Hardware Locks

A part of permanent Guardant dongle memory (EEPROM) is not available neither for reading nor for writing, and a part of it is read-only. The rest of the memory is fully available for reading and writing.

Clearly, hackers pay special attention to the contents of memory of any dongles. Surely, one can create a dongle emulator or its full hardware copy by retrieving the information from the dongle.

Permanent memory used in Guardant dongles enables setting hardware locks for reading and writing the memory contents. It is impossible to copy the memory contents protected by a hardware lock using any software methods – there are simply no tools available for it. The dongle just does not respond to attempts to read/write from/to protected memory areas.

Setting hardware locks is implemented on the lowest hardware level. This guarantees the inability to bypass them with software means.

Hardware locks can be set on or removed from any available area of dongle memory. They also can be used to expand or narrow the borders of the protected memory area. Hardware locks for reading and writing are set by default on descriptors and protected items created in Guardant dongles by the programming utility – this guarantees that hardware algorithms of Guardant dongles will not be copied or cloned. While programming the dongles with custommade utilities, ensure that the hardware locks are properly setup.