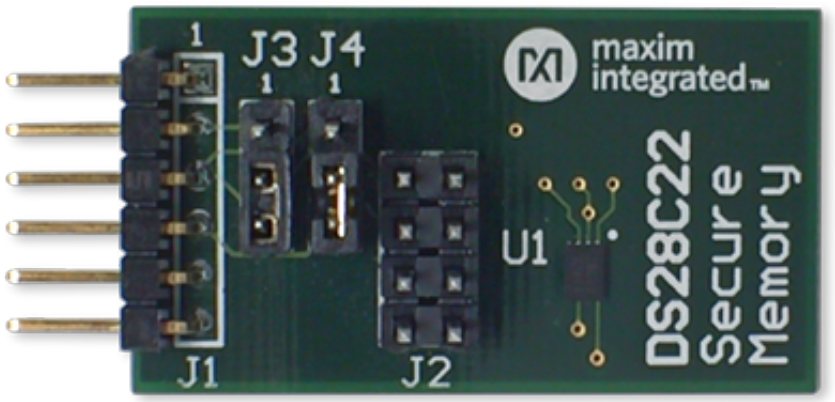
System Board 6134

MAXREFDES43#: SECURE AUTHENTICATION DESIGN WITH I2C SHA-256

Introduction

The proliferation of Internet-connected or Internet of Things (IoT) devices manifests itself in multiple applications including industrial, medical, and energy solutions. This increased connectedness requires enhanced security to protect IP, enable system features using software, and prevent counterfeiting. The MAXREFDES43# subsystem reference design uses the DS28C22 to immediately implement SHA-256 authentication on Xilinx FPGAs over an I^2C serial bus. The MAXREFDES43# differs from the MAXREFDES34#, which uses the DS28E15 to communicate over the single-contact 1-Wire® bus. The reference code defines a SHA-256 processor on the host FPGA.

MAXREFDES43# System Board



Enlarge+

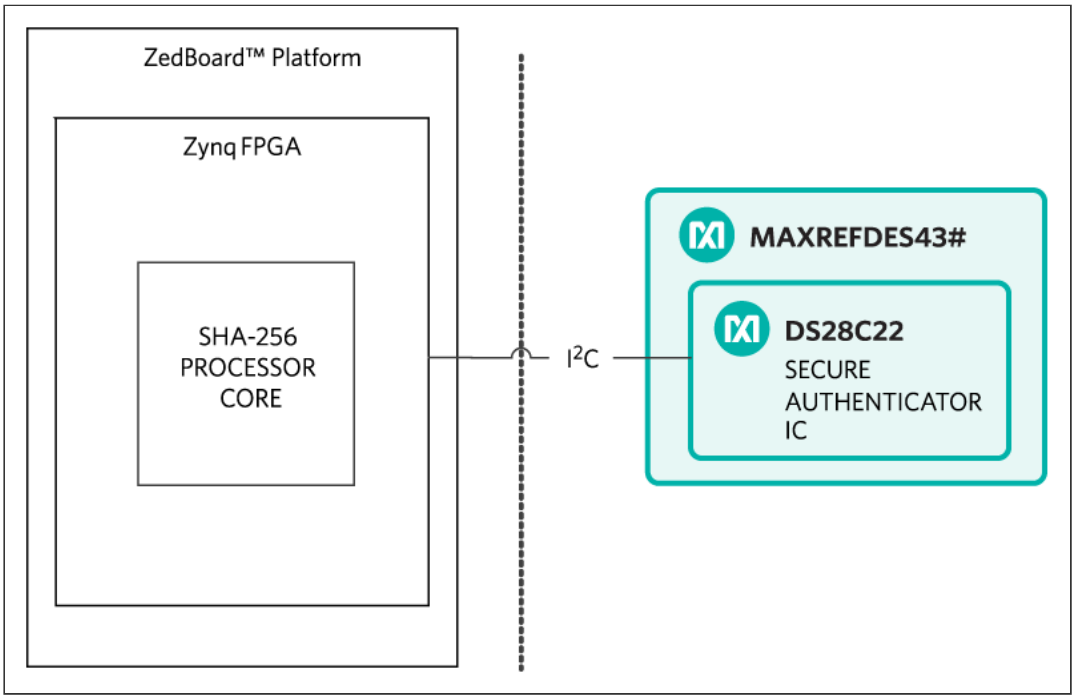


Figure 1. The MAXREFDES43# subsystem design block diagram with development platform.

Detailed Description of Hardware

The MAXREFDES43# interfaces with FPGA development boards using a 6-pin Pmod connector as illustrated. The MAXREFDES43# is configured with jumpers, J3 and J4, to allow for configuration with the ZedBoard and with alternate configurations. Both configurations are shown below. To interface with the ZedBoard, place jumpers between pins 2 and 3 of both J3 and J4. When plugging the MAXREFDES43# into a host board, make sure to correctly align the pins with the host Pmod connector, as shown in **Figure 2** and **Figure 3**.

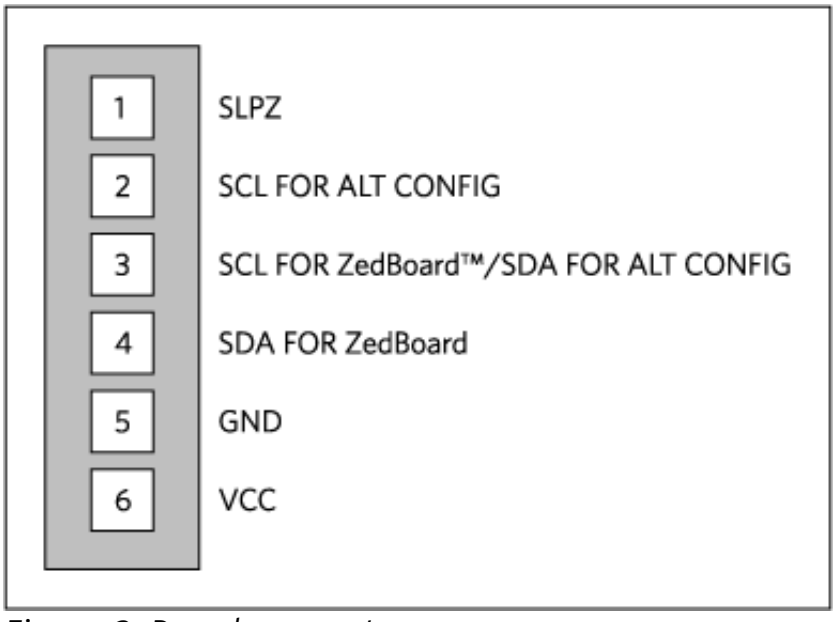


Figure 2. Pmod connector.

Figure 3. The MAXREFDES43# subsystem design correctly inserted into the ZedBoard development platform. Note that the MAXREFDES43# board is plugged into the top row of the Pmod connector on the ZedBoard.

Table 1 shows the supported platforms and ports.

Table 1. Supported Platforms and Ports

Supported Platforms	Ports
ZedBoard platform (Zynq®-7020)	JA1

For symmetric authentication schemes like SHA-256, protection of both the secure authenticator secret key, along with the FPGA secret key, are important. Symmetric authentication implementations with poor FPGA secret key security can be risky. To this end, the DS28C22 uses DeepCover® techniques to protect against invasive and noninvasive attacks on its secret key; the reference design spells out various techniques to protect the FPGA secret key.

Additional detail on secret key protection techniques may be found in application note 5803, "Safeguard Your FPGA System with a Secure Authenticator."

Detailed Description of Firmware for ZedBoard Platform

Detailed Description of Firmware for ZedBoard Platform

The MAXREFDES43# firmware design supports the ZedBoard kit and targets an ARM® Cortex®-A9 processor placed inside a Xilinx Zynq system-on-chip (SoC).

The firmware allows for immediate interfacing to the hardware. The firmware is written in C, developed using the Xilinx SDK tool, based on the Eclipse™ open source standard.

The firmware program sequence is used to compute and lock the secret (CLS), write page data to the DS28C22, and authenticate the DS28C22. The complete source code speeds customer development. Code documentation resides in the corresponding firmware platform files.

Quick Start

Required equipment:

- Windows® PC with two USB ports
- MAXREFDES43# board
- MAXREFDES43# supported platform (i.e., the ZedBoard kit)

Download, read, and carefully follow each step in the appropriate MAXREFDES43# Quick Start Guide.