TecSec® CKM® - A Simple Solution to Enterprise Management of Access Control to Information

Electronic Data in Healthcare—Streamlined Processes and Improved Quality of Services

The use of electronic mechanisms to store and transmit information is quickly becoming the standard across healthcare organizations. Paper records and forms are being replaced by electronic forms and applications, which use intranets (internal to organizations), extranets (between organizations) and the Internet (multiple organizations) as the mechanisms to transmit information.

The use of electronic mechanisms offers an organization much potential for cost savings through improved efficiency and enhanced quality of healthcare due to more accurate and timely information that is accessed by healthcare professionals. The Internet offers a unique opportunity for healthcare organizations to transmit electronic information such as patient information, electronic medical records, enrollment verifications and claims. In addition, electronic information in storage can be more easily accessed than paper information.

The use of electronic mechanisms can contribute to an organization's competitive advantages through streamlined business processes and improved quality of healthcare services to patients. The challenges for the organization are the ability to use electronic mechanisms in a secure manner and to protect patient information.

The Health Insurance Portability and Accountability Act (HIPAA)

The clock is ticking—do you have your HIPAA compliance solution in place?

The HIPAA Privacy (Final) and Security (Draft) Regulations cover the following requirements for the protection of patient information:

- Healthcare plans must obtain consent from patients about the release of medical information;
- Patients have the right to see their records and to request corrections;
- Health Plans and Providers must have administrative systems in place to protect health information;
- Information systems must protect data in transit and data at rest; and
- Access to data is based on a user's "need-to-know".

TecSec's Constructive Key Management® (CKM®) Technology, a Proven Information Security Solution for Healthcare Organizations, is a scaleable and proven solution for protecting electronic

data in transit and at rest. CKM® satisfies the information security requirements delineated in the Department of Health and Human Services (DHHS) proposed rule as described below:

SECURITY REQUIREMENT	CKM® SOLUTION
Access Control	Provided through Role Based Access Control (RBAC) that is "bound" to data at the object level with cryptography
Data Confidentiality	Access to each object is controlled by the data owner
Protection of Data in Transit and at Rest	Provided through RBAC to data at the object level that is persistent with the data
Authorization Controls	Provided through RBAC that is "bound" to data at the object level with cryptography
Data Authentication	Provided through Message Authentication Codes (MACs) used by CKM®
Entity Authentication	Provided by storing X.509v3 Certificates on CKM® Smart Token™
Electronic Signature	Provided by storing X.509v3 Certificates on CKM® Smart Token™ for Digital Signatures

TecSec's CKM® technology and methodology provides the means by which data and information can be protected in transit and at rest, at the object level, using cryptography. The technology is robust and scaleable to address a multitude of users and file-content types. This technology is designed to permit access to specific data/information to individuals who possess the necessary credentials (i.e., individuals holding the necessary organization-issued "authorizations" for access to the portions of the data/information of interest).

A user's credentials are included in his or her member profile and stored on an organization-issued token. The token can be soft (software) or hard (smart card, key fob, etc.). The organization designates individuals to manage credentials and tokens by using TecSec's CKM Enterprise Builder® Administration System. Users with the proper credentials will have the ability to decrypt and/or encrypt only those subsets of data/information in the repository that are required by virtue of their roles.

BENEFITS OF CKM®

The use of CKM® technology in an automated process provides the following key benefits within an organization:

- Streamlined business processes
- Processing efficiencies and improved quality of service to patients
- Access to information by healthcare professionals in "real-time"
- Data confidentiality that is determined and managed by the data owner

- Secure access to sensitive information by only those individuals who have a "need to know"
- Compliance with Congressional Regulations

Additional benefits realized by an organization using the CKM® technology are listed in the table below:

BENEFITS REALIZED	CKM® TECHNOLOGY
Integrated Enterprise Information Security and Information Management	The data owner controls access to information, based on roles, in a distributed environment.
Centrally Controlled, yet Distributed, Administration	The organization can control the environment and delegate local administrative privileges across the enterprise.
Role Based Access Control through Cryptographically Enforced Access Management	The organization can define fine-grained access control, at the object level, for data and information.
Enterprise-wide Scalability	The organization can remotely manage tokens across the enterprise in a distributed environment.
Built-in Cryptographic Key Recovery Key	Key and data recovery is controlled solely by the organization.
X.509v3 Digital Certificate Support for PKI Integration, Digital Signature Creation and Verification	The organization has the flexibility to choose which processes and X.509 certificates to use for identification and authentication (I&A) as well as for non-repudiation.
Standards -based	The organization can be assured that the technology has been through the peer review of ANSI.

TecSec's Innovative and Unique CKM® Technology is Robust and Scalable to Address Enterprise - Wide Data Privacy and Confidentiality Challenges.

For more information, please contact us at info@tecsec.com or visit us on the web at www.tecsec.com