

# Rng

How does Swivel Core generate security strings?.

Swivel uses the Java Secure Random number generator for all random numbers within PINsafe.

This class provides a cryptographically strong random number generator (RNG). .....

"A cryptographically strong random number minimally complies with the statistical random number generator tests specified in FIPS 140-2, Security Requirements for Cryptographic Modules, section 4.9.1. Additionally, SecureRandom must produce non-deterministic output and therefore it is required that the seed material be unpredictable and that output of SecureRandom be cryptographically strong sequences as described in RFC 1750: Randomness Recommendations for Security."

This is from the Sun JAVA website <http://java.sun.com/javase/6/docs/api/java/security/SecureRandom.html>