**TPM Suite**

---

**Features**

- Hardware based multi-use security
- Supports all DPX Series products that have Trusted Platform Module
- Software solutions for common gaming applications of TPM
- Platform authentication, software DRM, encryption, access control, random number generation

---

**Introduction**

The trusted platform module (TPM) chip included on Advantech-Innocore DPX Series main boards is an advanced security co-processor offering a high level of hardware-based security for application development and deployment.

The TPM hardware and software specification is an industry standard developed by the Trusted Computing Group consortium started by AMD, HP, IBM, Intel, Microsoft, Sony and Sun Microsystems.

**Feature Summary**

<table>
<thead>
<tr>
<th>Key TPM Features</th>
<th>Unique per-board RSA key</th>
<th>Generates, stores and protects RSA keys: keys never leave the TPM chip unprotected</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>RSA asymmetric encryption and signing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SHA-1 hashing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Generates random numbers to 1-million bit random-ness (as tested by US NSA)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Chip is physically secure from physical tampering</td>
</tr>
</tbody>
</table>

**What is the TPM Suite?**

TPM Suite is Advantech-Innocore’s software package to help the developer use the TPM chip and build security solutions needed to protect his intellectual property and investment in engineering resources.

**Typical Applications of TPM**

There are two principle applications of the TPM chip and supporting software:

- **Tie the application to the main board:** the application will only run on a main-board configuration you determine. Various identifiers can be used including:
  - Hardware configuration available
  - PCI devices
  - Version of BIOS
  - Version (model) of board
  - Specific board-unique key – tie the application to an individual board or range of boards

- **Tie the main board to the application:** the main board will only run the application you determine.

Only applications prepared with the correct encryption keys will load and run on the main board.
Key TPM Architecture Concepts:

Two key concepts in TPM architecture that allow the software architect to build strong security schemes are 1) Establishing Trust and 2) the use of Platform Configuration Registers.

Trust and Establishing Trust

- All code run by the processor is checked before it is run.
- A digest is derived from the code to be run and stored in a platform configuration register (see below).
- The digest is used as the basis of establishing whether the code is trusted.
- If un-trusted, application booting can be halted.
- Trust starts at the system BIOS and proceeds through system extension ROMs, MBR, OS loader and application code.

Platform Configuration Registers

- 24 in all, 8 for hardware use, 16 for software use; populated one-by-one as the system boots.
- Contain digests of key parts of the system, e.g. BIOS, PCI bus, Boot-disk MBR and partition table, OS loader, application software.
- Combined digests can be used to form the basis of an encryption/decryption key-pair which is used to encode your software. If the board configuration changes, so do the PCR values – consequently the encryption key changes and your application doesn’t run.
- Contents are difficult to reproduce without running exactly the same code.

Package Contents

- Libraries, drivers and developer resources
- Sample source code
- Sample precompiled binaries for Advantech-Innocore main boards.
- User manual describing key concepts, protection schemes and sample code.

Support Requirements

- Development machine: Advantech-Innocore DPX® Series motherboard with TPM Atmel AT97SC3203/4 TPM chip fitted
- Windows XP SP2 or Linux 2.6-based distribution
- Windows XP: Microsoft Visual C++ 6 or newer
- Linux 2.6: gcc 3.3 or higher.
- 256MB RAM
- 20MB disk space

Other References

- Trusted Computing Group Web Site: https://www.trustedcomputinggroup.org/home
- Atmel TPM Datasheet.

OEM Customization and Product Development

- Advantech-Innocore specializes in the fields of PC-based hardware design and software development. Our in-depth knowledge and global resources make us your ideal partner.
- Advantech-Innocore is part of the Advantech Co., Ltd. Group of Companies.
- Specifications subject to change. E&OE.
- Copyright © 2011 Advantech Co., Ltd.
- All rights reserved. Advantech-Innocore, the Advantech-Innocore Logo, DPX, ConnectBus are trademarks of Advantech Co., Ltd. in the UK, US and other countries.
- All other trademarks are acknowledged and respected.