

CKM® Workstation

A Comprehensive Security Solution

CKM® Workstation is a standards-based Information Sharing product comprised of a variety of utilities and functions. Data is protected by content, both when in transit or at rest.

By protecting and managing the data object (whether a message, a paragraph, a sentence or a word), information may be segmented with access to the information limited, such as on a Need to Know or Need to Share basis.

Access to information is enforced cryptographically and is based upon the Credentials, or security permissions, that are located on users' Tokens.

About TecSec®, Incorporated

TecSec, Incorporated, founded in 1990, is located in Northern Virginia's technology corridor. TecSec's focus is on Information Assurance and Information Access Management - enforced through cryptography.

TecSec®, Incorporated

1953 Gallows Road Suite 220
Vienna, Virginia 22182 USA

Tel: 703 744 8400

Fax: 703 506 1484

Email: sales@tecsec.com

Web: www.tecsec.com



About CKM Workstation

CKM Workstation consists of the following components:

- CKM Desktop
- CKM Word
- CKM Mail
- CKM Secrypt

Convenient and transparent, the basic CKM Desktop unit contains the CKM Runtime Environment (CKM RTE) and also consists of the following components:

- CKMfile
- CKMclipboard
- CKMweb

(See back for product details)

Features and Benefits

- Protection of Data In Transit and At Rest
- Role Based Access Control to Information (RBAC)
- Cryptographically Enforced Access Management (CEAM®)
- Access to information on a Need to Know basis
- Access to Information on a Need to Share basis
- Flexible Algorithm Selection
- Digital Signature Support
- PKI Interoperability
- Support for PKCS #11 Tokens
- Easy to Use
- Ideal for the "Road Warrior"



CKM Workstation

CKM Workstation consists of the following components:

The CKM® Desktop Suite (CKM Desktop) - Convenient and transparent, the basic CKM Desktop unit contains the CKM Runtime Environment (CKM RTE) and also consists of the following components:

- **CKM®file** is a file encryption tool that provides file level RBAC. This application supports digital signing and verifying of signatures, as well as integration with Microsoft® Outlook® for E-mail attachments. It has a user-friendly and intuitive drag-and-drop interface and includes a secure delete component.
- **CKM®web** is a web plug-in that integrates seamlessly with Microsoft® Internet Explorer. It allows you to decrypt files that have been encrypted using CKMfile and uploaded to the web. CKMweb also provides digital signature verification for files that have been digitally signed. CKMweb lends itself to rapid, broad distribution of confidential information.
- **CKM®clipboard** works with your built-in Microsoft® Windows® Clipboard to encrypt sensitive information. It enables you to cut or copy any kind of data (text, graphics, tables, multimedia files, etc.) from any Microsoft® Windows® program that has Clipboard support (Microsoft® Word®, Microsoft® Excel®, Microsoft® Notepad, Microsoft® Paint etc.), encrypt it and paste it into any other such program.
- **Recent enhancements to CKM Desktop include:**
 - Enhanced Token Management - The former CKM® tokens application has been seamlessly integrated into CKM Desktop. Token management is now being handled within CKM Desktop via a Tokens tab in the CKM Desktop Preferences window, giving end-users the same look, feel and usability as all other components of CKM Desktop.
 - CKM®file - not only allows a user to encrypt a file using Credentials and Certificates but now allows encryption using only a PKI Certificate.
 - CKM®clipboard - allows you to place an ActiveX® object inside of any supporting application as an icon that replaces the ciphertext used in previous releases. The ciphertext functionality is still available for those who prefer to display ciphertext.
 - PKI Interoperability - In addition to Entrust® PKI v6.0, Microsoft® Windows® 2000 PKI, RSA Keon® CA v6.02, Baltimore™ UniCERT v3.5.3, Sun™ ONE Certificate Server v4.7 (formerly iPlanet), Digital Signature Trust, Verisign Managed PKI v5.0 and many more, CKM Desktop is now interoperable with Access Certificates for Electronic Services (ACES) and DoD Interim External Certificate Authorities (IECA).

CKM® Mail - CKM Mail enhances Microsoft® Outlook® where it is well suited to a large network environment providing (1) content protection and (2) access control enforced cryptographically. Sensitive e-mail may be protected both in transit and at rest. Convenient and highly transparent, CKM Mail decrypts an incoming message or attachment with a click, assuming the recipient has the proper permissions (credentials). CKM Mail also provides the ability to digitally sign messages and attachments using assigned Certificates. These Certificates – along with a user's credentials, are located on the user's token.

CKM Mail, whether used to send encrypted messages or encrypted attachments or both, provides a convenient means of Information Sharing on a Need to Know basis.

CKM® Word - Using CKM Word and the common highlighting process, a data object is selected by the user, whether it be the entire message down to a paragraph, a word or even just a character. The credentials of the addressee (defined by the organizational role and responsibilities assigned to the addressee) determine the level of access. Graphic images, tables, media files and even engineering drawings can be protected. Read/write privileges may be differentiated. Parceling data in this manner controls user access, providing varied levels of access based on a user's "security permissions". CKM Word allows you to encrypt portions of the same document using different Credentials so that only those with a "need to know" can access the information they are intended to see - providing Role Based Access Control.

CKM® Secrypt® - CKM Secrypt is a disc encryption product that permits the user to protect sensitive information at rest. By designating one or more Workstation drives or folders as "Secrypt Volumes" all information placed in those Volumes is automatically encrypted using TecSec's standards-based CKM technology. Once a Secrypt Volume is created and an audience is specified for the encrypted content, only users holding the proper Credentials will be able to access and/or share the information contained in this Secrypt Volume. This audience can be redefined simply with the creation of new folders or subfolders. Ideal for use on a laptop by a frequent traveler, the entire memory may be encrypted and not just drives or folders. Thus, stolen laptops will yield nothing to the thief.

