EMBASSY® Key Management Server

The Solution for Trusted Computing Key Management

For Active Directory

Business applications with advanced security features that follow the Trusted Computing Group (TCG) standard are proliferating. Along with new security chips and applications comes an issue for businesses to provide administration and management for the new trusted systems. Wave Systems' **Embassy Key Management Server (EKMS)** addresses the most pressing infrastructure issue for today's trusted computing marketplace: to provide corporate-level backup and transition of the Trusted Platform Module (TPM) keys, certificates and passwords — also known as ***migration***.

TPM recovery is vital for all businesses and especially for those needing to retain or transfer access to encrypted data. Embassy Key Management Server eliminates the risk of serious data loss in the event that a TPM security chip or hard drive is corrupted, a password is forgotten or if a user leaves the organization. For example, organizations may need access to a former employee's encrypted data or TPM-secured keys for disaster recovery purposes. Security and data integrity must be maintained, while ensuring proper archive procedures and recovery by someone other than the original user. Further, transferring encrypted data to a replacement PC should be fast and straightforward.

Centralized Backup and Migration for Trusted Platforms

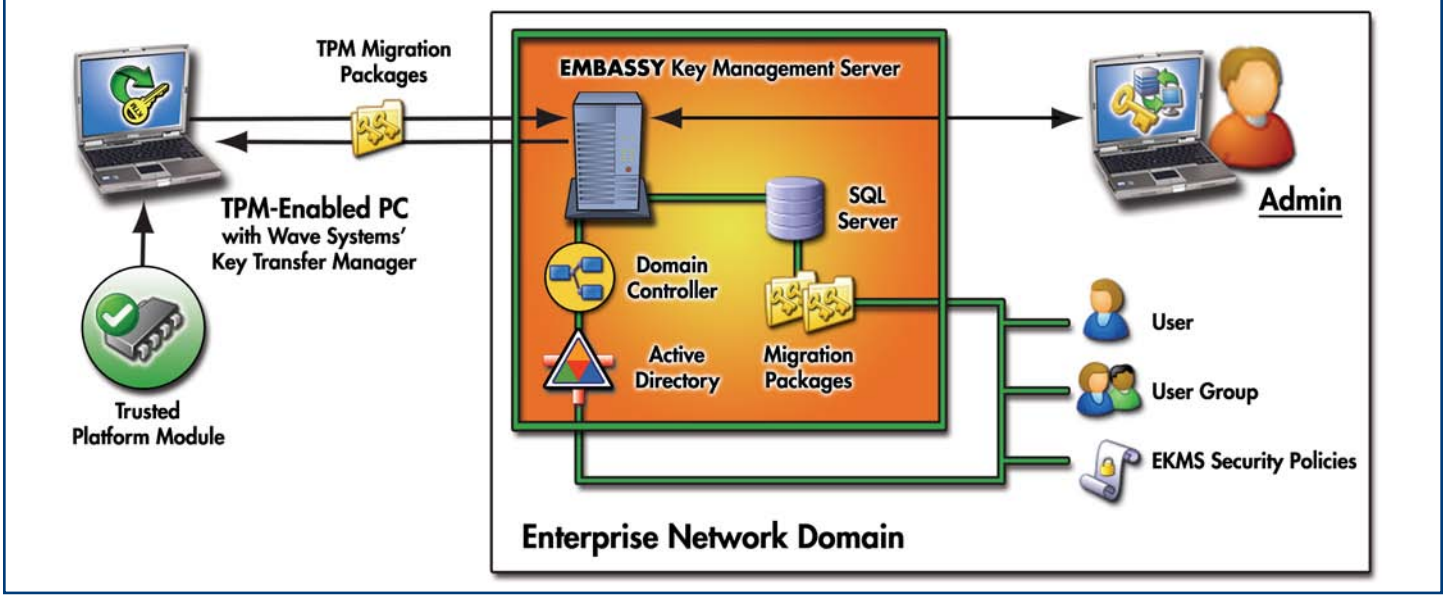
EKMS is a server software product for secure backup and restoration of protected keys from one TPM-enabled system to another, according to security policies defined on the server. The server works in conjunction with client software called **Key Transfer Manager (KTM)**.

The KTM client software formats TPM-secured keys, certificates and passwords into individual migration packages and securely transmits them to the server for storage and subsequent recovery. Retrieval of the archived information requires authorized access based upon the company's security policy settings.

Highlighted Features

- TPM key recovery to the same or different platform with binding to the same or different user.
- Full support of the TCG specifications and all TPM platforms.
- Supports Microsoft's Group Policy software distribution technology.
- Role-based user and user group authorization and administration.
- User-friendly MMC snap-in interface.
- Secure SSL communications from client to server.
- Tight controls over access to stored migration packages.
- Configurable event and audit logging related to migration activities, policy assignments, user enrollment and administrator actions.
- Advanced search functions.
- Summary reporting.

How EKMS Works within an Enterprise Network



EMBASSY® Key Management Server

EKMS gives the user and IT manager a straightforward way to ensure recovery of secure data when need arises. By allowing IT administrators to have control over the backup and security of the data, the business is satisfied that its TPM-secured intellectual property assets are secure and recoverable and that it complies with all data protection regulations.

Active Directory

EKMS uses Active Directory for user authentication and policy management. Access control and authentication is achieved by role-based authentication and is integrated with Active Directory user authentication. EKMS user accounts are one-to-one mapped to domain user accounts where Kerberos, certificate authentication or Windows network login may be chosen. This allows only domain users to have access to the server. User enrollment is automatic upon the system configuration and the user's Active Directory account is mapped to EKMS. Active Directory also stores the references to the user's migration packages.

User group creation and role assignment is supported through the Windows Server 2003 administration tools. Migration packages can be managed for individual users or user groups. Active Directory user group information is directly mapped to EKMS data.

User-to-User Binding

An administrator can designate migration packages to be downloadable by a different authorized user, which is helpful during employee turnover. User to group binding is also supported to facilitate migration package sharing.

Automated Client Setup Options

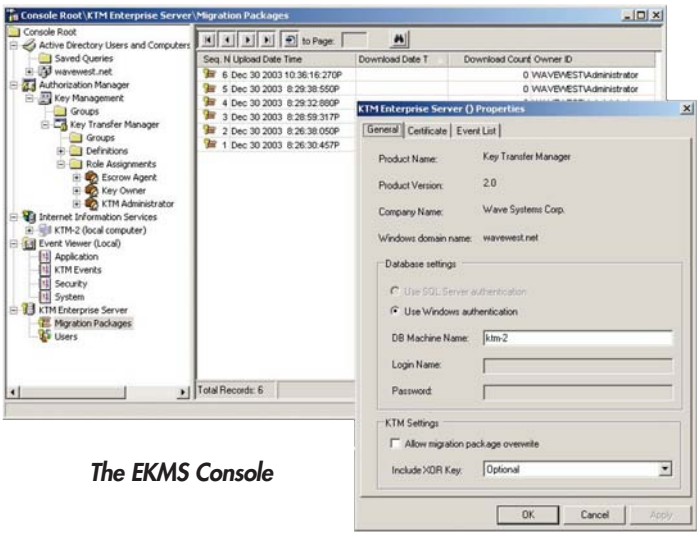
EKMS supports automated software distribution technologies for the client install; such as, Windows Server 2003 Group Policy and Microsoft SMS. EKMS includes unique features so that software administrators can centrally install and manage the client deployments throughout the organization. KTM client software may be installed and configured and can then perform the initial archive silently without user intervention.

Policy-Driven

EKMS is policy-driven and designed to work with trusted platforms and businesses having different security policies. The policy editor allows an administrator to set policies; such as, whether the user can specify a different archive location than the server. Policies are administered through Active Directory and the server policies override client settings.

Easy Administration

The EKMS administrative interface operates through a Microsoft Management Console (MMC) snap-in application. EKMS Administrators are conventional domain members with privileges to execute actions through the EKMS console (see figure below).



The EKMS Console

Technical Specifications

Supported operating system:

- Windows Server 2003 Domain and Active Directory

Software requirements:

- Microsoft® SQL Server or SQL Server Desktop Engine

Recommended hardware requirements:

- 512 MB RAM
- 50 GB hard drive space available
- Pentium or Xeon CPU

wave®

Wave Systems solves the most critical security problems for enterprises and government with solutions that are trustworthy, reliable and easy-to-use while offering a speedy return on investment. Wave's trusted computing solutions include strong authentication, data protection, advanced password management and enterprise-wide trust management services.
Please visit www.wave.com.

Part # 03-000162/version4.03

TRUSTED COMPUTING GROUP

The Trusted Computer Group (TCG) is a new industry group dedicated to embedding trust and security more broadly into computing platforms and devices. The TCG will work to create open standards that can be adopted for use in products and solutions across the spectrum of computing, including devices beyond the PC, to enable secure and trustworthy computing that can protect data, privacy and individual rights.

Wave Systems Corp.
480 Pleasant Street, Lee, MA 01238
tel (877) 228-WAVE • fax (413) 243-0045