



The trusted platform module (TPM) chip included on 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

Key TPM Features:

- Unique **per-board RSA key**;
- **Generates, stores and protects** RSA keys: keys never leave the TPM chip un-protected;
- RSA asymmetric encryption and signing;
- SHA-1 hashing;
- Generates random numbers to 1-million bit random-ness (as tested by US NSA);
- Chip is physically secure from physical tampering.

What is the TPM Suite?

TPM Suite is 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.

How?

Two of the key concepts in the TPM architecture allow you to have confidence in your security deployment.

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 right).

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:

16 in all, 8 for hardware use, 8 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:

The TPM Suite package includes the following

Libraries, drivers and developer resources

Sample source code

Sample precompiled binaries for Innocore main boards.

User manual describing key concepts, protection schemes and sample code.

Support Requirements:

Development machine:

Innocore DPX-112,116, 117, S305, S410, C605, C705

Atmel AT97SC3201/2 TPM chip fitted

Windows XP SP1 or 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.
- Innocore "Security Suite - Secure Boot Datasheet"