TecSec's CKM® – Enabling Secure Information Sharing & Collaboration

Collecting, analyzing and disseminating terrorism intelligence, sharing that information securely and collaborating with a large number of agencies is not a simple task. TecSec's CKM® can help with the tasks of secure Information Sharing and Collaboration.

CKM®, short for Constructive Key Management®, is a technology and methodology that enables secure information sharing and collaboration. CKM provides a framework for secure information sharing across agency lines. It provides Role Based Access Control to information and protects that information while in transit and at rest – regardless of transport and storage mechanism – enabling a collaborative threat warning process.

Permissions, referred to as Credentials, are attached to information. Access to that information is provided on a need-to-know and need-to-share basis as defined by the organization. Roles are determined by the system owner and can be designed to meet existing organizational structures and are flexible to accommodate ad-hoc groups or Communities of Interest.

CKM – A PROVEN SOLUTION

TecSec's Constructive Key Management® (CKM®) technology is a standards-based cryptographic key management technology. It is inherent to ANSI standard X9.69 (Framework for Key Management Extensions) and X9.73 (Cryptographic Message Syntax) and was designed in compliance with other industry standards. CKM is compatible with all leading Public Key Infrastructures (PKIs). TecSec's sixth generation CKM products are currently in the NIAP validation process at EAL2 augmented for Basic Robustness (as outlined in recent DoD Instruction 8500.2 – Information Assurance Implementation).

CKM is a proven solution that is being used to protect information and access to that information. For example:

- CKM technology is currently being employed as a solution for Critical Infrastructure Protection of SCADA systems—both for the Department of Energy and the Department of Homeland Security. Further, TecSec is part of a team supporting the American Gas Association (AGA) and the Gas Technology Institute (GTI) in developing the AGA 12 Report—a recommended practice for Cryptographic Protection of SCADA communications.
- TecSec is also part of the team recently awarded the US-Visit contract, which will provide an integrated, automated system to track pre-entry, entry, status management, and exit of visitors at air, land, and sea ports of entry. The system will enable authorized law

TecSec Incorporated
www.tecsec.com
Copyright 2010

Page 1
Proprietary

November 16, 2008
TSWL027
All Rights Reserved

enforcement and intelligence personnel to access entry and exit data, as well as reports and actions on foreign nationals who have overstayed their legal duration.

- CKM technology is a standard for the network of the federal agency administering Medicare/Medicaid, CMS (Centers for Medicaid and Medicare Services). Incoming and outgoing personal healthcare information (and stored data) that must meet the Privacy and Confidentiality requirements of HIPAA (Health Insurance Portability and Accountability Act) is becoming CKM protected.

- Boeing Digital Cinema (BDC). The technology and software is used to protect digital movies through the content distribution system.

ABOUT TECSEC

TecSec®, Incorporated, founded in 1990, is a privately held company located just outside of Washington, DC. Through a large library of patents and still growing intellectual property, TecSec provides: (1) Information Assurance products for the network and desktop, (2) Information Management and Dynamic, Assured Information Sharing through cryptographically enforced Role Based Access Control (RBAC) and (3) CKM Enabled® Solutions, for example, for Digital Rights Management (e.g. secure distribution of Hollywood movies) and for Critical Infrastructure Protection (e.g. SCADA, Utilities).

SUMMARY

In summary, CKM® addresses the challenges of secure Information Sharing and Collaboration and provides:

- Differentiated Role Based Access Control to information on a need-to-share and need-to-know basis – enforced through cryptography
- Content Protection at the Object Level
- Protection of information in transit and at rest – regardless of transport mechanism or storage device
- Available on-line and off-line
- Secure communication and collaboration for Communities of Interest

AN EXAMPLE OF SECURE INFORMATION SHARING AND DISSEMINATION

A threat is received at the Federal Level and analyzed. A Threat Alert needs to be dispersed to all agencies and accessed on a need-to-know and need-to-share basis.

TecSec Incorporated
www.tecsec.com
Copyright 2010

Page 2
Proprietary

November 16, 2008
TSWL027
All Rights Reserved

Different Access Control Credentials are applied to different parts of the Threat Alert.

The Threat Alert is distributed to all agencies - only those recipients with the proper Roles & Permissions will be able to access all or part of document.

TecSec Incorporated
www.tecsec.com
Copyright 2010

Page 3
Proprietary

November 16, 2008
TSWL027
All Rights Reserved