B6C7F
    derivedKey: 84F4CCA4 5C4F1D4E 063F1CE5 B95B6C7F
   gIntermediateDerivationKeyRegister[ 13 ] <- 84F4CCA4 5C4F1D4E 063F1CE5
B95B6C7F
   i: 12 gShiftRegister: 4096
   derivationData: 01018000 00020080 90123456 00001000
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00001000 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00001000 )
       result = 18690547 EB19D28E FAF5EF6D 22C271AA
    derivedKey: 18690547 EB19D28E FAF5EF6D 22C271AA
   gIntermediateDerivationKeyRegister[ 12 ] <- 18690547 EB19D28E FAF5EF6D
22C271AA
   i: 11 gShiftRegister: 2048
   derivationData: 01018000 00020080 90123456 00000800
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00000800 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00000800 )
       result = 492248FE E0FE87E8 B5DB7BB2 AC7BC955
    derivedKey: 492248FE E0FE87E8 B5DB7BB2 AC7BC955
   gIntermediateDerivationKeyRegister[ 11 ] <- 492248FE E0FE87E8 B5DB7BB2
AC7BC955
   i: 10 gShiftRegister: 1024
   derivationData: 01018000 00020080 90123456 00000400
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00000400 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00000400 )
       result = 4BF8EB1D AF9F4244 332ED016 63EB654E
    derivedKey: 4BF8EB1D AF9F4244 332ED016 63EB654E
   gIntermediateDerivationKeyRegister[ 10 ] <- 4BF8EB1D AF9F4244 332ED016
63EB654E
   i: 9 gShiftRegister: 512
   derivationData: 01018000 00020080 90123456 00000200
```

```
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00000200 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00000200 )
        result = CF16FEBC 5CFD1A74 1A328056 4A9681F2
     derivedKey: CF16FEBC 5CFD1A74 1A328056 4A9681F2
   gIntermediateDerivationKeyRegister[ 9 ] <- CF16FEBC 5CFD1A74 1A328056
4A9681F2
   i: 8 gShiftRegister: 256
   derivationData: 01018000 00020080 90123456 00000100
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00000100 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00000100 )
        result = 065355A6 A3DD4C22 60BDDDFA 0C16704E
     derivedKey: 065355A6 A3DD4C22 60BDDDFA 0C16704E
   gIntermediateDerivationKeyRegister[ 8 ] <- 065355A6 A3DD4C22 60BDDDFA
0C16704E
   i: 7 gShiftRegister: 128
   derivationData: 01018000 00020080 90123456 00000080
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00000080 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00000080 )
        result = 089F6B98 9CA13D49 A6A0317F 85460CE5
     derivedKey: 089F6B98 9CA13D49 A6A0317F 85460CE5
   gIntermediateDerivationKeyRegister[ 7 ] <- 089F6B98 9CA13D49 A6A0317F
85460CE5
   i: 6 gShiftRegister: 64
   derivationData: 01018000 00020080 90123456 00000040
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00000040 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00000040 )
        result = C13BDA0A 56D6998E 544E0A10 A3D979DA
     derivedKey: C13BDA0A 56D6998E 544E0A10 A3D979DA
   gIntermediateDerivationKeyRegister[ 6 ] <- C13BDA0A 56D6998E 544E0A10
A3D979DA
   i: 5 gShiftRegister: 32
   derivationData: 01018000 00020080 90123456 00000020
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00000020 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00000020 )
        result = 1ED39390 B4448C69 819EB55F 4C616564
     derivedKey: 1ED39390 B4448C69 819EB55F 4C616564
   gIntermediateDerivationKeyRegister[ 5 ] <- 1ED39390 B4448C69 819EB55F
4C616564
   i: 4 gShiftRegister: 16
   derivationData: 01018000 00020080 90123456 00000010
```

```
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00000010 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00000010 )
        result = 7459762E ED7F51D0 8567ED65 98DFBEA2
     derivedKey: 7459762E ED7F51D0 8567ED65 98DFBEA2
   gIntermediateDerivationKeyRegister[ 4 ] <- 7459762E ED7F51D0 8567ED65
98DFBEA2
   i: 3 gShiftRegister: 8
   derivationData: 01018000 00020080 90123456 00000008
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00000008 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00000008 )
        result = 718EE6CF 0B27E53D 5F7AF99C 4D8146A2
     derivedKey: 718EE6CF 0B27E53D 5F7AF99C 4D8146A2
   gIntermediateDerivationKeyRegister[ 3 ] <- 718EE6CF 0B27E53D 5F7AF99C
4D8146A2
   i: 2 gShiftRegister: 4
   derivationData: 01018000 00020080 90123456 00000004
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00000004 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00000004 )
        result = 0EEFC7AD A628BA68 878DA916 5A8A1887
     derivedKey: 0EEFC7AD A628BA68 878DA916 5A8A1887
   gIntermediateDerivationKeyRegister[ 2 ] <- 0EEFC7AD A628BA68 878DA916
5A8A1887
   i: 1 gShiftRegister: 2
   derivationData: 01018000 00020080 90123456 00000002
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00000002 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00000002 )
        result = 2F34D68D E10F68D3 8091A73B 9E7C437C
     derivedKey: 2F34D68D E10F68D3 8091A73B 9E7C437C
   gIntermediateDerivationKeyRegister[ 1 ] <- 2F34D68D E10F68D3 8091A73B
9E7C437C
   i: 0 gShiftRegister: 1
   derivationData: 01018000 00020080 90123456 00000001
   Derive_Key(derivationKey = 1273671E A26AC29A FA4D1084 127652A1 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00000001 deriveType
= KeyType._AES128 )
      AES_Encrypt_ECB(key = 1273671E A26AC29A FA4D1084 127652A1 data = 01018000
00020080 90123456 00000001 )
        result = 4F21B565 BAD9835E 112B6465 635EAE44
     derivedKey: 4F21B565 BAD9835E 112B6465 635EAE44
   gIntermediateDerivationKeyRegister[ 0 ] <- 4F21B565 BAD9835E 112B6465
635EAE44
 gCounter <- 1
```

```
Counter:  1    ( 0x1 )
Generate_Working_Keys(sessionKeyUsage = KeyUsage._PINEncryption sessionKeyType =
KeyType._AES128 )
  Set_Shift_Register -> gShiftRegister: 1 gCurrentKey: 0
  gCounter: 1
  derivationData: 01011000 00020080 90123456 00000001
    Derive_Key(derivationKey = 4F21B565 BAD9835E 112B6465 635EAE44 keyType =
KeyType._AES128 derivationData = 01011000 00020080 90123456 00000001 deriveType
= KeyType._AES128 )
       AES_Encrypt_ECB(key = 4F21B565 BAD9835E 112B6465 635EAE44 data = 01011000
00020080 90123456 00000001 )
         result =  AF8CB133 A78F8DC2 D1359F18 527593FB
      derivedKey: AF8CB133 A78F8DC2 D1359F18 527593FB
  sessionKey: AF8CB133 A78F8DC2 D1359F18 527593FB
    Update_State_for_next_Transaction()
       Update_Derivation_Keys(deriveKeyType = KeyType._AES128 )
         gCurrentKey: 0
         baseKey: 4F21B565 BAD9835E 112B6465 635EAE44
         i: 0 gShiftRegister: 1
         derivationData: 01018000 00020080 90123456 00000001
         Derive_Key(derivationKey = 4F21B565 BAD9835E 112B6465 635EAE44 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00000001 deriveType
= KeyType._AES128 )
            AES_Encrypt_ECB(key = 4F21B565 BAD9835E 112B6465 635EAE44 data =
01018000 00020080 90123456 00000001 )
              result =  30E54D3C 69B22501 A7FC4396 9D81D5C0
           derivedKey: 30E54D3C 69B22501 A7FC4396 9D81D5C0
         gIntermediateDerivationKeyRegister[ 0 ] <-  30E54D3C 69B22501 A7FC4396
9D81D5C0
      gIntermediateDerivationKeyRegister[ 0 ] <- 0 )
      gCounter <- 2

PIN Encryption Key:               AF8CB133 A78F8DC2 D1359F18 527593FB

Counter:  2    ( 0x2 )
Generate_Working_Keys(sessionKeyUsage = KeyUsage._PINEncryption sessionKeyType =
KeyType._AES128 )
  Set_Shift_Register -> gShiftRegister: 2 gCurrentKey: 1
  gCounter: 2
  derivationData: 01011000 00020080 90123456 00000002
    Derive_Key(derivationKey = 2F34D68D E10F68D3 8091A73B 9E7C437C keyType =
KeyType._AES128 derivationData = 01011000 00020080 90123456 00000002 deriveType
= KeyType._AES128 )
       AES_Encrypt_ECB(key = 2F34D68D E10F68D3 8091A73B 9E7C437C data = 01011000
00020080 90123456 00000002 )
         result =  D30BDC73 EC9714B0 00BEC66B DB7B6D09
      derivedKey: D30BDC73 EC9714B0 00BEC66B DB7B6D09
  sessionKey: D30BDC73 EC9714B0 00BEC66B DB7B6D09
    Update_State_for_next_Transaction()
       Update_Derivation_Keys(deriveKeyType = KeyType._AES128 )
         gCurrentKey: 1
         baseKey: 2F34D68D E10F68D3 8091A73B 9E7C437C
         i: 1 gShiftRegister: 2
         derivationData: 01018000 00020080 90123456 00000002
```

```
        Derive_Key(derivationKey = 2F34D68D E10F68D3 8091A73B 9E7C437C keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00000002 deriveType
= KeyType._AES128 )
           AES_Encrypt_ECB(key = 2F34D68D E10F68D3 8091A73B 9E7C437C data =
01018000 00020080 90123456 00000002 )
              result = 3D22F4D5 FE33128F 48449786 55B59C67
          derivedKey: 3D22F4D5 FE33128F 48449786 55B59C67
        gIntermediateDerivationKeyRegister[ 1 ] <- 3D22F4D5 FE33128F 48449786
55B59C67
        i: 0 gShiftRegister: 1
        derivationData: 01018000 00020080 90123456 00000003
        Derive_Key(derivationKey = 2F34D68D E10F68D3 8091A73B 9E7C437C keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00000003 deriveType
= KeyType._AES128 )
           AES_Encrypt_ECB(key = 2F34D68D E10F68D3 8091A73B 9E7C437C data =
01018000 00020080 90123456 00000003 )
              result = 031504E5 30365CF8 12642385 40518318
          derivedKey: 031504E5 30365CF8 12642385 40518318
        gIntermediateDerivationKeyRegister[ 0 ] <- 031504E5 30365CF8 12642385
40518318
     gIntermediateDerivationKeyRegister[ 1 ] <- 0 )
     gCounter <- 3

PIN Encryption Key:               D30BDC73 EC9714B0 00BEC66B DB7B6D09

Counter:  3    ( 0x3 )
Generate_Working_Keys(sessionKeyUsage = KeyUsage._PINEncryption sessionKeyType =
KeyType._AES128 )
  Set_Shift_Register -> gShiftRegister: 1 gCurrentKey: 0
  gCounter: 3
  derivationData: 01011000 00020080 90123456 00000003
    Derive_Key(derivationKey = 031504E5 30365CF8 12642385 40518318 keyType =
KeyType._AES128 derivationData = 01011000 00020080 90123456 00000003 deriveType
= KeyType._AES128 )
       AES_Encrypt_ECB(key = 031504E5 30365CF8 12642385 40518318 data = 01011000
00020080 90123456 00000003 )
        result = 7D69F01F 3B45449F 62C7816E CE723268
     derivedKey: 7D69F01F 3B45449F 62C7816E CE723268
  sessionKey: 7D69F01F 3B45449F 62C7816E CE723268
    Update_State_for_next_Transaction()
       Update_Derivation_Keys(deriveKeyType = KeyType._AES128 )
         gCurrentKey: 0
         baseKey: 031504E5 30365CF8 12642385 40518318
         i: 0 gShiftRegister: 1
         derivationData: 01018000 00020080 90123456 00000003
         Derive_Key(derivationKey = 031504E5 30365CF8 12642385 40518318 keyType =
KeyType._AES128 derivationData = 01018000 00020080 90123456 00000003 deriveType
= KeyType._AES128 )
           AES_Encrypt_ECB(key = 031504E5 30365CF8 12642385 40518318 data =
01018000 00020080 90123456 00000003 )
              result = ABF18287 8DE14289 44F872AC 43EDDC75
          derivedKey: ABF18287 8DE14289 44F872AC 43EDDC75
        gIntermediateDerivationKeyRegister[ 0 ] <- ABF18287 8DE14289 44F872AC
43EDDC75
     gIntermediateDerivationKeyRegister[ 0 ] <- 0 )
```

```
     gCounter <-  4

PIN Encryption Key:                7D69F01F  3B45449F  62C7816E  CE723268

Counter:   4     (  0x4  )
Generate_Working_Keys(sessionKeyUsage =  KeyUsage._PINEncryption  sessionKeyType =
KeyType._AES128  )
  Set_Shift_Register -> gShiftRegister:  4  gCurrentKey:  2
  gCounter:  4
  derivationData:  01011000  00020080  90123456  00000004
    Derive_Key(derivationKey =  0EEFC7AD  A628BA68  878DA916  5A8A1887  keyType =
KeyType._AES128  derivationData =  01011000  00020080  90123456  00000004  deriveType
=  KeyType._AES128  )
       AES_Encrypt_ECB(key =  0EEFC7AD  A628BA68  878DA916  5A8A1887  data =  01011000
00020080  90123456  00000004  )
         result =   91A05883  18EC2673  214271F7  0137896E
     derivedKey:  91A05883  18EC2673  214271F7  0137896E
  sessionKey:  91A05883  18EC2673  214271F7  0137896E
    Update_State_for_next_Transaction()
       Update_Derivation_Keys(deriveKeyType =  KeyType._AES128  )
         gCurrentKey:  2
         baseKey:  0EEFC7AD  A628BA68  878DA916  5A8A1887
         i:  2  gShiftRegister:  4
         derivationData:  01018000  00020080  90123456  00000004
         Derive_Key(derivationKey =  0EEFC7AD  A628BA68  878DA916  5A8A1887  keyType =
KeyType._AES128  derivationData =  01018000  00020080  90123456  00000004  deriveType
=  KeyType._AES128  )
            AES_Encrypt_ECB(key =  0EEFC7AD  A628BA68  878DA916  5A8A1887  data =
01018000  00020080  90123456  00000004  )
              result =   4B6CA65C  425B1629  CDF84059  0F2F2605
          derivedKey:  4B6CA65C  425B1629  CDF84059  0F2F2605
         gIntermediateDerivationKeyRegister[  2  ] <-   4B6CA65C  425B1629  CDF84059
0F2F2605
         i:  1  gShiftRegister:  2
         derivationData:  01018000  00020080  90123456  00000006
         Derive_Key(derivationKey =  0EEFC7AD  A628BA68  878DA916  5A8A1887  keyType =
KeyType._AES128  derivationData =  01018000  00020080  90123456  00000006  deriveType
=  KeyType._AES128  )
            AES_Encrypt_ECB(key =  0EEFC7AD  A628BA68  878DA916  5A8A1887  data =
01018000  00020080  90123456  00000006  )
              result =   D30F7D93  51DA5844  8A2F5E92  B4EE3B7D
          derivedKey:  D30F7D93  51DA5844  8A2F5E92  B4EE3B7D
         gIntermediateDerivationKeyRegister[  1  ] <-   D30F7D93  51DA5844  8A2F5E92
B4EE3B7D
         i:  0  gShiftRegister:  1
         derivationData:  01018000  00020080  90123456  00000005
         Derive_Key(derivationKey =  0EEFC7AD  A628BA68  878DA916  5A8A1887  keyType =
KeyType._AES128  derivationData =  01018000  00020080  90123456  00000005  deriveType
=  KeyType._AES128  )
            AES_Encrypt_ECB(key =  0EEFC7AD  A628BA68  878DA916  5A8A1887  data =
01018000  00020080  90123456  00000005  )
              result =   C2A7AC32  8A5DA2D6  002D6246  5BFC028B
          derivedKey:  C2A7AC32  8A5DA2D6  002D6246  5BFC028B
         gIntermediateDerivationKeyRegister[  0  ] <-   C2A7AC32  8A5DA2D6  002D6246
5BFC028B
```

```
     gIntermediateDerivationKeyRegister[  2  ] <-  0  )
     gCounter <-  5

PIN Encryption Key:                91A05883  18EC2673  214271F7  0137896E

Counter:   5     (  0x5  )
Generate_Working_Keys(sessionKeyUsage =  KeyUsage._PINEncryption  sessionKeyType =
KeyType._AES128  )
  Set_Shift_Register -> gShiftRegister:  1  gCurrentKey:  0
  gCounter:  5
  derivationData:  01011000  00020080  90123456  00000005
    Derive_Key(derivationKey =  C2A7AC32  8A5DA2D6  002D6246  5BFC028B  keyType =
KeyType._AES128  derivationData =  01011000  00020080  90123456  00000005  deriveType
=  KeyType._AES128  )
       AES_Encrypt_ECB(key =  C2A7AC32  8A5DA2D6  002D6246  5BFC028B  data =  01011000
00020080  90123456  00000005  )
         result =   35A43BC9  EFEB09C7  56204B57  E3FB7D4D
     derivedKey:  35A43BC9  EFEB09C7  56204B57  E3FB7D4D
  sessionKey:  35A43BC9  EFEB09C7  56204B57  E3FB7D4D
    Update_State_for_next_Transaction()
       Update_Derivation_Keys(deriveKeyType =  KeyType._AES128  )
         gCurrentKey:  0
         baseKey:  C2A7AC32  8A5DA2D6  002D6246  5BFC028B
         i:  0  gShiftRegister:  1
         derivationData:  01018000  00020080  90123456  00000005
         Derive_Key(derivationKey =  C2A7AC32  8A5DA2D6  002D6246  5BFC028B  keyType =
KeyType._AES128  derivationData =  01018000  00020080  90123456  00000005  deriveType
=  KeyType._AES128  )
            AES_Encrypt_ECB(key =  C2A7AC32  8A5DA2D6  002D6246  5BFC028B  data =
01018000  00020080  90123456  00000005  )
              result =   E61C7FB5  44669AF1  E49D8264  FF8E3979
           derivedKey:  E61C7FB5  44669AF1  E49D8264  FF8E3979
         gIntermediateDerivationKeyRegister[  0  ] <-  E61C7FB5  44669AF1  E49D8264
FF8E3979
     gIntermediateDerivationKeyRegister[  0  ] <-  0  )
     gCounter <-  6

PIN Encryption Key:                35A43BC9  EFEB09C7  56204B57  E3FB7D4D

Counter:   6     (  0x6  )
Generate_Working_Keys(sessionKeyUsage =  KeyUsage._PINEncryption  sessionKeyType =
KeyType._AES128  )
  Set_Shift_Register -> gShiftRegister:  2  gCurrentKey:  1
  gCounter:  6
  derivationData:  01011000  00020080  90123456  00000006
    Derive_Key(derivationKey =  D30F7D93  51DA5844  8A2F5E92  B4EE3B7D  keyType =
KeyType._AES128  derivationData =  01011000  00020080  90123456  00000006  deriveType
=  KeyType._AES128  )
       AES_Encrypt_ECB(key =  D30F7D93  51DA5844  8A2F5E92  B4EE3B7D  data =  01011000
00020080  90123456  00000006  )
         result =   02DCC6CD  1201A3A2  CA709955  9C862123
     derivedKey:  02DCC6CD  1201A3A2  CA709955  9C862123
  sessionKey:  02DCC6CD  1201A3A2  CA709955  9C862123
    Update_State_for_next_Transaction()
       Update_Derivation_Keys(deriveKeyType =  KeyType._AES128  )
```

```
        gCurrentKey:  1
        baseKey:  D30F7D93  51DA5844  8A2F5E92  B4EE3B7D
        i:  1  gShiftRegister:  2
        derivationData:  01018000  00020080  90123456  00000006
        Derive_Key(derivationKey =  D30F7D93  51DA5844  8A2F5E92  B4EE3B7D  keyType =
KeyType._AES128  derivationData =  01018000  00020080  90123456  00000006  deriveType
=  KeyType._AES128  )
           AES_Encrypt_ECB(key =  D30F7D93  51DA5844  8A2F5E92  B4EE3B7D  data =
01018000  00020080  90123456  00000006  )
             result =   CEFC0CA4  9F3B228D  56E26121  524ADD9D
          derivedKey:  CEFC0CA4  9F3B228D  56E26121  524ADD9D
        gIntermediateDerivationKeyRegister[  1  ] <-   CEFC0CA4  9F3B228D  56E26121
524ADD9D
        i:  0  gShiftRegister:  1
        derivationData:  01018000  00020080  90123456  00000007
        Derive_Key(derivationKey =  D30F7D93  51DA5844  8A2F5E92  B4EE3B7D  keyType =
KeyType._AES128  derivationData =  01018000  00020080  90123456  00000007  deriveType
=  KeyType._AES128  )
           AES_Encrypt_ECB(key =  D30F7D93  51DA5844  8A2F5E92  B4EE3B7D  data =
01018000  00020080  90123456  00000007  )
             result =   A8253CEE  D9AC042C  54F75D35  C8352278
          derivedKey:  A8253CEE  D9AC042C  54F75D35  C8352278
        gIntermediateDerivationKeyRegister[  0  ] <-   A8253CEE  D9AC042C  54F75D35
C8352278
     gIntermediateDerivationKeyRegister[  1  ] <-  0  )
     gCounter <-  7

PIN Encryption Key:                 02DCC6CD  1201A3A2  CA709955  9C862123

Counter:   7     (  0x7  )
Generate_Working_Keys(sessionKeyUsage =  KeyUsage._PINEncryption  sessionKeyType =
KeyType._AES128  )
  Set_Shift_Register -> gShiftRegister:  1  gCurrentKey:  0
  gCounter:  7
  derivationData:  01011000  00020080  90123456  00000007
    Derive_Key(derivationKey =  A8253CEE  D9AC042C  54F75D35  C8352278  keyType =
KeyType._AES128  derivationData =  01011000  00020080  90123456  00000007  deriveType
=  KeyType._AES128  )
       AES_Encrypt_ECB(key =  A8253CEE  D9AC042C  54F75D35  C8352278  data =  01011000
00020080  90123456  00000007  )
        result =   6ECF912F  3B18CA11  A7A27BB6  0705FD09
     derivedKey:  6ECF912F  3B18CA11  A7A27BB6  0705FD09
  sessionKey:  6ECF912F  3B18CA11  A7A27BB6  0705FD09
    Update_State_for_next_Transaction()
       Update_Derivation_Keys(deriveKeyType =  KeyType._AES128  )
        gCurrentKey:  0
        baseKey:  A8253CEE  D9AC042C  54F75D35  C8352278
        i:  0  gShiftRegister:  1
        derivationData:  01018000  00020080  90123456  00000007
        Derive_Key(derivationKey =  A8253CEE  D9AC042C  54F75D35  C8352278  keyType =
KeyType._AES128  derivationData =  01018000  00020080  90123456  00000007  deriveType
=  KeyType._AES128  )
           AES_Encrypt_ECB(key =  A8253CEE  D9AC042C  54F75D35  C8352278  data =
01018000  00020080  90123456  00000007  )
             result =   34E30CEB  DE41AE72  8F736F1A  07DDE77A
```

```
          derivedKey:  34E30CEB  DE41AE72  8F736F1A  07DDE77A
        gIntermediateDerivationKeyRegister[  0  ] <-  34E30CEB  DE41AE72  8F736F1A
07DDE77A
     gIntermediateDerivationKeyRegister[  0  ] <-  0  )
     gCounter <-  8

PIN Encryption Key:                6ECF912F  3B18CA11  A7A27BB6  0705FD09

Counter:  8    (  0x8  )
Generate_Working_Keys(sessionKeyUsage =  KeyUsage._PINEncryption  sessionKeyType =
KeyType._AES128  )
  Set_Shift_Register -> gShiftRegister:  8  gCurrentKey:  3
  gCounter:  8
  derivationData:  01011000  00020080  90123456  00000008
    Derive_Key(derivationKey =  718EE6CF  0B27E53D  5F7AF99C  4D8146A2  keyType =
KeyType._AES128  derivationData =  01011000  00020080  90123456  00000008  deriveType
=  KeyType._AES128  )
       AES_Encrypt_ECB(key =  718EE6CF  0B27E53D  5F7AF99C  4D8146A2  data =  01011000
00020080  90123456  00000008  )
        result =  4D9DF3FB  EE3448FC  3E676D04  320A90F5
     derivedKey:  4D9DF3FB  EE3448FC  3E676D04  320A90F5
  sessionKey:  4D9DF3FB  EE3448FC  3E676D04  320A90F5
    Update_State_for_next_Transaction()
       Update_Derivation_Keys(deriveKeyType =  KeyType._AES128  )
         gCurrentKey:  3
         baseKey:  718EE6CF  0B27E53D  5F7AF99C  4D8146A2
         i:  3  gShiftRegister:  8
         derivationData:  01018000  00020080  90123456  00000008
         Derive_Key(derivationKey =  718EE6CF  0B27E53D  5F7AF99C  4D8146A2  keyType =
KeyType._AES128  derivationData =  01018000  00020080  90123456  00000008  deriveType
=  KeyType._AES128  )
            AES_Encrypt_ECB(key =  718EE6CF  0B27E53D  5F7AF99C  4D8146A2  data =
01018000  00020080  90123456  00000008  )
              result =  FFBF6177  C5B969E2  73B8529F  C1D5C117
           derivedKey:  FFBF6177  C5B969E2  73B8529F  C1D5C117
         gIntermediateDerivationKeyRegister[  3  ] <-  FFBF6177  C5B969E2  73B8529F
C1D5C117
         i:  2  gShiftRegister:  4
         derivationData:  01018000  00020080  90123456  0000000C
         Derive_Key(derivationKey =  718EE6CF  0B27E53D  5F7AF99C  4D8146A2  keyType =
KeyType._AES128  derivationData =  01018000  00020080  90123456  0000000C  deriveType
=  KeyType._AES128  )
            AES_Encrypt_ECB(key =  718EE6CF  0B27E53D  5F7AF99C  4D8146A2  data =
01018000  00020080  90123456  0000000C  )
              result =  6AAF97F3  576E0698  9D85C22E  42EFE35B
           derivedKey:  6AAF97F3  576E0698  9D85C22E  42EFE35B
         gIntermediateDerivationKeyRegister[  2  ] <-  6AAF97F3  576E0698  9D85C22E
42EFE35B
         i:  1  gShiftRegister:  2
         derivationData:  01018000  00020080  90123456  0000000A
         Derive_Key(derivationKey =  718EE6CF  0B27E53D  5F7AF99C  4D8146A2  keyType =
KeyType._AES128  derivationData =  01018000  00020080  90123456  0000000A  deriveType
=  KeyType._AES128  )
            AES_Encrypt_ECB(key =  718EE6CF  0B27E53D  5F7AF99C  4D8146A2  data =
01018000  00020080  90123456  0000000A  )
```

```
            result =  D4601366  796D6B3F  054A668A  B9C62188
         derivedKey:  D4601366  796D6B3F  054A668A  B9C62188
        gIntermediateDerivationKeyRegister[  1  ] <-  D4601366  796D6B3F  054A668A
B9C62188
        i:  0  gShiftRegister:  1
        derivationData:  01018000  00020080  90123456  00000009
        Derive_Key(derivationKey =  718EE6CF  0B27E53D  5F7AF99C  4D8146A2  keyType =
KeyType._AES128  derivationData =  01018000  00020080  90123456  00000009  deriveType
=  KeyType._AES128  )
          AES_Encrypt_ECB(key =  718EE6CF  0B27E53D  5F7AF99C  4D8146A2  data =
01018000  00020080  90123456  00000009  )
            result =  DF5B4FCF  D90DA7BB  35C15102  3B43E41E
         derivedKey:  DF5B4FCF  D90DA7BB  35C15102  3B43E41E
        gIntermediateDerivationKeyRegister[  0  ] <-  DF5B4FCF  D90DA7BB  35C15102
3B43E41E
     gIntermediateDerivationKeyRegister[  3  ] <-  0  )
     gCounter <-  9

PIN Encryption Key:               4D9DF3FB  EE3448FC  3E676D04  320A90F5
```