



Build vs. Buy

Publication date: **February 25th, 2008**



© Copyright 2006-2008, LINOMA SOFTWARE

LINOMA SOFTWARE is a division of LINOMA GROUP, Inc.



System i Field Encryption (Build vs. Buy)

Challenge

System i (iSeries) customers are under increasing pressure to maximize the protection of sensitive data within their applications. This sensitive data may include credit card numbers, bank account numbers, social security numbers, financial information and other personal data. The best method for ensuring the highest protection of this data is by using strong encryption technology with effective key management and auditing.

The System i operating system does not offer an integrated out-of-the-box solution to meet the comprehensive requirements for encryption, key management, security controls and auditing. Therefore, organizations must decide if they should attempt to build their own custom solution or acquire a 3rd party product to meet their needs.

In this whitepaper, we cover the issues and questions that need to be addressed by organizations which may be considering building their own custom solution. We also indicate the benefits and features of Linoma Software's *Crypto Complete* product for protecting sensitive data.

Building a Custom Solution

If an organization is considering building their own custom encryption solution, they would first have to become very knowledgeable about any regulations and PCI requirements which govern their organization. Their development staff would also have to learn how to properly implement encryption/decryption technologies, as well as become an expert in proper key management and security/auditing requirements.

Organizations which have tried to implement their own custom encryption solution have experienced a multitude of issues and shortcomings, some of which are listed below:

- IBM's encryption APIs have a steep learning curve and can be difficult to implement correctly with the right settings.
- Significant application changes must often be made to call the encryption APIs whenever sensitive data is added or changed.
- Database field definitions have to be changed to accommodate the resulting encrypted data (i.e. changing field types from numeric to alpha and/or expanding field sizes).
- Sensitive data is not encrypted when entered/changed outside of the applications (i.e. using database utilities like DFU).
- Key management does not meet the stringent PCI requirements.
- Key values are not properly protected from unauthorized use.
- It is difficult to rotate keys without re-encrypting all existing data.
- Audit trails are typically non-existent or limited.
- A custom solution typically does not address enterprise needs.

The significant amount of time and money that would need to be expended for the development, testing and documentation of a custom encryption solution is not practical for most organizations. A custom solution may also have liability implications if it is not implemented properly and does not meet the various regulations and PCI requirements.

System i Field Encryption (Build vs. Buy)

Building a Custom Solution - Questions

Listed below are questions that an organization needs to address if they are considering building their own encryption solution for the System i. For each question listed, we have indicated how the *Crypto Complete* product addresses the issue.

Data Encryption Keys

How will Data Encryption Keys be created (random, passphrase-based, manually entered)?

Crypto Complete allows an organization to specify (at the policy level) if Keys can be randomly generated, passphrase generated or manually entered. This provides flexibility and control in how keys are generated.

How will you control which users can create, change and delete Data Encryption Keys?

Crypto Complete allows an organization to specify the users (Key Officers) which are authorized to create, change and delete Data Encryption Keys. Even users with *ALLOBJ or *SECADM authority can be restricted from managing Data Encryption Keys.

How will you implement dual-control (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key)?

Crypto Complete allows an organization to specify (at the policy level) the number of password parts that must be entered to generate a Master key. Each password part can be required to be entered by a unique user id. This dual-control security feature prevents a single user from being able to reconstruct a Key on their own.

Where will the Data Encryption Keys be stored on the System i?

Crypto Complete stores Data Encryption Keys (DEKs) within Key Stores, which are created as *VLDL (Validation List) objects on the System i. The Keys stored within the Key Stores are encrypted with a Master Encryption Key and cannot be utilized without proper authority.

Storing the clear Key value in the program source code or a data area <u>will not</u> comply with PCI standards.
--

How will the Data Encryption Keys be protected from unauthorized use?

Crypto Complete allows an organization to secure access to the Key Stores (which hold the Data Encryption Keys) using System i object authority. If a user attempts to use a Key from an unauthorized Key Store, then that event will be logged in Crypto Complete's audit journal.

Can the actual clear values of the Data Encryption Keys be viewed by programmers or others?

Crypto Complete allows an organization to specify (at the policy level) if the clear values of the Data Encryption Keys can be viewed/exported. By default, these Key values cannot be viewed or exported, in which they will remain encrypted within the Key Stores.

Will the Data Encryption Keys be protected (encrypted) with Master Keys? If so, how will you control who can create and manage Master Keys?

Crypto Complete encrypts Data Encryption Keys using Master Keys. Up to 8 Master Keys can be created per environment. An organization can indicate which users (Key Officers) are authorized to create and manage Master Keys.

System i Field Encryption (Build vs. Buy)

How will audit trails be generated when Keys are created, changed, etc?

Crypto Complete automatically creates audit log entries when Keys are created, changed and deleted. The audit log entries are stored in an IBM journal file and cannot be modified. Audit reports can be generated by user, date/time range and audit type.

How easy will it be to rotate (change) Data Encryption Keys? Will existing data have to be re-encrypted?

Crypto Complete allows an organization to rotate Data Encryption Keys at any time without having to change application source code and without having to re-encrypt existing data.

How will you recover the Data Encryption Keys in a disaster recovery situation?

Crypto Complete stores the Data Encryption Keys within Key Stores, which are validation list objects on the system. An organization should save these objects as part of their normal backups and restore them in a disaster recovery situation.

Data Encryption and Integrity

Will field sizes have to be expanded to store the encrypted values?

With Crypto Complete, in most cases an organization will not have to expand their field sizes to store the encrypted values. If the field (to encrypt) is alphanumeric and is divisible by 16 or 24, then Crypto Complete allows you to store the encrypted values within the existing field. Otherwise, Crypto Complete can store the encrypted values into a separate external file, which it will create and manage for you automatically.

Will numeric field types have to be changed to alpha types in order to store the encrypted values?

Crypto Complete can encrypt numeric fields and store the encrypted values into a separate external file, which it will create and manage for you automatically. This allows you to not have to change numeric field types to alpha.

Which programs will have to be modified to encrypt the field values?

Crypto Complete can automatically encrypt the field values when they are added or changed in the file, without requiring an organization to change existing programs. This is accomplished through the use of efficient database SQL triggers which automatically capture any inserts or updates of the field.

How will you control which users can encrypt and decrypt data?

In Crypto Complete, users can encrypt or decrypt data only if they are authorized to the Key Store objects which contain the requested Data Encryption Keys. The Key Stores can be authorized by individual user ids or group profiles.

How will you encrypt data that is entered through database utilities (i.e. DFU)?

The SQL trigger approach in Crypto Complete will automatically encrypt field values which are inserted or updated in the file. The triggers will capture and encrypt data that is entered through any application, database utility and outside sources (i.e. JDBC and ODBC).

How will you ensure the data is encrypted properly so it can be decrypted by authorized users?

Crypto Complete is a proven solution that is used in numerous mission-critical production environments. If the Crypto Complete documentation is followed properly by the organization, then the data can be decrypted by authorized users.

System i Field Encryption (Build vs. Buy)

How will audit trails be generated when sensitive data is decrypted?

CRYPTO COMPLETE includes comprehensive audit trails for meeting the most stringent security requirements. Audit log entries are 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 created
- When Key Stores are created or modified
- 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 stored in an IBM journal file and cannot be modified. Audit reports can be generated by user, date/time range and audit type.

How would your organization recover Keys in a disaster recovery situation?

Crypto Complete includes easy-to-follow detailed documentation on how to properly backup and restore Keys for disaster recovery. Documentation is also provided on how to replicate Keys to high-availability (HA) systems.

Flexibility

If you ever need to encrypt another field in the future, how easy will it be to implement?

Crypto Complete's innovative Field Encryption Registry allows authorized users to quickly specify the fields to encrypt within their database files. For each field entered into the Registry, the user can specify the field name, database file name, encryption Key and algorithm, and if SQL triggers should be used to automatically encrypt the field values. Additional fields can be added to the Registry at any time in the future.

How easy will it be to create additional Keys and change Keys in the future?

Crypto Complete's flexible Key Management solution allows authorized users to create additional Keys and change existing Key attributes as needed. New Keys can be specified for encrypting new fields or the Keys can be rotated for existing fields at any time.

Documentation

Will documentation exist on how the encryption solution is implemented so other programmers can maintain the solution?

Crypto Complete includes both a comprehensive Users Guide and Programmers Guide. The Users Guide provides over 100 pages of detailed instructions on how to utilize Crypto Complete's Key Management and Field Registry menus and commands. This guide includes a "Getting Started" section along with helpful diagrams and a Q&A section. Each command parameter also has comprehensive on-line help text.

Crypto Complete's Programmers Guide provides documentation on how to properly use Crypto Complete's APIs with program examples. Source code examples are also included in the Crypto Complete library.

Linoma's support staff can be called with any questions or issues. Also, customers can view Linoma's on-line support forum for Crypto Complete.

System i Field Encryption (Build vs. Buy)

If another field needs to be encrypted in the future, will documentation exist on how a programmer can properly implement the encryption (and decryption) for that field?

Crypto Complete's Users Guide contains detailed documentation on how to set up fields for encryption in the Field Encryption Registry. The Programmers Guide includes instructions and examples of how to decrypt fields from within applications.

Will your management be confident that the solution complies with industry standards for proper key management and protection of sensitive data?

Crypto Complete was designed to offer the best possible key management and data protection possible for the System i. The design was reviewed by leading industry experts in this field and has passed data security audits.

PCI standards

Would your solution comply with sections 3.4, 3.5 and 3.6 of the PCI Data Security Standard 1.1?

Sections 3.4, 3.5 and 3.6 of the PCI Standard contain the requirements for protecting credit card information and implementing effective key management. A whitepaper is available from Linoma Software which contains the wording of these section requirements along with documentation on how Crypto Complete satisfies each requirement.

Would your encryption solution pass a PCI audit?

The Crypto Complete solution is implemented at organizations which have undergone and passed PCI audits. You are welcome to talk to Linoma's reference accounts using Crypto Complete.

Operating System Upgrades

Would your encryption solution be compatible with future releases of the Operating System (OS)?

Linoma Software is in IBM's Developers Program, which allows us to receive pre-releases of the OS from IBM. This allows us to test all of our products, including Crypto Complete, with these new OS releases before our customers upgrade.

If any changes are required by Linoma to make a product compatible with a new IBM OS release, the product updates will be issued to customers (whom are on maintenance) before the new OS release ships.

Investment

How many hours will be required for your programmers to become knowledgeable about encryption technologies, proper key management, IBM's APIs, etc.

How many hours would be required to change all applications needed to encrypt the field values?

How many hours would be required to test and document all the application changes?

Considering the hours needed to invest, how much will the custom encryption solution ultimately cost to build?

System i Field Encryption (Build vs. Buy)

Crypto Complete

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

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.

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)
- Integrated Symmetric 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 (DES)
- 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
- Comprehensive audit trails and reporting
- Support for multiple environments

Crypto Complete helps organizations to successfully comply with the latest PCI data security standards, HIPAA, Sarbanes-Oxley and State Privacy laws.



Linoma Software is a member of the PCI Security Standards Council.

System i Field Encryption (Build vs. Buy)

Advantages of *Crypto Complete* over a custom solution

There are many benefits which an organization would realize by utilizing *Crypto Complete* versus attempting to build their own custom solution:

- *Crypto Complete* is a proven solution that can be implemented quickly without making major application changes.
- *Crypto Complete* allows an organization to implement strong encryption and key management without having to become an expert in those technologies.
- *Crypto Complete* works on OS/400 releases starting at V5R2.
- *Crypto Complete* is straightforward to install and upgrade.
- *Crypto Complete* was designed to integrate rapidly with other applications.
- *Crypto Complete* is fully documented with comprehensive on-line help text and manuals.
- *Crypto Complete* enables organizations (which store credit card numbers) to become compliant with the latest PCI Data Security Standards.
- *Crypto Complete* is supported by Linoma Software's highly-technical customer service and development team.
- *Crypto Complete* allows organizations to continue to focus their development resources on enhancing their core applications.

System i Field Encryption (Build vs. Buy)

Symmetric Key Management

Symmetric Key Cryptology (also known as Secret Key or Private Key Cryptology) is a form of cryptology in which the same Key can be used to encrypt and decrypt data.

Symmetric Keys must be strong enough for the intended application. Because the strength of the Symmetric Key is determined by its length, the longer the key, the harder it is for high-speed computers to break the code. Within *Crypto Complete*, Symmetric Keys may be generated up to 256 bit lengths to provide a high level of protection.

The Symmetric Key values must be kept secret to prevent unauthorized decryption of sensitive data. Controls must therefore exist to protect the confidentiality and access to the Symmetric Keys. *Crypto Complete* provides an integrated and comprehensive Symmetric Key Management System to establish those controls.

Cipher: A pair of algorithms (mathematical processes) used to encrypt and decrypt data.

Key: The information needed to control the detailed operations of the Cipher. In contrast to human-generated passwords, Keys are more secure since they are computer-generated and are represented as an obscure series of bits (1001110...).

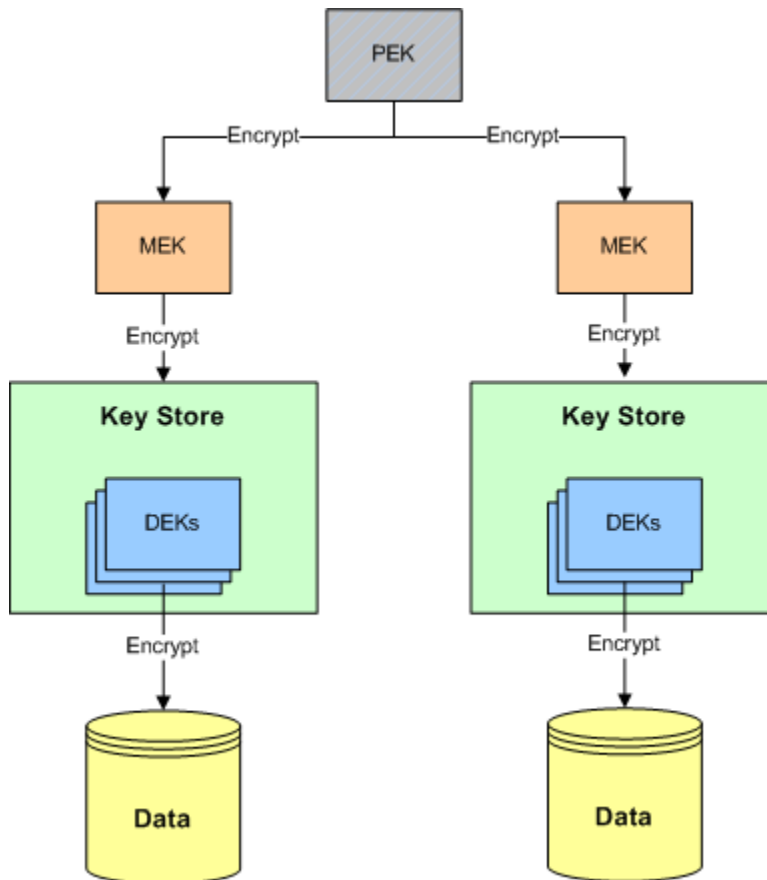
Crypto Complete's Symmetric Key Management System allows organizations to:

- 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
- Produce detailed audit logs

System i Field Encryption (Build vs. Buy)

***Crypto Complete* Symmetric 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.

System i Field Encryption (Build vs. Buy)

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.

System i Field Encryption (Build vs. Buy)

About Linoma Software

Founded in 1994, Linoma Software provides innovative technologies to consistently meet evolving needs for encryption, data transmission and application modernization. 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.

Linoma's success has been built on being very responsive to our customer's requirements. So if you have suggestions on how we can improve our products to better serve your organization, please let us know.

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