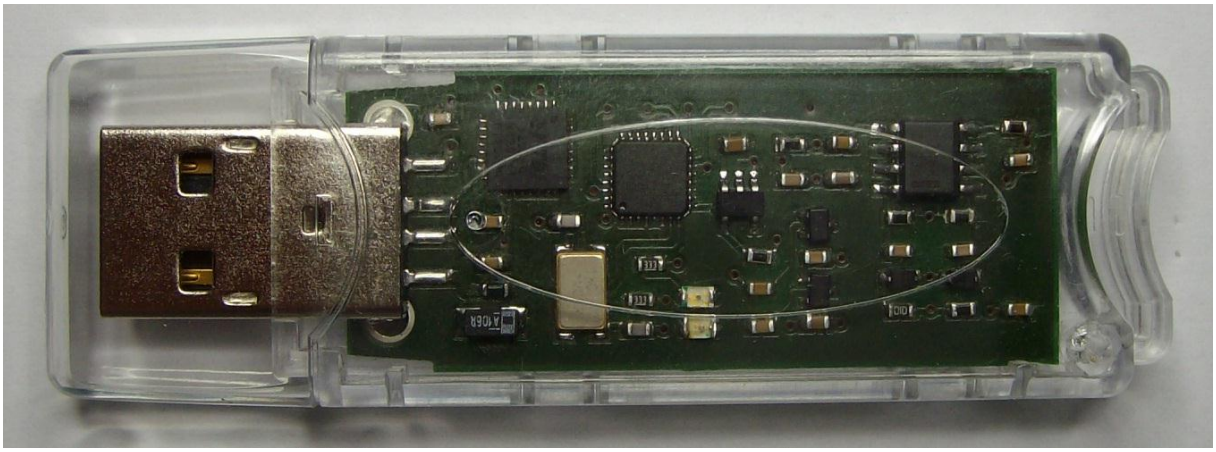
Physikalischer Zufallszahlen Generator

PRG320-4

USB1.1-Interface

Permanente Generierung von Zufallszahlen der Klasse PTG.3

- Kontinuierliche Generierung kryptografisch sicherer Zufallszahlen
- Thermisches Rauschen mit hoher Entropie als Zufallsquelle
- Kryptografisch sichere Zufallszahlen auch im erweiterten Temperaturbereich
- Permanente statistische Online-Kontrolle (P2-Generator nach AIS31)
- Permanente Überwachung der Rauschquelle
- Erfüllt alle Kriterien nach AIS31, NIST und Diehard
- Garantierte konstante Qualität durch automatischen Selbstabgleich
- Für den internen Einsatz in Embedded Systeme und PCs



Mit dem PRG320 steht ein professioneller Zufallsgenerator der Klasse PTG.3 (hybrider Zufallsgenerator) für die permanente Generierung von kryptografisch sicheren Zufallszahlen zur Verfügung. Dieser Zufallsgenerator hat ein USB-Interface (virtuelle COM) und **arbeitet ohne Kommando-Interface**. Nach PON werden kontinuierlich Zufallszahlen mit hoher Geschwindigkeit ausgegeben. Ein permanent im Hintergrund laufendes Sicherheitssystem garantiert, dass bei Ausfall oder Manipulation der Rauschquellen die Zufallsausgabe sofort eingestellt und solange weiter getestet wird, bis alle Qualitätskriterien wieder eingehalten werden.

Die generierten Zufallszahlen sind garantiert kryptografisch sicher und werden vorzugsweise zur Entropieerhöhung und -bereitstellung in Sicherheitsapplikationen verwendet. Unter Linux gibt es bekanntlich immer wieder Probleme mit der Bereitstellung von Zufall im Entropie-Pool. Besonders kritisch wird die Situation, wenn keine Eingabegeräte an einem Server zur Verfügung stehen.

Die Qualität der vom PRG320 erzeugten Zufallszahlen ist qualitativ unvergleichlich höher und sicherer, als jede andere Art der Zufallserzeugung. Zum Verifizieren dieser Aussage stehen diverse Analysen des Zufallsgenerators, auch unter erhöhter thermischer Belastung, zur Verfügung. Die hohe Ausgabegeschwindigkeit des PRG320 ermöglicht eine Füllung des Entropie-Pools (4096 Bit) in max. 30ms. Eine kryptografische Nachbearbeitung der ausgegebenen Zufallsdaten ist prinzipiell nicht erforderlich.

Thermische Rauschquellen für das Zufallssignal sind Z-Dioden. Mittels Differenzverstärker und Schmitt-Trigger-Schaltkreis wird das Rauschsignal verstärkt und digitalisiert. Ein nachgeschalteter Mikrocontroller tastet das Zufallssignal ab und konvertiert es nach einer Bearbeitung mit Mayer-Einwegfunktionen zu einem USB1.1-Interface.

Technische Eigenschaften:

Abmessungen:	75x25x5 (mm)
Stromversorgung:	ca. 40mA aus USB-Port
Temperaturbereich:	-20°C..+85°C
Schnittstelle:	USB1.1 als virtuelle COM-Schnittstelle, 921.600 Bit/s, Protokoll 8,N,1
Qualitätssicherung:	automatischer Selbstabgleich von Verstärkung und Digitalisierung, permanenter Online-Test und Überwachung der Rauschquelle
0/1-Verhältnis:	ohne digitale Nachbearbeitung garantiert im Bereich 0,49..0,51 (> 8.000 Bit)
Entropie:	>7,997 Bit/Byte, aus Zufallsrohdaten nach Shannon ermittelt

Der PRG320 beinhaltet Schutzrechte für den Teil des physikalischen Zufallsgenerators.