



NTRU Core TCG Software Stack

The NTRU Core TCG Software Stack (CTSS) provides the essential core interface and security services framework for any application or platform that relies on the Trusted Platform Module (TPM) as specified by the Trusted Computing Group (TCG).

Features

The NTRU CTSS is designed in accordance with the TCG TSS standard and is enhanced with strong, standards compliant cryptographic libraries. The CTSS provides a set of software components that allows applications and peripherals to take advantage of a platform's TPM hardware module in a coordinated, consistent, and portable manner.

- Fully compliant with TCG specifications and guidance for standard TSS design
- Strong, standards compliant cryptographic services built-in
- Interoperable with all 1.1b compliant TPMs
- Modular design enables addition of custom functionality
- Supports application defined security policies
- Protects authorization data within the local process
- Thread-safe design
- Supports local and remote TPMs
- Design and implementation techniques in accordance with industry best practices for protecting against security vulnerabilities
- Designed for portability with current support for Windows XP/2000 and Linux 2.4 platforms
- Ability to leverage TPM custom features
- Flexibility for future interoperability with TPM 1.2 and the Microsoft Next Generation Secure Computing Base (NGSCB)

Architecture

The NTRU CTSS is comprised of three components: the TCG Service Provider (TSP), the TCG Core Services (TCS), and the TCG Device Driver Library (TDDL).

TCG Service Provider - The TSP is a thread-safe application library that provides the primary application-level interface to the TSS.

- Implements application-defined policy for management of authorization secrets
- Marshals data for TCS
- Manages cryptographic resources within local process

TCG Core Services - The TCS is a Windows system service (daemon, in Linux) that coordinates access to the TPM hardware.

- Accepts connections from both local and remote processes
- Serializes commands to the TPM from multiple processes and threads
- Coordinates secure management of limited TPM resources
- Maintains logs of all operations the platform owner has chosen to audit
- Manages the platform credentials so that the software can prove to remote platforms that it is working with a valid TPM.

TCG Device Driver Library - The TDDL is the hardware driver for the TPM.

- Provides drivers for industry leading TPMs

NTRU CTSS Feature Set

The NTRU CTSS provides the following benefits to developers of trusted applications and peripherals.

Feature	Benefit
TCG standards based design.	The underlying TCG strong hardware security provides higher levels of assurance for new and existing applications.
Designed in strict accordance with the TCG TSS/TPM interface specifications leveraging NTRU's strong TCG standards expertise.	Allows the application developer to focus on their core competencies.
Optimized, industry standard cryptographic services leveraging NTRU's strong cryptographic expertise.	Ensures secure, interoperable implementations.
Designed from the start in accordance with best practices for protecting against malicious activity.	The application developer can have confidence that the underlying API is designed to protect sensitive resources.
Application defined security policies.	Security policies defined to meet the needs of the end user.
Industry standard cryptographic services: RSA encrypt/decrypt OAEP RSA encrypt/decrypt RSAES-PKCSv15 RSA sign/verify RSASSA PKCS1-V1_5 HMAC-SHA1 RFC2202 AES	Time-tested cryptographic services protect your application data.

Trademark Acknowledgement: Windows, etc are the trademarks or registered trademarks of Microsoft Corporation in the USA and other countries. All other trademarks and registered trademarks are acknowledged and remain the property of their respective owners.

