APPLICATION NOTE 7229

SECURE USB DONGLE APPLICATION EXAMPLE USING THE MAX32520

By: Shawn Brooks

Abstract: Secure dongle application example using the MAX32520 ChipDNA™ Secure Microcontroller with Secure Boot.

Introduction

This application note describes how the MAX32520 can be used to provide security services to a host personal computer through a high-speed USB connection. The MAX32520FTHR evaluation kit (EV kit) and software are discussed as a potential platform for rapid application development and experimentation.

System Design

A secure USB dongle consists of a USB interface and a microcontroller. The microcontroller must offer a few key security features:

- Tamper detection
- Secure and authenticated code execution
- Secure encryption key storage
- Protected unique authentication values

The MAX32520 meets the requirements with Maxim Integrated patented ChipDNA™ physically unclonable function (PUF) technology, secure key storage, encrypted firmware execution, and secure bootloader.

The system block diagram below illustrates a typical secure dongle application using a high-speed USB bridge and the MAX32520, which interface through a 4-bit QSPI™ bus. This design is implemented in the MAX32520FTHR, a low-cost Adafruit-compatible Feather® board available from Maxim Integrated.

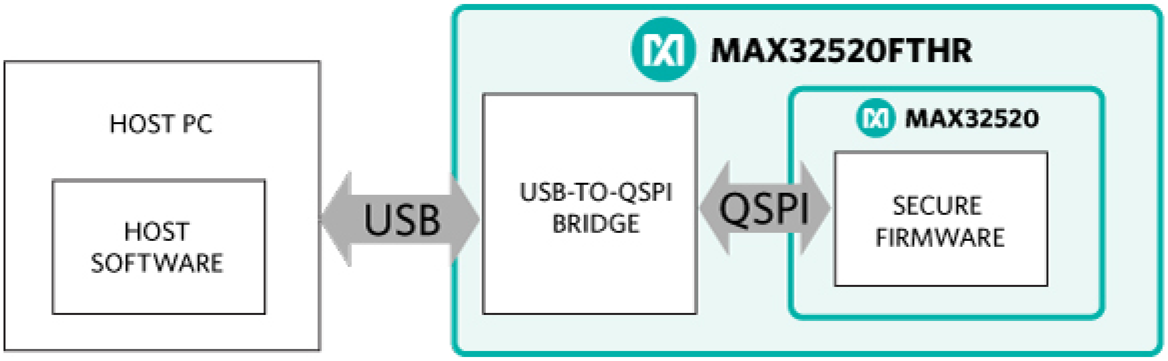

Figure 1. System architecture.

Root of Trust

The first requirement of a secure dongle is firmware image authentication and encryption. The MAX32520 contains a secure bootloader that authenticates and executes firmware images placed in the flash. Firmware images must be signed and encrypted using user-specific keys, which are assigned during IC manufacturing. An internal tamper detection mechanism erases these keys if a tamper event is detected. This mechanism runs independent of the CPU. Without the keys, the bootloader fails to authenticate and decrypt the firmware image.

The internal tamper detection mechanism monitors physical, electrical, and thermal aspects of the chip. Additionally, the MAX32520 provides CPU-independent external tamper detection signals which can be used to implement PCB-specific protection mechanisms.

USB Communication

The host communicates with the secure dongle over USB. This traffic should be encrypted to prevent reverse engineering of the communication protocol. This is easily implemented on the dongle by using the MAX32520 symmetric and asymmetric elliptical engines. The host software is more difficult to secure. PC specific software solutions typically involve system monitoring and code execution obfuscation techniques.

The MAX32520FTHR implements USB connectivity using the FTDI FT4222 USB-to-QSPI bridge. On the host side, FTDI provides cross-platform libraries to ease USB-specific software development. This design has two points of possible external attack—at the USB interface and at the QSPI interface. Both interfaces are protected if the communication stream is encrypted.

Application Specific Functions

Once the firmware, PC software, and the communication link are secured, the PC software application can implement a variety of authentication, license, and cryptographic functions such as:

- Machine-specific licensing
- User-specific licensing
- Functional licensing with expiration
- Strategic or mass data cryptography
- Host code authentication and cryptography

MAX32520FTHR Experimentation Platform

The MAX32520FTHR can be used as a starting point for secure dongle designs. It comes pre-programmed with test keys, which enable quick and convenient application development. Example device firmware and host software for the MAX32520FTHR are available on the board's product page at www.maximintegrated.com. The MaximSDK, also available on the product page, provides a GNU toolchain with Eclipse™ support and code encryption/signing tools.

For more information on using the software associated with the MAX32520FTHR, refer to the documentation included in the software package on the MAX32520FTHR product page.

Conclusion

Secure embedded designs require code security and tamper detection as well as authentication and encryption mechanisms. The MAX32520 provides these features alongside the widely accepted and easy to use ARM Cortext-M4 processor in one small, low-power package.

Trademarks

Eclipse is a trademark of Eclipse Foundation, Inc.
Feather is a registered trademark of Limor Fried DBA Adafruit Industries.
Arm and Cortex are registered trademarks of Arm Limited.
ChipDNA is a trademark of Maxim Integrated Inc.
QSPI is a trademark of Motorola, Inc.

Related Parts		
MAX32520	ChipDNA Secure Arm Cortex M4 Microcontroller	Free Sample
MAX32520FTHR	Evaluation Kit for the MAX32520	

Next Steps	
EE-Mail	Subscribe to EE-Mail and receive automatic notice of new documents in your areas of interest.

APP 7229: 26 Jun, 2020
APPLICATION NOTE 7229, AN7229, AN 7229, APP7229, Appnote7229, Appnote 7229

FOLLOW US

Newsroom Events Blogs

About Us
Customer Testimonials
Careers
Contact Us
Customer Support
Technical Support

Ordering FAQ
Worldwide Franchised Distributors
Investor Relations
Corporate Responsibility

Contact Us Careers Legal Privacy Cookie Policy Site Map