**1-      Translate a PIN from BDK to BDK or ZPK Encryption (3DES & AES DUKPT) – Host Command ‘G0’**

AES256 BDK-1: S10128B0AN00E00018EF09BD77B7CCBEAFD5E0A9AFFD54F4539D2005B06C10DE6D4A8B2D28A7D50A6B3C389EAFB1C769CD1B45559E478E1A0B79E09BC369B232E

Double DES ZPK: S1009672TN00E0001FC64B8587BA23D080F26ABE15F00DBEF2F0958A0FE8BC6A192C0A5A755E46D2873E9557A0C8FF75C

AES256 ZPK: S1012872AN00E00012F7D60079CEE441216C3FE226F4088EE2D2CD6FECF7FFB2D4A229D1DF48DE4122CD7DD2291879449CD7ABC21A729F0234181C86AECD5EDDF

AES PIN BLOCK: 02CA705E8DDB047E1DC15C501796B280 (Clear PIN: 6500, PAN: 4543601234567882)

a.       We would like to translate a pin block from ISO 9564-1 Format 4 PIN Block(AES PIN Block) to ISO 9564-1 Format 0. Source PIN Block encrypted under DUKPT PIN Encryption Key which is derived from BDK-1 using “KSN” and “Transaction Counter”. Destination key type is ZPK and it is “'T2' – double length DES key”. But we are getting an error as described below:

                                                               i.      REQ: G0 S10128B0AN00E00018EF09BD77B7CCBEAFD5E0A9AFFD54F4539D2005B06C10DE6D4A8B2D28A7D50A6B3C389EAFB1C769CD1B45559E478E1A0B79E09BC369B232E S1009672TN00E0001FC64B8587BA23D080F26ABE15F00DBEF2F0958A0FE8BC6A192C0A5A755E46D2873E9557A0C8FF75C 000 FFFF12345601234400000001 02CA705E8DDB047E1DC15C501796B280 48 01 4543601234567882 ;

                                                             ii.      RSP: 15 (Invalid input data (invalid format, invalid characters, or not enough data provided))

b.      We successfully translate by sending 2 additional host commands. But we would like to achieve this with one command as we have explained in item 1.a. Here are the steps how we can do it: First step, we translate the PIN Block to AES ZPK with same PIN Block format. Second step, we translate the PIN Block from ISO 9564-1 Format 4 PIN Block to ISO 9564-1 Format 1 PIN Block which is encrypted under double length DES ZPK. Third and final step, using the same double length DES ZPK for both source and destination key, we translate the PIN Block from ISO 9564-1 Format 1 PIN to ISO 9564-1 Format 0.

                                                               i.      First step REQ: G0 S10128B0AN00E00018EF09BD77B7CCBEAFD5E0A9AFFD54F4539D2005B06C10DE6D4A8B2D28A7D50A6B3C389EAFB1C769CD1B45559E478E1A0B79E09BC369B232E S1012872AN00E00012F7D60079CEE441216C3FE226F4088EE2D2CD6FECF7FFB2D4A229D1DF48DE4122CD7DD2291879449CD7ABC21A729F0234181C86AECD5EDDF 000 FFFF12345601234400000001 02CA705E8DDB047E1DC15C501796B280 48 48 4543601234567882 ;

                                                             ii.      First step RSP: 04 BA5CCFE6B134F3E946CA1018E76BF06D 48

                                                            iii.      Second step REQ: CC S1012872AN00E00012F7D60079CEE441216C3FE226F4088EE2D2CD6FECF7FFB2D4A229D1DF48DE4122CD7DD2291879449CD7ABC21A729F0234181C86AECD5EDDF S1009672TN00E0001FC64B8587BA23D080F26ABE15F00DBEF2F0958A0FE8BC6A192C0A5A755E46D2873E9557A0C8FF75C 12 BA5CCFE6B134F3E946CA1018E76BF06D 48 05 4543601234567882 ;

                                                           iv.      Second step RSP: 04 D205557E56B99D82 05

                                                             v.      Third and final step REQ: CC S1009672TN00E0001FC64B8587BA23D080F26ABE15F00DBEF2F0958A0FE8BC6A192C0A5A755E46D2873E9557A0C8FF75C S1009672TN00E0001FC64B8587BA23D080F26ABE15F00DBEF2F0958A0FE8BC6A192C0A5A755E46D2873E9557A0C8FF75C 12 D205557E56B99D82 05 01 360123456788

                                                           vi.      Third and final step RSP: 04 B34A29C70FADE002 01 (PIN value is 6500 and verified)

c.       Another strange behavior is, when we try to translate the PIN Block from ISO 9564-1 Format 4 PIN Block to ISO 9564-1 Format 0 as explained in “Second step” with one modification, the command is executed successfully but the format of PIN block becomes invalid:

                                                               i.      REQ: CC S1012872AN00E00012F7D60079CEE441216C3FE226F4088EE2D2CD6FECF7FFB2D4A229D1DF48DE4122CD7DD2291879449CD7ABC21A729F0234181C86AECD5EDDF S1009672TN00E0001FC64B8587BA23D080F26ABE15F00DBEF2F0958A0FE8BC6A192C0A5A755E46D2873E9557A0C8FF75C 12 BA5CCFE6B134F3E946CA1018E76BF06D 48 01 4543601234567882 ;

                                                             ii.      RSP: 04 7A09B6A7743D5D91 01 (Clear PIN Block is not correctly padded. PIN block: 046545BC9FEDCBA9, PAN: 4543601234567882)

**2-      Export Key under an RSA Public Key – Host Command ‘GK’**

[…] => stands for binary input

AES256 BDK-2: S1012841AN00S0001F3519C7B62DE6C0424EA6FE5A967990CAC7376DF876294AC8B2219A231C280132506C65EAB72ACA2B2626AB78078B649A6D7439727481A6D436F02

RSA Public Key in Thales Keyblock

RSA Public Key in DER encoding

a.       We would like to export a BDK-2 under an RSA Public Key. Hsm responses with an undefined error when we execute the below command:

                                                               i.     

                                                             ii.      RSP: D3 (D3 is not listed in “Error Codes” section. It is also not indicated in specific error codes for the response section.)

