Hardware Algorithms

Hardware algorithms – mathematical functions for encrypting data processed inside the dongle without using computer resources.

Hardware algorithms serve for encrypting the information required for running the protected application. When the protection system is correctly organized, the use of hardware algorithms makes the removing of API functions calls from the application code useless: in this case the data required by the application will not be decrypted. Besides, the availability of hardware algorithms significantly complicates the logic of Guardant dongles operation.

The use of hardware algorithms is the main way of ensuring quality and efficiency of application protection.

Hardware algorithms are implemented in a dongle microprogram written into the microcontroller along with descriptors stored in the dongle memory. The microprogram of Guardant dongle is an unchangeable part of the algorithm – it cannot be read or modified. The descriptor (set of data stored in dongle memory available to the protection developer) serves for forming an algorithm of a specific type and its parameters.

See Chapter **Hardware Algorithms**, User's Manual, Part 2 for more information on descriptors of hardware algorithms.

GrdUtil.exe allows for creating, editing and removing hardware algorithms descriptors.

Algorithm creation dialog is a wizard with several pages:

- Add algorithm (new field)
- Algorithm properties
- Time dependencies (for RTC dongles only)
- Algorithm determinant (except ECC160 algorithm)
- ECC160 key pair (for ECC160 algorithm only)

While working with hardware algorithms it is presumed that all actions are performed with their descriptors.

After completing the current dialog, click **[Next]** to move to the next page.