



FOX RANDOMCARD

A hardware-based true random number generator.

A true random number generator [often abbreviated as TRNG] is a computational or physical device designed to generate a sequence of numbers or symbols that lack any pattern, i.e. appear random. Computer-based systems for random number generation are widely used, but often fall short of this goal, though they may meet some statistical tests for randomness intended to ensure that they do not have any easily discernible patterns. (Source: http://en.wikipedia.org/wiki/Random_generator)

HIGH-SECURITY OFFLINE FILE ENCRYPTION

In a large number of high-security scenarios, truly random data is required to ensure the security of a system. This random data is used to generate, for example, secret keys and challenges. In order to guarantee the security of the system it is vital that the random data used is truly unpredictable.

The only way to produce truly random data is to use a True Random Number Generator as a source.

TRUE RANDOM NUMBER GENERATOR

The Fox RandomCard is a PCMCIA-type card that contains a hardware-based True Random Number Generator (TRNG). Importantly, the Fox RandomCard is officially approved by the Dutch AIVD for use up to SECRET level (Stg. GEHEIM).

INTO ANY SYSTEM

The Fox RandomCard itself contains a software library and API for use on the target system. This API enables developers to tightly integrate the Fox RandomCard into any system.

The Fox RandomCard is also available in a production-ready Random Generation Workstation. The Workstation is a pre-installed system containing a Fox RandomCard, and which can be used as an offline generation station for random data. Particularly useful, an already existing key generation system (KGS) for generating crypto keys can be easily integrated into this Workstation. In this case, the built-in the Fox RandomCard supplies the random data needed by the KGS.





SYSTEM/SECURITY OVERVIEW

The Fox RandomCard is all about security. One of the main features of any random source is that it has to be unpredictable. A major risk that compromises the unpredictability is tampering with the random source during transportation. To mitigate this risk, the design of the Fox RandomCard makes it possible to ensure the genuineness of the device from within the software.

The genuineness test is conducted from within the Fox RandomCard by the firmware, which performs multiple security checks to ensure that the system has not been tampered with. In addition, a secure channel is set-up with the client application to guarantee that random data is actually generated from within the secure part of the Fox RandomCard.

DETAILS

To facilitate this, the Fox RandomCard uses authentication and a secure channel to guarantee that the RandomCard is genuine, un-tampered and fully operational. During initialization of the card, the secure channel is set-up between the card and the software library. This channel uses a 2048 bit RSA key for authentication, thus guaranteeing that the software is actually communicating with a genuine, un-tampered RandomCard. During the key-exchange phase, a 112-bit 3-DES key is negotiated. This key is then used to sign all random data generated by the card. By verifying the signature on the received random data, the software can guarantee that the TRNG was actually used to generate this random data.

DETAILS

The PCMCIA-type Fox RandomCard comes with:

- A driver which runs under
 - Linux 2.6.11, 2.6.17 and higher
 - Windows XP
 - Windows 2000
- An API

The Fox Random Generation Workstation consists of:

- A PC Workstation
- A built-in Fox RandomCard

For more information, please contact:

Fox-IT BV
Olof Palmestraat 6
P.O. Box 638
2600 AP Delft
The Netherlands

Phone: +31 (0)15 284 79 99
Fax: +31 (0)15 284 79 90
E-mail: sales@fox-it.com
Website: www.fox-it.com

Algemene Inlichtingen- en Veiligheidsdienst



Per undas adversas

* The AIVD is the Netherlands General Intelligence and Security Service. Our products are evaluated and approved by this organization before they can be used by the government for the protection of state secrets.

