Constructive Key Management® and Smart Token™:

A Comprehensive Overview

MANAGING ENTERPRISE RELATIONSHIPS AND INFORMATION

Table of Contents

SECTION		PAGE
1	Constructive Key Management® (CKM®) Technology: Introduction	3
2	CKM Technology: Administrative Concepts	5
2.1	CKM Domain	5
2.1.1	Trusted Domain Relationships	6
2.1.2	Untrusted Domain Relationships	6
2.2	Domain Authority	7
2.3	Domain Profile	7
2.4	CKM Workgroups	7
2.5	Workgroup Administrator	8
2.6	Workgroup Profile	8
2.7	Member Profile	8
2.8	Profile Storage	8
2.9	CKM Membership Keys	9
2.10	Global Keys	9
3	CKM Technology: The Process	9
3.1	Role-Based Access Control	9
3.2	The Security Paradigm and Data States	10
3.3	Algorithms and Keys	11
3.4	The CKM Combiner Function	11
3.5	The CKM Header	12
3.6	The CKM Session	13
3.7	Identification and Authentication	13
3.8	Revocation of Member Access	13
3.9	Key Recovery	14
4	The Smart Token™	14
5	Asymmetric Key Encryption, PKI, and CKM	15

All Rights Reserved

6 The Power of CKM: Solutions 16
6.1 One-to-Many Distribution 16
6.2 Dynamic Data Separation 17
6.3 Distinct Separate Reality 17
6.4 N-tier Distribution 18
6.5 Flexible Role and Responsibility Assignment 18
6.6 Smart Cards as Physical & Logical Security Device 18
7 CKM and Smart Token: A Comprehensive View 18
Appendix A. Standards 20
Appendix B. Export Considerations 22

List of Figures

FIGURE PAGE
Figure 1.0-1 Protection through Trust and Standards 4
Figure 1.0-2 Smart Token Avenue to Protection through Trust and Standards 5
Figure 2.1.1-1 The CKM Hierarchy 6
Figure 3.1-1 Role Based Access Control Through CKM® 10
Figure 3.4-1 CKM Combiner Function 12
Figure 4.0-1 The Smart Token 15
Figure 6.1-1 A CKM Concept 17
Figure 7.0-1 CKM and Smart Token: The CKM Security Layer 19

Copyright 2010
All Rights Reserved

1 Constructive Key Management® (CKM®) Technology: Introduction

Constructive Key Management (CKM) is a process by which an organization can manage the flow of and access to information at the basic object level. CKM is a cryptographic key management technique that embeds access attributes and other selected parameters within the object itself. The architecture is a flexible key management system that incorporates the strengths of both asymmetric and symmetric encryption elements. Included in the architecture is an encryption key generation process based on key values and asymmetric credentials, a random value process, and an infrastructure to support the distribution and management of the generated elements.

CKM is a key management architecture that can be represented as a symmetric only design, or, with additional asymmetric elements, can be expanded into a more advanced trust model. The latter trust model is based on a suite of financial community standards - the American National Standards Institute (ANSI) standards. The founding standard is X9.69, "Framework for Key Management Extensions" for which the symmetric design and infrastructure architecture is modeled. Inherent in the design is key recovery that allows the System Owner 100% recovery of each encrypted object.

The CKM key management architecture may be viewed as a whole system's identification, authentication, access control, and encryption cycle supported by a management infrastructure.

Some terminology is needed to understand the underlying process. The key used in the encryption of an object is called the Working Key. It may be used as a session key or a message encrypting key that is required by a symmetric encryption algorithm such as Data Encryption Standard (DES). The working key, constructed from several pieces of information (called 'Value'), is used to initialize a symmetric key encryption algorithm, and is then discarded. The same pieces of information used in constructing the working key for encryption are used to reconstruct the working key for decryption. The function that combines the values to create a working key is called the CKM Combiner™ and is central to the CKM encrypting process.

Access control is provided in CKM by applying credentials in the encryption of information. Either symmetric or asymmetric values are associated with each credential depending on the trust design. Read/write separation is cryptographically enforced with an asymmetric key design. Read access is equivalent to decryption rights and write access is equivalent to encryption rights.

In addition to access control, a broader key management strategy may include a configurable identification capability and a third-party trust authentication capability as illustrated in Figure 1.0-1.

All Rights Reserved

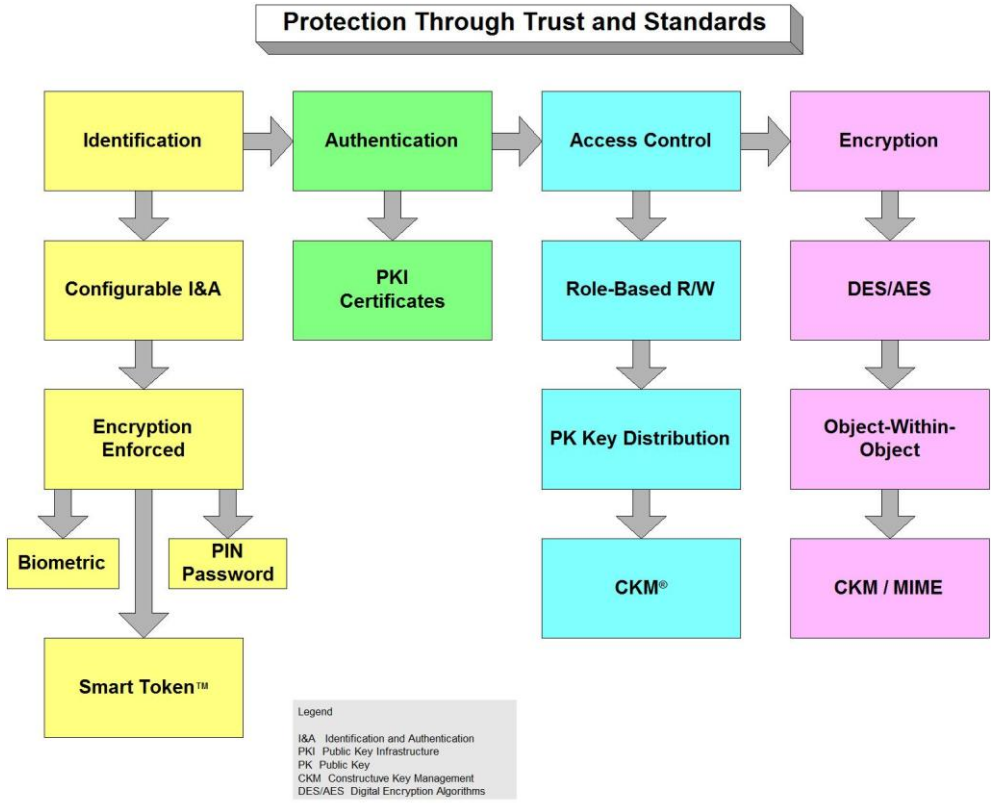


Figure 1.0-1 Protection through Trust and Standards

Credentials may be associated with an application that defines one or more member identity elements such as a biometric function, a Smart Token™ identity, or a PIN/Password. CKM is used to bind the identity elements to an encrypted object through an encryption process. The Identification and Authentication (I&A) object may consist of private keying functions that can authenticate the member to the network and other members, and other functions that may need to be stored secretly that are included in a Member Profile. Once the identity of a member has been established, the member may need to authenticate that identity through a third party trust model referred to as Public Key Infrastructure (PKI). The essential part of PKI is a certificate that includes a verifiable digital signature, which in itself is a mathematical hash of information that is then encrypted through an asymmetric process. The PKI authentication support is managed through a Smart Token™[1]. Figure 1.0-2 illustrates a Smart Token and its interaction with:

1. A configurable I&A process,
2. Two types of asymmetric key pairs identified as Public Key and CKM Membership Key,
3. Non secure applications,
4. Payment functions, and
5. Data that acts on a physical access function.

[1] For a more detailed discussion on the Smart Token™, please see Section 4.

Copyright 2010
All Rights Reserved

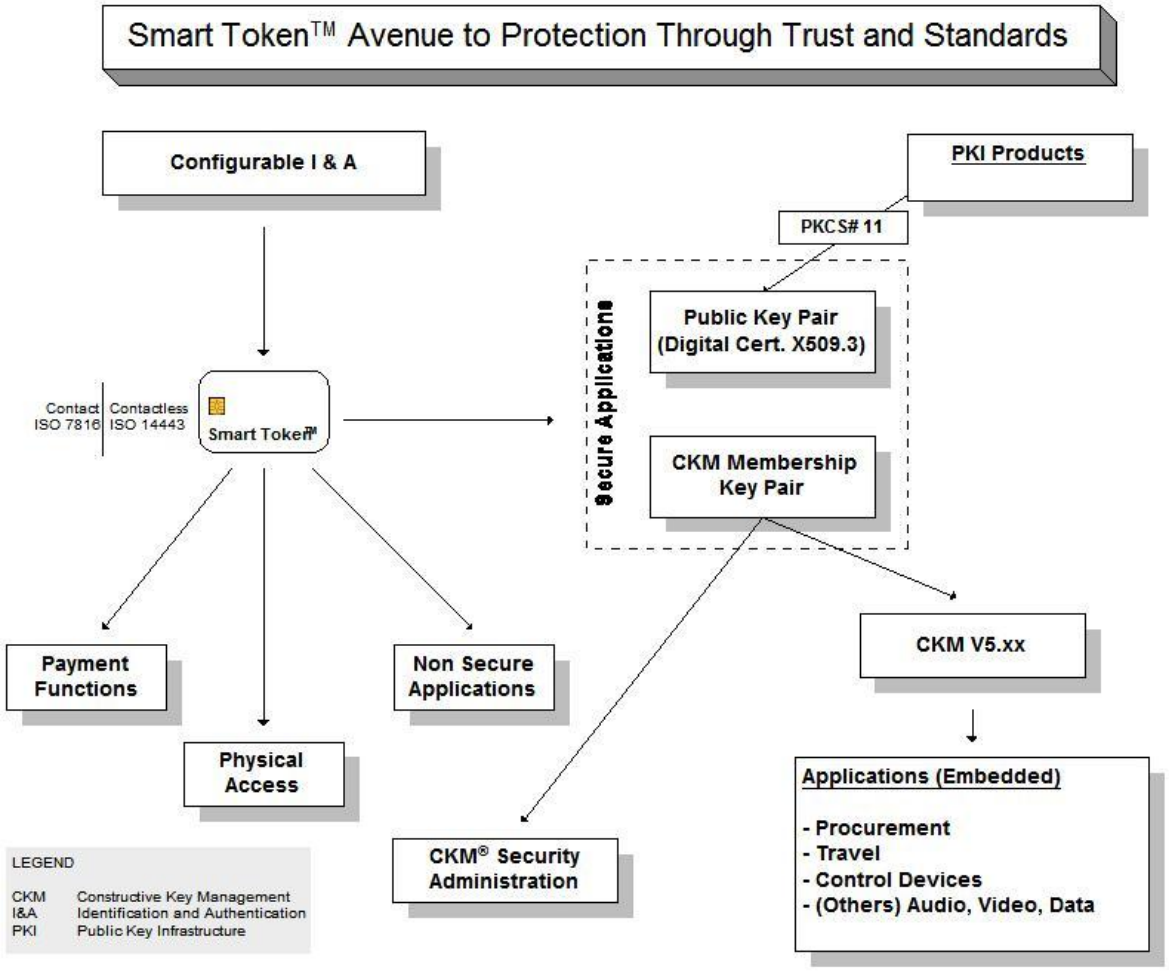


Figure 1.0-2 Smart Token Avenue to Protection through Trust and Standards

The Smart Token is used as a bridge to multiple authentication and encryption platforms with varying degrees of encryption enforcement and binding.

2 CKM Technology: Administrative Concepts

CKM Administration is based on several core concepts that apply to any CKM setup—even if some are made to be transparent. This section provides an introduction to each of these critical concepts. Additionally, concepts that are not strictly required but are very common and aid in understanding CKM administration are also discussed.

2.1 CKM Domain

The highest unit of organization in a CKM System is the 'Domain'. A CKM Domain is a unique, independent entity that includes all CKM resources needed to function on its own. CKM policies, procedures, and roles are all determined at the domain level.

Although it is the largest unit of organization supported within CKM, domains are fully scalable to a wide variety of needs. A CKM Domain may be as large as an entire enterprise or as small as a single member. One type of application might, for example, establish a unique domain for each member installation, while small businesses would likely establish a single domain for the

All Rights Reserved

company, and large enterprises would establish many domains for major divisions, different locations, or other organizational structures.

While domains are freestanding and independent, they do not need to be isolated. CKM Domains may share access rights and privileges with other domains in a trusted relationship. Additionally, members may participate as members of multiple domains even if a trust relationship between the domains has not been established. The CKM Domain may have a direct relationship with a PKI Certificate Authority (CA).

2.1.1 Trusted Domain Relationships

A CKM Domain may provide specified access rights and privileges to members of another domain by establishing a trust relationship. The trust relationship is established when one domain provides a subset of its CKM Credentials to another domain. Credentials are shared only at the domain level and may not be sent directly to members of another domain until a trusted relationship has been established. Once trust has been established, the second domain maintains and distributes "imported" credentials using its own methods and policies, and these credentials are stored in the same Member Profile as the member's normal credentials. Once distributed, members of the second domain may use the imported credentials to share information with members of the external domain; but they continue to be bound by the policies and procedures of the domain in which they hold membership—their LogOn Domain. If a PKI CA is included in the key management architecture, a third-party authentication model may be added to the overall trust relationship.

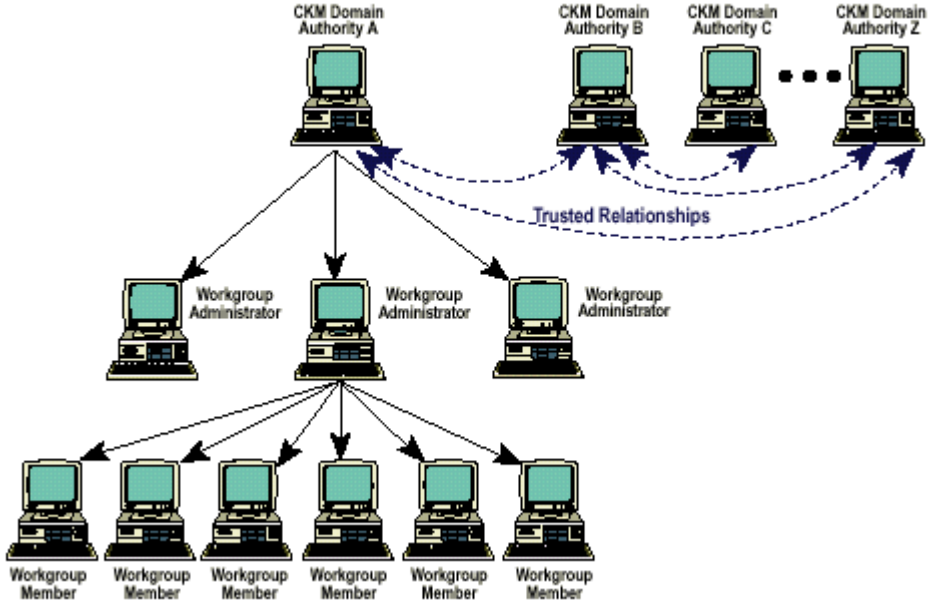


Figure 2.1.1-1 The CKM Hierarchy

2.1.2 Untrusted Domain Relationships

An individual may be a member of several CKM Domains regardless of whether the domains have established a trust relationship. That is, two or more domains may grant membership independently to the same individual. In this case, CKM sees the single individual as several members—one for each domain. In this type of untrusted relationship, the member will log

Copyright 2010
All Rights Reserved

onto each domain independently, use separate Member Profiles for each domain, and be provided credentials to access information only within that domain and with its trusted domains.

PLEASE NOTE: Some storage mediums (such as smart cards with less memory) do not have sufficient space to hold multiple member profiles. Therefore, the ability to log on to multiple domains may not be available in all situations.

2.2 Domain Authority

The Domain Authority (DA) provides top-level management to a CKM Domain. Although some decisions must be made by the person or persons assuming the responsibility of the Domain Authority, many DA functions may be automated.

Typically, the Domain Authority sets up the domain by performing the following functions:

- Names the domain and creates its unique Domain Value (used in cryptographic functions)
- Establishes and updates a Maintenance Value (used to update cryptographic values)
- Sets policy defining the outer parameters of CKM use
- Establishes and digitally signs the role-based credentials used by CKM to cryptographically enforce access control to information
- Selects and optionally renames the cryptographic algorithms available in the domain
- Selects and configures Identification & Authentication objects available in the domain
- Registers workgroups and their administrators through which credentials are distributed (workgroups are discussed later in this document)
- Digitally signs individual membership keys and authorizations related to CKM enrollment
- Registers and digitally signs CKM-enabled applications
- Creates and distributes Workgroup Profiles defining a subset of credentials, algorithm permissions and policy settings available to each workgroup
- Determines trust relationships with other domains

CKM allows members to receive credentials, policy settings, and algorithm permissions only if signed by the Domain Authority—even if some of these values are imported from other domains. Members are bound to the Domain Authority via the DA's CKM Membership Key issued to the member. The DA's CKM Membership Key is then used to verify the DA's signature when receiving credentials and related material.

2.3 Domain Profile

A Domain Profile refers to all credentials, policy settings, and algorithm permissions established by the Domain Authority and available within the domain. The Domain Profile also includes the domain's name and value, the maintenance value, and other information identifying the domain.

2.4 CKM Workgroups

A CKM Domain consists of at least one and usually several workgroups. A workgroup clusters members (or smaller workgroups) based on common needs and rights to information. Workgroups are often established to parallel departments, locations, projects, or other natural organizational subdivisions.

All Rights Reserved

2.5 Workgroup Administrator

Workgroups are typically managed by a Workgroup Administrator (WA). The responsibilities performed at this level may be by a person interacting with software, or may be automated in part or in full. These responsibilities typically include the following:

- Refining policy settings to provide further restrictions than those granted to the Workgroup by the Domain Authority
- Registering the individuals who become the members of the Workgroup
- Assigning subsets of credentials and algorithm permissions available in the Workgroup Profile to individual Member Profiles
- Signing and distributing Member Profile Updates to Workgroup Members

2.6 Workgroup Profile

The Workgroup Profile contains all credentials and algorithm permissions available for distribution to the members of a specific workgroup. It also includes the policies governing the workgroup's use of CKM. Workgroup Profiles may differ from other profiles in the same domain—defining the unique rights and needs of each group. Workgroup Profiles are created by the Domain Authority.

2.7 Member Profile

A Member Profile includes the credentials, algorithm permissions, and enforced policy settings assigned to an individual by a Workgroup Administrator. The Member Profile also includes the individual's private asymmetric CKM Membership Key, used to decrypt profile and other membership information sent to the member by the Workgroup Administrator. The member's "public" CKM Membership Key is retained by the Workgroup Administrator and is not posted for public use as in a PKI. The Member Profile also includes the "public" CKM Membership Keys of the Domain Authority and Workgroup Administrator. Also, it may optionally include one or more PKI individual private keys and digital certificates used for encryption or signing in other cryptographic systems. See Figure 1.0-2.

Members may receive profile and membership information from the single Workgroup Administrator whose Membership Key has been issued in the Member Profile. All updates to Member Profiles are signed by the Workgroup Administrator and must be verified by the WA's CKM Membership Key held by the member.

Members may be assigned to a different Workgroup Administrator only by receiving a new WA Membership Key signed by the Domain Authority. Additionally, credentials may be updated or added to the Member Profile only if signed by the Domain Authority and verified using the DA's CKM Membership Key held by the member. In this manner, each individual is bound to a specified workgroup and a specified domain.

2.8 Profile Storage

A Member Profile may take many forms. It may be stored locally on a member's workstation, on removable storage such as a floppy disk, on a network server, or on a physical token such as a smart card. Storing a Member Profile on a token provides the highest security and portability. The form of the Member Profile is configurable by the DA. One of the policies carried within

Copyright 2010
All Rights Reserved

the profiles determines where profiles are allowed to reside. The form of the Member Profile is also dynamically scalable, i.e. if the profiles are not found in the one location, then CKM will look to the next location until the installed list of locations is exhausted. If a profile is not found in any of the allowed places, then CKM will prevent the member from initiating a session.

2.9 CKM Membership Keys

All persons participating in a CKM system are associated with a unique pair of asymmetric keys known as CKM Membership Keys. These keys are used to insure the privacy, authenticity, and authority of profiles during the CKM Profile Distribution Process.

2.10 Global Keys

CKM provides the ability to interact with other cryptographic and verification services through a Global Key. The Global Key is an asymmetric key generated by CKM or supported third -party Certificate Authority (CA) products or services. When desired, it is used by CKM to digitally sign encrypted information -providing member and message authentication. It may also be used by third -party applications that implement the PKCS # 11 standard.

3 CKM Technology: The Process

3.1 Role-Based Access Control

Under a role-based access control (RBAC) system, rights and permissions are assigned to organizational roles, rather than to each member. Rights and permissions are acquired by members based on their assignment to roles. As members' assignments change, their rights and permissions are changed to reflect their new roles. CKM, with its method of using credentials reflecting information flow and boundaries, is well suited to an RBAC system. Figure 3.1-1 illustrates how the design offers a method to anticipate data boundaries without knowing member identities. The identity process is done prior to the access control process. RBAC is inherent in the access control process.

All Rights Reserved

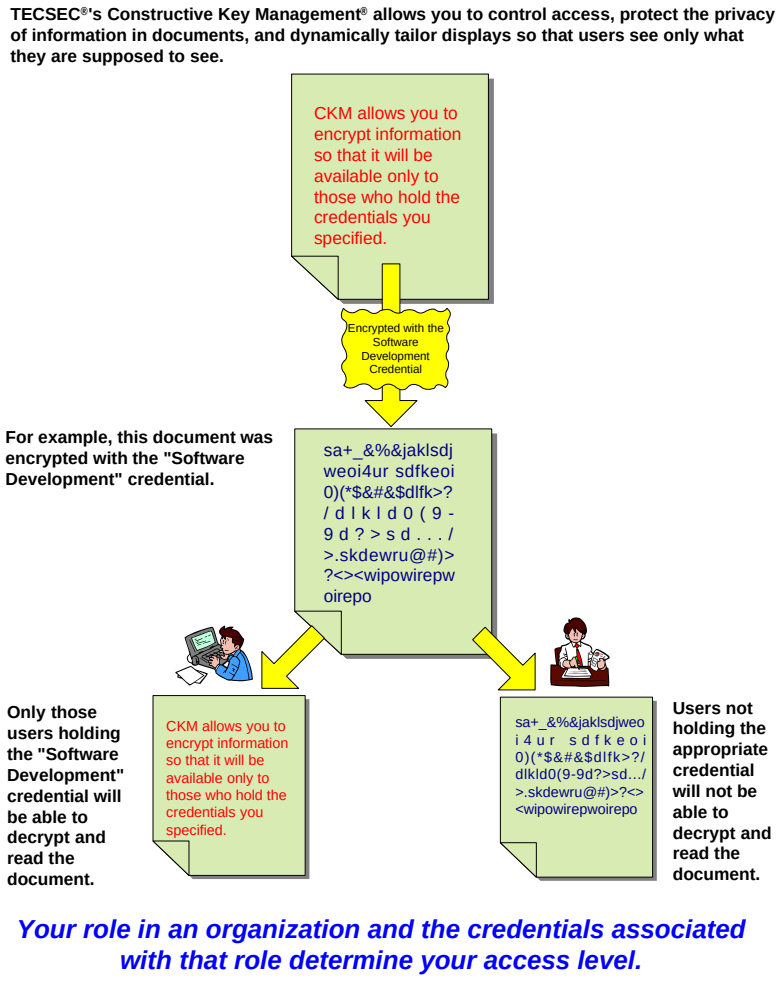


Figure 3.1-1 Role Based Access Control Through CKM®

3.2 The Security Paradigm and Data States

Adequate security is the condition at which protective measures have been employed that reduces risk of loss to an acceptable operational and financial level. Total effectiveness depends on the synergistic interaction of various measures employed that reduce threats and/or vulnerabilities. This synergistic interaction forms a trust model. That is, one security measure alone does not provide adequate security. Only when all are taken together does adequate security result.

Encryption is a tool that mitigates certain vulnerabilities and thus reduces risk. To form an effective information security trust model a member must be bound to data. CKM begins with strong Identification that is bound to the encryption of objects that in turn ensures integrity and access control from encryption to decryption.

Since CKM is client-oriented, the trust model may be scaled to many members: 1) by distributing the workload to member workstations and Smart Tokens, and; 2) by making the encrypted object the basis of trust adjudication instead of a network-based server. The network server is not required for the CKM trust model. Once profiles have been distributed to members, denial of

All Rights Reserved

service is minimized since CKM encryption and decryption is not dependent on network communications for security protection.

Data may be viewed at any given time of being in certain states:

- **Data at rest**: data objects are in a fixed state in a storage capacity. An example of this state is an e-mail file that is managed within a store and forward system.
- **Data in transit**: data objects that are being transmitted in a communication channel during a period of time.
- **Data in process**: data objects that are in static memory areas being manipulated by a computer operating system and/or one or more applications.

CKM can provide a key management and control scheme for various data states. It is a suitable key management and control scheme for both data-at-rest and data-in-transit. Data-in-process security is dependent for the most part on operating system and hardware-based control mechanisms.

3.3 Algorithms and Keys

Cryptographic algorithms (or ciphers) are mathematical formulas that, along with a cryptographic key, render plaintext material or clear communications into an encrypted state and vice versa. A cryptographic key is expressed as a random series of bits of a certain length.

Algorithms are generally referred to as symmetric or asymmetric (public-key). CKM uses both symmetric and asymmetric algorithms.

Symmetric algorithms use the same key for encryption and decryption. They are sub-divided into block ciphers and stream ciphers. Block ciphers process plaintext in groups, often 64 bits (e.g.: DES). Stream ciphers generally process plaintext one bit or character at a time.

Asymmetric (public-key) algorithms use different keys for encryption and decryption. Generally, one key is considered the public key and is posted for others to use as an encryption key or a digital signature verification key. The other key is considered a private key and is held by its owner to be used for decryption and/or digital signature generation.

3.4 The CKM Combiner Function

The role of the CKM combiner is to create a working key from the domain, maintenance, and random values. The combiner process uses a standardized triple DES (3XDES) algorithm. The output of the combiner function is the working key. Figure 3.4-1 illustrates the combiner function.

All Rights Reserved

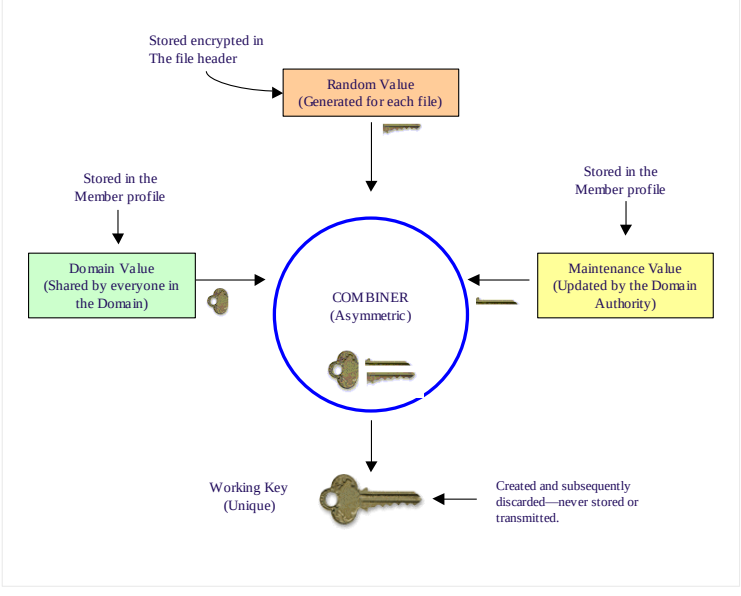


Figure 3.4-1 CKM Combiner Function

The working key is destroyed immediately after an object is encrypted. In order for recipients to be able to decrypt the object, certain information is given to them either within an object header or by a separate channel. The random value is encrypted with the keys generated for each credential selected by the encryptor (originator). It is important to note that it is not possible to recreate the working key solely from information provided in the object header.

The working key is used with a symmetric encryption algorithm such as DES or a future Advanced Encryption Algorithm (AES). Since the working key is destroyed immediately after an object is encrypted, information pointing to specific data required to reconstruct and apply the values, credentials, and other functions are included in an encrypted header. The header encrypting key is managed through the same scheme as the maintenance value, and both can be updated concurrently.

Read and Write access, and the protection of the random value are done through a triple DES process that derives keys from hashing the credentials. If symmetric key cryptography is used for random value encryption, the keys associated with each applied credential are concatenated, in order, and then hashed. If asymmetric key cryptography is used, a Diffie-Hellman static key pair is associated with each credential and subsequent encryption process is done to derive the keying material used to encrypt the random value. The process results in other parameters that are included in the member's profile and an additional level of assurance within the combiner functionality.

3.5 The CKM Header

A CKM encrypted object's header must be available to decrypt an encrypted object. The CKM header contains, among other things, the encrypted random value that was used in constructing the working key.

All Rights Reserved

Since the header is encrypted with a key known to all in the domain, the header of every object encrypted by CKM may be read by anyone in the domain. Note that if public keys are used as Credentials, the random value is not revealed to those who do not have cryptographic Read permission (private value) for all the credentials used.

3.6 The CKM Session

The Domain Authority and Workgroup Administrators may set idle time limits for members. Based on the security risk, the maximum idle time during each CKM session may be centrally controlled. Session idle time limits are included in each member's profile and may not be reset by the member. Generally, the member is required to repeat the identification and authentication process in order to restart a timed out session.

3.7 Identification and Authentication

Identification is the process of identifying the member. Authentication is the process of validating that identity. CKM profiles are encrypted with an identity process. In order to access profiles, members must provide proof of identity. This proof may consist of presenting valid User Identification (UID) along with a correct password. It may also consist of presenting a biometric scan. Authentication occurs at the workstation when valid identification is presented for the profile that was issued by a Workgroup Administrator.

A Workgroup Administrator creates each member's profile. Among the data included in each profile is the member's identification. The member may not change the UID supplied by the Workgroup Administrator. Each time a profile is used to encrypt an object, the identity of the profile used is placed in the header so each recipient may verify the identity of the encryptor. Trust is assumed since only a Workgroup Administrator may issue profiles and only a Workgroup Administrator may designate UIDs.

3.8 Revocation of Member Access

Any cryptosystem must have the means to revoke a member's access. Revocation refers to preventing access to material encrypted subsequent to revocation. It does not refer to preventing access to material encrypted during a member's period of legitimate access. Once the decision to revoke is made, new encryption access denial should be as complete and rapid as security risks warrant. CKM has multiple means to revoke members. The introduction of selected features of a PKI further enhances revocation, especially in higher security environments. The basic CKM revocation methods are listed below:

- Profile time-to-live limits provide a routine, periodic method of removing member access, just as credit cards expire. As profiles expire, they may simply not be renewed.
- Updated maintenance values eliminate access to those without the new value. New maintenance values have backward utility so that material encrypted with a previous maintenance value may be decrypted with a subsequently issued one. The DA may choose to issue a new maintenance value and not give it to certain members, thus revoking their access. This facility is particularly useful in responding to—or preventing—certain security attacks by outsiders and/or former workgroup members,

All Rights Reserved

since all an administrator has to do to forestall such attacks is issue a new maintenance value to all approved members.

- Protected maintenance values may be stored on a particular network directory. Revocation can be executed immediately by simply removing a member's maintenance value from the server.
- Requiring that profiles be stored on a particular network directory means these profiles must be used on the designated directory and nowhere else. Revocation can be executed immediately simply by removing a member's profiles from the server.
- If a PKI architecture is part of the overall security, a Certificate Revocation List (CRL) may be used in the revocation capabilities.

3.9 Key Recovery

Key recovery refers to the ability to recreate or retrieve working keys. CKM technology is unique in that unlike in private key escrow and session key escrow, CKM does not escrow anything. CKM provides the Domain Authority -and to a limited extent the Workgroup Administrator - with the ability to reconstruct all working keys, since the DA created all the system keys, as well as all the credentials. If the header or its equivalent is made available to the DA, the working key can be reconstructed.

This key recoverability of CKM is a critical advantage for two reasons:

First, all organizations need an ability to recover encrypted files when the primary encryption keys have been lost. Modern high strength encryption is virtually unbreakable, so locking up vital intellectual property and then losing the keys means that data would be lost forever. In typical commercial use, employee turnover, computer failures, loss of tokens, and other catastrophes happen to a significant percentage of organizations every year. Thus, it is in the organization's best financial and security interests to have a simple recovery capability in case a workgroup member loses his or her keys. CKM provides a simple key recovery capability.

Second, modern high strength symmetric encryption is subject to government control in many countries. In the United States, the export of strong encryption is regulated. These regulations are continually being revised to address the demands of electronic commerce and national security issues. TECSEC, Incorporated has been granted a unique export license. See Appendix B for more details.

4 The Smart Token™

A smart card is a thin piece of plastic the size of a credit card but with a processor, some memory, and metal contacts so that Input/Output (I/O) can take place. ISO 7816 provides the specification for smart cards. As a CKM token, smart cards store Member Profiles. I/O between an ISO smart card and a workstation is relatively slow, making session logon relatively lengthy. Nevertheless, with the greater storage and processing capability becoming available today, smart cards hold much promise for secure, portable information storage, as well as possessing the advantage of three-factor security (something you know [a PIN], plus something you have [the smart card], plus something you are [biometrics]).

Copyright 2010
All Rights Reserved

Secure storage in the case of a smart card means that data is either stored in a secure area of memory that can only be accessed by the smart card operating system, or data is encrypted with keys stored in a secure area of memory.

Figure 4.0-1 The Smart Token

Smart card tokens are a more secure CKM profile storage option, that provide additional flexibility in terms of the ability to carry portable data (e.g., electronic cash, biological ID templates, etc.), as well as other smart card applications such as debit and credit card accounts, GSM phone card capability, health care information, and other organization-specific applications.

5 Asymmetric Key Encryption, PKI, and CKM

A flexible key management architecture supports Asymmetric Key Encryption, PKI, and CKM. These three technologies offer capabilities that meet the requirements of secure electronic commerce. Encryption can effectively address emerging privacy and liability issues. The closed domain nature of an established CKM encryption boundary within a business interest can separate data and effectively delineate liability.

The inherent features of asymmetric key can offer an encryption enforced Read and Write separation for accessing data and a means to ensure integrity and confidentiality for a member's security profile without a PKI infrastructure. A PKI certificate architecture offers an infrastructure for third-party trust authentication. As an adjunct to the 509v3 certificate are attributes that can be correlated to CKM credentials to provide encryption-enforced access

Copyright 2010
All Rights Reserved

control. The granular, object-based encryption capability of CKM provides confidentiality to objects such as a file or a database. The symmetric properties of CKM can ensure key recovery. Role-based access control can be enforced through CKM and provide a multicast capability to support a group of participants in many-to-many or one-to-many applications.

A business can now select key management methods that more closely reflect their security needs. The response to these demands focuses more on selecting the proper mix rather than selecting between competing encryption technologies.

6 The Power of CKM: Solutions

Cryptography and its related elements are generally viewed as merely a utility, the sole purpose of which is to provide security and confidentiality to data and voice storage and communications. This is true of most cryptographic key management schemes and encryption software applications. However, it is not true for CKM. The ability to selectively encrypt objects within objects and the granting of role-based access to these objects sets CKM apart from other key management methods. CKM attributes provide the basis for solving business communications problems in uniquely beneficial ways.

6.1 One-to-Many Distribution

CKM allows for a one-to-many distribution of encrypted objects when the distributor does not know the identity and related access rights of each of the many, including future members within the domain. This provides the basis for secure broadcast of sensitive material. Secure CKM one-to-many distributions can be used for numerous employee, medical, customer, and vendor applications.

All Rights Reserved

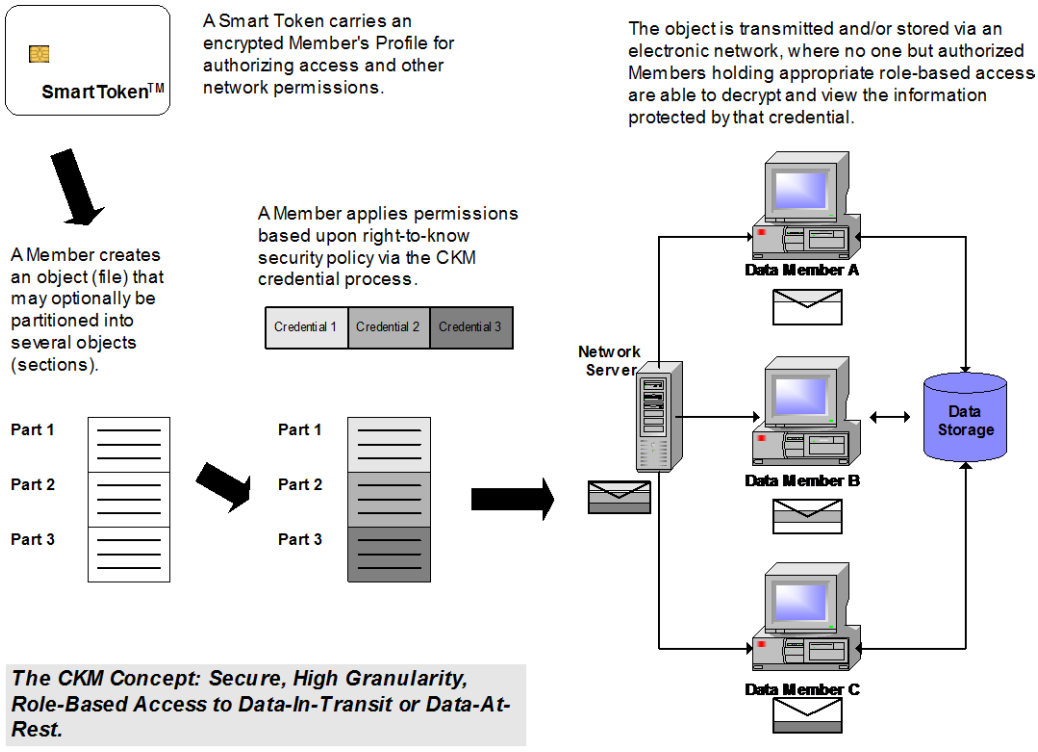


Figure 6.1-1 A CKM Concept

For example, sensitive corporate documents can be encrypted with CKM and placed on a company Intranet web server. Access to each document is based on the access rights within each member's profile. Another example is a confidentiality sensitive database containing medical information. Access would be specifically limited to those with a right to know specific patient information, such as patient identification, financial, current medical condition, and medical history.

6.2 Dynamic Data Separation

CKM separates data cryptographically. Each set of credentials used within a domain separate that data from all other data within the domain. This data separation is enforced cryptographically, but not by separate physical architectures that may tend to be fixed. With CKM, data separation—including layers within layers (objects within objects)—can be dynamically changed to meet organizational requirements regarding information flow and access boundaries. In essence, CKM can provide dynamic, cryptographically enforced private networks within a larger organizational network.

6.3 Distinct Separate Reality

CKM can take one or more encrypted objects and encrypt them within another encrypted object. It is this object-within-an-object that provides CKM with the ability to selectively decrypt objects according to access rights previously given to members.

For example, management desires to post a memorandum to all employees on its Intranet web server. In addition, management wishes to include additional confidential information for Managers. With CKM, the portion of the document intended for all employees would be encrypted with the domain value. The portion of the document pertaining to management

All Rights Reserved

would be encrypted using a credential limited to managers. When employees download and decrypt the document, all employees would view the common information. Managers would also view the restricted information. With CKM, it is possible to have each member view an object or objects and not know their access differs from others.

6.4 N-tier Distribution

Administrative functions may be separated into as many levels as needed for security and workload needs. Organizations may continue to use the included 3-tier system consisting of a Domain Authority, Workgroup Administrators and Workgroup Members, or they may customize this system for more or less separation of functions and levels of distribution. Other organizations may opt to develop a fully customized system implementing services in an entirely different way.

6.5 Flexible Role and Responsibility Assignment

Administrative roles and responsibilities are not bound, a priori, to any level or component. If the standard role assignments of Domain Authority, Workgroup Administrator, and Workgroup Member do not meet an organization's needs, applications may be customized for other assignments. Responsibilities may be moved up or down the distribution hierarchy or roles may be assigned in a completely different manner.

6.6 Smart Cards as Physical & Logical Security Device

Many smart cards are merely extended credit cards. TECSEC believes a higher capacity CKM-enabled smart card called a Smart Token™ will provide organizations with numerous new application possibilities. CKM provides cryptographically enforced separation for all applications.

A member's physical access rights can be encrypted and stored on the card. The card can be used as a key to allow access to sensitive areas in the system. The card can also allow access to software-controlled communications equipment, as well as other equipment requiring limited access such as in certain manufacturing and defense environments. The same card can allow logical access to an organization's information assets. The card can carry a member's CKM profiles and perform the cryptographic key generation process. The card allows for portability and flexibility. A member may move from one computing or access device to another and have appropriate access. Uses for the Smart Token are limited only by card capacity and imagination—all enabled by CKM.

7 CKM and Smart Token: A Comprehensive View

CKM and the Smart Token do not exist in a vacuum. Other parts of the system reside on the member's desktop computer, and on the administrator's computer system elsewhere on the network. Servers are not required by the CKM architecture, but the architecture will accommodate servers easily in the system if required.

All Rights Reserved

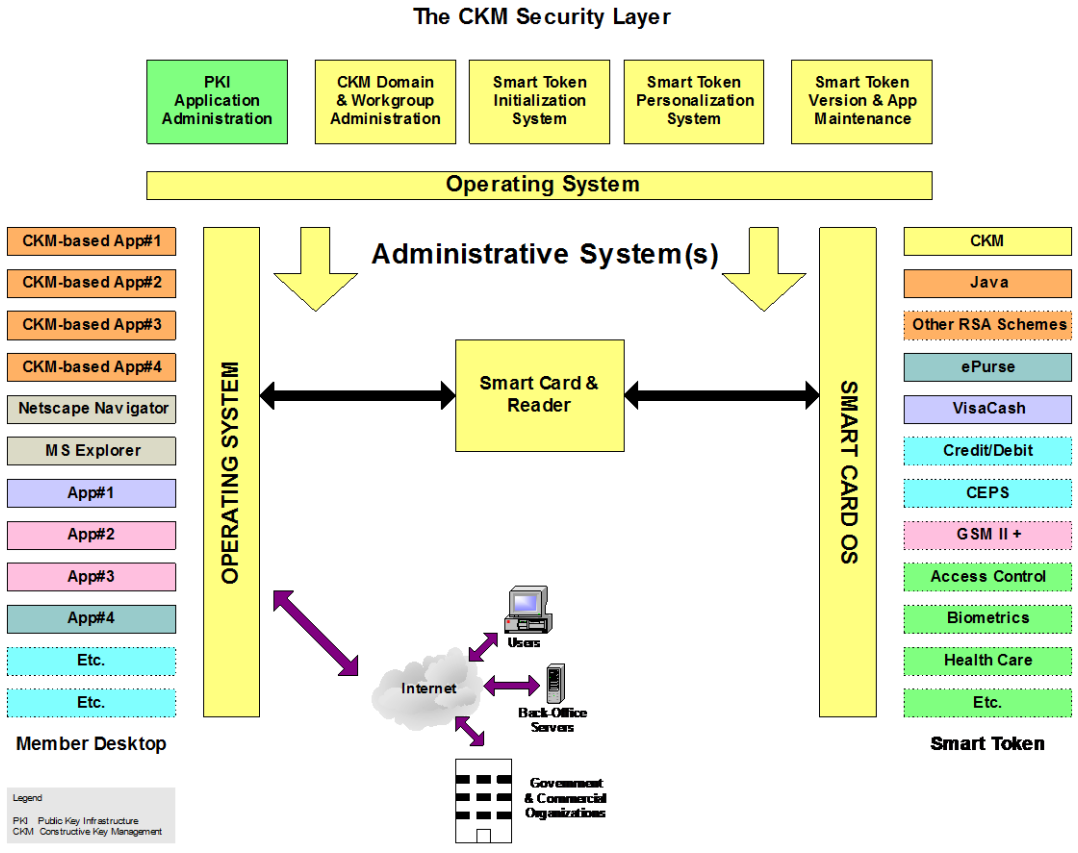
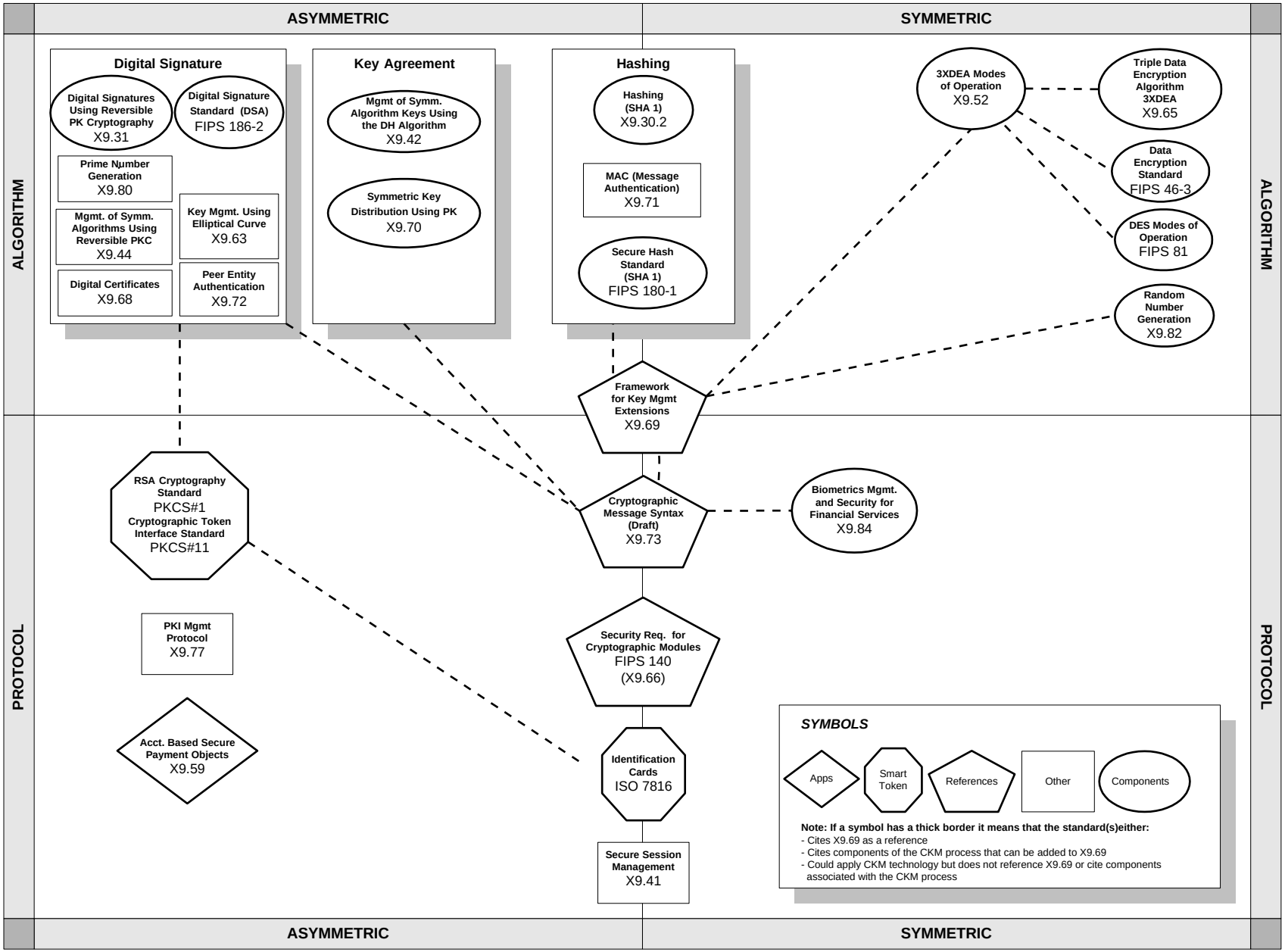


Figure 7.0-1 CKM and Smart Token: The CKM Security Layer

Appendix A. Standards



Copyright 2010
All Rights Reserved

Standards

FIPS 46-3 - Data Encryption Standard
FIPS 81 - DES Modes of Operation
FIPS 140 - Security Requirements for Cryptographic Modules (X9.66)
FIPS 180-1 - Secure Hash Standard (SHA1)
FIPS 186-2 - Digital Signature Standard (DSA)

ISO 7816 - Identification Cards

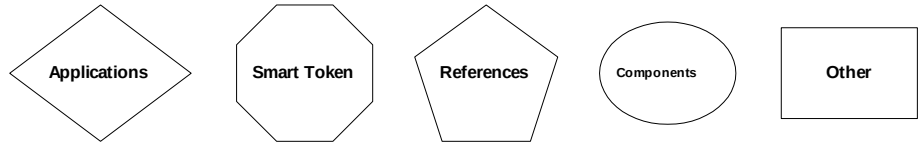
PKCS #1 - RSA Cryptography Standard
PKCS#11 - Cryptographic Token Interface Standard

X9.30.2 - Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry, Part 2: The Secure Hash Algorithm (SHA)
X9.31 - Digital Signatures Using Reversible PK Cryptography
X9.41 - Security Services Management for the Financial Industry
X9.42 - Management of Symmetric Algorithm Keys Using the Diffie-Hellman Algorithm
X9.44 - Management of Symmetric Algorithm Keys Using Reversible Public Key Cryptography
X9.52 - Triple Data Encryption Algorithms Modes of Operation
X9.59 - For the Financial Services Industry: Account Based Secure Payment Objects
X9.63 - Key Agreement and Key Management Using Elliptic Curve - Based Cryptography
X9.65 - Triple DEA Implementation
X9.68 - Digital Certificates for High Transaction Volume Financial Systems
X9.69 - Framework for Key Management Extensions
X9.70 - Symmetric Key Distribution using Public Key
X9.71 - MAC - Message Authentication
X9.72 - Peer Entity Authentication Using Public Key
X9.73 - Cryptographic Message Syntax
X9.77 - PKI Management Protocols
X9.80 - Prime Number Generation
X9.82 - Random Number Generation
X9.84 - Biometric Information Management and Security

Acronyms

3XDEA - Triple Data Encryption Algorithm
CKM - Constructive Key Management
CMS - Cryptographic Message Syntax
DEA - Data Encryption Algorithm
DES -Data Encryption Standard
DH - Diffie-Hellman
FIPS - Federal Information Processing Standards
IEEE - Institute of Electrical and Electronics Engineers
IETF - Internet Engineering Task Force
IPSec - Internet Security
ISO - International Organization for Standardization
LDAP - Lightweight Directory Access Protocol
MSP - Message Security Protocol
NCITS - National Committee for Information Technology Standards
PKCS - Public Key Cryptography Standards
PK - Public Key
PKI - Public Key Infrastructure
PKIX - Internet Public Key Infrastructure
SET - Secure Electronic Transaction
SHA - Secure Hash Algorithm
S-HTTP - Secure HyperText Transfer Protocol
SSL - Secure Sockets Layer

Symbols



Note: If a symbol has a thick border it means that the standard(s) either:
- Cites X9.69 as a reference
- Cites components of the CKM process that can be added to X9.69
- Could apply CKM technology but does not reference X9.69 or cite components associated with the CKM process

All Rights Reserved

Appendix B. Export Considerations

The White House recently announced a relaxation of US encryption export policy. Although specific regulations have not been issued, the following rules are anticipated.

After a one time review and approval, products with up to 128-bit (symmetric) key length may be exported without restriction to customers in most countries. There are some restricted country destinations, mostly for national security reasons. An annual reporting to the US Department of Commerce listing the identity of foreign purchasers may be required.

Since CKM encryption technology features 100% key recovery by the system owner, TESCEC has been granted an unrestricted export license for its CKM-2000 product line -except to prohibited country destinations. TECSEC's CKM-2000 family of products uses Triple DES algorithms and up to 392-bit (symmetric) key length. Based on CKM's 100% key recovery feature, it is believed that future CKM products, after one-time product reviews, may be exported with any key length and any algorithm.

All Rights Reserved