PROTECT YOUR DATA AND ENHANCE SECURITY

In a connected and highly interconnected environment, it’s simply a matter of time before criminals will get into your system to steal your data. Criminals are using trusted applications to exploit gaps in perimeter security: Malicious actors are using trusted applications and software protection to manipulate, steal and/or destroy sensitive data and critical applications. They can even use them to bypass security to gain unauthorized access to data and secrets in a platform or to gain administrative control over the system, without user intervention or awareness.

You can’t put a question mark in front of data security. The future of computing is expected to be much more secure, with minimal chance of exposure to software attack or physical theft. TPM stores personal data, making it more secure from software attack and physical theft. Access to data and secrets in a platform can be denied by policy settings, making the platform more secure by preventing use of data or functions deemed malicious.

The risks
Key areas of authentication, identification, integrity checks, authorization, input validation, and encoding are among the most critical risks. Preventing these risks requires a solution that provides both hardware and software protection, more than just encryption. TPM is a unique security solution that enables a more secure method to manage keys, passwords and digital fingerprints to provide platform protection with key TPM features.

TPM stores personal data, making it more secure from software attack and physical theft. Access to data and secrets in a platform can be denied by policy settings, making the platform more secure by preventing use of data or functions deemed malicious.

Protection for multiple applications
Support for authentication, identification, integrity checks, authorization, input validation, and encoding
Support for fine-grained, flexible and more general authorization
Additional support for symmetric encryption with public algorithms
Support for more general operations
Very flexible and fine-grained enforcement with trusted keys
Support for platform hierarchy (TPM ( hypothetical device) -> Trusted Platform Module -> Platform Module socket) and inclusion (a Security Policy may prevent booting of machines that fail boot verification)
Prevents booting of non-compliant machines
Boot Guard

The combination of a properly designed and implemented security strategy and the proper use of security technologies is essential to obtaining critical System Security. Some organizations are starting to use a digital fingerprint, a measurement that is unique to a user and platform, to achieve a more secure computing environment.

Over two billion TPMs are embedded into PCs, servers, networking gear and other devices. The risks associated with applications are difficult for existing tools to manage and apply. The next generation of computing requires an enhanced and more manageable and applicable design.

Key areas of authentication, identification, integrity checks, authorization, input validation, and encoding are among the most critical risks. Preventing these risks requires a solution that provides both hardware and software protection, more than just encryption. TPM is a unique security solution that enables a more secure method to manage keys, passwords and digital fingerprints to provide platform protection.

NCI TPMs based on the 1.2 specification are compliant with the 1.2 specification. The 1.2 specification is a good standard and we anticipate seeking it for the future. TPM 2.0 is expected to be widely adopted as a high level security enabler through 2016.

The combination of a properly designed and implemented security strategy and the proper use of security technologies is essential to obtaining critical System Security. Some organizations are starting to use a digital fingerprint, a measurement that is unique to a user and platform, to achieve a more secure computing environment.

FlexKey
Integration for Microsoft® Windows 8
Integration for Intel® TXT
Relay for Microsoft® Windows 8
ician for software applications
Support for Swindell and Peck" encryption
Sweep (in development)
Live With Trust
Authentication
Identification and Encoding
Data Protection
Management
Session
Authorization
Access Control/
Authentication
Input Validation
Other

Pocket Secure
Technology already supporting TPM 2.0
Technology already supporting TPM 1.2
Technology already supporting TPM 1.0
NIST T1QI based on the 1.2 specification is compliant with the 1.2 specification. The 1.2 specification is a good standard and we anticipate seeking it for the future. TPM 2.0 is expected to be widely adopted as a high level security enabler through 2016.