Trusted Computing: Trusted Platform Policy Management and Strong Authentication

Trusted Computing is on a path from leading edge to mainstream as the number of installed enterprise trusted PCs reaches the tens of millions, as estimated by a leading industry analyst group. Also proliferating is the number of manufacturers offering trusted PC choices. For IT managers, finding a straightforward and unified method for managing the different platform types, tools, and behavior is becoming increasingly complicated.

Businesses and government agencies that purchased these advanced Trusted Computing systems with embedded Trusted Platform Module (TPM) security chips now require a means to effectively administer them. A TPM is a dedicated microchip enabled for security-specific capabilities. Specifications for the TPM have been developed and promoted by an industry standards organization called the Trusted Computing Group (TCG).

Working within the framework of the TCG, Wave Systems has developed the EMBASSY® Trust Suite portfolio of applications and server infrastructure solutions to address authentication, access control, data protection and privacy concerns in the enterprise and in government markets.

Wave’s solution addressing Trusted Computing policy management and strong authentication is called the EMBASSY Security Center. The EMBASSY Security Center manages trusted PC security settings related to setup, user authentication, and backup and recovery.

Features

- **Centralized TPM Management** — Wave’s EMBASSY Security Center facilitates the initial platform setup process, changing the owner password, and setting up or modifying security-based machine policies. TPM platform management features include status information verifying the state of the TPM and installed software.

- **Strong Authentication** — The EMBASSY Security Center contains multifactor authentication capabilities for Windows login, network/domain login, unlock computer, secure application login, and authentication to the TPM. This feature enables users to select from various authentication mechanisms including individual passwords, a master password, biometrics, or any combination thereof. Fingerprint authentication provides an additional level of strong authentication.

- **Robust Password Management** — Streamlined password management is provided by the EMBASSY Security Center through caching and automatic recall of passwords from TPM-secured storage, valuable for securely managing the situations where passwords are required by a Trusted Platform.
• **TPM Key Archive Capability** — A main function of the TPM is to generate keys. When the TPM’s keys are used to encrypt data, the user and enterprise need assurance that the keys are properly backed up for disaster recovery. Backup and restore of allowed TPM keys is also included in the EMBASSY Security Center. For users with Wave’s Key Transfer Manager application installed, the EMBASSY Security Center provides the interface for advanced key management capabilities such as server backup, automated identification and backup of keys, scheduled backup, and individual key viewing and management.

**Benefits**

• **Hardened Security Solution** — By leveraging the intrinsic benefits of PCs with TPMs, the EMBASSY Security Center optimizes security while adding flexibility and convenience to PC users in an enterprise.

• **Interoperable Across Trusted Platforms** — The EMBASSY Security Center enables the enterprise to deploy Trusted Platforms from multiple manufacturers using a single management system. Standardizing on the EMBASSY Security Center reduces support and training costs.

• **Security Policies & User Preferences in One Location** — The EMBASSY Security Center provides centralized management of security policies at the machine and user levels. The robust user security preferences include secure Windows login, simplified password management, fingerprint authentication, and emergency recovery of Trusted Platform keys.

• **Simplified Security** — Additional security many times entails more complexity and even additional passwords to remember. The EMBASSY Security Center’s password management features simplify the usage of secure functions allowing users to select the password behavior desired.

• **TCG 1.2 Support** — In addition to TCG version 1.1b, the EMBASSY Security Center supports Trusted Platforms conforming to TCG version 1.2, the latest Trusted Computing Group (TCG) standard.

• **PC Transfer and Recovery** — When a Trusted Platform malfunctions, whether it is the Trusted Platform Module (TPM) security chip, motherboard, or hard drive, the EMBASSY Security Center has the tools to provide backup and easy recovery so that users can continue to access sensitive data and documents. These same key management functions ease the transition to a new secure PC.

• **Multifactor Authentication** — Based on the familiar three factors of authentication, the EMBASSY Security Center controls secure authentication beyond passwords with the flexibility to combine (1) a password - something you know (2) the TPM security chip - something you have, and (3) a fingerprint - something you are.
Technical Specifications

Supported Platforms:

• Select Intel Desktop Boards
• IBM PCs with the Embedded Security Subsystem
• HP PCs with HP ProtectTools Embedded Security
• Fujitsu Lifebook Notebook PC

Supported TPM Security Chips:

• TCG specification version 1.1b
• TCG specification version 1.2

Supported Operating Systems:

• Windows 2000 (with SP4)
• Windows XP Home Edition (with SP2)
• Windows XP Professional Edition (with SP2)

Supported Biometric Devices - Those containing the following models of sensors by AuthenTec:

• AuthenTec AES3500
• AuthenTec AES4000

Check with your biometric device manufacturer to determine if your device contains one of these sensors or view a listing at http://www.wave.com/products/esc_listing.html.

EMBASSY Trust Suite 4.0

The EMBASSY Security Center is included in Wave’s EMBASSY Trust Suite (ETS) 4.0. ETS 4.0 is a core set of secure client applications and infrastructure services that deliver trusted applications in an intuitive, yet secure, manner. ETS 4.0 delivers a variety of secure business productivity capabilities in an easy-to-understand format, and is compatible with all TCG-Compliant secure hardware platforms.

ETS 4.0 provides extended security features including document protection and collaboration, password management, digital signatures, and robust key management.

To purchase or for more information, please email us at securesolutions@wavesys.com or call us at (877) 228-WAVE. For more information on Wave Systems’ EMBASSY Security Center, please visit http://www.wave.com/products/esc.html.