

The R200-USB TRNG Units

This datasheet apply to

R210-USB, R220-USB, R230-USB

True Random Number Generator

- ◆ Easy to install and use.
- ◆ Moderate pricing.
- ◆ Driver support for Windows 98, Win 2000, and XP.
- ◆ Driver support for Linux⁽¹⁾.
- ◆ Driver support for Apple OS-8, OS-9 and OS-X.
- ◆ Driver support for Open BSD 2.9+ and Free BSD version 4.7+.
- ◆ Conventional API or emulated Virtual Serial Port driver.
- ◆ Existing SG100 installations may be upgraded without application software modifications.
- ◆ Test commands: Communication tests and access to the raw random bit stream.
- ◆ USB radio frequency filter: "Radio amateur" compatible.
- ◆ Internal Fail-Safe reset circuit guarantee continuous operation.
- ◆ No messy cables: Plug directly into your PC!
- ◆ On-line testing of random numbers: No dependence on mathematical assumptions.
- ◆ Automatic on-line supply voltage compensation.
- ◆ Not sensitive to sparks/ESD.
- ◆ Full support for hot plugging.
- ◆ HCIA processing of random numbers (patented technology).

⁽¹⁾ Linux driver support see note below

Specifications

Physical Dimensions

The R200-USB unit is 32.3 mm x 18.6 mm x 72.2 mm. The R200 can be directly plugged into a PC USB port, or attached using an USB A-male <--> USB-A-female extension cable. (The use of an extension cable is possible but not recommended.)

Operating Voltage

The USB nominal operating voltage is 5.0 volts. The R210-USB and R220-USB series TRNG units operate at 4.4-5.5 volts that is taken from the USB port. The R230-USB operate at 4.6-5.5 volts.

The R200-USB series include overvoltage protection, to protect against possible transients during PC power-up. The current consumption is 30 mA (Idle). 3A command current is 51 mA. A current figure of 52mA is reported in the device descriptor for the R210-USB.

Hardware Random Number Source

The R200 units use Johnson noise from a combination of a resistor and the input impedance of the analog amplifier. The R210/R220/R230 may use slightly different amplifier circuits. Amplification is high - 15.000 to 30.000 times -- making the shielding very demanding.

Sample System

The reference voltage to the sample system comparator is dynamically controlled by a Proportionally-Integrating "PI" regulator. The setting of the integrator and the reference voltage can be monitored externally. The regulator compensates for variations in operating voltage, the temperature, and other factors.

Temperature Range

The R200-USB series TRNG units are designed for a modest temperature range of 5°C-45°C (storage and operating). Higher temperatures (above 85°C) may reduce the operating life of the unit. Storage or operating the device above 100°C may damage the device. Lower temperatures than 5°C (non-condensing) pose no problem, but we don't guarantee operation at these temperatures at this time. At low temperatures we recommend that the unit is run at full speed, as the dissipated heat may protect the unit from moisture.

Reliability of Device

Previous versions of the FTDI USB drivers is well known to have some problems. The FTDI drivers have recently been updated, reducing these problems considerably, especially on Windows XP and Windows 2000. If you experience problems with the USB unit or the FTDI drivers first make sure that the latest version of the FTDI drivers is being used.

The Linux USB driver, the Linux USB serial driver, and the FTDI Linux serial port driver is currently being worked over by the Linux community, in order to fix some known problems and bugs. If you experience a problem with the FTDI USB serial driver for Linux, please check if installing another version of a driver, or if installing a patch may help you. Please see:

<http://www.linux-usb.org/>
<http://www.linux-usb.org/devices.html>
<http://www.qbik.ch/usb/devices/>

We have found some additional patches for the FTDI Linux driver on a temporary site, see <http://www.kroah.com/linux-usb/todo.html>

Even if a correct driver has been installed it is, however, not possible to guarantee continuous operation of an USB device as an external event such as a contact glitch or an ESD pulse, in the ground system, may corrupt the USB data link. For the R200-USB series of TRNG units this kind of problems can be overcome by adding software support for re-connecting the device, should the data link be lost. The R200-USB unit will remain operational due to the internal Fail-Safe reset circuit, that will re-connect the device in case there is an error. The Fail-Safe reset circuit is an analog reset circuit, so it can not go inoperational due to a digital crash or software bug. In fact it also monitor the correct operation of the internal software functions.

Note that, in a typical installation, these protective measures only come into play:

- If the R200 unit is touched (producing a contact glitch).
- If the R200 is accidentally removed from the computer (datalink broken).
- If another USB device is plugged into or out from the computer (USB power glitch).
- If the USB system is subject to an ESD spark in a communication line or in the ground system.
- If the R200 is subject to electrical experiments or testing.
- If the driver software is being debugged.

A restart/reset cycle typically take 15 seconds.

Lifetime of Device

The effective lifetime of the device is yet to be determined, but is expected to be several years (continuous operating or storage). Lifetime of device is not expected to be degraded by operating the device all the time.

USB Compliance

The R200 series are USB 1.1 compliant. Due to the radio-frequency filter the USB compliance is reduced as follows:

Maximum USB cable length: 1.5 m guaranteed (USB spec. say 5.0 m).

USB Sleep Mode: Supported by hardware but not implemented. The Sleep current is about 10mA (USB say 0.5mA max). Please contact Protego Information if you plan to "sleep" an R200 unit on a battery powered portable computer.

Drivers and Software

The R200 use FTDI drivers <http://www.ftdichip.com/>

The installed chip is the **FT245AM**. You may attach several R200 devices to the same computer. If you experience problems on a particular computer or platform please consult the FTDI site for driver upgrades. For a problem on Linux see note above.

Speed

The R210 produce (min) $10 \cdot 1024$ (8-bit) bytes/second = 0.08 Mbits/s.

The R220 produce (min) $50 \cdot 1024$ (8-bit) bytes/second = 0.39 Mbits/s.

The R230 produce (typ) $261 \cdot 1024$ (8-bit) bytes/second = 2.04 Mbits/s.

The output throughput for the R210 and R220 is normally not USB limited, as the USB circuit include a data buffer. For the R230 the output throughput is deperent on the overall load on the USB system, and may also depend on the operating system. The speed of the unit depend on the ambient temperature.

Statistical Tests

The R200 units pass the Crypt-X statistical tests and simple frequency tests. Due to that the HCIA technology is used, it is known that the units will always pass complex statistical tests. See the HCIA section below for details.

Install Instructions

Complete, operating system dependent install instructions (with pictures), is available on the software distribution for Windows 2000 and Windows 98. To install the device, proceed as follows:

Plug the R200 unit into the computer. Wait until the device connect, and the install wizard appears. Check that a correct productidentity string is displayed. Select "Search for a suitable driver for my device (recommended)". Specify a location (CD, hard disk) where the R200 driver is stored, and do not specify other locations. Windows will detect the driver "USB-200.inf". Install the driver.

Linux install instructions to appear later.

R200 Command List

Communication between an application and the R200-USB unit is by a command set. The commands consist of one or two characters, and they are case sensitive. The first command character is a digit '0'..'9' and the second is a letter 'A'..'Z'. The digit shall be entered in ASCII text form. The R200-USB unit will expect that a two byte command will arrive in the same USB frame. The commands are grouped as follows:

Group 0: Reset, Stop, and Boot commands

Group 1: Unit test commands.

Group 2: Lottery application commands. At time of writing, none is yet implemented.

Group 3: HCIA powered TRNG random numbers.

Group 4: Pseudo random number source, with HCIA and TRNG processing testmodes.
Not yet implemented.

Group 7: Reserved for OEM customer's use.

Commands Supported by All Units

- 0** Analog power off/ Idle loop.
- 0B** Force a Power on reset -- with delay.
- 0X** Force a Power on reset -- immediately.
- 1P** Turn power on to analog TRNG unit.
- 1C** Set up memory with constants and output to USB.
- 1N** Set up memory with constants: Numeric sorted data, and output to USB.
- 1T** Run a TRNG test and output to USB.
- 1D** DC level adjust routine. (Comparator reference voltage).
- 3A** Fullspeed TRNG data using HCIA processing and on-line hardware tests.

Additional commands supported by the R210 unit

none

Additional commands supported by the R220 unit

none

Additional commands supported by the R230 unit

- 1R** Output speed test - the R230 output a constant byte repeatedly for test purposes. The settings of the operating system, or the input buffer size, may be adjusted.
- 1F** Fast access to the raw noise stream. A continuous stream is output similar to the 3A command.

Block Commands

For test purposes there are a few test commands. The 1C/1N commands make the R200 return a constant string of data. This is intended for device test and communication/cable test purposes. The test blocks also include a 24 bit checksum. (The data is a constant, so the checksum is also a constant.)

The raw random numbers may be accessed by the 1T test command. This command also returns current DC sample voltage (obfuscated encoding) and the integrator part of the DC regulator (also some encoding). The 1T also makes the raw random numbers available to various kinds of external tests.

Stream Commands

The **3A** command provides the highest output speed of the device. The output is TRNG bias-free random numbers for encryption and gaming applications.

The 3A Commands

The command has a built-in timeout of about 15 seconds. If the command shall be aborted, issue a "0" command or ignore that and wait for the timeout. When the timeout triggers an "0X" command is issued.

Sending Commands

A two-letter command must reach the R200 in the same package. Therefore you must transmit both letters using the same API call.

Drivers and Software

TODO: Do and Don'ts in the FTDI drivers!

For Windows see the application examples in the software distribution.

Application Example

For Windows we include a test program that runs the 1C/1N/1T commands, and one application that runs the 3A command. These applications run using the "Direct" Windows drivers.

On-Line Statistical Tests

Inside the R200 units computational resources are extremely limited. This is a problem especially for the R230 as this is a high-speed device. Due to this the following statistical test has been implemented:

A sample is taken from the raw random number source. A frequency table is built. The frequency table is then converted into the corresponding information rate. The unit pass the test if the information rate is estimated to be above 97% of true randomness.

The information rate is well established as a test for randomness. This test have been used in our SG100 series of TRNG units since 1996, and is well known especially for a very low false-rejection rate.

If the test fails, the R200 unit will lock, and will no longer produce any output. The test is iterated approximately 20 times/minute.

SG100 Back-Compatibility

TODO: Install instructions for the USB DLL driver.

R200-USB Radio Frequency Filter

Most of our customers use the R200:s for applications like computer security or gambling, where a certain amount of secrecy is necessary. But an USB device (any USB device!!) must have a high drive capability to meet the USB specification. With 100mA drive strength and an output frequency well over 100MHz this specification is perhaps more similar to the specification of a radio transmitter than a cable device. We are thus worried about that the serial output stream would be easy to intercept using a radio receiver.

A standard/recommended USB connection transmit the random numbers on several frequencies, where the highest that we found was at 628 MHz. Our estimation is that in this frequency range the USB signal may be detectable at quite some distance. We therefore use a modified USB interface with a high frequency filter. We have also designed the R200 device for direct plugging into the computer, so that no cable is necessary. For test purposes we have used a Sony ICF-2001D shortwave receiver with a 25 feet wire antenna and an AOR AR8000 wideband receiver.

Our most recent test results from the laboratory indicate that, with the high-frequency filter applied, it is almost impossible to detect the USB signal using any of the two radios even if the receiver antenna is put right next to the device. This give us assurance that it will not be possible to detect and reconstruct the USB signal at some distance in the far-field, using any kind of antenna, receiver, or other equipment. We will later run a laboratory test, to measure the emitted radio frequency field, as we have done with the SG100.

The high-frequency filter limit the maximum extension cable length that may be used with the SG210. Using an extension cable also increase the risk that the signal may be obtained with a

radio receiver, as the cable may work as an antenna. We have, however not noticed any increase in emitted radio frequency field when we attach the R200 test unit to a computer using an 1 m (3 feet) extension cable. We can also use the unit with a 2m (6 feet) cable. (The USB maximum is 5 m cable length.)

R200 HCIA Technology

When processing random numbers the goal is that there should not be any way to un-do the processing, as this may lead to statistical biasing, making the output fail some statistical test. A similar situation is when a cipher process a statistically biased plaintext into cipher(text).

This leads towards a search for the "best" processing algorithm, where "best" may have different value at different times. There exist several hundred pseudo-random-number algorithms and several hundred published encryption systems.

But we may twist the problem around, and instead of observing and studying the processing method/algorithm and search for the "best" one, we study the evaluation system. The possibility that opens: The only important thing is that no statistical deficiency is ever found. This is not equivalent to that none exist! Possibly we can hide the statistical deficiencies? How would a random number processing be constructed if it can hide any statistical deficiency; and generally how would a system be constructed if its properties cannot be determined from its output signals?

Software!

Software, or an implementation in the form of a general-purpose machine that process software instructions, have the property that observing the output cannot enable us to identify the input software nor can we generally reveal any of its properties. If we could there would exist an algorithm that read an output string from a software (any software!) and then answer some question about the software, such as if there is a bug in the software or not.

We conclude that the "best" algorithm is anyone, or none at all, depending on one's view. You may read more about the R200:s in

"The HCIA Cipher Technology"

<http://www.protego.se/pdf/hcia.pdf>

(The above report could be a bit demanding. We have set aside a few R230:s as a reward should anyone ever come through this report!)

Order and Production

All three models may now be ordered from Protego Information.
We normally ship R200-USB units within four working days from order.

Price List

The price may be adjusted to support special application areas. You may also OEM the product and sell it under a different brand name. The pricelist below apply for single units at time of writing:

R210-USB EUR 270/each.

R220-USB EUR 495/each.

R230-USB EUR 995/each.

Contact

Protego Information AB
Ideon Gamma Science Park
SE - 223 70 Lund
SWEDEN
E-mail/R200: sales at protego.se
Voice: +46 46 286 36 30 (Protego Information)
Fax: +46 46 286 36 40
<http://www.protego.se>