

# **Overview**

Data encryption is fast becoming a requirement for many businesses in that personal and trade secret information are targets of a wide array of attacks including identity theft, fraud, and corporate espionage. These attacks can come from internal or external sources. Companies are capturing personal information from their employees (e.g., Social Security numbers, birth dates, salaries, etc.) and from their clients (e.g., credit card numbers and expiration dates, phone numbers, etc.). Other corporate information needing protected are product specifications and product recipes.

CryptoMondo is an interface and enhancement to the JD Edwards (JDE) World Enterprise Resource Planning (ERP) system that allows users to manage the use and update of sensitive information for an organization. It uses the Linoma Crypto Complete product as a basis to perform the encryption/decryption of fields inside JDE World and the JDE Generic Exit function to display unencrypted data and to manage security surrounding encrypted fields.

## **New Features in V1.1**

1. Each entry can have its own encryption key and field masking (Character and position)
2. Each entry can have its key rotated from the management screen
3. The entry in CryptoComplete can be shown from the management screen
4. Constants are now used as defaults
5. The security exit program is now a parameter on the constants with default add/change/delete security fields
6. Special Date Functionality for files with more than 766 records
7. New batch process to update fields in a related file with the actual value from the original encrypted file. (i.e. Payroll tax records / W2)
8. The workbench screen now shows the current status of activation/deactivation of entries
9. All Action Code screens allow the use of the F5 key for Update/Redisplay

## **New Features in V1.2**

1. Encrypted fields can now be selected in Data Selection on DreamWriter when using File Output Type '8'
2. Encrypted fields can now be used in WorldWriter
3. Non-JDE fields can be encrypted through a new wizard, and the security matrix can be applied to those fields for updating.
4. An alternative data dictionary item can be used to automatically create a generic exit for a field (i.e. TX2 on the screen could actually be encrypted by TAX).
5. A new manual 'translation' window has been added that can be used when the actual value is known and the encrypted value's key is needed for data selection.
6. Encrypted fields automatically have logical files created (to support the manual translation window)
7. A reset status option (12) has been added for any "stuck" or out of sync entries between CryptoComplete and CryptoMondo
8. Added the F00944 for compilation purposes.
9. Added the F96012 and F96012LA for multiple Common Libraries
10. Added the J00CLMSG and J00SNDMSG programs and source.
11. Modified the J82001 program for A7.3 users.

## **CryptoMondo Concepts**

CryptoMondo introduces several new concepts to the JD Edwards Security applications including the following:

### **Encrypted Fields**

An encrypted field is a part of a database file selected by the user that hides/masks the actual value of the data contained within. Encrypted fields can be character or numeric. Crypto Complete allows for encrypted fields to be stored within the database field or stored in an external file. CryptoMondo always uses the external file option so that the value stored in the original database field points to a record number in the external file.

When an encrypted character field is displayed on the screen, a masking character and position are used so that the value displayed within JD Edwards is obviously an encrypted value. If the field is not masked, it may confuse the user into thinking that the data stored within the database is incorrect.

For instance, if there was no masking used and the Social Security number was encrypted the value contained in the SSN field would be the number of the record from the external file where the encrypted value is stored. If there is a masking character, the value stored would still contain the record number but would now be either preceded by or followed by the masking character.

### **Activation/Deactivation**

Activation of an encrypted field hides the actual value inside of the field and replaces it with the record number from the external file storing the encrypted data. Additionally database triggers are placed on the file for Add, Update, and Delete operations for each field having an encryption definition.

Deactivation reverses this process by restoring the decrypted value to the original database file, removes the database triggers that were installed during activation, and eliminates the external file storing the encrypted data.

### **Field Level Security**

Field Level Security ensures that only authorized users have the ability to View, Add, Update, or Delete encrypted data. Programs attempting to access encrypted fields are screened to ensure that:

1. The field has an encryption definition in the F98652 file.
2. The program attempting to make the change is listed in the F98655 file.
3. The User's authorization is validated against the information stored in the F98654 file.

If any of these screens fail, an error message is generated. Otherwise the desired action occurs.

## **Batch Processing with Encrypted Fields**

Reports that contain encrypted fields will display the record number of the external file wherein the encrypted value is stored. If a character field is encrypted the masking will also be displayed.

CryptoMondo adds an option to the DREAM Writer setup screens. The File Output Type on the Additional Parameters of the DREAM Writer Menu can now be defined as '8' instructing the DREAM Writer system to call a secondary program to decrypt the file into a temporary file and allow programs to use the data in an unencrypted state. Fields will only be decrypted if the user has view capability on the particular field.

WorldWriter can also be used with CryptoMondo with no modifications. Fields will ~~not~~ **only** be decrypted if the user has view capability on an encrypted field.

