README

NATIVE AND NON-NATIVE LIBRARIES THAT PROVIDE AES ENCRYPTION

PAK ARCHIVES
============
2 PAK archives are provided:

1. pkaesr(AES for TNS/R system)
   - aestalb(TAL build file)
   - aesptalb(PTAL build file)
   - aesh(source library file)
   - aese(external function declaration file TAL/PTAL)
   - aes(TNS C library)
   - aesnrp(TNS/R C library that can be used from PTAL application - MAIN function in the library)
   - aesnr(TNS/R C library)
   - aestals(source for simple TAL application using aes library)
   - aestal(simple TAL application binded together with aes library)
   - aesptals(source for simple PTAL application using aesnrp library)
   - aesptal(simple PTAL application binded together with aesnrp library)

2. pkaese(AES for TNS/E system)
   - aestalb(TAL build file)
   - aesptalb(PTAL build file)
   - aesh(source library file)
   - aese(external function declaration file TAL/PTAL)
   - aes(TNS C library)
   - aesnep(TNS/E C library that can be used from PTAL application - MAIN function in the library)
   - aesne(TNS/E C library)
   - aestals(source for simple TAL application using aes library)
   - aestal(simple TAL application binded together with aes library)
   - aesptals(source for simple PTAL application using aesnep library)
   - aesptal(simple PTAL application binded together with aesnep library)

LIBRARY INFO
============
1. AES library provides 128, 192 and 256 bit encryption

LIBRARY FUNCTION INFO
=====================
1. AES functions
   - aes_set_key(sets the required encryption/decryption key)
   - aes_encrypt(provides encryption on 16bytes data block - ECB)
   - aes_decrypt(provides decryption on 16bytes data block - ECB)
   - aes_cbc_encrypt(provides MACing encryption - CBC)
   - aes_cbc_decrypt(provides MACing decryption - CBC)
   - aes_self_test(AES self test using hard coded test vectors)

Note: Detail info about all functions is inside aesh source library file.

MEMORY DATA MODEL
=================
1. XMEM(large-memory model)
2. WIDE(wide data model)