DATASHEET *(Cybersecurity)*

Crypto Complete Encryption Suite for IBM i

helpsystems

WSS

Worldwide Software Solutions

Crypto Complete protects sensitive data using strong encryption, tokenization, integrated key management and auditing. Crypto Complete allows organizations to encrypt database fields, backups and IFS files quickly and effectively with its intuitive screens and proven technology.

This innovative solution is vital for protecting confidential information and expediting compliance with PCI DSS standards, federal regulations (e.g. HIPAA, Sarbanes-Oxley) and state privacy laws.

Crypto Complete can be installed within a few minutes and requires no source code changes for encryption. The commands in Crypto Complete have comprehensive on-line help text and are accessible through intuitive native IBM i menus.

PRODUCT SUMMARY

KEY FEATURES

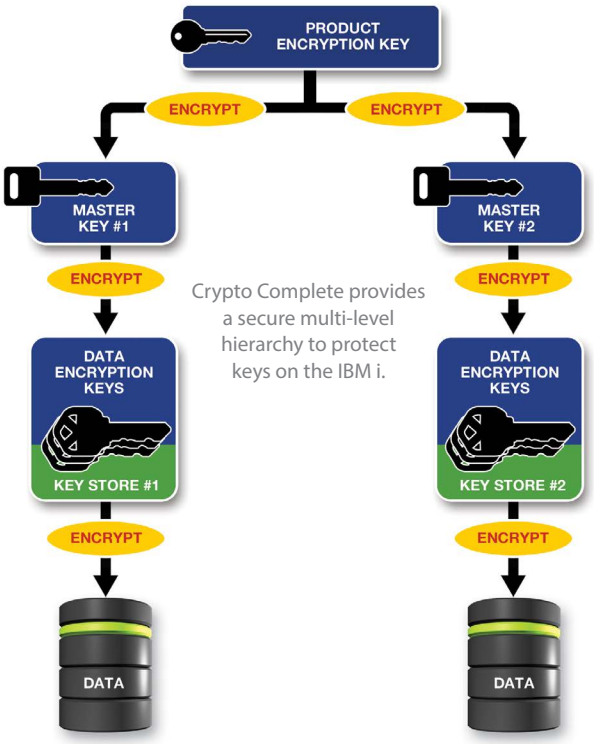
- Key Management
- Backup Encryption
- Field Encryption
- Tokenization
- Audit Trails

SYSTEM REQUIREMENTS

IBM i 7.1 or higher

Key Management

Crypto Complete includes an advanced Key Management system which resides natively on the IBM i. This Key Management system is seamlessly integrated with Crypto Complete's policy controls, encryption functions and auditing facilities to provide a comprehensive data protection solution. Together with the integrated security on IBM i, organizations can strictly control access to key maintenance/usage activities and meet compliance requirements such as PCI DSS.



Crypto Complete provides a secure multi-level hierarchy to protect keys on the IBM i.

Key Features:

- Provides policy settings for compliance requirements (e.g. dual control, separation of duties)
- Allows controlling which users are authorized to manage keys
- Generates strong key values up to 256 bits in length
- Organizes keys into one or more key store objects
- Encrypts storage of keys using Master Encryption Keys (MEK)
- Controls access to keys by user profile, group profile and/or authorization lists
- Prohibits the retrieval of underlying key values
- Produces detailed audit logs on all key management activities

Crypto Complete also provides interfaces for securely sharing keys with other systems such as point-of-sale (POS) systems, Windows, Linux and AIX.

Backup Encryption

Crypto Complete is a software-based solution that allows IBM i customers to encrypt backups using their existing hardware. Backups can be protected using keys from Crypto Complete's Key Management System to provide strong security. Commands are provided to encrypt and backup any user data on the IBM i including libraries, objects and IFS files.

Key Features:

- Utilizes AES (Advanced Encryption Standard) for encryption
- Encrypts and saves to existing backup media
- Incorporates into existing backup processes (e.g. CL programs, BRMS, schedulers)
- Saves disk space and time by not generating intermediate save files
- Protects backups with either passphrases or keys
- Stores key labels with encrypted backups to simplify restores
- Optionally backs up to the Integrated File System (IFS)
- Reduces disaster recovery costs since no special hardware is required

Straightforward commands are provided to restore and decrypt libraries, objects and IFS files which were saved using Crypto Complete's backup processes. These commands can be restricted to authorized users only.

Field Encryption

Crypto Complete will protect sensitive database fields on IBM i using strong encryption algorithms of AES or TDES. You can encrypt almost any database field with Crypto Complete including:

- Credit card numbers (PAN)
- Health-related information
- Social security numbers
- Drivers license number
- Bank account numbers
- Financial data

With Crypto Complete's innovative Field Encryption Registry, you can simply indicate the database fields to encrypt. When a field is "activated" in the registry, Crypto Complete will perform a mass encryption of the current values for that field. Crypto Complete can then automatically encrypt the field values on an ongoing basis as new database records are added and when existing field values are changed. This automated feature saves significant time and money for customers, since applications do not need to be changed for data encryption.

Access to data can be tightly controlled at the field/user level. Only designated security administrators can grant authority to the decrypted or masked values. Decryption of any data can be fully audited in Crypto Complete, which will log the user id, date, time, job information and key utilized.

Tokenization

Tokenization should be considered when sensitive data is stored on multiple systems throughout an organization. Tokenization is the process of replacing sensitive data with unique identification numbers (e.g. tokens) and storing the original data on a central server, typically in encrypted form.

By centralizing sensitive data onto a single system, tokenization can help thwart hackers and minimize the scope of compliance audits such as PCI. Tokenization can be used to protect any sensitive data including credit card numbers (PAN), bank account numbers, social security numbers, drivers license numbers and other personal identity information.

"Crypto Complete has been doing its job quietly for a couple of months now. Just a couple of weeks ago I needed to add the encryption of a field in a new file and the process was easily added. The software is well-designed. There are not a lot of software products that impress me, but I have to say that I really like the way Crypto Complete works. It was easy to implement and allowed us to meet all the requirements for securing our data to get PCI compliant."

– Will Crowe, Love's Travel Stops and Country Stores

Key Features:

- Centralizes key management and policies on a single server
- Supports tokenization of data from diverse systems including IBM i, Windows, Linux, AIX, etc.
- Provides remote connections to token functions through secure HTTPS protocol
- Auto-assigns token identifiers from the central token server
- Encrypts and stores tokenized data into scalable DB2 physical files
- Allows securing data elements by User Profile, Group Profile and/or Authorization Lists
- Provides centralized audit logs and message alerts

Audit Trails

Crypto Complete includes comprehensive auditing 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 loaded or set
- When Key Stores are created or translated
- When Data Encryption Keys (DEKs) are created, changed or deleted
- 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 can be displayed and printed using a variety of selection criteria, including date/time range, user and audit type. Alert messages can also be sent to QSYSOPR, QAUDJRN, email and SYSLOG.

helpsystems

www.helpsystems.com

About HelpSystems

Organizations around the world rely on HelpSystems to make IT lives easier and keep business running smoothly. Our software and services monitor and automate processes, encrypt and secure data, and provide easy access to the information people need.

WSS

Worldwide Software Solutions

www.wssitalia.it

Informazioni su WSS

Da vent'anni, propone sul mercato italiano soluzioni software di produzione estera e servizi innovativi con specializzazione su IBM i (anche con copertura 24/7), in ambito RMS - gestione remota dei sistemi e AMS - sviluppo e gestione degli applicativi.