**ITBUSINESSEDGE**
YOUR TECHNOLOGY INTELLIGENCE *AGENT*

QuinStreet ●●● 10400 Linn Station Road, Suite 100 ●●● Louisville, KY 40223

# Framework for Designing Cryptographic Key Management Systems

This Framework for Designing Cryptographic Key Management Systems (CKMS) is a description of the topics to be considered and the documentation requirements (henceforth referred to as requirements) to be addressed when designing a CKMS. The CKMS designer satisfies the requirements by selecting the policies, procedures, components (hardware, software, and firmware), and devices (groups of components) to be incorporated into the CKMS, and then specifying how these items are employed to meet the requirements of this Framework.

A CKMS consists of policies, procedures, components and devices that are used to protect manage and distribute cryptographic keys and certain specific information, called (associated) metadata herein. A CKMS includes any device or sub-system that can access an unencrypted key or its metadata. Encrypted keys and their cryptographically protected (bound) metadata can be handled by computers and transmitted through communications systems and stored in media that are not considered to be part of a CKMS.

Included in this ZIP file are:
- Intro Page.pdf
- Terms and Conditions.pdf
- Designing Cryptographic Key Management Systems.pdf