

COMPLEX PROTECTION FOR SECURED MESSAGING

Abstract

The present invention is relating to system and method for protecting the IM software, comprising:

- a. A hardware platform with CPU/MCU, RAM, One-Time Programmable memory for bootloader
- b. An operating system
- c. A bunch of Operating System Services, accessible for applications
- d. An IM software

Where:

- a. IM software is the only application (except OS and its services) executed on a hardware platform
- b. IM software region of memory is inaccessible by instructions, executed from other processes (OS services). Any instruction accessing IM software memory should cause a hardware exception
- c. IM software is capable of reading and writing OS services regions of memory for parameters transfer and results gaining

[Figure 1]