

# Trusted Computing Services



## NTRU: Enabling Trusted Computing

*NTRU Professional Services provides first-class consulting to make secure, cost-effective, market-leading trusted computing products possible*

### The NTRU Advantage

The evolving state of trusted computing standards and products requires vendors to closely monitor the latest developments the standardization process and have an understanding of the intricate relationship between the various components of a trusted computing system. With its deep involvement in the standardization effort and its exceptional record of TCG consultancy, NTRU is the preeminent choice for consulting in trusted computing. The unparalleled security expertise of the NTRU team shortens the development cycle of security products and protects vendors against embarrassing and costly security flaws. NTRU customers can be assured of a secure and correct security design that will be delivered in a professional and timely manner. Through proper security design, NTRU can help minimize development costs, reduce the need for costly future upgrades and avoid the enormous expense of product recalls and redesigns.

NTRU is working closely with Microsoft and other key customers to design compelling products that will facilitate the trusted computing revolution while protecting the privacy of users. In addition, NTRU has been a key development partner in TCG, identifying security and privacy risks in the TPM 1.2 specification and helping to ensure that the related standards support the stated security and privacy goals. Through its ongoing participation in TCG and its continuing work with Microsoft, NTRU will continue to be the leader in security consulting for trusted computing initiatives.

### About NTRU Professional Services

NTRU has a world-class team of cryptographers, security analysts and security engineers who have developed industry-leading security technologies and products. NTRU Professional Services works with customers at every stage of the development cycle, delivering a complete package of consulting services in audit and analysis, architecture and design, and implementation. NTRU's extensive experience includes efforts in trusted computing, security certification, protocol design, security audit and analysis, architecture design and secure cryptographic implementation and integration.

#### TCG expertise including:

- TCG Specifications, architecture and protocols
- TCG user privacy
- TCG Software Stack (TSS) design and implementation
- NGSCB specification, architecture and protocols
- Trusted I/O (TCG and NGSCB)
- Cryptographic standards
- Cryptographic
- Implementation
- Security engineering
- Standard cryptographic protocols
- FIPS 140-2 cryptographic module design and assessment
- Common Criteria component design and assessment



# Trusted Computing Services

2

## NTRU expertise spans trusted computing products including:

- Trusted chipset
- Trusted software
- TPM/TSS
- Input devices
- Display devices
- Biometric devices
- Remote authentication systems

## Enabling Trusted Computing

- Exceptional record of TCG consultancy for blue-chip clients
- Unparalleled expertise shortens development cycle and improves time to market
- Produce secure, cost-effective, market-leading trusted computing products

NTRU consultants have built a strong reputation for ensuring the correctness of security designs. Since 2002, NTRU has been a trusted partner with Microsoft in the development of secure TCG specifications and in Microsoft's broader Next-Generation Secure Computing Base (NGSCB) efforts. NTRU has also led security standardization efforts in basic technology standards groups such as IEEE P1363, ANSI X9 and CEES, and in wireless security standards such as IEEE 802.15.3, IEEE 802.15.4 and ZigBee. In addition, NTRU has assisted customers in the certification process for FIPS 140-2 compliant devices and in developing custom designed embedded cryptographic libraries including both public-domain and proprietary algorithms.

## Trusted Computing

Trusted computing is poised to revolutionize PC and device security. Vendors entering the trusted computing market need security experts that understand the security and privacy requirements of this space as well as the integration issues. NTRU's team of consultants provides timely, secure, and correct design and development services to producers of innovative security products in trusted computing. NTRU shortens the learning curve and enables vendors to quickly and efficiently integrate their security products into this exciting new area.

Trusted computing has historically been the realm of expensive, user-hostile, high security government platforms, but the Trusted Computing Group (TCG) aims to bring this technology into the mainstream. With the availability of PCs containing Trusted Platform Modules (TPMs) conforming to the TCG Main Specification version 1.1b, applications are becoming available that take advantage of an increased trust level in parts of the computer itself. But the arrival of these new PCs does not in itself enable users to take full advantage of the potential in trusted computing. The truly compelling applications will require changes to security service providers, operating systems, motherboards, user input, and user output drivers and devices. Experts in security integration, design and development are needed to ensure that the security components defined in the TCG standard are leveraged correctly to produce secure and trusted components and systems, while protecting the privacy of users. NTRU understands how to unlock the full potential of trusted computing to deliver the greatest value to your customers.

