# Family of Guardant Dongles

As of the time of publishing the manual, the family of Guardant dongles included the following:

## Guardant Sign

A high-speed, cross-platform dongle with hardware-based public-key cryptography and capability to operate in a driverless mode. The dongle is designed to provide copyright security to standalone applications. Innovative protection technologies implemented in Guardant Sign are used in all current models of Guardant dongles.

The dongle is based on a highcapacity 32-bit RISC platform. The operating speed is several times higher than that of previous generation dongles. Memory size: 4KB.

Guardant Sign supports Windows (including Windows CE) and Linux, has the capability to run without installing drivers – HID mode, contains public- (ECC160) as well as private-key algorithms (AES and GSII64), prevent multiple copies of a protected application.

The dongle has built-in protection against the exchange protocol analysis based on the dongle and Guardant API mutual authentication and use of single-session keys to encrypt data transmissions.

The primary feature set implemented in previous generation dongles is also supported: protected items, GSII64 hardware algorithms (with additional modes of operation), HASH64, RND64.

## Guardant Time

A high-speed, cross-platform dongle with built-in real-time clock and self-contained power supply. An RTC version of Guardant Sign keeping all of the advantages of the original feature set. Used for protection and time-based licensing of standalone software applications.

Just like Guardant Sign, the dongle is based on a 32-bit RISC microprocessor. Its operating speed is several times higher than that of previous generation dongles. Memory size: 4KB.

The dongle supports all features implemented in Guardant Sign: hard-ware-based public- and symmetric-key algorithms (ECC, AES, GSII64), HID mode, Linux support, preventing multiple instances of a protected application, hardware protection against traffic analysis.

In addition to these features, the real-time clock provides advanced scenarios for time-based software licensing: algorithm activating/deactivating at a specified date, setting of a time frame for the algorithm to operate and more.

Tight integration of licensing policies with the dongle's hardware algorithms significantly increases the level and effectiveness of protection.

## Guardant Code

A high-speed cross-platform dongle, in which the advanced features of Guardant Sign are optimally combined with the capability to load and execute an application inside the dongle. Designed to provide protection for high-cost, standalone applications.

32-bit hardware platform based on Cortex M3 architecture provides the dongle with reliable, high-speed data transmission over an encrypted channel and high-speed computation including floating point numbers.

The technology of Guardant Code supports the software development using high-level programming languages, specifically, the volume of loadable code may be on the order of 20,000 lines (in C).

It is also possible to call encryption algorithms, as well as a hardware-based random number generator, directly from the loadable code.

There is also a serial version of the Guardant Code with an RTC module.

## Guardant Sign Net /Time Net

A product subline designed to provide effective protection and licensing of network software applications, including time-based licensing. It contains the network versions of Guardant Sign and Guardant Time while preserving and maintaining all the capabilities and features of their local modifications.

A new, high-performance hardware platform, high speed operation, public- and symmetric-key encryption algorithms, HID mode, Linux support, hardware protection against the exchange protocol analysis.

In addition, Guardant Time Net provides with extended scenarios of time-based application licensing: activating/deactivating of the hardware algorithm at a specified date, setting of a time frame during which the algorithm will be operational.

The main advantage of the new dongles versus the previous generation is the tunneling of network traffic. I.e. information being transmitted via network is encrypted using the session keys generated between the protected application and the dongle without any intermediaries.