Protected command APDU:

CLA	INS	P1	P2	Lc	Command Data Field	Le
'0C'	'A4'	'02'	'0C'	'15'	cmd_data	'00'

Document SIC:

2. Set EF.COM as the currently selected file and send affirmative response to IS:

Unprotected response APDU:

SW1	SW2
'90'	'00'

a) Build DO'99':
DO99 = '99029000'

b) Compute "Retail MAC" of DO99 with KS_{mac}:
- Increment SSC:
SSC = '887022120C06C228'
- Concatenate SSC and DO99:
N = '887022120C06C22899029000'
- Compute MAC:
CC = 'FA855A5D4C50A8ED'

c) Build DO'8E':
DO8E = '8E08FA855A5D4C50A8ED'

d) Construct response data:
resp_data = '990290008E08FA855A5D4C50A8ED'

Protected response APDU:

Response Data Field	SW1	SW2
resp_data	'90'	'00'

IS:

3. READ BINARY of the first 4 bytes:

Unprotected command APDU:

CLA	INS	P1	P2	Le
'0C'	'B0'	'00'	'00'	'04'

a) Mask class byte and pad command header:
cmd_header = '0CB0000080000000'

b) Build DO '97':
DO97 = '970104'

c) Concatenate cmd_header and DO97:
M = '0CB000008000000970104'

d) Compute “Retail MAC” of M with KS_{mac}:
- Increment SSC:
  SSC = ‘887022120C06C229’
- Concatenate SSC and M:
  N = ‘887022120C06C2290CB0000080000000
  970104’
- Compute MAC:
  CC = ‘ED6705417E96BA55’

e) Build DO‘8E’:
DO8E = ‘8E08ED6705417E96BA55’

f) Construct command data:
cmd_data = ‘9701048E08ED6705417E96BA55’

Protected command APDU:

CLA	INS	P1	P2	Lc	Command Data Field	Le
‘0C’	‘B0’	‘00’	‘00’	‘0D’	cmd_data	‘00’

Document SIC:

4. Return 4 bytes of EF.COM starting at offset 0:

data = ‘600D5F01’

Unprotected response APDU:

Response Data Field	SW1 SW2
data	‘90’ ‘00’

a) Pad data:
p_data = ‘600D5F0180000000’

b) Encrypt p_data using TDEA with KS_{enc}:
enc_data = ‘F9435D056E27C52E’

c) Build DO‘87’:
DO87 = ‘870901F9435D056E27C52E’

d) Build DO‘99’:
DO99 = ‘99029000’

e) Concatenate DO‘87’ and DO‘99’:
M = ‘870901F9435D056E27C52E99029000’

f) Compute “Retail MAC” of M with KS_{mac}:
- Increment SSC:
  SSC = ‘887022120C06C22A’
- Concatenate SSC and M:
  N = ‘887022120C06C22A870901F9435D056E
  27C52E99029000’
- Compute MAC:
  CC = ‘0C15238078E0A4C9’

g) Build DO‘8E’:
DO8E = ‘8E080C15238078E0A4C9’

h) Construct response data:
resp_data = '870901F9435D056E27C52E990290008E
080C15238078E0A4C9'

Protected response APDU:

Response Data Field	SW1 SW2
resp_data	'90' '00'

IS:

5. READ BINARY of the remaining 11 bytes:

Unprotected command APDU:

CLA	INS	P1	P2	Le
'0C'	'B0'	'00'	'04'	'0B'

a) Mask class byte and pad command header:
cmd_header = '0CB0000480000000'

b) Build DO '97':
DO97 = '97010B'

c) Concatenate cmd_header and DO97:
M = '0CB000048000000097010B'

d) Compute "Retail MAC" of M with KS_{mac}:
- Increment SSC:
SSC = '887022120C06C22B'
- Concatenate SSC and M:
N = '887022120C06C22B0CB0000480000000
97010B'
- Compute MAC:
CC = '40900A27C4C390D6'

e) Build DO'8E':
DO8E = '8E0840900A27C4C390D6'

f) Construct command data:
cmd_data = '97010B8E0840900A27C4C390D6'

Protected command APDU:

CLA	INS	P1	P2	Lc	Command Data Field	Le
'0C'	'B0'	'00'	'04'	'0D'	cmd_data	'00'

Document SIC:

6. Return 11 bytes of EF.COM starting at offset 4:

data = '04303130305C04616B6567'

Unprotected response APDU:

Response Data Field	SW1 SW2
data	‘90’ ‘00’

a) Pad data:
p_data = ‘04303130305C04616B65678000000000’

b) Encrypt p_data using TDEA with KS_{enc}:
enc_data = ‘B3CD0334417393661AA9B39206EC89CC’

c) Build DO‘87’:
DO87 = ‘871101B3CD0334417393661AA9B39206
EC89CC’

d) Build DO‘99’:
DO99 = ‘99029000’

e) Concatenate DO‘87’ and DO‘99’:
M = ‘871101B3CD0334417393661AA9B39206
EC89CC99029000’

f) Compute “Retail MAC” of M with KS_{mac}:
- Increment SSC:
SSC = ‘887022120C06C22C’
- Concatenate SSC and M:
N = ‘887022120C06C22C871101B3CD033441
7393661AA9B39206EC89CC99029000’
- Compute MAC:
CC = ‘0747E8CEC180EB48’

g) Build DO‘8E’:
DO8E = ‘8E080747E8CEC180EB48’

h) Construct response data:
resp_data = ‘871101B3CD0334417393661AA9B39206
EC89CC990290008E080747E8CEC180EB
48’

Protected response APDU:

Response Data Field	SW1 SW2
resp_data	‘90’ ‘00’

B.10.2 Example Using Configuration 2

Static document keying material:
K_{doc} = ‘55CA83CC52EC6454DE7AFB1D3DA66F4E’

Compute Basic Access Keys

Input: K_{seed} = K_{doc}

Encryption Key (K_{enc}) computation

1. Concatenate K_{seed} and c (c = 1):
   D = '55CA83CC52EC6454DE7AFB1D3DA66F4E
   00000001'

2. Calculate the hash of D:
   $H_{SHA-1}(D)$ = 'EF8E4DCE3D33E8C6E690509A7DA5186C
   C35B94BF'

3. Form key:
   K_{enc} = 'EF8E4DCE3D33E8C6E690509A7DA5186C'

Message Authentication Key (K_{mac}) computation

4. Concatenate K_{seed} and c (c = 2):
   D = '55CA83CC52EC6454DE7AFB1D3DA66F4E
   00000002'

5. Calculate the hash of D:
   $H_{SHA-1}(D)$ = '94B140FB3E4B557CCC3A225E794C077B
   14518E58'

6. Form key:
   K_{mac} = '94B140FB3E4B557CCC3A225E794C077B'

Authentication and Establishment of Session Keys:

IS

1. Request an 8 byte random challenge from the document's SIC:

   Command APDU:

CLA	INS	P1	P2	Le
'00'	'84'	'00'	'00'	'08'

Document SIC:

2. Generate random challenge and return it to IS:
   RND.ICC = 'E72450C17A59DF40'

   Response APDU:

Response Data Field	SW1 SW2
RND.ICC	'90' '00'

IS:

3. Generate an 8-byte random challenge and 16-byte random keying material:
   RND.IFD = '41C51B949D4FD786'
   K.IFD = '766F9E2B2B503AFBEB420BED8D1A73A8'

4. Concatenate RND.IFD, RND.ICC and K.IFD:
   S = '41C51B949D4FD786E72450C17A59DF40
   766F9E2B2B503AFBEB420BED8D1A73A8'

5. Encrypt S using AES with key K_{enc}:
   E_IFD = '80AEE3D8F601067546C4512979F1344E
   F62E0045A94BD21A97E9AE2FE578AAB0'

6. Compute CMAC over E_IFD with key K_{mac}:
M_IFD = '320F4C5677E3618A'

7. Construct command data for MUTUAL AUTHENTICATE and send command to the document's SIC:
cmd_data = '80AEE3D8F601067546C4512979F1344E
F62E0045A94BD21A97E9AE2FE578AAB0
320F4C5677E3618A'

Command APDU:

CLA	INS	P1	P2	Lc	Command Data Field	Le
'00'	'84'	'00'	'00'	'28'	cmd_data	'28'

Document SIC:

8. Generate 16-byte random keying material:
K.ICC = 'C1655F49E136D12B8522B1C99510E71B'

9. Calculate XOR of K.IFD and K.ICC:
K_{seed} = 'B70AC162CA66EBD06E60BA24180A94B3'

10. Derive session keys:
KS_{enc} = 'AB9497F5819AB69A25A7798789061CF8'
KS_{mac} = '1FBF06A0DE775C473D64B5E9933290D3'

11. Initialize send sequence counter:
SSC = '7A59DF409D4FD786'

12. Concatenate RND.ICC, RND.IFD and K.ICC:
R = 'E72450C17A59DF4041C51B949D4FD786
C1655F49E136D12B8522B1C99510E71B'

13. Encrypt R using AES with key K_{enc}:
E_ICC = '649E3A8F8D48E22ADB7AAE09FE17BA43
377D9CAF94EFBD7BAF9707088DF6489F'

14. Compute CMAC over E_ICC with key K_{mac}:
M_ICC = '1CCE566F1FE43D65'

15. Construct response data and send response APDU to the IS:
resp_data = '649E3A8F8D48E22ADB7AAE09FE17BA43
377D9CAF94EFBD7BAF9707088DF6489F
1CCE566F1FE43D65'

Response APDU:

Response Data Field	SW1	SW2
resp_data	'90'	'00'

IS:

16. Calculate XOR of K.IFD and K.ICC:
K_{seed} = 'B70AC162CA66EBD06E60BA24180A94B3'

17. Derive session keys:
KS_{enc} = ‘AB9497F5819AB69A25A7798789061CF8’
KS_{mac} = ‘1FBF06A0DE775C473D64B5E9933290D3’

18. Initialize send sequence counter:
SSC = ‘7A59DF409D4FD786’

Secure Messaging:

IS:

1. SELECT EF.COM (file identifier = ’01 1E’):

Unprotected command APDU:

CLA	INS	P1	P2	Lc	Command Data Field
‘00’	‘A4’	‘02’	‘00’	‘02’	’01 1E’

a) Mask class byte and pad command header:
cmd_header = ‘0CA4020C800000000000000000000000’

b) Pad data:
p_data = ‘011E800000000000000000000000000’

c) Encrypt p_data using AES with KS_{enc}:
enc_data = ‘4FF75761BC5C1ECE82AE43F70938D50F’

d) Build DO‘87’:
DO87 = ‘8711014FF75761BC5C1ECE82AE43F709
38D50F’

e) Concatenate cmd_header and DO87:
M = ‘0CA4020C800000000000000000000000
8711014FF75761BC5C1ECE82AE43F709
38D50F’

f) Compute CMAC of M with KS_{mac}:
- Increment SSC:
SSC = ‘7A59DF409D4FD787’
- Concatenate padded SSC and M:
N = ‘0000000000000007A59DF409D4FD787
0CA4020C800000000000000000000000
8711014FF75761BC5C1ECE82AE43F709
38D50F’
- Compute MAC:
CC = ‘6204A7709D0E128B’

g) Build DO‘8E’:
DO8E = ‘8E082CF23B10E4D30044’

h) Construct command data:
cmd_data = ‘8711014FF75761BC5C1ECE82AE43F709
38D50F8E086204A7709D0E128B’

Protected command APDU:

CLA	INS	P1	P2	Lc	Command Data Field	Le
'0C'	'A4'	'02'	'0C'	'1D'	cmd_data	'00'

Document SIC:

2. Set EF.COM as the currently selected file and send affirmative response to IS:

Unprotected response APDU:

SW1	SW2
'90'	'00'

a) Build DO'99':
DO99 = 'xx99029000'

b) Compute CMAC of DO99 with KS_{mac}:
- Increment SSC:
SSC = 'xx7A59DF409D4FD788'
- Concatenate padded SSC and DO99:
N = 'xx00000000000000007A59DF409D4FD788
99029000'
- Compute MAC:
CC = 'xx2CF23B10E4D30044'

c) Build DO'8E':
DO8E = 'xx8E082CF23B10E4D30044'

d) Construct response data:
resp_data = 'xx990290008E082CF23B10E4D30044'

Protected response APDU:

Response Data Field	SW1	SW2
resp_data	'90'	'00'

IS:

3. READ BINARY of the first 4 bytes:

Unprotected command APDU:

CLA	INS	P1	P2	Le
'0C'	'B0'	'00'	'00'	'04'

a) Mask class byte and pad command header:
cmd_header = 'xx0CB000008000000000000000000000000'

b) Build DO '97':
DO97 = 'xx970104'

c) Concatenate cmd_header and DO97:
M = 'xx0CB000008000000000000000000000000
970104'

d) Compute CMAC of M with KS_{mac}:
- Increment SSC:
  SSC = '7A59DF409D4FD789'
- Concatenate padded SSC and M:
  N = '00000000000000007A59DF409D4FD789
  0CB000008000000000000000000000000
  970104'
- Compute MAC:
  CC = '3BEE3045A87E2A15'

e) Build DO'8E':
DO8E = '8E083BEE3045A87E2A15'

f) Construct command data:
cmd_data = '9701048E083BEE3045A87E2A15'

Protected command APDU:

CLA	INS	P1	P2	Lc	Command Data Field	Le
'0C'	'B0'	'00'	'00'	'0D'	cmd_data	'00'

Document SIC

4. Return 4 bytes of EF.COM starting at offset 0:

data = '600D5F01'

Unprotected response APDU:

Response Data Field	SW1 SW2
data	'90' '00'

a) Pad data:
p_data = '600D5F0180000000000000000000000'

b) Encrypt p_data using AES with KS_{enc}:
enc_data = 'D60D14976646FB2304A0155F6BC6E42D'

c) Build DO'87':
DO87 = '871101D60D14976646FB2304A0155F6B
C6E42D'

d) Build DO'99':
DO99 = '99029000'

e) Concatenate DO'87' and DO'99':
M = '871101D60D14976646FB2304A0155F6B
C6E42D99029000'

f) Compute CMAC of M with KS_{mac}:
- Increment SSC:
  SSC = '7A59DF409D4FD78A'
- Concatenate padded SSC and M:
  N = '0000000000000007A59DF409D4FD78A
  871101D60D14976646FB2304A0155F6B
  C6E42D99029000'
- Compute MAC:
  CC = 'D2165D993B20F73B'

g) Build DO'8E':
DO8E = '8E08D2165D993B20F73B'

h) Construct response data:
resp_data = '871101D60D14976646FB2304A0155F6B
C6E42D990290008E08D2165D993B20F7
3B'

Protected response APDU:

Response Data Field	SW1	SW2
resp_data	'90'	'00'

IS:

4. READ BINARY of the remaining 11 bytes:

Unprotected command APDU:

CLA	INS	P1	P2	Le
'0C'	'B0'	'00'	'04'	'0B'

a) Mask class byte and pad command header:
cmd_header = '0CB000048000000000000000000000000'

b) Build DO '97':
DO97 = '97010B'

c) Concatenate cmd_header and DO97:
M = '0CB000048000000000000000000000000
97010B'

d) Compute CMAC of M with KS_{mac}:
- Increment SSC:
  SSC = '7A59DF409D4FD78B'
- Concatenate padded SSC and M:
  N = '0000000000000007A59DF409D4FD78B
  0CB000048000000000000000000000000
  97010B'
- Compute MAC:
  CC = '36F9817F84E009C8'

e) Build DO'8E':
DO8E = '8E0836F9817F84E009C8'

f) Construct command data:
cmd_data = '97010B8E0836F9817F84E009C8'

Protected command APDU:

CLA	INS	P1	P2	Lc	Command Data Field	Le
‘0C’	‘B0’	‘00’	‘04’	‘0D’	cmd_data	‘00’

Document SIC:

4. Return 11 bytes of EF.COM starting at offset 4:

data = ‘04303130305C04616B6567’

Unprotected response APDU:

Response Data Field	SW1 SW2
data	‘90’ ‘00’

a) Pad data:
p_data = ‘04303130305C04616B65678000000000’

b) Encrypt p_data using AES with KS_{enc}:
enc_data = ‘36B83A1FBAC98D89DDDA2235AD29A8BB’

c) Build DO‘87’:
DO87 = ‘87110136B83A1FBAC98D89DDDA2235AD
29A8BB’

d) Build DO‘99’:
DO99 = ‘99029000’

e) Concatenate DO‘87’ and DO‘99’:
M = ‘87110136B83A1FBAC98D89DDDA2235AD
29A8BB99029000’

f) Compute CMAC of M with KS_{mac}:
- Increment SSC:
SSC = ‘7A59DF409D4FD78C’
- Concatenate padded SSC and M:
N = ‘00000000000000007A59DF409D4FD78C87110136B83A1FBA
C98D89DDDA2235AD29A8BB99029000’
- Compute MAC:
CC = ‘C9338D9966514BBB’

g) Build DO‘8E’:
DO8E = ‘8E08C9338D9966514BBB’

h) Construct response data:
resp_data = ‘87110136B83A1FBAC98D89DDDA2235AD
29A8BB990290008E08C9338D9966514B
BB’

Protected response APDU:

Response Data Field	SW1 SW2
resp_data	‘90’ ‘00’