RSA-OAEP Encryption Scheme

D. Intellectual property statement

September 28, 2000

The RSA public-key cryptosystem is protected by U.S. Patent #4,405,829, which is exclusively licensed to RSA Security Inc. by the Massachusetts Institute of Technology. The patent was due to expire on September 20, 2000. On September 6, 2000, RSA Security announced that, effective immediately, it would no longer enforce the patent. RSA Security does not claim ownership of any additional intellectual property needed to implement and practice the RSA public-key cryptosystem contained within U.S. Patent #4,405,829.

The submission describes the use of RSA with three or more primes, which is claimed in U.S. Patent #5,848,159. Such use is optional and is not required to implement the RSA-OAEP algorithm but may offer performance benefits.

As part of the process of developing the IEEE Std 1363-2000, information was requested from patent holders on a large number of algorithms. Assurances considered to meet the IEEE patent policy were obtained for the algorithms in the standard including RSA-OAEP. Further information may be obtained from the IEEE Standards Department; copies are also available from http://grouper.ieee.org/groups/1363.

RSA Security makes no other representations regarding intellectual property claims by other parties.

RSA Security hereby grants NESSIE the right to use the reference code included with this submission for its evaluation (including any evaluation conducted by outside researchers) free of charge. Other use (e.g., in commercial or non-commercial products) requires written permission from RSA Security.

RSA Security will update the NESSIE project if there are changes to the intellectual property position for this submission.