



How Crypto Complete Helps You Meet PCI DSS Requirements

Crypto Complete protects sensitive data on the IBM System i using strong encryption, integrated key management and auditing. With its intuitive screens and proven technology, Crypto Complete allows organizations to quickly and effectively meet their security initiatives.

- Automated encryption of database fields within System i database files
- Encryption of System i files, objects and libraries (backup encryption)
- Integrated Symmetric Key Management with key lengths up to 256 bits
- Rotation of encryption keys without having to re-encrypt existing data
- Decryption of fields as full values or masked values
- Advanced Encryption Standard (AES) and Data Encryption Standard (TDES)
- Comprehensive audit trails and reporting

Crypto Complete meets the PCI DSS requirements for encryption and key management. Here are the requirements and how Crypto Complete addresses them:

3.4 – Render Primary Account Number (PAN), at a minimum, unreadable anywhere it is stored.

Crypto Complete provides strong encryption for protecting field-level data and backup media on the System i (AES and TDES).

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

3.5.1 – Restrict access to keys to the fewest number of custodians necessary.

3.5.2 – Store keys securely in the fewest possible locations and forms.

Crypto Complete includes a comprehensive key management solution that allows an organization to designate the Key Officers, who are authorized to create and manage Master Encryption Keys (MEKs) and Data Encryption Keys (DEKs). DEKs are stored in secure Key Store objects on the System i, to which an organization can control access using i5/OS object security.

3.6 – Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data.

3.6.1 – Generation of strong keys.

Crypto Complete allows the creation of strong symmetric keys using the AES (up to 256 bits) and TDES encryption standards.

3.6.2 – Secure key distribution.

Crypto Complete stores DEKs within Key Stores, which are created as *VLDL objects. These DEKs are encrypted with the MEKs.

3.6.3 – Periodic changing of keys, as deemed necessary and at least annually.

Crypto Complete lets an organization rotate keys as needed, without changing application source code or re-encrypting existing data.

3.6.5 – Destruction of old keys.

Crypto Complete allows authorized users to remove keys when they are no longer needed. The Key Officer must have designated authority to change the keys.

3.6.6 – Split knowledge and establishment of dual control of keys (it requires two or three people, each knowing only their part of the key, to reconstruct the whole key).

Crypto Complete uses MEKS to protect the DEKs. An MEK can be generated only if all passphrase parts are entered exactly as they were on the original system. Each MEK can have up to 8 passphrase parts, each of which must be entered by a different Key Officer.

3.6.7 – Prevention of unauthorized substitution of keys.

Crypto Complete requires that only an authorized key officer be able to change keys. Data can be decrypted only if the Key Label name is specified and if the user has authorized access to the Key Store in which the key resides.

3.6.8 – Revocation of old or invalid keys.

Crypto Complete allows authorized Key Officers to remove keys when they are no longer needed.

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

Crypto Complete includes comprehensive auditing for meeting the most stringent security requirements. Audit entries are stored in a tamper-proof journal file that can be secured by user id.



800.949.4696
www.linomasoftware.com