20 October 2004

JOHAN DU TOIT control tests
NEDBANK

TEST 1: DES ECB 2 BLOCKS :
key: "_NEDBANK" = 5F4E454442414E4B
Data 1: = 5893270400461300 0000 (Padded to right with zero's)

eECBKey(Data1) = **9510AAF119958AB4 CE9CC1F6D5887109**

TEST 2: DES ECB 1 BLOCK
key: "_NEDBANK" = 5F4E454442414E4B
Data 2: = 3031323334353637

eECBKey(Data2) = **B9AB68CBAB048AB0**

TEST 3: DES CBC 2 BLOCKS :
key: "_NEDBANK" = 5F4E454442414E4B
IV: = 0000000000000000
Data 1: = 5893270400461300 0000 (Padded to right with zero's)

eCBCKey(Data) = **9510AAF119958AB4** ???????????????? (Second block not generated – no tool for this)

TEST 4: DES CBC 1 BLOCKS :
key: "_NEDBANK" = 5F4E454442414E4B
IV: = 0000000000000000
Data 2: = 3031323334353637

eCBCKey(Data2) = **B9AB68CBAB048AB0**

PETER ZUUR
XLINK Test results:

ECB?

DES ECB MODE

KEY _NEDBANK

Key set to _NEDBANK ...

TEST 1: DES ECB 2 BLOCKS :

encr \x58\x93\x27\x04\x00\x46\x13\x00\x00\x00

Result: = 0x**9510AAF119958AB4 CE9CC1F6D5887109**

ENCR 01234567

TEST 2: DES ECB 1 BLOCK :

Result: = **0xB9AB68CBAB048AB0**

iv?

IV=0x0000000000000000

ecb off

ecb?

DES CBC MODE

TEST 3: DES CBC 2 BLOCKS :

encr \x58\x93\x27\x04\x00\x46\x13\x00\x00\x00

Result: = 0x**9510AAF119958AB4** E0D843714D0FBE9C (Second block not verified – Nedcor does not have a test tool)

TEST 4: DES CBC 1 BLOCK :

ENCR 01234567

Result: = **0xB9AB68CBAB048AB0**

Summary:

All 4 tests performed were successfully verified against expected DEC ECB and CBC results.

The tests did not include any Key management or TRSM (Tamper Resistant Security Module) verification and thus no comments are expressed on these issues.

J. du Toit
Information Security Date: / /2004

Signature:

Peter Zuur
XLink Date: / /2004

Signature: