NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms

January 31, 2005

Sharon S. Keller

National Institute of Standards and Technology

Information Technology Laboratory

Computer Security Division

TABLE OF CONTENTS

1 Introduction

This document, the "NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms" specifies the NIST-recommended addition to the underlying document *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*, ANSI X9.31-1988, random number generator. It specifies how to use 3-Key Triple DES and AES as the core of the X9.31 RNG.

2 ANSI X9.31 Appendix A.2.4 Using 3-Key Triple DES

Let ede*X(Y) represent the DEA multiple encryption of Y under the key *X.
Let *K be 3-key Triple DES, 3 64 bit keys.

This *K is reserved only for the generation of pseudo random numbers.

Let V be a 64-bit seed value which is also kept secret, and XOR be the exclusive-or operator. Let DT be a date/time vector which is updated on each iteration. I is an intermediate value. A vector R is generated as follows (Note for Triple DES implementations: DT, I and R are 64-bits each.):

I = ede *K(DT)
R = ede *K(I XOR V) and a new V is generated by V = ede*K(R Xor I).

3 ANSI X9.31 Appendix A.2.4 Using AES

Let ede*X(Y) represent the AES encryption of Y under the key *X.
For AES 128-bit key, let *K be a 128 bit key.
For AES 192-bit key, let *K be a 192 bit key.
For AES 256-bit key, let *K be a 256 bit key.

This *K is reserved only for the generation of pseudo random numbers.

Let V be a 128-bit seed value which is also kept secret, and XOR be the exclusive-or operator. Let DT be a date/time vector which is updated on each iteration. I is a intermediate value. A vector R is generated as follows (Note for AES implementations DT, I, and R are 128-bits each.):

I = ede *K(DT)
R = ede *K(I XOR V) and a new V is generated by V = ede*K(R Xor I).

Appendix A References

[1] *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*, ANSI X9.31-1988, September 1998.