Platform independent overall security architecture in multi-processor system-on-chip integrated circuits for use in mobile phones and handheld devices

A. Ashkenazi\textsuperscript{a} and D. Akselrod\textsuperscript{b}

\textsuperscript{a}Freescale Semiconductor Inc., 6501 William Cannon Drive West, Austin, Texas 78735, United States
\textsuperscript{b}Electrical and Computer Engineering Department, McMaster University, Hamilton, ON, Canada L8S 4K1

Abstract

A platform independent security architecture for use in Multi-Processor System-on-Chip integrated circuits, primarily oriented for mobile phones and handheld devices, is presented. The suggested architecture provides an enhanced security protection scheme for use in smartphones, PDA’s, as well as other similar systems. Sensitive data storage facilities, cryptographic engines, and physical protection mechanisms such as debug port access control are presented and described in detail. The proposed secure architecture has been incorporated as a part of an application processor which in turn is embedded in a number of smartphone and handheld products. System operation is discussed and hardware realization and experimental results of the proposed architecture are described.

Keywords: Security architecture; Mobile phones; Handheld devices; Wireless security; Platform-independent security architecture