About Constructive Key Management®

Constructive Key Management® (CKM) provides Cryptographically Enforced Management of keys, objects, and access. CKM's Object Level Access Control (OLAC) techniques allow users to control anything that can be named, from a character, page, image or sound in a document to a field in a database. In addition, CKM's Role Based Access Control (RBAC) techniques cryptographically enforce who should be able to see which piece of data or information. The approach of differentially encrypting data based on the need-to-know principle allows secure communication among groups of individuals with a variety of roles. Those individuals who have a legitimate need to view information have access to it, while others don't.

TecSec's Constructive Key Management® (CKM) technology is a standards-based and patented cryptographic key management technology that uniquely resolves critical information security and information management complicated by today's vastly networked world. The need to identify authorized users, protect and control sensitive information assets, and restrict access to information in compliance with privacy statutes and regulations has never been greater.

CKM uses encryption not only to ensure data confidentiality, but also to provide selective access to information. When encrypting with CKM, users label information with *Credentials*, attributes which define the rights required to access the particular information. Users holding matching *Credentials* will be able to decrypt the information, while those who do not have the appropriate *Credentials* will be unable to view that particular information. For example, a document may be labeled Proprietary or Sensitive, and it may also be encrypted with other *Credentials* which further identify who may have access to the information.

Behind the scenes, each *Credential* is associated with a public and private key pair. The public key provides encryption (writing) capabilities. The private key provides decryption (reading) capabilities. When encrypting, each of these assigned *Credentials* (public key values) is combined with other values and random information to construct a key. This key is used with any number of cryptographic algorithms to encrypt the information, and is then destroyed. The same key will never be used again to encrypt other information.

Once encrypted, the information is unreadable until it is decrypted using the same set of *Credentials* (private key values) and the same algorithm. Since CKM immediately destroys the key, it must later reconstruct it to decrypt the information. It does this by using a header that it attaches to the encrypted information, along with other cryptographic data retrieved from the user's Member Profile.

In the header, CKM includes identifiers to the *Credentials* applied, but not the actual values. When decrypting, CKM attempts to retrieve the values needed to build the key from the receiver's set of *Credentials*. If the receiver holds the appropriate *Credentials*, CKM will be able to construct the key needed to decrypt the information. If not, the information will remain unreadable. This process is transparent and requires no instructions or intervention from the user.

CKM technology provides a mathematical method that cryptographically binds different access elements together. These elements can uniquely represent users (identity components), application processes, information, media, business rules and scope. When these various elements or security descriptives are uniquely combined and mathematically proven through cryptography, the goals of content based, role based access and distributed information security can be achieved.

TecSec is a privately held company located outside of Washington DC. Its focus is on Information Security and Secure Access Management of Information - enforced through Cryptography. TecSec's market focus for CKM includes Healthcare, Digital and Asset Rights Management, and Homeland Security and Defense - including the Utilities Sector.