### How it works

The Entropy Key collects random data by using two P-N semiconductor junctions and an effect called Avalanche Noise.  This essentially means it measures the unpredictable timing of electrons quantum-tunnelling through the junction.

These two junctions are attached to a CPU which samples them at high frequency, forming two streams of bits which are analysed using Üli Maurer's universal test for random bit generators both individually, and XORed together.  This gives us a conservative estimate of how random they are, as well as letting the device detect generator failure or correlation.

The device then debiases the streams using von Neumann, producing two streams of bits each approximately half and half ones and zeros. These streams are then again analysed to estimate their entropy, before being fed into a cryptographic hash. A count of the entropy estimated to have been added is maintained.  Once this value is at least 150% of the output side of the hash, it is finalised and added to an output queue.

Once 20000 bits have been collected, the block is subjected, as a whole, to the randomness tests stipulated by FIPS 140-2.  As perfectly random data can fail this test, the device only locks itself out if a statistically significant number of failures have been detected over time. The output blocks are then split into 32 byte packets and encrypted and MACed using a session key that is routinely recalculated using a shared secret between host and key.  As a result, each 256 bit block of data sent to the host was formed from around 3840 bits read from the quantum effect generators.

The host driver software either injects the data directly into the OS's own random pool where support exists, or makes the entropy available to other programs using a well-understood and supported protocol, popularised by a program called EGD.

The Entropy Key can also automatically detect some physical attacks, such as temperature and voltage changes and opening of the case (as the product is injected with epoxy; opening the case will destroy it).

http://www.entropykey.co.uk/   ekey@simtec.co.uk

SIMTEC
ELECTRONICS

# Entropy Key

# Quick Start Guide

The Entropy Key is a small, unobtrusive and easily installed USB device that generates high-quality random numbers, or entropy, which can improve the performance, security and reliability of servers, desktops and laptops. It can also be used with scientific, gambling and lottery applications, or anywhere where good random numbers are needed.

The Entropy Key contains two high-quality quantum noise sources, and an ARM Cortex CPU that actively measures and checks all generated random numbers, before encrypting them and sending them to the server. It also actively detects attempts to corrupt or sway the device. It aims towards FIPS 140-2 Level 2 compliance with some elements of levels 3 and 4, including tamper-evidence, tamper-proofing, role-based authentication, and detection of environmental attacks. If it detects that either of its two generators has failed, may be about to fail, or if it detects a physical or environmental attack, it will automatically shut down.

The Entropy Key generates a continuous stream of very high-quality random numbers, ready to be mixed into the entropy already collected by your computer. This means that when your computer requires random numbers, which is usually for very security-sensitive tasks such as certificate and key creation, administration, VPN access, and even customer-facing web requests, the random numbers used to secure them will be even stronger.