



PCI Compliance Whitepaper

Publication date: July 27th, 2009



© Copyright 2007-2009, LINOMA SOFTWARE

LINOMA SOFTWARE is a division of LINOMA GROUP, Inc.



Table of Contents

Introduction	3
Crypto Complete Overview	4
PCI DSS and Crypto Complete	5
PCI DSS 3.3	5
PCI DSS 3.4	5
PCI DSS 3.5	6
PCI DSS 3.6	7
PCI DSS 3.6.1	7
PCI DSS 3.6.2	7
PCI DSS 3.6.3	8
PCI DSS 3.6.4	8
PCI DSS 3.6.5	8
PCI DSS 3.6.6	9
PCI DSS 3.6.7	9
PCI DSS 10.0	10
Crypto Complete Key Hierarchy	11
About Linoma Software	13

Introduction

The Payment Card Industry (PCI) is a coalition of credit card companies including American Express®, Discover®, MasterCard® and Visa®. The PCI has created a Data Security Standard (PCI DSS) which details the security requirements for credit card merchants, service providers and processors. Any organization that stores, processes or transmits cardholder data is required to comply with the PCI DSS.

If cardholder data is accessed by unauthorized individuals, an organization may be subject to the following liabilities and fines associated with non-compliance with PCI DSS:

- Punitive fines for non-compliance with PCI DSS.
- All fraud losses incurred from the use of the compromised account numbers from the date of the compromise forward.
- Cost of re-issuing cards associated with the compromise.
- Cost of any additional fraud prevention/detection activities required.
- Potentially the revocation of an organization's merchant account, resulting in their inability to process future credit card transactions.

In response to the increasing cases of stolen and lost cardholder data, the PCI DSS has been enhanced with stringent security requirements. To view the latest version of the PCI DSS, visit the URL of <https://www.pcisecuritystandards.org>

A helpful self-assessment questionnaire has also been developed by the PCI, which is also available on their web site . This questionnaire will help an organization determine how well they are complying with the PCI DSS.

The PCI DSS is multifaceted with requirements for security management, policies, procedures, network architecture, cryptology, key management and other protective measures. This whitepaper focuses on the portions of the PCI DSS which address cryptology (encryption) and key management for protecting cardholder data.

Crypto Complete Overview

Crypto Complete is a comprehensive solution for protecting sensitive data on the IBM System i (iSeries) through strong encryption technology, integrated key management and audit trails.

The design of *Crypto Complete* allows organizations to implement encryption quickly using intuitive screens and commands, while providing a high degree of protection. Every effort has been made in *Crypto Complete* to minimize the application changes needed, allowing an organization to implement encryption successfully for less time and money.

Data encryption has traditionally been very difficult and time-consuming to implement. In the past, major application changes were required to expand database field sizes and implement complicated API calls to encrypt/decrypt data. Additionally, organizations were not meeting stringent Key Management requirements by not properly securing and controlling their encryption Keys.

Crypto Complete Features

Crypto Complete includes the comprehensive features needed to satisfy stringent requirements for encryption and key management. The primary capabilities of *Crypto Complete* are:

- Automated encryption of database fields within System i database files
- Encryption of System i files, objects and libraries (backup encryption)
- Encryption of files located on the Integrated File System (IFS)
- Integrated Key Management
- Rotation of encryption keys without having to re-encrypt existing data
- Encryption of small database fields without requiring field expansion
- Encryption of both alphanumeric and numeric database fields
- Decryption of fields as full values or masked values
- Strong encryption with key lengths up to 256 bits
- Compliance with Advanced Encryption Standard (AES) and Data Encryption Standard (TDES)
- Intuitive i5/OS menus and commands with on-line help text
- Program calls and ILE procedures (APIs) for encrypting/decrypting data within native applications
- Stored procedures and SQL functions for encrypting/decrypting data through SQL
- Restrict programmers from accessing decrypted values, even if they have *ALLOBJ authority
- Security alert messages to email addresses, message queues and journals
- Comprehensive audit trails and reporting
- Support for multiple environments

PCI DSS and Crypto Complete

Specific sections in the PCI Data Security Standard (DSS) focus on the cryptology and key management requirements for organizations. The wording of these DSS sections is listed in the following pages. For each section listed, a response is indicated on how *Crypto Complete* addresses the requirement.

PAN is the abbreviation for *Primary Account Number*. This is the account number associated with a credit, debit or charge card. This is usually the same as the number on the card.

PCI DSS 3.3

Requirement

3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).

Response

Using *Crypto Complete's* granular authority controls, you can indicate which users (or groups) have access to the full PAN and which users have access only to the masked PAN. When defining the PAN's field settings in *Crypto Complete*, you can specify the formatting of its masked value. For example, a mask can be specified to show only the last four digits (e.g. *****1234) or first six digits (e.g. 485620*****). All other digits can be substituted with a special character such as an asterisk.

PCI DSS 3.4

Requirement

3.4 Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs) by using any of the following approaches:

- One-way hashes based on strong cryptography
- Truncation
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key management processes and procedures.

The MINIMUM account information that must be rendered unreadable is the PAN.

Response

Crypto Complete provides strong cryptology (encryption) for protecting data on System i. The popular cryptology standards of Advanced Encryption Standard (AES) and Triple Data Encryption Standard (TDES) are provided in *Crypto Complete*.

The AES and TDES standards are widely used throughout the corporate and government sectors for encrypting sensitive data. The *National Institute of Standards and Technology (NIST)* also approves the AES and TDES standards for protecting top secret information within the federal government.

Although PCI DSS does not specifically state the cryptology standards which must be utilized, most organizations are using AES cryptology to protect credit card information. AES is the latest

Crypto Complete

encryption standard (approved by NIST in 2001) and offers strong protection (using keys up to 256 bits in length) with good performance.

Crypto Complete also includes a comprehensive key management solution for System i. This key management solution allows organizations to perform the following:

- Establish policy settings on how Symmetric Keys can be created and utilized
- Indicate which users can create and manage Symmetric Keys
- Randomly generate strong Symmetric Keys
- Protect Symmetric Keys using Master Encryption Keys
- Protect the recreation of a Master Encryption Key by requiring passphrases from up to 8 users
- Organize Symmetric Keys into one or more Key Stores
- Restrict access to Key Stores using i5/OS object authority
- Restrict the retrieval of the actual Symmetric Key values
- Provide separation of duties (i.e. the creator of a Symmetric Key can be restricted from using the Key to encrypt and/or decrypt data)
- Control which users can utilize Symmetric Keys to encrypt and decrypt data

PCI DSS 3.5

Requirement

3.5 Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse.

3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary

3.5.2 Store cryptographic keys securely in the fewest possible locations and forms

Response

Crypto Complete includes a comprehensive key management solution for System i. This solution allows an organization to indicate the Key Officers (Custodians) which are authorized to create and manage Master Encryption Keys (MEKs) and Data Encryption Keys (DEKs).

A Master Encryption Key (MEK) is a special Symmetric Key used to protect (encrypt) the Data Encryption Keys (DEKs). An organization can create up to eight MEKs per environment on the System i. A MEK is generated by the product using passphrases entered by designated users. Depending on the organization's key policy, up to eight different passphrases can be required to be entered (by different users) in order to generate a MEK.

The encrypted Data Encryption Keys (DEKs) are contained within Key Stores. Each Key Store is created as a *VLDL (Validation List) object on the System i.

An organization can control access to the Key Store *VLDL object using i5/OS object security. Object *Change authorities can be granted only to those users that are allowed to manage the keys within the Key Store. Object *Use authority can be granted only to those users that are allowed to use the keys (for encrypting/decrypting data) within the Key Store.

Crypto Complete

PCI DSS 3.6

3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:

PCI DSS 3.6.1

Requirement

3.6.1 Generation of strong cryptographic keys

Response

Crypto Complete allows the creation of strong symmetric keys using the AES and TDES encryption standards. For AES, the key length can be specified up to 256 bits to offer the highest protection.

By default, keys are randomly generated by *Crypto Complete* to offer the best security. Depending on the Key Policy settings specified in *Crypto Complete*, the actual value of the Key will never be known to the user or applications. The Keys will simply be referred to by a user-defined label.

Depending on the Key Policy, a Key can additionally be generated based on a user-entered passphrase, salt and iteration count using the PBKDF2 standard (pseudorandom key function as detailed in RFC2898).

PCI DSS 3.6.2

Requirement

3.6.2 Secure cryptographic key distribution

Response

Crypto Complete stores Data Encryption Keys (DEKs) within Key Stores, which are created as *VLDL (Validation List) objects on the System i. The DEKs within the Key Stores are encrypted with Master Encryption Keys (MEKs).

The Key Store *VLDL objects can be distributed to other systems over non-secure connections. The targeted systems will only be able to utilize the Data Encryption Keys (DEKs) within the Key Stores if they implement the same Master Encryption Keys (MEKs). MEKs can only be regenerated by entering the exact passphrase values as were entered on the original system.

Crypto Complete

PCI DSS 3.6.3

Requirement

3.6.3 Secure cryptographic key storage

Response

Crypto Complete stores Data Encryption Keys (DEKs) within Key Stores, which are created as *VLDL (Validation List) objects on the System i. The DEKs within the Key Stores are encrypted with Master Encryption Keys (MEKs).

The Key Store *VLDL objects can be saved to backup media and other systems. The restoring system will only be able to utilize the Data Encryption Keys (DEKs) within the Key Stores if that system implements the same Master Encryption Keys (MEKs). MEKs can only be regenerated by entering the exact passphrase values as were entered on the original system.

PCI DSS 3.6.4

Requirement

3.6.4 Periodic cryptographic key changes

- As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically
- At least annually

Response

Crypto Complete allows periodic changing of Keys (rotating Keys) as required by the organization. Only authorized Key Officers (custodians) are allowed to rotate Keys in *Crypto Complete*. Keys can be rotated at any time without having to change customer's applications. Existing encrypted data can be translated (re-encrypted) to any new Keys by using commands provided, without any programming requirements.

Crypto Complete can store the Key identifier on a per-record basis, which allows a mixture of Keys for a single PAN column (field).

PCI DSS 3.6.5

Requirement

3.6.5 Retirement or replacement of old or suspected compromised cryptographic keys

Response

Crypto Complete allows authorized Key Officers (custodians) to remove Keys when they are no longer needed. The Key Officer must have *change authority to the Key Store *VLDL object in order to remove a Key from it.

As an alternative option, an old Key can be restricted from encrypting new data while still allowing the Key's use for decrypting existing data. This option allows for the destruction of the Key only after existing data has been re-encrypted under a new Key.

Crypto Complete

PCI DSS 3.6.6

Requirement

3.6.6 Split knowledge and establishment of dual control of cryptographic keys

Response (Split Knowledge)

In *Crypto Complete*, the policy can be configured to restrict Key Owners (the creators of the Keys) from using those Keys to encrypt and/or decrypt data. This creates a separation of duties in which Key Owners will only be able to create and manage Keys, whereas a different set of authorized users will be able to utilize those Keys.

Response (Dual Control)

Master Encryption Keys (MEKs) are used to protect (encrypt) Data Encryption Keys in *Crypto Complete*. A MEK can be generated (reconstructed) only if all passphrase parts are entered exactly as they were entered on the original system. Each MEK can have up to 8 passphrase parts. To provide dual control, the *Crypto Complete* policy can be configured to require that each passphrase part is entered by a different Key Officer (custodian).

PCI DSS 3.6.7

Requirement

3.6.7 Prevention of unauthorized substitution of cryptographic keys

Response

Within *Crypto Complete*, only an authorized Key Officer (custodian) is allowed to change Keys for an entry in the Field Encryption Registry. Data can only be decrypted if the proper Key Label name is specified and if the user is authorized to the Key Store in which the Key resides.

Crypto Complete

PCI DSS 10.0

Requirement

10.0 Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

Response

Crypto Complete includes comprehensive auditing for meeting the most stringent security requirements. Audit log entries are automatically generated for the following events:

- When any Key Policy settings are changed
- When Key Officers are added, changed or removed
- When Master Encryption Keys (MEKs) are loaded or set
- When Key Stores are created or translated
- When Data Encryption Keys (DEKs) are created, changed, exported or deleted
- When Field Encryption Registry entries are added, changed, removed, activated or deactivated
- When any functions are denied due to improper authority
- When data is encrypted or decrypted with a Key that requires logging of those events

The audit log entries are sent to an IBM journal file. Entries in the journal file cannot be altered. Each entry in the journal is assigned an "Entry Type", which indicates the event which generated the audit log entry. For each entry, *Crypto Complete* will store an audit description, user, date, time, job name, job number and any application-supplied comments.

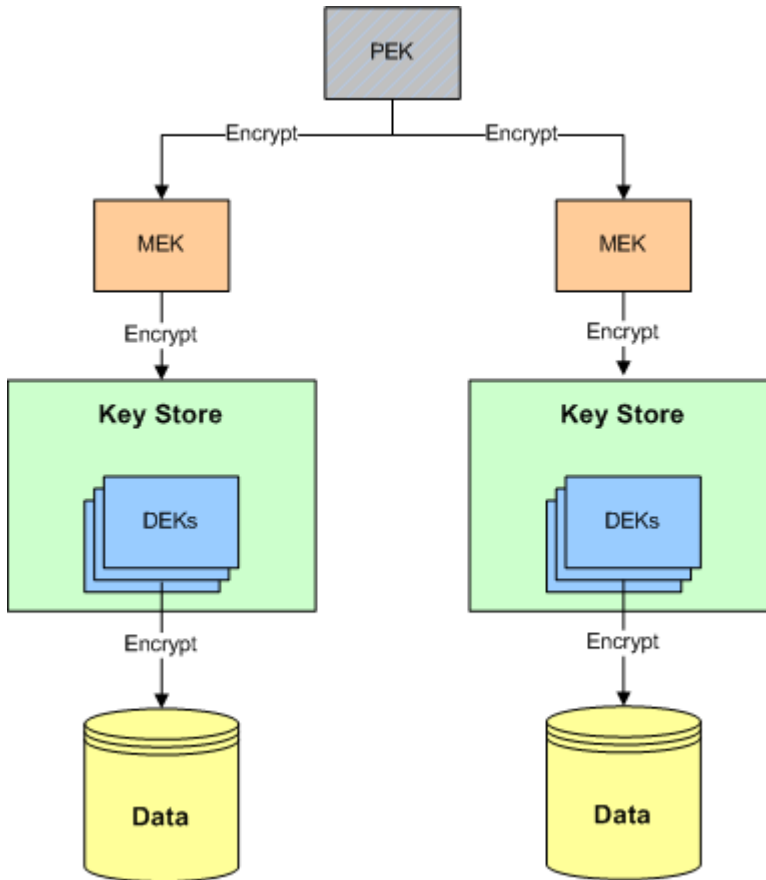
A command is provided to allow authorized users to print the *Crypto Complete* audit log entries. This command provides selection criteria of date and time ranges, audit types and user ids. For each audit entry printed, it will include the audit date, time, user, job name, job number, audit type and message. Example:

11/13/08 13:14:38 Crypto Complete Audit Log						
Date	Time	Type	User	Job Name	Job #	System
06/01/2008	15:21:01	06	MSMITH	QPADEV0001	657766	PRD54
CRA0018 AUDIT: Key store PRODDATA/KS1 was created.						
06/02/2008	15:22:35	10	MSMITH	QPADEV0001	657766	PRD54
CRA0020 AUDIT: Key CREDIT_CARD_KEY created in Key Store PRODDATA/KS1.						
06/03/2008	15:45:12	41	MARYJ	QPADEV0006	657766	PRD54
CRA0043 AUDIT: Key SSN_KEY in PRODDATA/KS2 used to DECRYPT data. SSN for cust. 837626						
06/03/2008	15:45:12	41	MARYJ	QPADEV0006	657766	PRD54
CRA0043 AUDIT: Key BA_KEY in PRODDATA/KS2 used to DECRYPT data. Bank# for cust. 837626						

Security Alerts can also be configured to send notifications when any Key Management activities are performed. These notifications can be sent to email addresses, message queues and journals. Alerts can also be sent when authority errors occur in *Crypto Complete*, such as when an unauthorized user attempts to access a Key Store.

Crypto Complete Key Hierarchy

Crypto Complete provides a multi-level security architecture to protect Symmetric keys on the System i. The diagram for this hierarchy is outlined below (with descriptive text following the diagram).



DEK - Data Encryption Key

A Data Encryption Key (DEK) is a Symmetric Key which is used to encrypt and decrypt data. An organization can create one or more DEKs using *Crypto Complete*. For instance, a DEK could be created to encrypt/decrypt credit card numbers and a second DEK could be created to encrypt/decrypt social security numbers.

A DEK should be randomly generated by *Crypto Complete* in order to provide the highest degree of protection. Depending on your organization's key policy, you can additionally have *Crypto Complete* generate a DEK which is based on a passphrase entered by the user.

Crypto Complete

Key Store

Data Encryption Keys (DEK) are contained within Key Stores. You can create one or more Key Stores on the System i using *Crypto Complete*. For instance, one Key Store could be used to contain DEKs for protecting Order Entry data, and a second Key Store could be used to contain DEKs for protecting Payroll data.

A Key Store is created as a *VLDL (Validation List) object on the System i. You can control access to the Key Store *VLDL object using i5/OS object security.

MEK – Master Encryption Key

A Master Encryption Key (MEK) is a special Symmetric Key used to protect (encrypt) the Data Encryption Keys (DEKs) contained in a Key Store. An organization can create up to 8 MEKs per environment on the System i. For instance, a MEK could be used to encrypt the Order Entry DEKs contained in a Key Store, and a second MEK used to encrypt the Payroll DEKs contained in another Key Store.

A MEK is generated by *Crypto Complete* using passphrases entered by designated users. Depending on the organization's key policy, up to 8 different passphrases can be required (by different users) in order to generate a MEK.

PEK – Product Encryption Key

A PEK is used by *Crypto Complete* to protect (encrypt) the Master Encryption Keys (MEKs) and user-defined settings (i.e. Key Policy, Key Officers, etc).

Crypto Complete automatically generates the PEK using a combination of the System i serial number and a secret value. The PEK only resides in memory as-needed and is never stored.

About Linoma Software

The Company

Founded in 1994, Linoma Software provides innovative technologies for protecting sensitive data and automating data movement. Linoma Software has a diverse install base of over 3,000 customers around the world including Fortune 500 companies, non-profit organizations and government entities.

How to Contact Linoma Software

Electronic

Sales sales@linoma.com
Support support@linoma.com
Website www.linomasoftware.com

Phone Numbers

Toll-free: 1-800-949-4696
Outside USA: (402) 944-4242
Fax: (402) 944-4243

Address

Linoma Software
1409 Silver Street
Ashland, NE 68003 USA