amp inc
Memory and Storage Solutions for today's world
Accelerated Memory Production, Inc.

Using AES 256 bit Encryption

April 16

2014

There are many questions on How To Support AES256 bit encryption in an Industrial, Medical or Military Computer System.

Programmable Encryption for Solid State Disks

Programmable Encryption for Solid State Disks

There are many questions that are being asked on how to use AES256 bit encryption and what is needed in the system to support a Solid State Drive (SSD). Most commercial SSD use self-generating keys that encrypt the data contents. The method to protect this data is by enabling the SSD password feature. When a programmable encryption key is used, it replaces the need for a password and only requires the correct 32 byte code sequence to be written to the SSD to enable the SSD and the encryption/decryption functionality. While this is a short answer, the security requirement of how the SSD is utilized in the system deserves the most attention.

What are the security requirements and how will they be implemented?

The encryption capabilities that are being described here are for the amp inc SATA*prime* product series SSD where the entire drive is encrypted, and utilizes a managed programmable encryption key. Each individual drive has self-encryption capabilities and can be keyed identical or individually. Each SSD encrypts data written to minimize the loss of system data transfer performance.

The purpose of encrypting the SSD is to protect the data stored on the SSD from being accessed by non-authorized individuals. The management of the authorization of who can access the system must be determined. Most computer systems utilize a BIOS during the power on cycle of a computer system. The BIOS is responsible for managing the authorization process based on the method defined by the security parameters established by the system designer. The BIOS will challenge the user to enter the correct security sequence for access. Depending on the type and method of challenge, the BIOS is notified that the challenge is valid or invalid, and if valid, the BIOS would load the correct encryption key sequence stored in a protected location. Once the key is written to the SSD, the data is accessible or system OS is bootable.

What is needed to support a SSD data encryption

The main focus of the document is to identify the different component pieces that you need to review and determine what is needed for your application. Here are some questions to be answered.

1. What are your security requirements?
2. How are the Keys Issued, Authorized and Managed?
3. Is there Physical Presence Interface required and where is it located?

Review the documentation provided on our USB thumb drive or download them from Trusted Computer Group (TCG) www.trustedcomputinggroup.org

Introduction

The Trusted Computer architecture is platform-independent and intended to enhance trust in computing platforms. As such, the TPM Main Specification is general in specifying both hardware and software requirements. The goal of the TCG member companies is to ensure compatibility among implementations within each type of computing architecture.

Below is a list of documents available from www.trustedcomputinggroup.org,

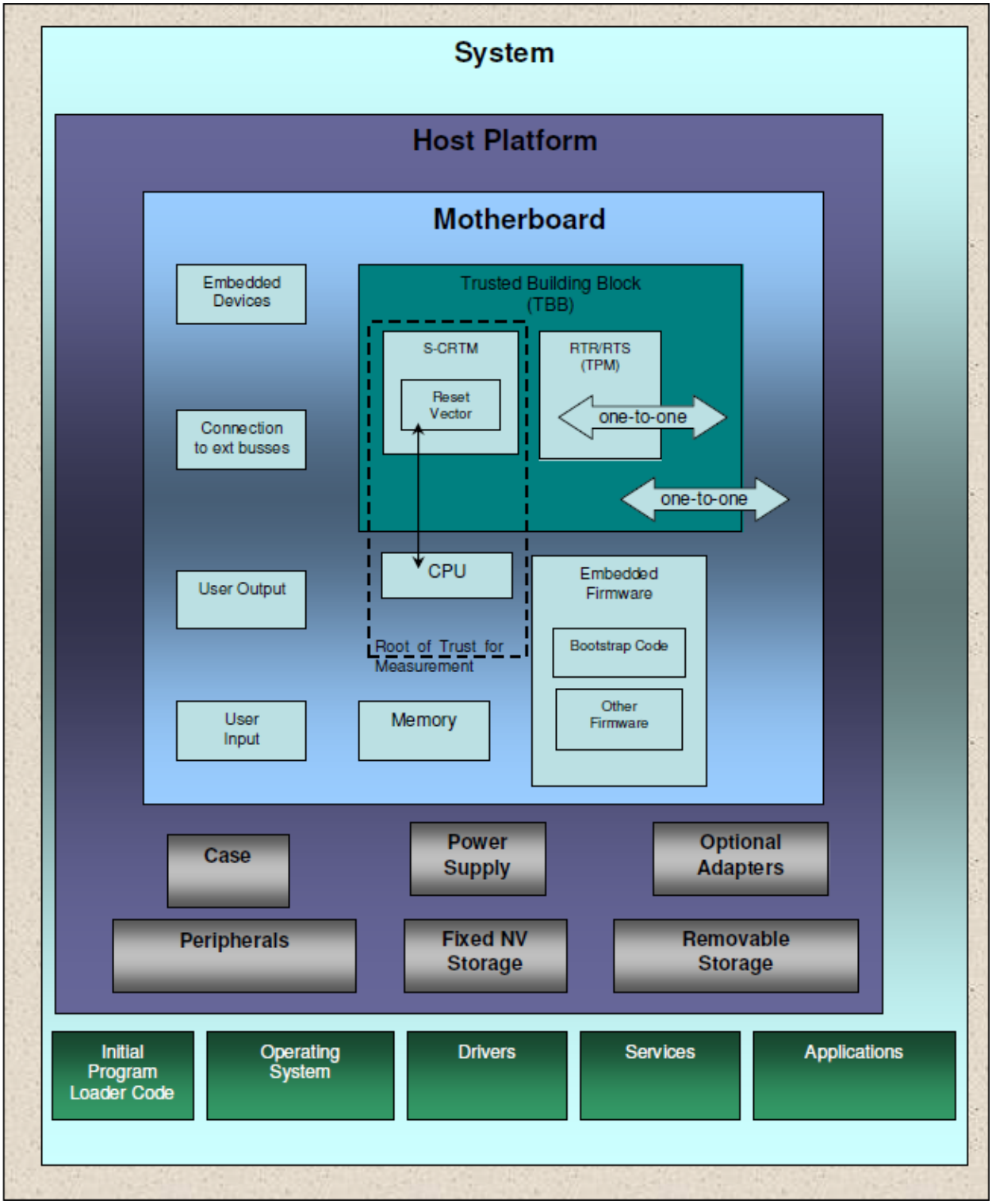
PP_TPM_spec12_rev116_final
TPM Main-Part 1 Design Principles_v1.2_rev116_01032011
TPM Main-Part 2 TPM Structures_v1.2_rev116_01032011
TPM Main-Part 3 Commands_v1.2_rev116_01032011

To help in the review process, I have included additional references to documents that will help in understanding the requirements for implementing the security features. Review the document Physical Presence Interface Specification Version 1.2. This document discusses the Physical Presence of hardware and BIOS interface requirements.

Summary of Physical Presence Interface Specification.

Table of Contents

Example of a Trusted System



amp inc is evaluating the Atmel AT97SC3205 Trusted Platform Module LPC Interface component to validate our feature requirements. An interface is provided on many motherboard solutions and is readily available for purchase.

The AT97SC3205 short form data sheet is included on our USB thumb drive and some of the features are highlighted.

See Atmel-8883AS_TPM-AT97SC3205T-I2C- DataSheet-0220.
The complete document is available under NDA.

- Compliant to the Trusted Computing Group (TCG) Trusted Platform Module (TPM) Version 1.2 Specifications
- Single-chip Turnkey Solution
- Hardware Asymmetric Crypto Engine
- Atmel AVR® RISC Microprocessor
- Internal EEPROM Storage for RSA Keys
- 400kHz Fast Mode/100kHz Standard Mode I2C Operation
- Secure Hardware and Firmware Design and Device Layout
- FIPS-140-2 Module Certified Including the High-quality Random Number Generator (RNG), HMAC, AES, SHA, and RSA Engines
- NV Storage Space for 2066 bytes of User Defined Data
- 3.3V Supply Voltage
- 28-lead Thin TSSOP or 32-pad QFN Packages
- Offered in Commercial (0°C to 70°C) and Industrial (-40°C to +85°C) Temperature Range

To summarize how the technology is utilized for an embedded system, your BIOS will need to be modified to challenge the user for the correct security phase. If authorized, the BIOS would access a secure data storage location that contains the encryption keys. The BIOS would then write the keys to their specific SSD to enable access. Remember that when the system is powered off, the key should be cleared and when in standby state, the user must be challenged to access the system.