Quiddikey in Software

Intrinsic-ID's Quiddikey™ in Software is a key storage product that extracts the key from the unique device fingerprint originating from the deep submicron manufacturing process variations. It is designed to protect a device and its content against counterfeiting and cloning. It is available as platform independent software libraries (ANSI C) and can be implemented seamlessly on any processor that has an uninitialized SRAM block, even when the device is already deployed in the field. The Quiddikey Software package has been ported with certified reliability on the SmartFusion® Customizable System-on-Chip (cSoC), using the embedded ARM® Cortex™-M3 processor.

Functionality

Secure key storage

Advantages

- Very secure key storage: the key is not present when the device is powered off
- Protects against cloning of devices and systems
- Enables a cost reduction through a lower bill-of-materials for systems with security functionality

  The SmartFusion cSoC provides a high level of integration, including an ARM Cortex-M3 processor with memory and many standard peripherals, nonvolatile memory for the Quiddikey firmware and activation code data, a general-purpose FPGA fabric with SRAM blocks, and analog components—all on one device

  Quiddikey in Software provides an alternative to on-chip nonvolatile memory for secure key storage
- Software-only solution requires just two of the SmartFusion cSoC's many 4K-bit SRAM blocks to be mapped to the Cortex-M3 memory space
- Supports legacy systems and can be deployed in existing devices

Applications

- Secure elements for mobile contactless payments and streaming media protection
- Protection of software, content and data against piracy through software/hardware binding
- Flexible system for secure boot (anti-virus protection)
- Control word protection in Pay TV Systems

Specification Example

Assumptions

- Storage of a 128 bit key (AES)
- Platform: ARM Cortex-M3 SmartFusion cSoC

Requirements

Code memory	±20 kbyte
SRAM	±1 kbyte (two 4-Kbit SRAM blocks)
Nonvolatile memory (for activation code data)	±1 kbyte

Parameter

Enrollment speed (clock cycles)	5M
Reconstruction (clock cycles)	6M

.

August 2011