When a card reader encrypts track data, the injected KSN is used to derive a session key.

1.0 OBTAIN KSN / EncryptedPIN:  
1.1 PYTHON TESTHARNESS



1.2 FDRC TRANSACTION LOG  
FD-Transaction-Log.PNG

THE FOLLOWING VALUES ARE USED FOR THIS EXAMPLE:

KSN: FFFF987654321F800EF0  
IV: 199E5B4D3BCD648F  
Encrypted Track Data: 58AE53EDB7A148B7961C847546E39309B471AE75FB53F2D3C4C2BC2D8DD39841

2.0 USING DUPKT IN BP-TOOLS

2.1 Select Payments -> DUKPT -> DUKPT (ISO 9797)

Enter the following in the ‘PEK derivation’ TAB:

BDK: 0123456789ABCDEFFEDCBA9876543210  
KSN: FFFF987654321F800EF0  
DATA: 58AE53EDB7A148B7961C847546E39309B471AE75FB53F2D3C4C2BC2D8DD39841

Obtain Derived PEK: 044A0CC2130D0581CDB3CF49ECCA9F88

A screenshot of a computer

Description automatically generated

Switch to ‘DUKPT DATA’ TAB and DECODE for DATA with ‘Data Variant’ selected

A screenshot of a computer

Description automatically generated

Obtain KEY: CF522535D4F7B6EBDFD7B00160ECD521

2.2 Switch to Cipher -> DES Window in BP-TOOLS

Update values for Key, Data, and IV to DECODE  
 A screenshot of a computer

Description automatically generated

Decoded data: 5A08222360008970001157112223600089700011D49122010123456789800000

2.3 Take Decoded DATA and use a TLV tool to represent it in a more readable format

<https://emvlab.org/tlvutils/>

A screenshot of a computer

Description automatically generated  
 A screenshot of a computer

Description automatically generated