Wearable Computer Requires Radisys COM Express Module with Specific Trusted Platform Module (TPM) Support

Case Study

radisys®

Industry/Market

Military equipment manufacturer.

The Challenge

Developing a military-grade wearable computer was difficult since few Trusted Platform Modules (TPMs) support an extended temperature range.

The Business Environment

In 2006, the U.S. Army started requiring that every PC it purchased include a TPM.[1]

The Solution

The equipment manufacturer required support for an extended temperature TPM device on their COM Express-based carrier board. Radisys implemented the TPM support as a standard BIOS offering, which enabled a COTS-based COM Express solution.

The Benefits

The equipment manufacturer was able to offer a differentiated solution and save considerable development cost compared to doing a design in-house.

Customer Profile

The equipment manufacturer supplies fully rugged, custom computers, including ultra-rugged mobile PCs.

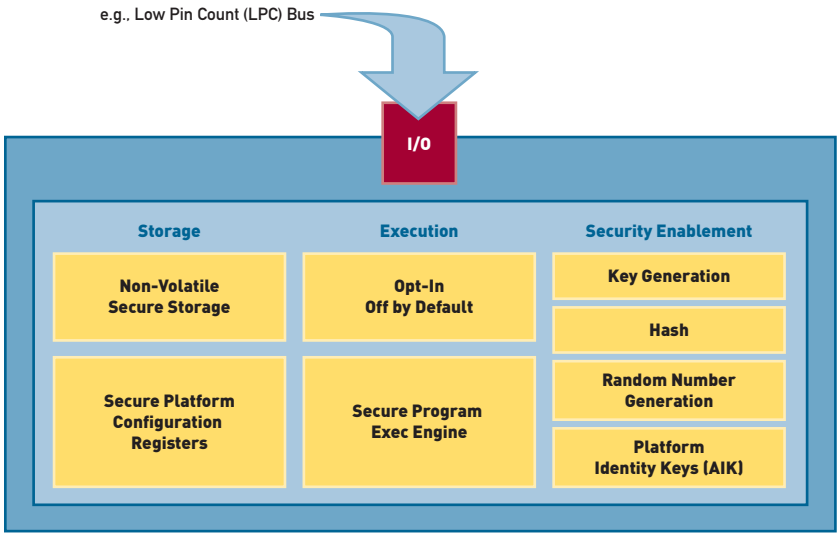
To address data encryption and device authentication needs, the U.S. Department of Defense stipulates that all new computer assets (e.g., server, desktop, laptop and PDA) include a Trusted Platform Module (TPM).[2] A TPM is an on-board secure cryptoprocessor that encrypts and safely stores system secrets, like security keys. This directive also applies to wearable computers that must be qualified to MIL-STD-810 for temperature, altitude, vibration, shock, salt fog, drop and explosive atmosphere.

Selecting and integrating a TPM for a Mil/Aero application is non-trivial, as most typically require specific BIOS support and many TPMs on the market are not specified to operation over the extended temperature range. A manufacturer of wearable computers sought a COM Express module that would provide standard support for the specific ruggedized TPM solution they had selected. As no such modules were already available on the market, the equipment manufacturer requested Radisys to add the TPM to their Procelerant® CEZ5XT COM Express module as a standard product offering. Radisys designed-in the selected TPM device into its next BIOS release, performed the necessary validation and offered the COM Express module/BIOS combination as a standard product. As a result, the manufacturer could leverage a differentiated military grade product that provided a first-to-market competitive advantage.

> *As TPM becomes a check off requirement for most military computers, we have been adding this feature to many of our extended temperature COM Express modules.*
>
> **Lorraine Orcino** COM Express Product Line Manager at Radisys

TPM Overview

Promoting a safer computing environment, the Trusted Computing Group developed the Trusted Platform Module (TPM) specification. The not-for-profit organization defined a device containing a cryptographic engine and protected storage to securely store passwords, certificates, encryption keys and other information used to authenticate a platform. Additionally, a TPM can store a platform measurement (i.e., a "unique" hash value of the system) that strengthens the authentication process by ensuring the platform is what it claims to be and has not been breached.[3] As a result, there's added protection against illicit access (e.g., stolen device) and tampering because the TPM will seal off data and secrets when there are unauthorized platform configuration changes. A TPM provides multi-prong protection (see graphic on page 3): securing storage, executing only trusted programs and implementing advanced cryptography.



Components of a Trusted Platform Module (TPM)[3]

Adding a Custom Feature to a Standard Product

Making matters rather complicated, the customer not only required wearable computers to have a TPM and supporting BIOS software, but both had to be incorporated into a standard product. Radisys supported this special request by integrating the TPM into its low power CEZ5XT BIOS, validating the revised board and overseeing the development of the enhancement. In the end, the wearable computer manufacturer was able to deliver a differentiated product without incurring the large expense of doing the module design themselves.

Powerful, Yet Low Power

On the battlefield, real-time video encoding/decoding and other compute-heavy tasks were previously confined to vehicles, and command and control centers. Today, these applications are available on-foot, giving mobile soldiers greater situational awareness. Enabling longer missions through extended battery life, the Radisys CEZ5XT delivers powerful performance with sub-5 watt power dissipation, making it ideal for battery powered handheld or mobile applications. In one of the smallest COM footprint possible, this module is based on the low power Intel® Atom™ processor (1.6 GHz) and has up to 2GB memory, a microSD socket and Gigabit Ethernet, and operates over an extended temperature (-250C to +700C) voltage range. Now, with support for an integrated TPM, equipment manufacturers have a ruggedized computing solution for power and space constrained applications.

[1] Source: http://www.army.mil/ciog6/news/500Day2006Update.pdf
[2] Source: http://iase.disa.mil/policy-guidance/dod-dar-tpm-decree07-03-07.pdf
[3] Source: Trusted Computing Group website, http://www.trustedcomputinggroup.org/resources/trusted_platform_module_tpm_summary

radisys.

Corporate Headquarters
5435 NE Dawson Creek Drive
Hillsboro, OR 97124 USA
503-615-1100 | Fax 503-615-1121
Toll-Free: 800-950-0044
www.radisys.com | info@radisys.com

intel Embedded Alliance Premier