Quiddikey on Microsemi ProASIC3 FPGAs

Intrinsic-ID, a spinout of Royal Philips Electronics, introduces Quiddikey™ security IP on Microsemi's ProASIC®3E low power FPGAs. Intrinsic-ID's Quiddikey is a key storage product that extracts the key from the unique device fingerprint originating from deep submicron manufacturing process variations. It is designed to protect a device and its content against counterfeiting and cloning. Quiddikey is available as FPGA netlist IP.

Functionality

Secure key storage

Advantages

- Protects against cloning of devices and systems
- Enables a cost reduction through a lower bill-of-materials for systems with security functionality by eliminating the need for embedded nonvolatile memory for key storage
- Immediately available on Microsemi's FPGA devices

Applications

- Streaming media protection
- Protection of software, content and data against piracy through software/hardware binding
- Flexible system for secure boot (anti-virus protection)
- Secure network infrastructure
- Automotive and navigation

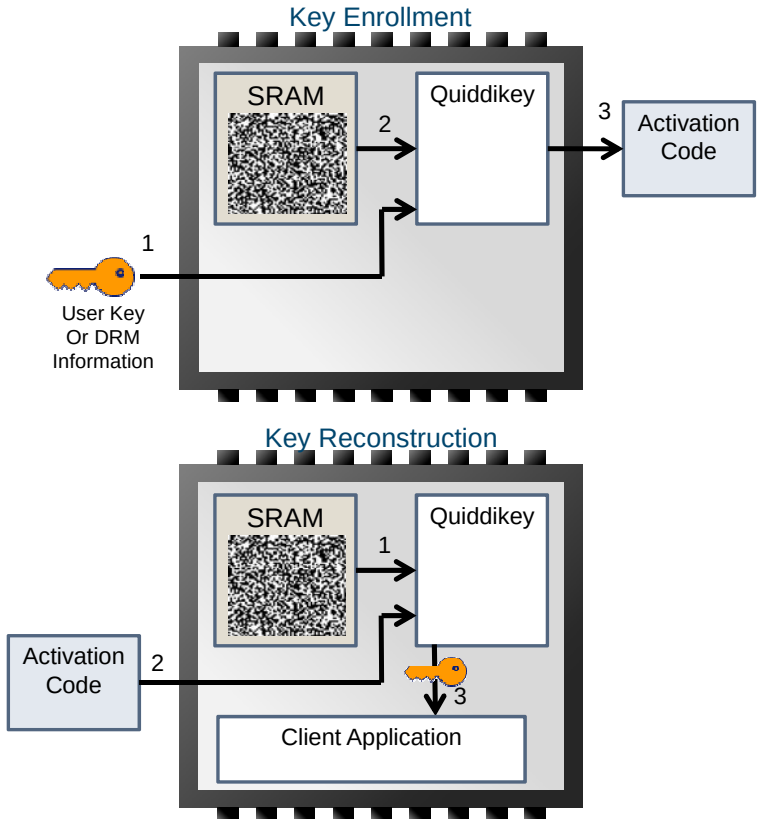
Quiddikey Reference Implementation

- Implemented on ProASIC3E A3PE1500 FPGA onto a ProASIC3 Starter Kit Board
- Storage of a 256-bit key (AES)
- Uses 4 kBytes of SRAM that is configured on the FPGA itself
-

Quiddikey has two main functional modes: Enrollment and Key Reconstruction. A user-defined key is programmed in Enrollment mode**.** Quiddikey retrieves the start-up data from the memory (SRAM) and generates the corresponding activation code. This is a one-time procedure. Quiddikey also supports device-unique keys. In Key Reconstruction mode, the activation code is used in combination with a new SRAM start-up reading to reconstruct the user-defined key.

August 2011

Key Enrollment and Reconstruction



The Quiddikey implementation for the ProASIC3E device comes with an Interface Specification and User Guide Manual, synthesis example, VHDL testbench and simulation scripts. The user can add additional logic around Quiddikey as part of a larger design.

Quiddikey Reference Implementation Characteristics

Quiddikey Parameter	**Value**
Key size	256 bits
SRAM size	1040 x 16 bits
Activation code size	2120 bytes
Number of ProASIC3E FPGA cells	7979
Number of ProASIC3E FPGA RAMs (512 x 9)	8

.

Microsemi Corporate Headquarters
2381 Morse Avenue, Irvine, CA 92614
Phone; 949.221.7100 · Fax: 949.756.0308
www.microsemi.com