TCG2 eModule Guide

Introduction to the TCG2 eModule

Enhancing security authentication across embedded, cloud, IoT, mobile, server and client systems with the TCG2 eModule

INTRODUCTION TO TCG AND TPM

The Trusted Computing Group (TCG) is a nonprofit organization formed to standardize secure computing through industry-wide standards and specifications. The PC-Client workgroup within TCG is most relevant for the Aptio V TCG module because it describes how various PC-based systems can be protected.

The Trusted Platform Module (TPM) is at the center of protection principles adopted by the PC-Client work group. TPM is a crypto-processor that provides digital signatures, random number generation and protected storage in a secure environment.

More information about the PC-Client workgroup specifications can be found at www.trustedcomputinggroup.com.

MAJOR FEATURES SUPPORTED

The primary task of the Aptio TCG2 module is to hash BIOS data into Platform Configuration Registers (PCR) of the TPM hardware for Trusted Operating Systems to use. The following features are supported by the Aptio TCG2 module:

- Generic support for all TPM 1.2 compliant TPM hardware
- Generic support for all TPM 2.0 compliant TPM hardware
- Hashing of BIOS data into TPM PCRs as required by the PC-Client workgroup
- TCG ACPI Physical Present Interface Support based on the latest TCG Physical Presence Interface Specifications
- Ability to manage TPM 1.2 and TPM 2.0 devices via BIOS Setup
- Support for OEM Specific needs in relation to provisioning their TPM devices
- Support for windows Bitlocker™ feature and other TPM related industry features such as Intel Trusted Technology
- Additional progress code support to signify TPM initialization

COMPONENT DESIGN

The component provides industry based protocols such as the TCG protocol (TPM 1.2) or the TCG2 Protocol (TPM 2.0) for communicating directly with the TPM. This provides an abstraction that allows customers to communicate with the TPM without having to deal with the hardware interface to the TPM.

HIGHLIGHTS:

- **Compatible with Aptio Core 5.0.0 and above**
- **eModule defines SDL tokens for specific platform needs**
- **Advanced setup options**
- **Provides support for the Physical Presence Interface specification**
- **Seamless operation with operating systems compliant with TCG-related specifications**
- **Support for Windows Bitlocker™ feature and other TPM-related industry features such as Intel Trusted Technology**

American Megatrends

American Megatrends Inc. | ami.com
5555 Oakbrook Parkway, Bldg. 200
Norcross, GA 30093 | 770.246.8600

For more information: http://ami.com