



CryptoMondo

User Guide

(JD Edwards World Data Encryption System)

Version 1.2

Palazzo, Inc.
1660 Seventeenth Street Suite 201
Denver, CO 80202 USA

©Palazzo, Inc., 2008-2010
All Rights Reserved Worldwide

Information in this document is subject to change without notice. While this document does not represent a commitment on the part of Palazzo, Inc., it represents the general software direction for this enhancement. The software described in this document is furnished under a license agreement and may be used or copied only in accordance with the terms of the agreement.

Standard software license warranty applies to standard software. Standard Response Line/Software Update agreement applies to standard software.

J.D.Edwards and WorldSoftware are trademarks of Oracle Corporation. CryptoMondo and Palazzo are trademarks of Palazzo, Inc. CryptoComplete is a trademark of Linoma Software. All other trademarks are property of their respective companies.

Table of Contents

Page

OVERVIEW	5
New Features in V1.1	5
New Features in V1.2	5
CryptoMondo Concepts	6
Encrypted Fields	6
Activation/Deactivation	6
Field Level Security	6
Batch Processing with Encrypted Fields	6
CRYPTOMONDO PROCESS	8
CryptoMondo Menu	8
CryptoMondo Constants	9
Crypto Complete	9
Default Padding (Formerly Masking)	10
Default Security	10
Available Functions/Options	11
Work with Symmetrical Keys	11
Retrieve Listing	12
Update and Redisplay	13
Enhanced Help	13
Work with Encrypted Fields	15
Available Functions	16
Constants	16
Create New J.D.Edwards Encryption Entry Wizard	16
Create New Non-J.D.Edwards Encryption Entry Wizard	23
Available Options	28
Activate	29
Deactivate	31
Copy to New Library List	34
Go to Data Dictionary	35
Show Library/Libraries	35
Show Screens	36
Show User Security	38
Show Exit Program Security	38
Delete/Cancel	39
Rotate Keys	39
Show CryptoComplete entry	41
Generic Exit Definitions	43
Special Value Retrieval	45
Batch Processing with Encrypted Fields	49

Updating Related Files	51
ADDITIONAL ENCRYPT MENU FEATURES	53
Crypto Complete Main Menu	53
Work With Key Officers.....	54
Work With Field Encryption.....	54
INSTALLATION REQUIREMENTS	57
Prerequisites.....	57
JD Edwards World	57
Crypto Complete.....	57
Install/Upgrade CryptoMondo.....	57
APPENDICES	57
Appendix A – Restrictions	57
Appendix B – ‘*RRN’ working programs.....	58
Appendix C – Code Examples for Customization	60

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

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 be decrypted if the user has view capability on an encrypted field.

CryptoMondo Process

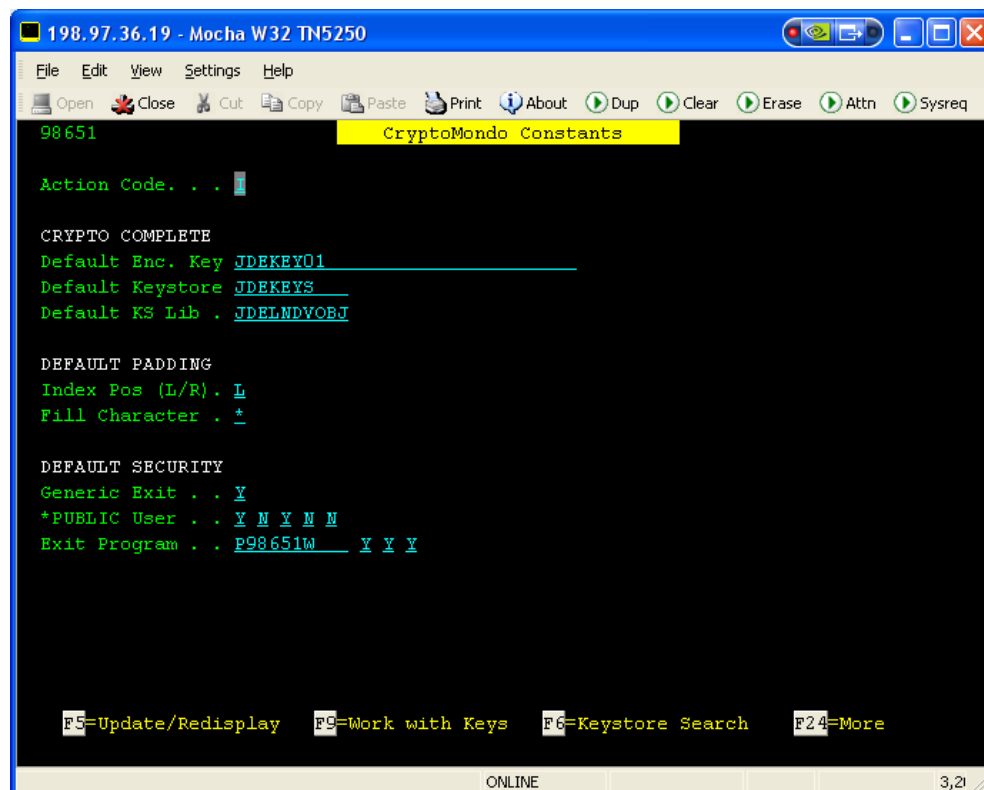
CryptoMondo Menu

Access the CryptoMondo main menu by entering ENCRYPT on the command line. The Crypto Complete Setup and CryptoMondo Setup menu selections are displayed. From here you can access Linoma's Crypto Complete menus work with CryptoMondo setup and/or processing screens. ***Note: If you have Menu Security on then be sure to secure this menu as you have your other menus by using the MENUS command.**



CryptoMondo Constants

Access the CryptoMondo Constants application (P98651) by entering 14/ENCRYPT on the command line. These constants are used by the CryptoMondo and Crypto Complete software systems as defaults for field encryption.



The values displayed are stored in the F98651 table and come shipped with the software. The Constant sections include 1) Crypto Complete, 2) Default Padding, and 3) Default Security.

Crypto Complete

- The Encryption Key field identifies the default Encryption key label (EKCKEYLBL) used by Crypto Complete when adding a field encryption entry.
- The Key Store identifies the file portion of the ENCKEYSTR when adding a field encryption entry.
- The Library Name identifies the library portion of the ENCKEYSTR when adding a field encryption entry.

Default Padding (Formerly Masking)

Masking helps users identify fields that are encrypted. These are the default values for alphanumeric fields:

- The Index Position field identifies whether masking of an encrypted character field is from the left or the right.
- The Fill Character field identifies the character used to mask encrypted fields. The following are not permitted to be used as fill characters:
 - Numbers 0 – 9
 - The dash (-) character
 - The quote (') characterAll other characters are permitted.

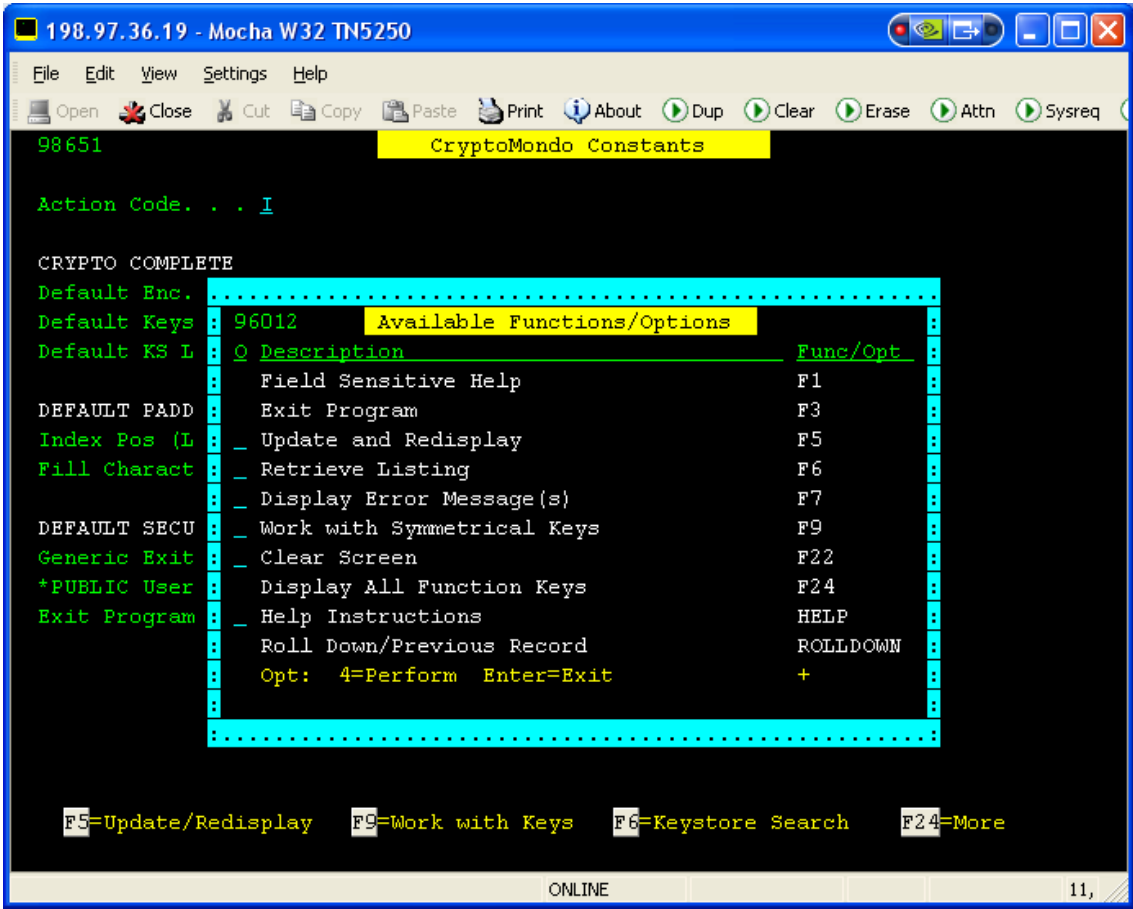
=

Default Security

- The Generic Exit field is used to set the default security for any new Generic Exit function key that is created by CryptoMondo.
- The User Security fields are used to set the default security for the *PUBLIC user when defining any new encrypted field. The fields are as follows:
 - View – Ability to view the unencrypted value
 - Insert – Ability to insert new values in an encrypted field
 - Update – Ability to update values of an encrypted field
 - Delete – Ability to delete values within an encrypted field
 - Debug – Ability to use the debug feature in order to maintain encrypted fields
- The Exit Program fields are used to set the default exit program (CryptoMondo comes with P98651W) and security for the program entries. The fields are as follows:
 - View – Ability for the exit program to view the unencrypted value
 - Insert – Ability for the exit program to insert new values in an encrypted field
 - Update – Ability for the exit program to update values of an encrypted field

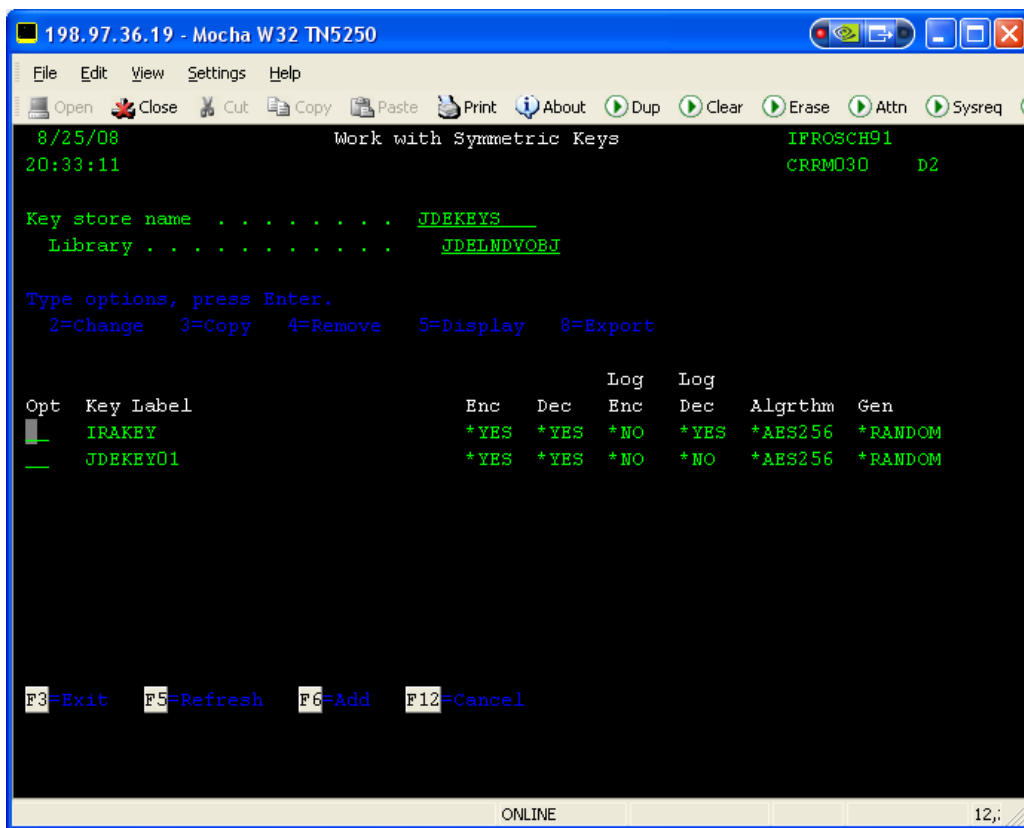
Available Functions/Options

In addition to the standard JDE function keys normally found by pressing F24, the CryptoMondo Constants screen also includes “Update and Redisplay”, “Work with Symmetrical Keys”, “Retrieve Listing”, and Enhanced Help.



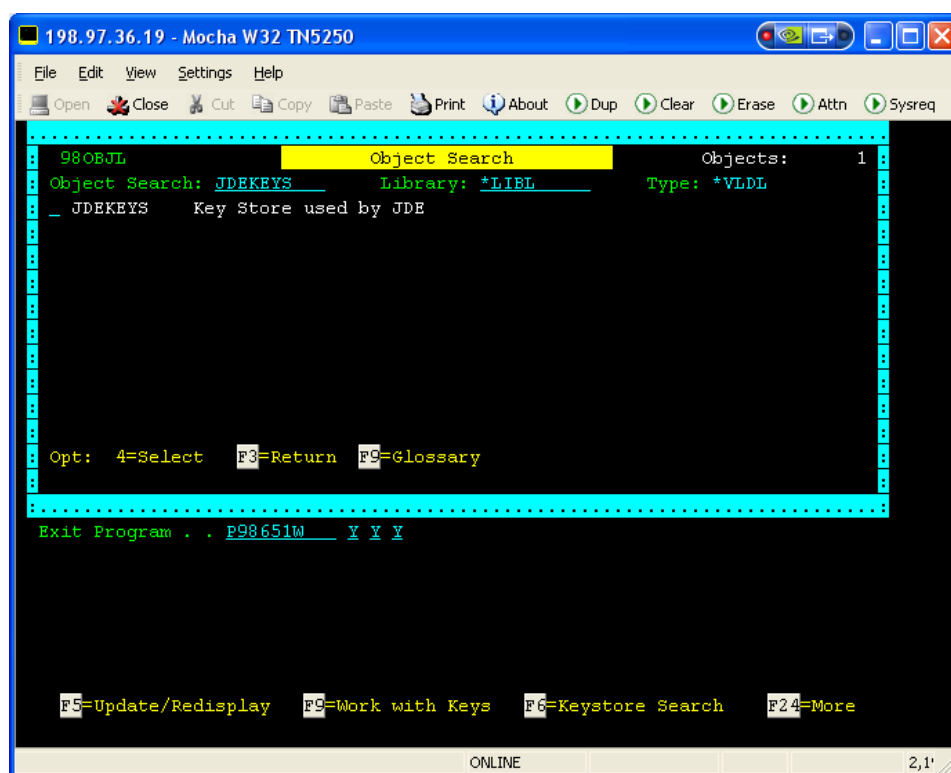
Work with Symmetrical Keys

Pressing F9 displays the Crypto Complete Work with Symmetrical Keys screen where a user can see the Key Labels defined in the *DEFAULT Key Store. See the Crypto Complete User’s Guide for further information regarding Symmetrical Keys.



Retrieve Listing

Pressing F6 displays the JDE Object Search window defaulting to Type *VLDL (validation list). The default validation list used by CryptoMondo is the value in the default keystore. This window will also occur when pressing F1 on the default keylist, but using the value from the key store library field

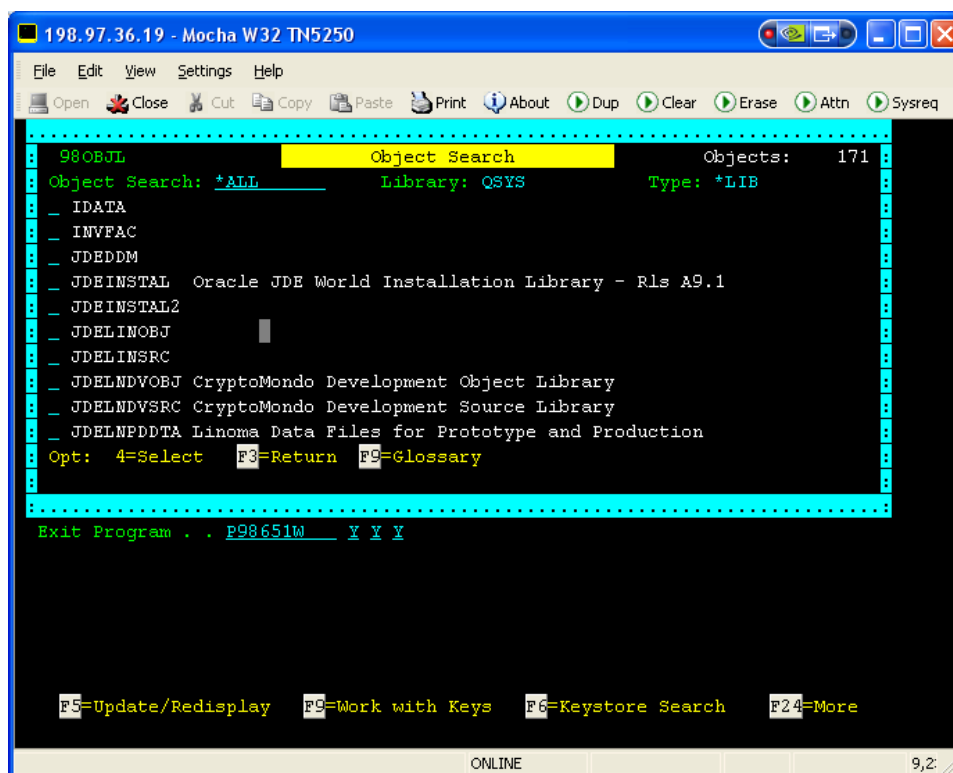


Update and Redisplay

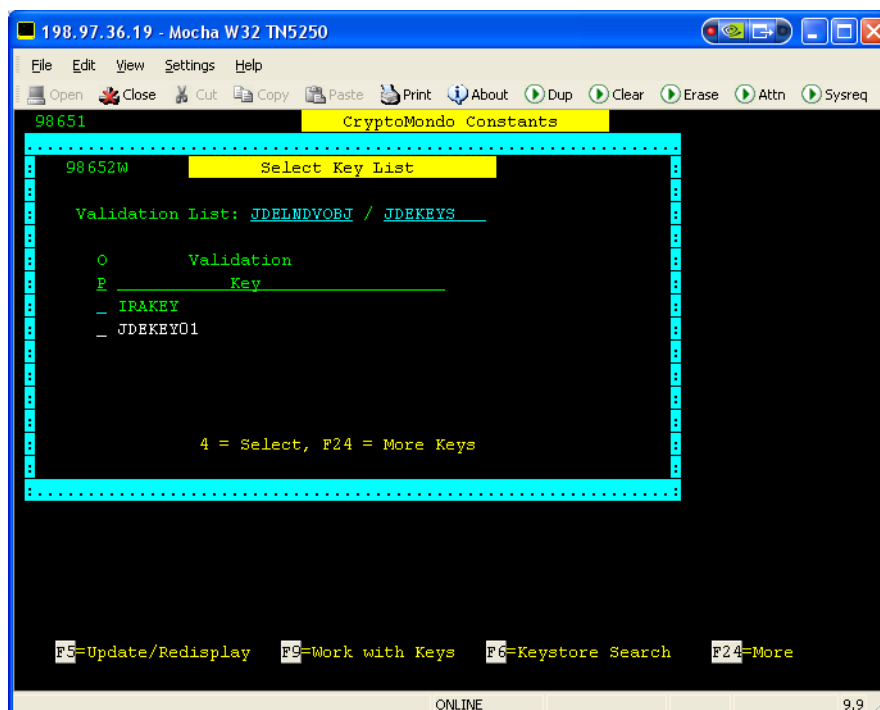
Pressing F5 allows you to update and redisplay any changes that you have made on the screen.

Enhanced Help

When pressing F1 on the Default KS Lib field, the system will show the JDE Object Search window defaulting to Type *LIB (library).



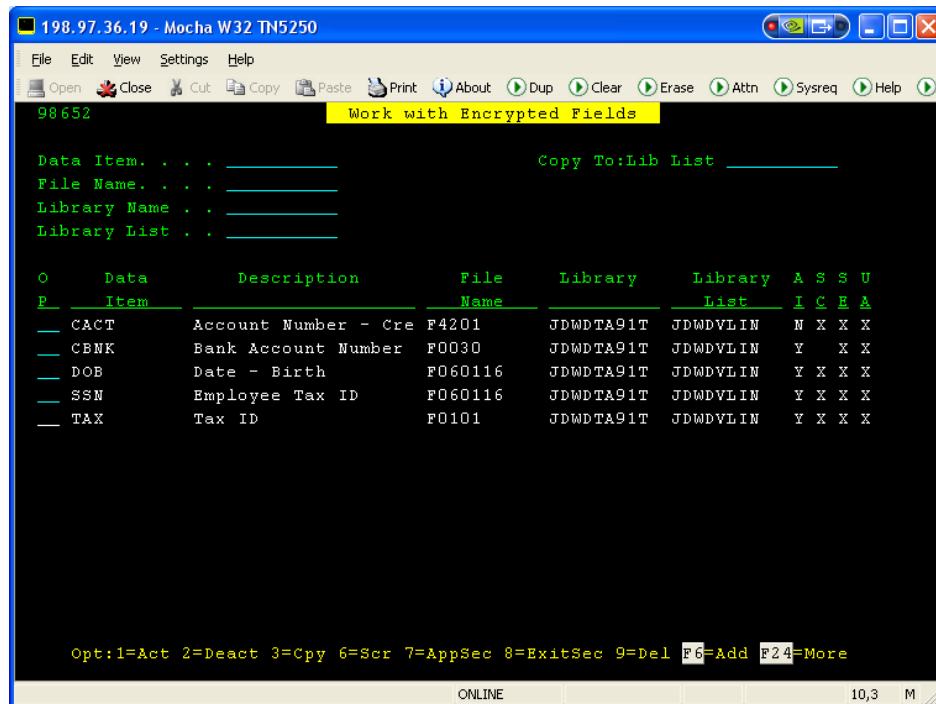
Pressing F1 on the Default Enc. Key with values on the Default Keystore and the Keystore Library results in a search screen for the key to use:



These screens will appear anywhere those fields are used in the system.

Work with Encrypted Fields

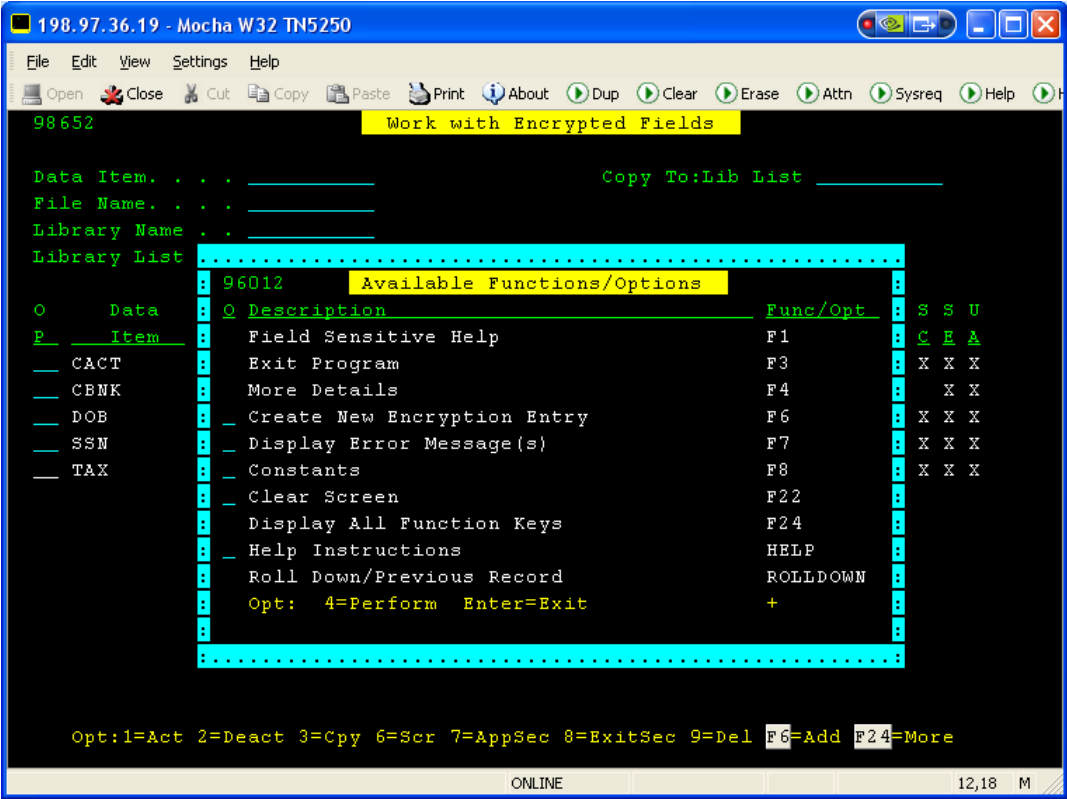
Access the Work with Encrypted Fields application (P98652) by entering 15/ENCRYPT on the command line.



Program P98652 maintains the Encrypted Fields used within the JDE application. By pressing enter upon entering the application the data from the F98652 file is displayed including the Data Item, Description, File Name, Library, Library List, Active/Inactive flag, Exit Program Selected flag, Field Level Security flag, Exit Program Security flag.

Available Functions

In addition to the standard JDE function keys normally found by pressing F24, the Work with Encrypted Fields screen also includes “Create New Encryption Entry” and “Constants”.

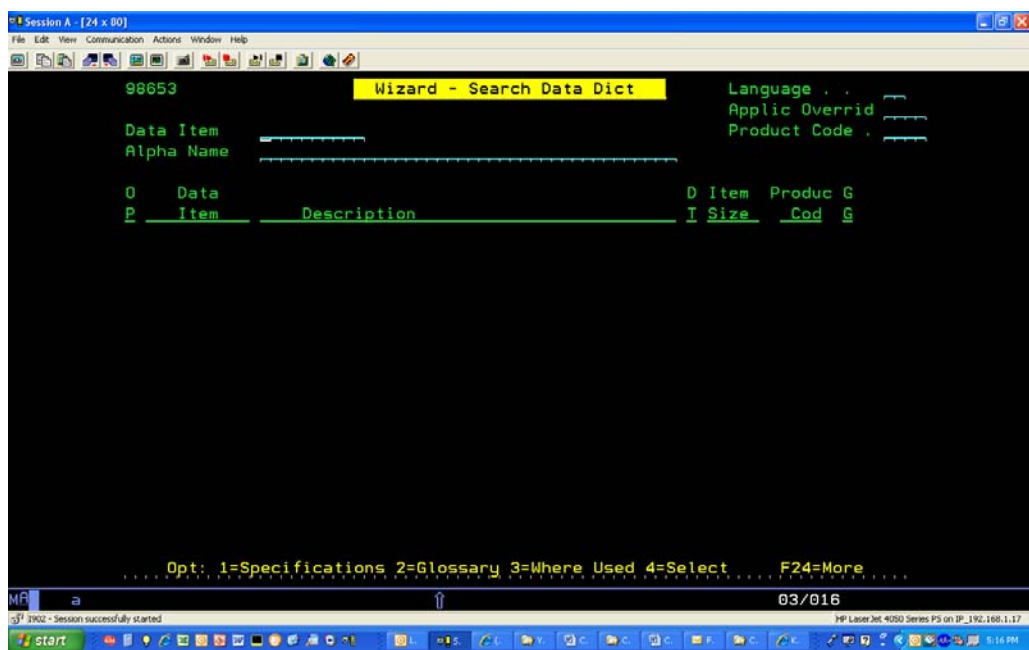


Constants

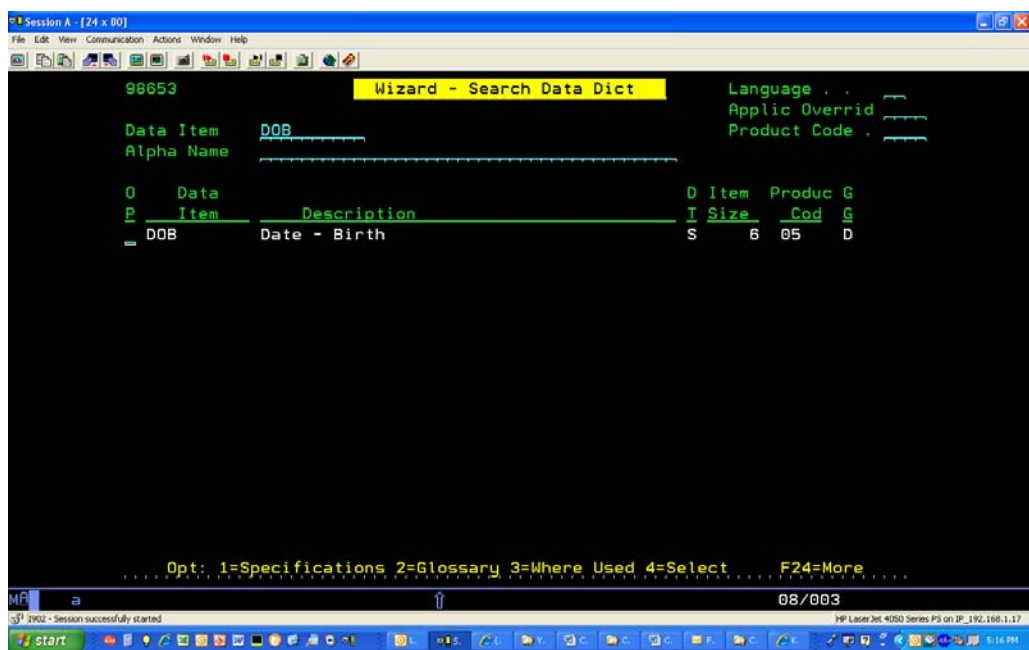
Pressing F8 executes the Encryption Constants (P98651) program displaying the CryptoMondo Constants.

Create New J.D.Edwards Encryption Entry Wizard

Pressing F6 begins the Create New Encryption Entry process by executing the Wizard – Search Data Dictionary (P98653) application. The user can enter a data dictionary item (e.g. SSN, SAL, DOB) or a partial enter in the Alpha Name field to list all JDE Data Dictionary items that match the criteria.

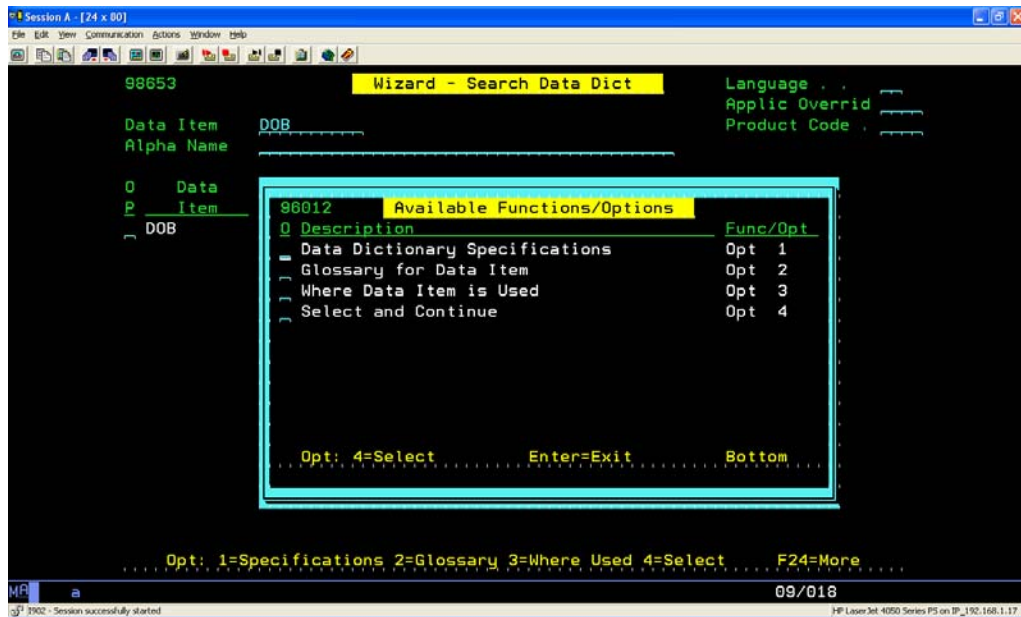


For this example, we'll choose DOB. Enter DOB in the Data Item and press enter.

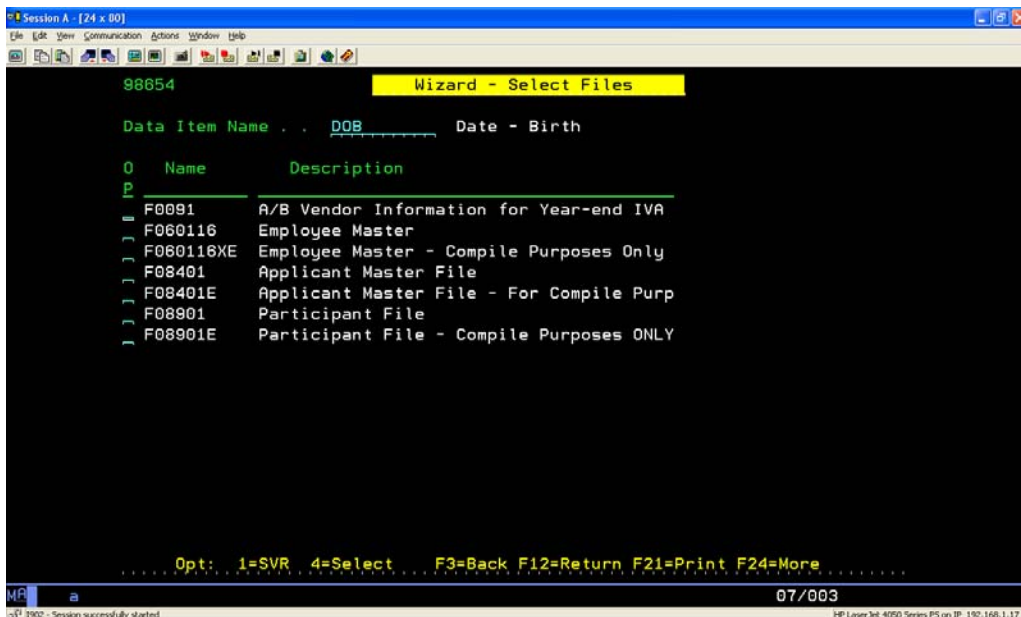


The options available on the P98653 program include:

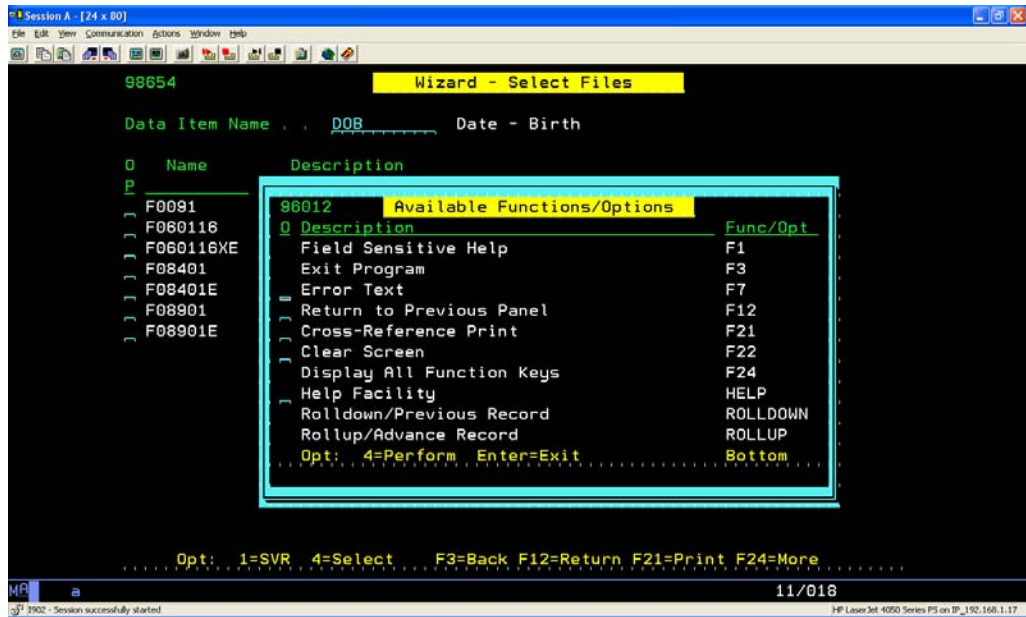
1. Data Dictionary Specifications
2. Glossary for Data Item
3. Where Data Item is Used
4. Select and Continue



Entering 4 on the Option field next to the DOB entry executes the Wizard – Select Files (P98654) application. The P98654 program displays all the files where the DOB Data Dictionary item is used. This program uses the JDE Cross Reference utility to identify the available files so be sure that the Cross Reference files are up to date. If not, execute the Build Cross-Reference (P980010) program.

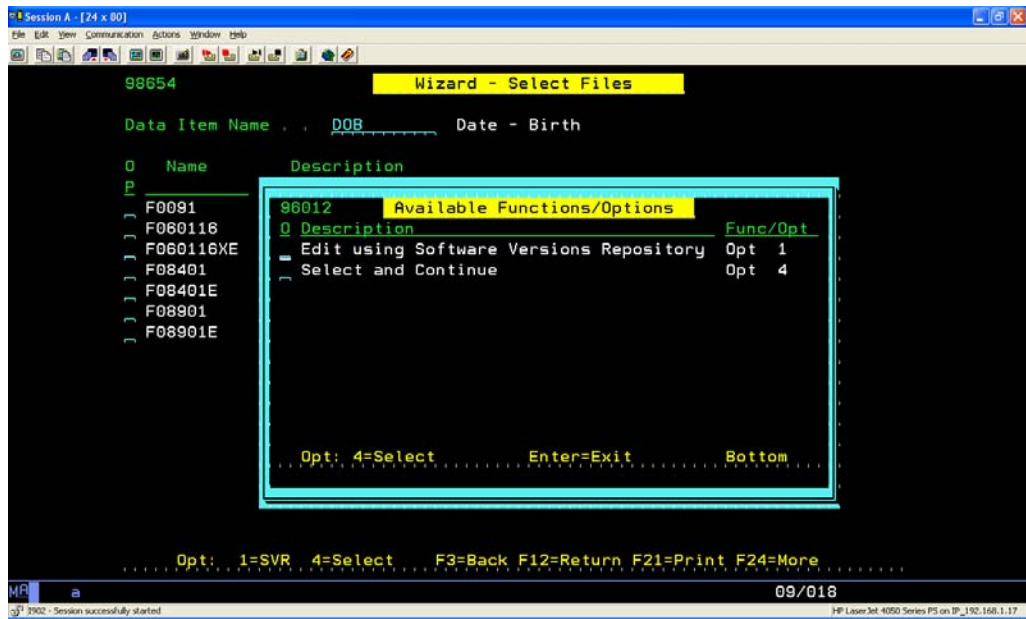


The Function Keys available on the P98654 program in addition to the standard JDE Function Keys include “Return to Previous Panel” and “Cross-Reference Print”.

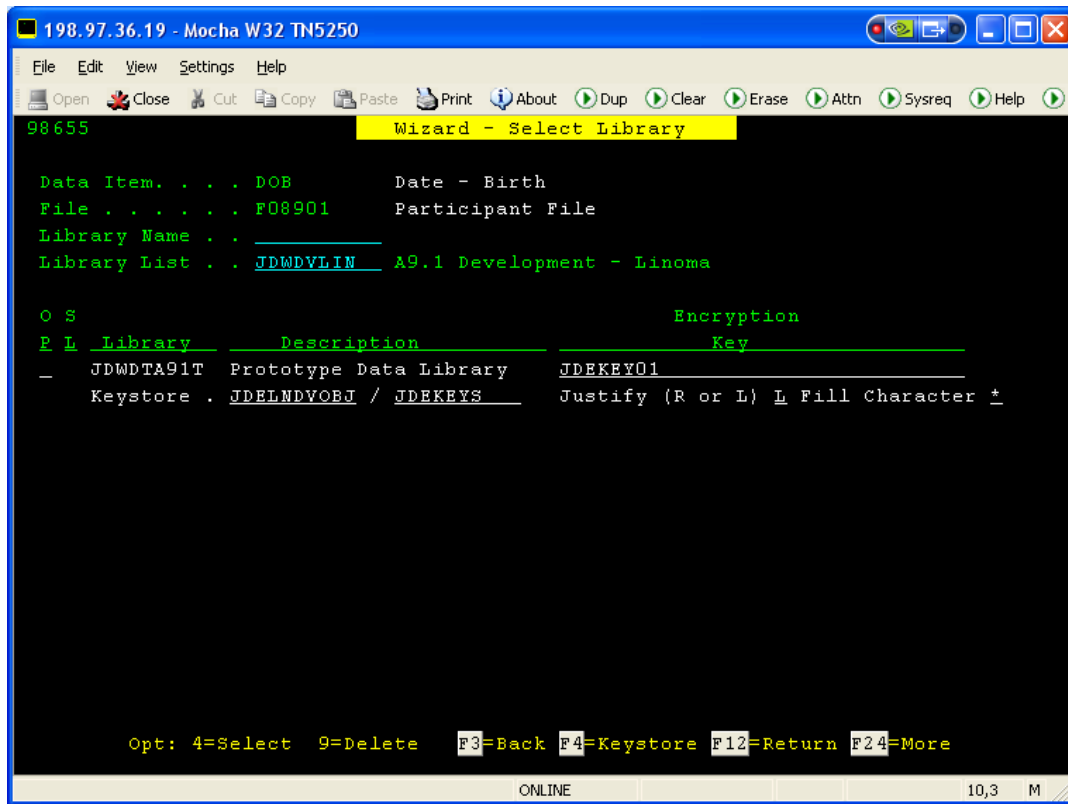


The Options available on the P98654 program include:

1. Edit using Software Versions Repository
4. Select and Continue

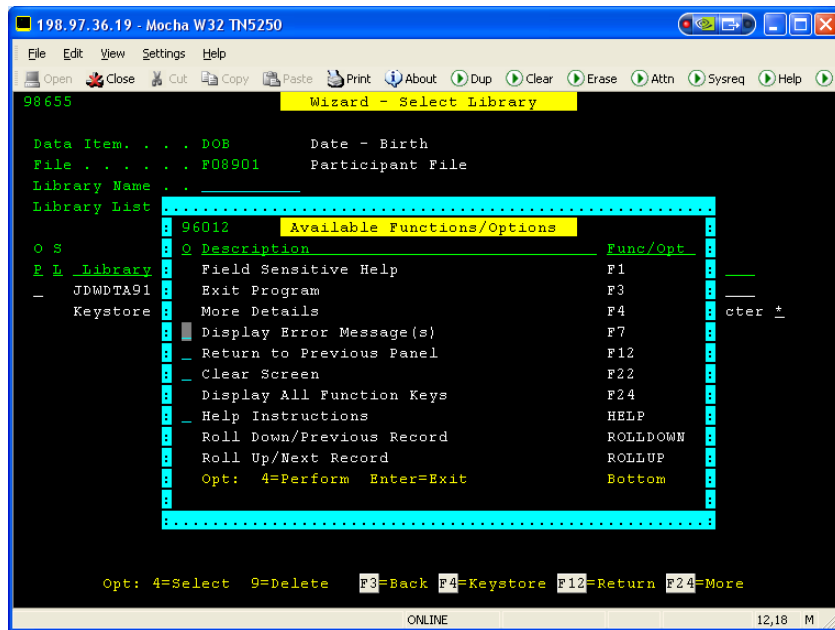


Entering 4 on the Option field next to the F08901 entry executes the Wizard – Select Library (P98655) application. The P98655 program displays the library containing the selected file based on the current Library List.



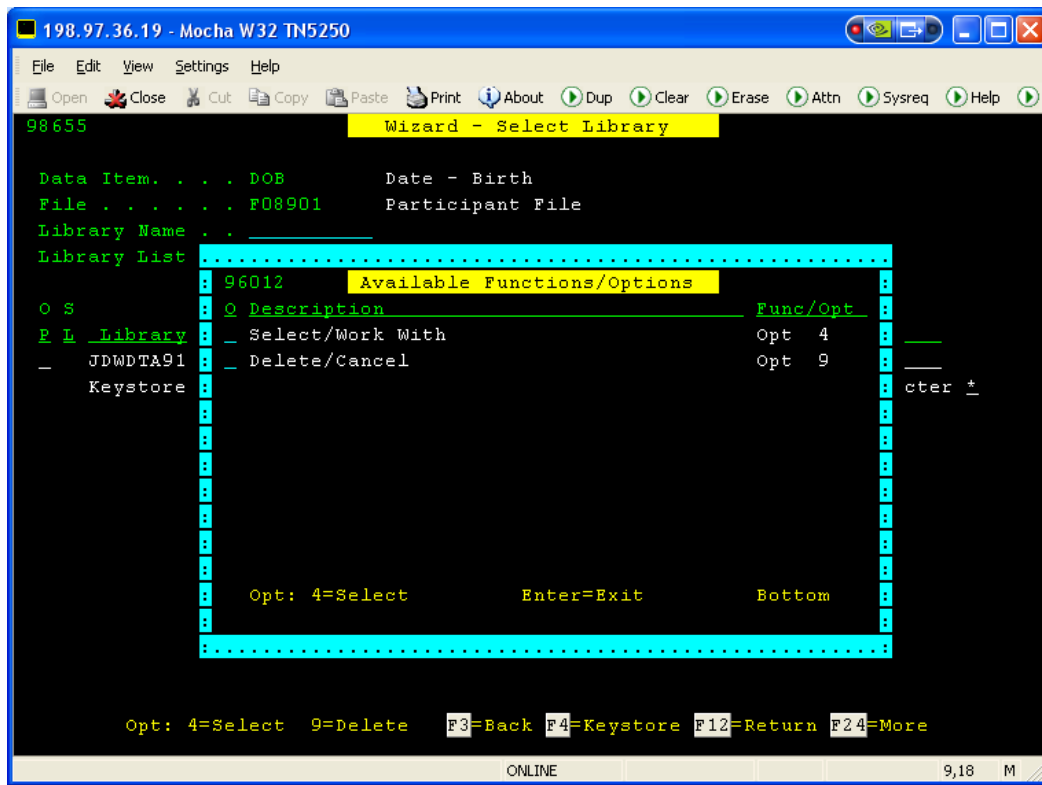
Upon entry, the system loads the default Keystore and Encryption Key information from the constants. The Justify and Fill Character are used for alphanumeric fields only and default from the constants. These can be overridden for each encryption entry.

The Function Key available on the P98654 program in addition to the standard JDE Function Keys is “Return to Previous Panel”.

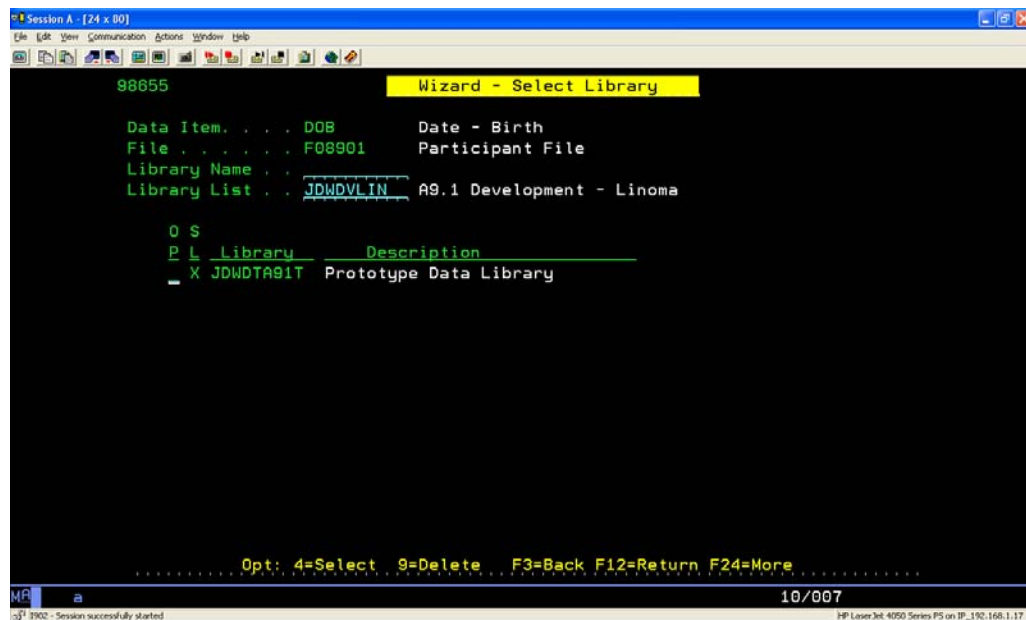


The Options available on the P98655 program include:

4. Select/Work With
9. Delete/Cancel

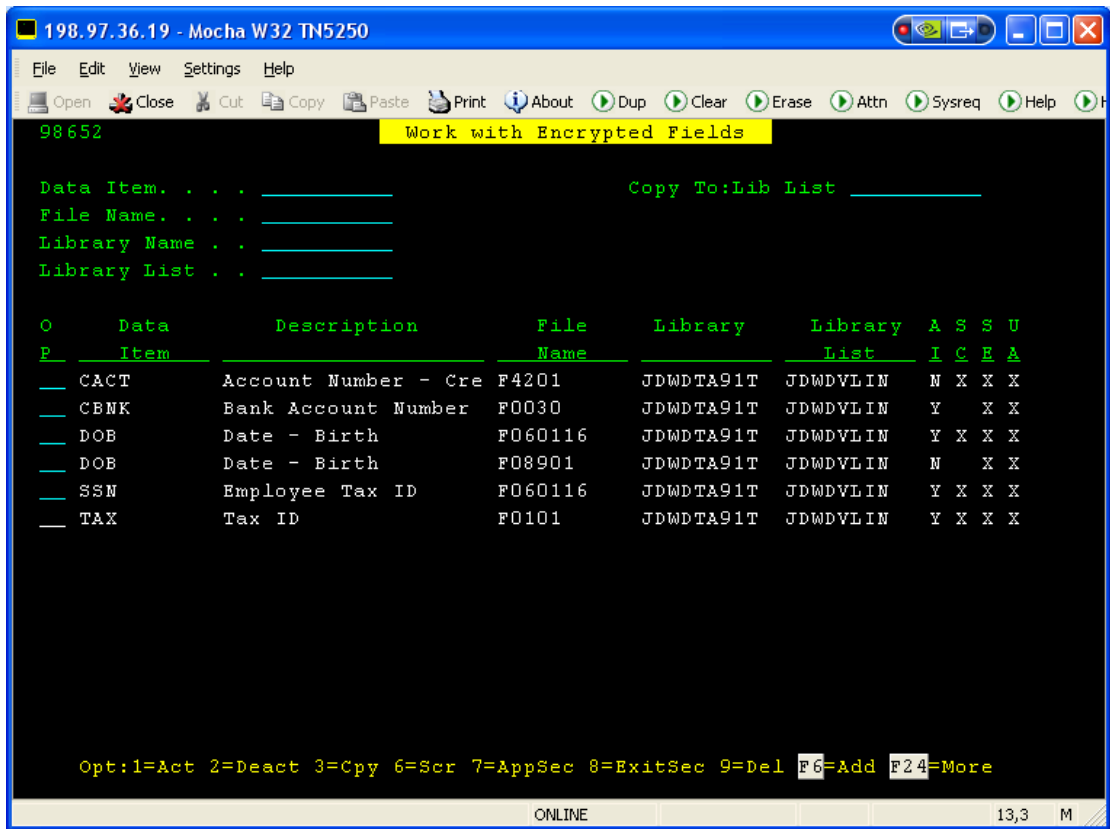


Entering 4 on the Option field next to the Library entry and pressing enter changes the Selection flag to X. This will add a registry entry for the field into the CryptoMondo registry and create default security for *PUBLIC in the security matrix screens.



Entering 9 on the Option field next to a selected Library entry and pressing enter changes the Selection flag to blank. This will remove a registry entry for the field from the CryptoComplete registry and remove default security records for *PUBLIC.

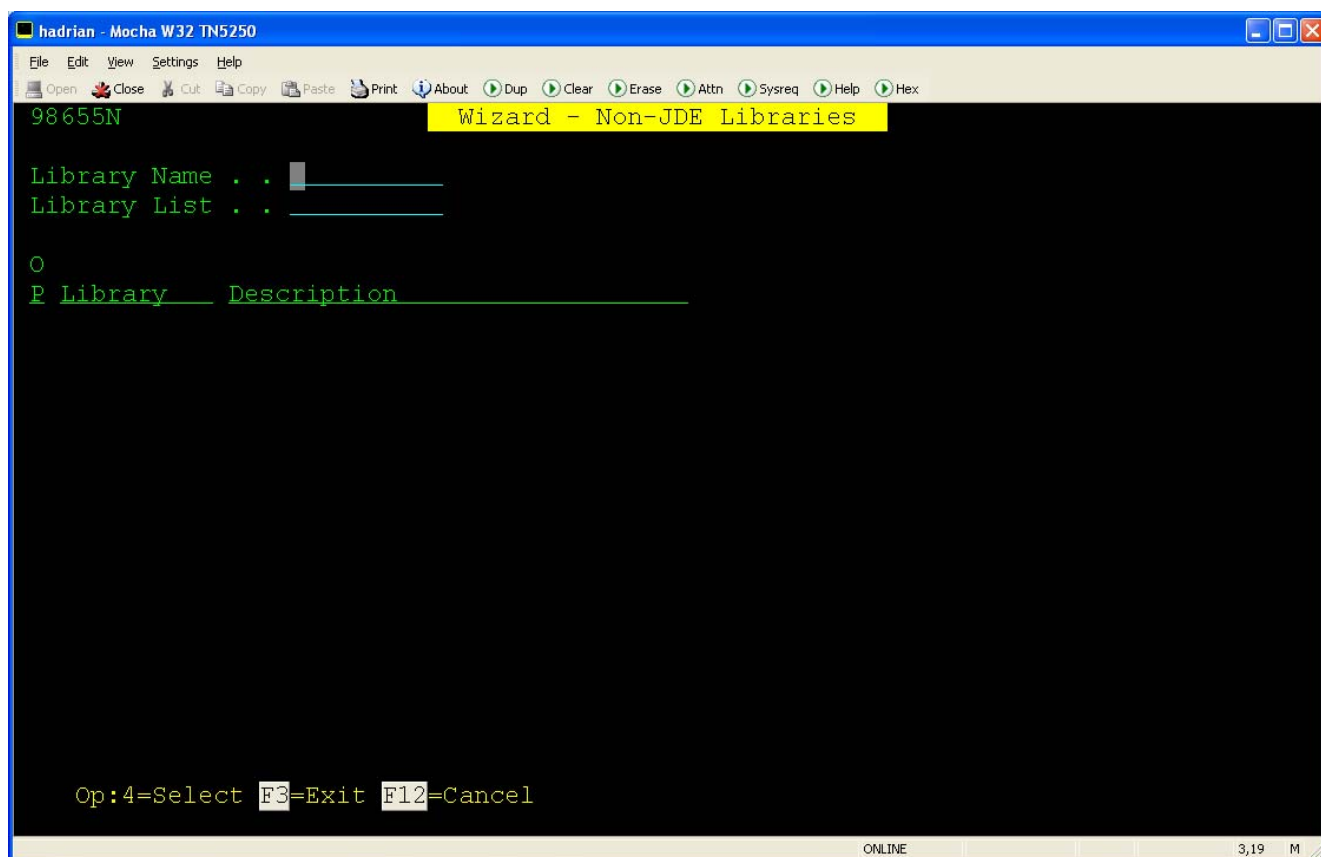
Press the F3 key 3 times or press F12 to return to the Work with Encrypted Fields screen. The new entry is now displayed.



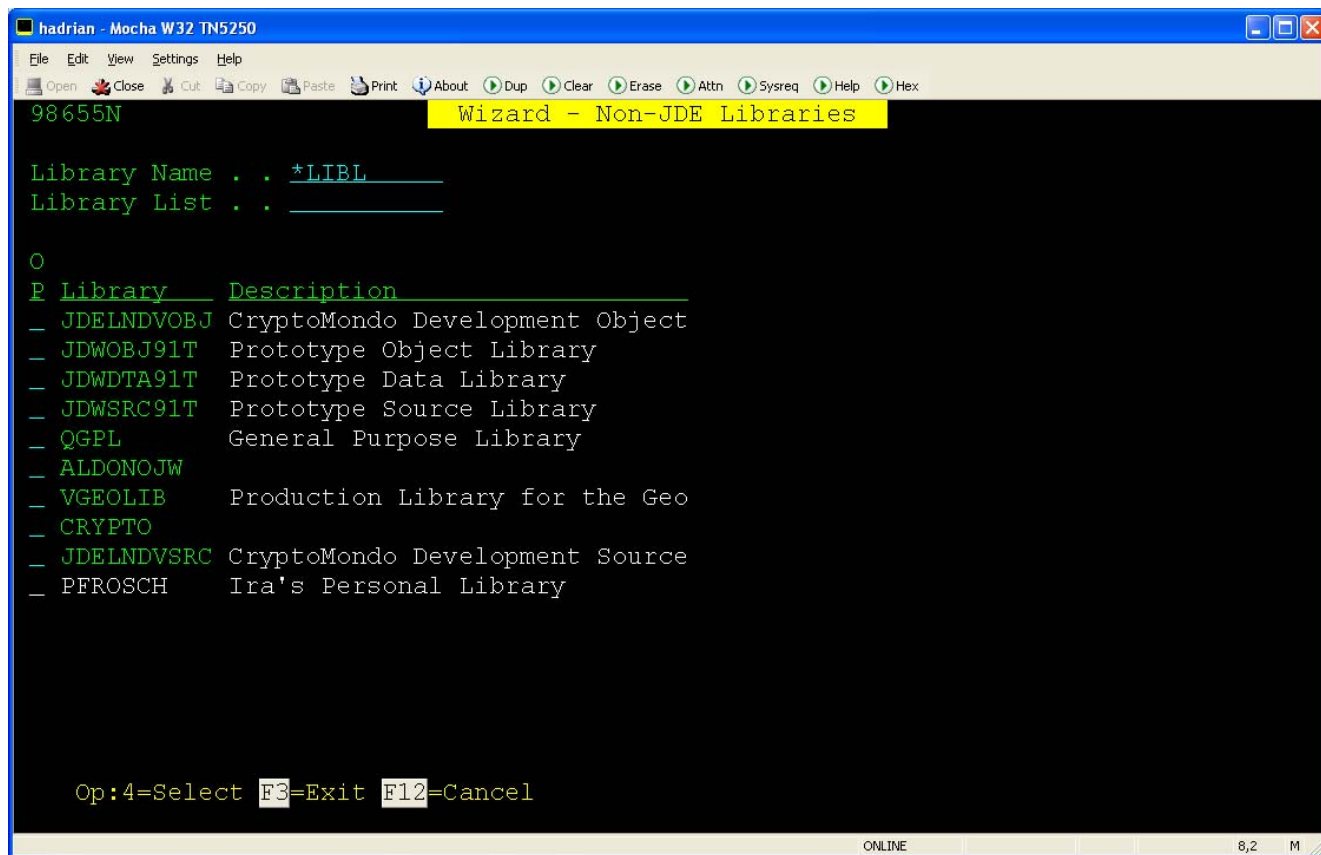
Create New Non-J.D.Edwards Encryption Entry Wizard

CryptoMondo can also encrypt non-J.D.Edwards files/fields. This is done in reverse order of JDE, as it is presumed there is no data dictionary support for these files.

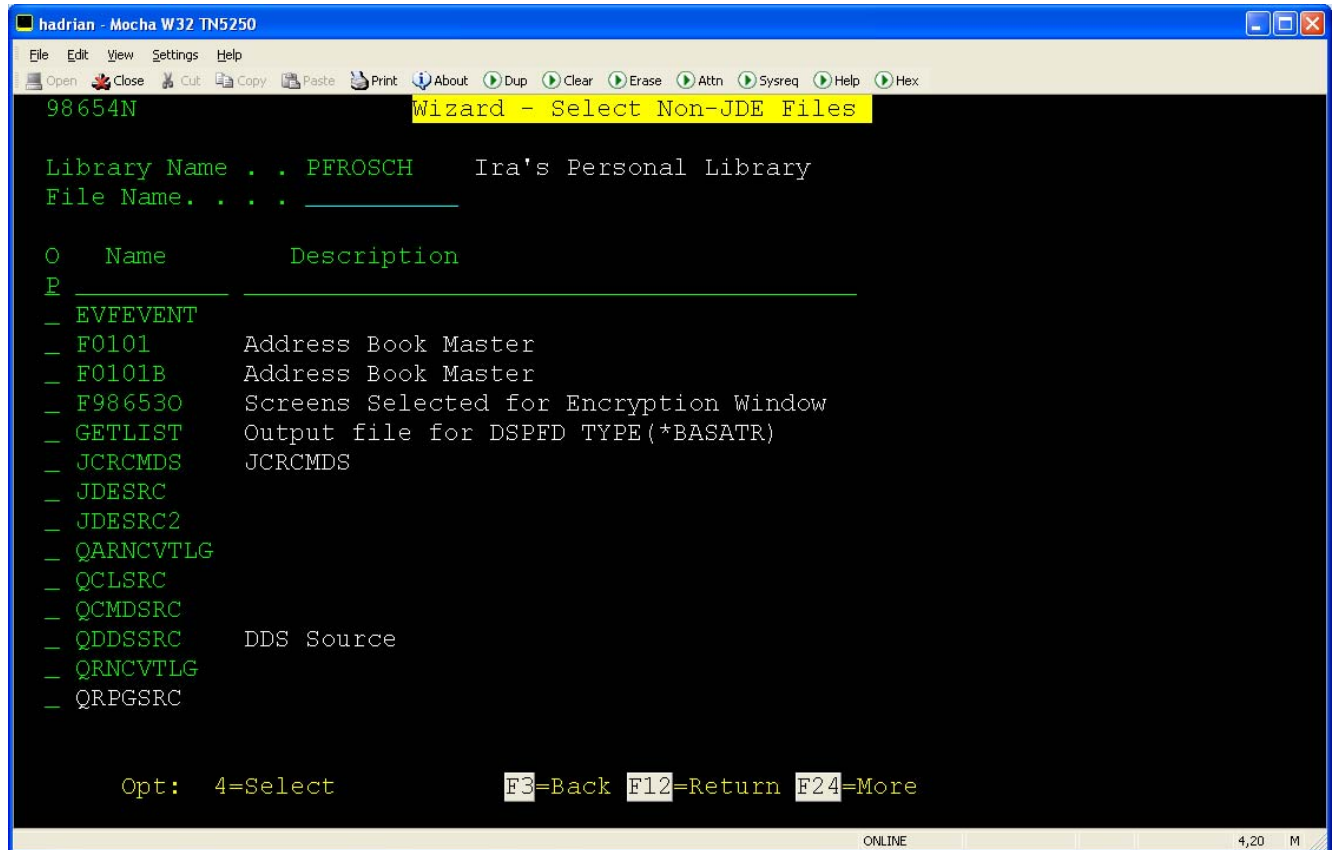
Pressing F10 begins the Create New Non-JDE Encryption Entry process by executing the Wizard – Non-JDE Libraries (P98655N) application. The user can enter a Library or a Library List to see the available libraries.



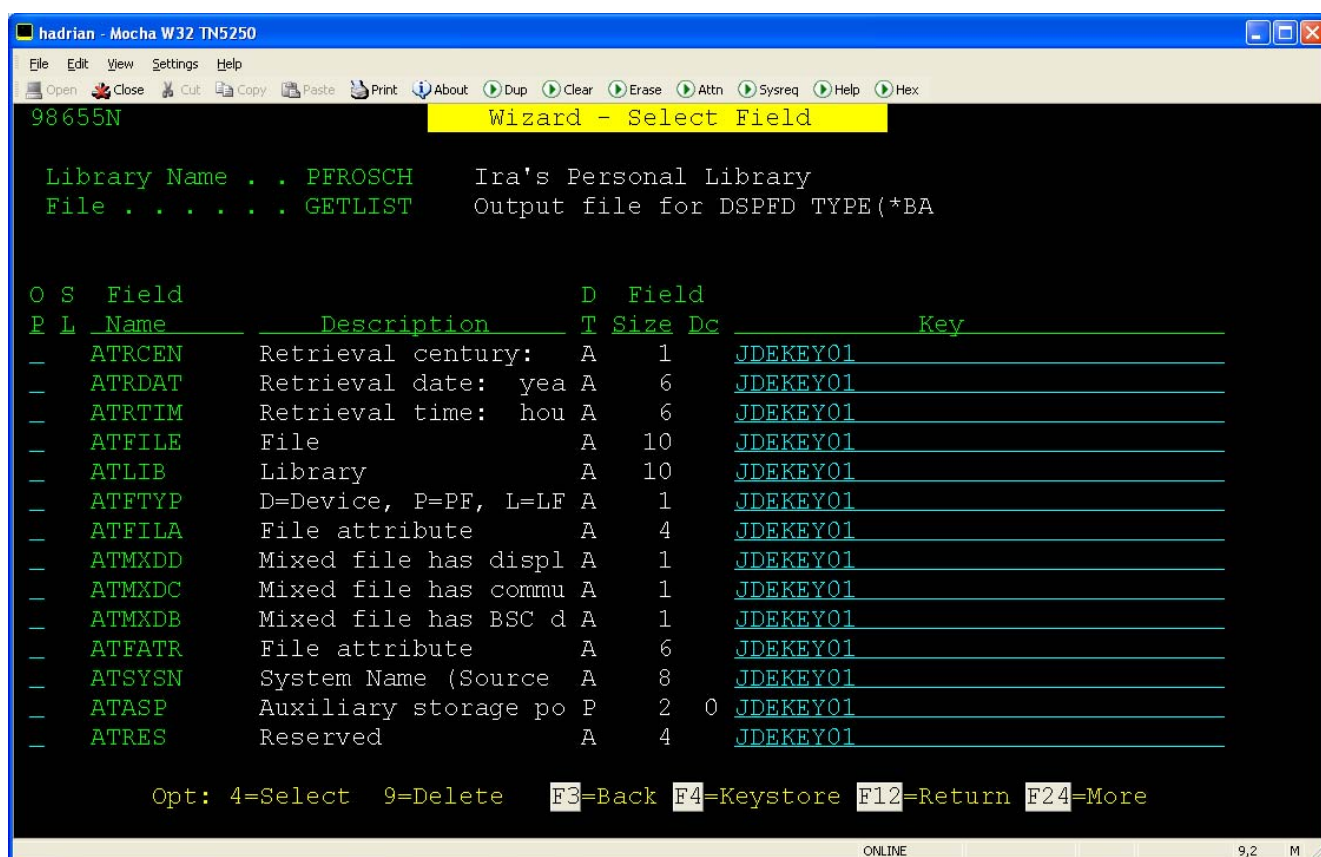
Pressing Enter defaults the Wizard to use “*LIBL” in the Library Name



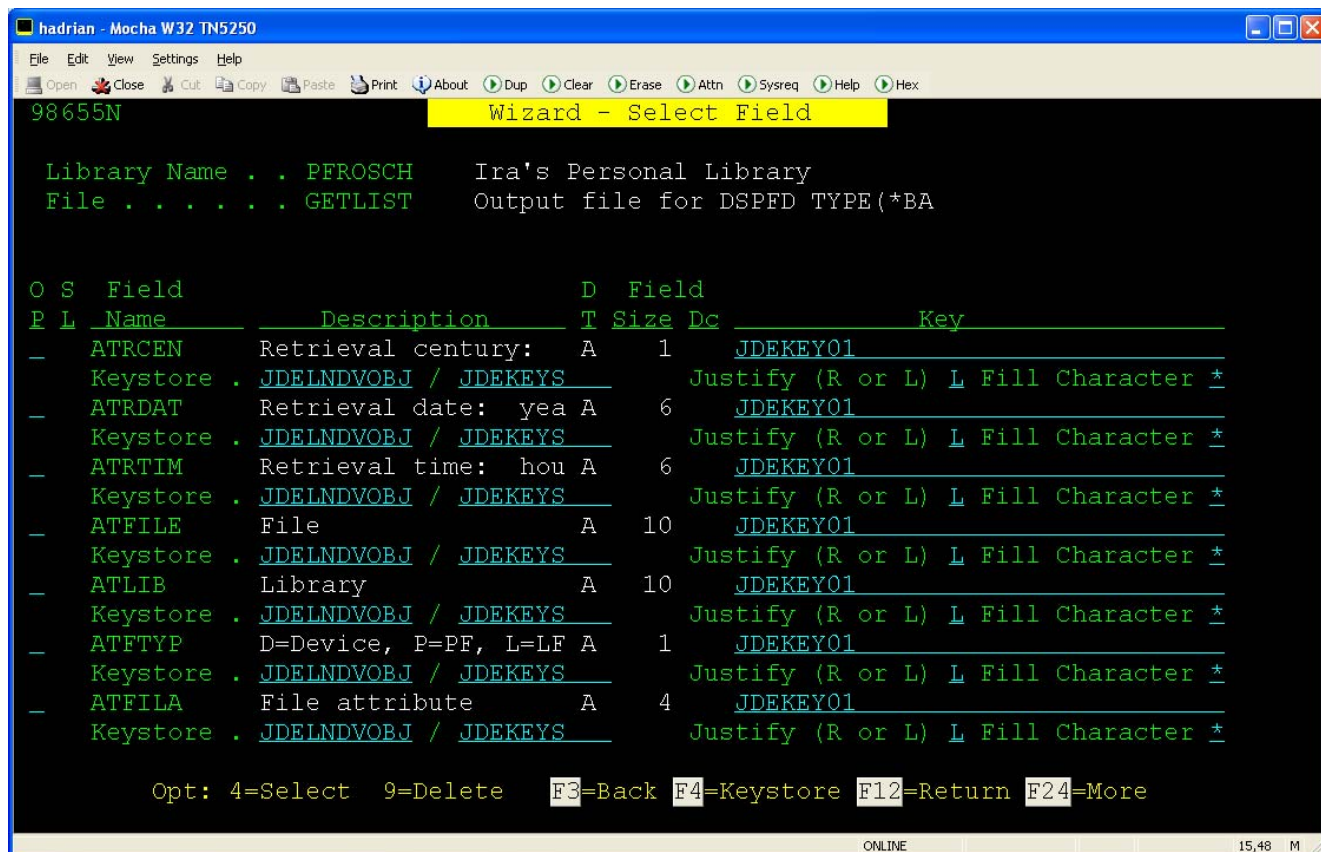
Pressing 4 next to a library will bring up the Select Non-JDE File screen (P98654N) that shows all files in the selected library.



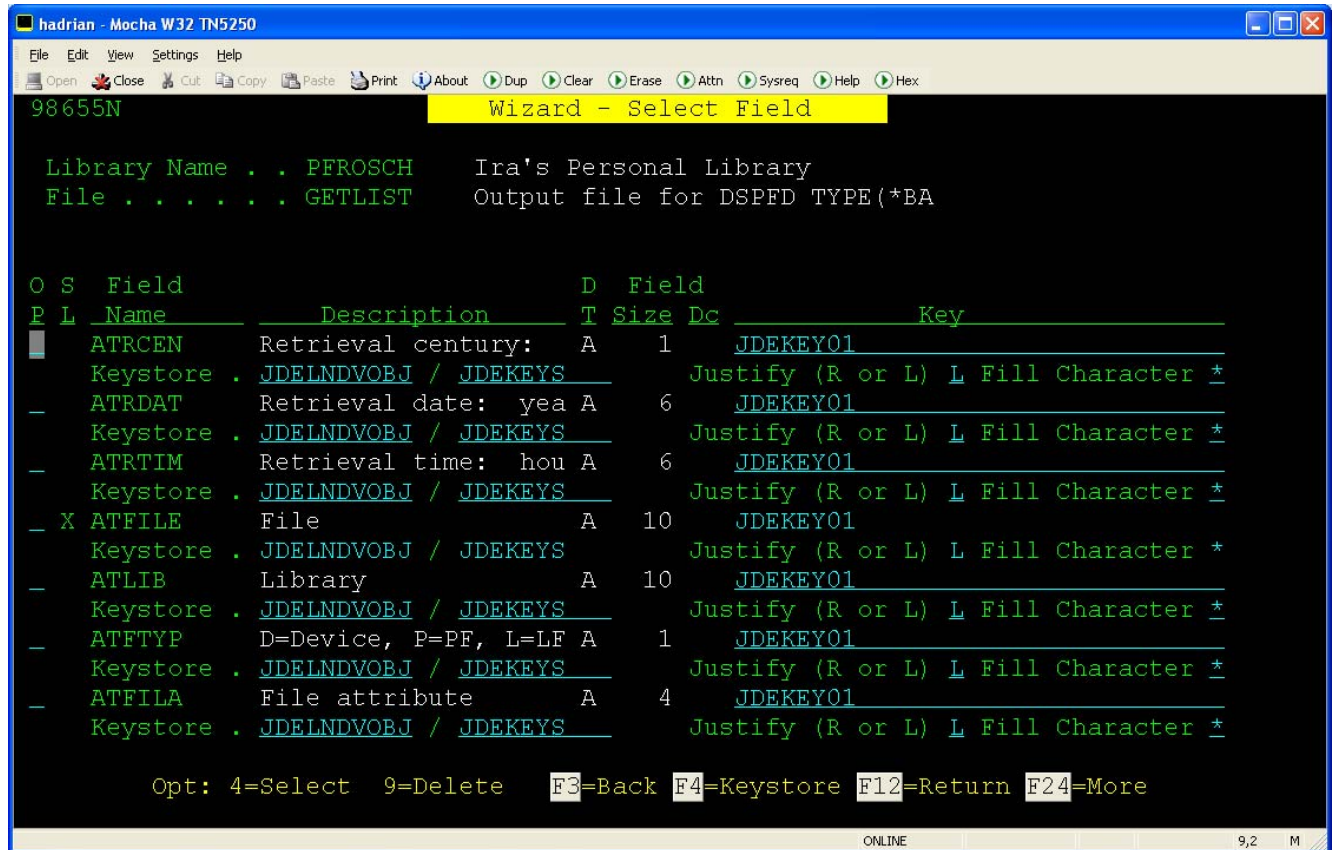
Entering 4 in the option field next to the file brings up the field list for the selected file.



Pressing F4 allows the changing of the key store and justification of alphanumeric fields



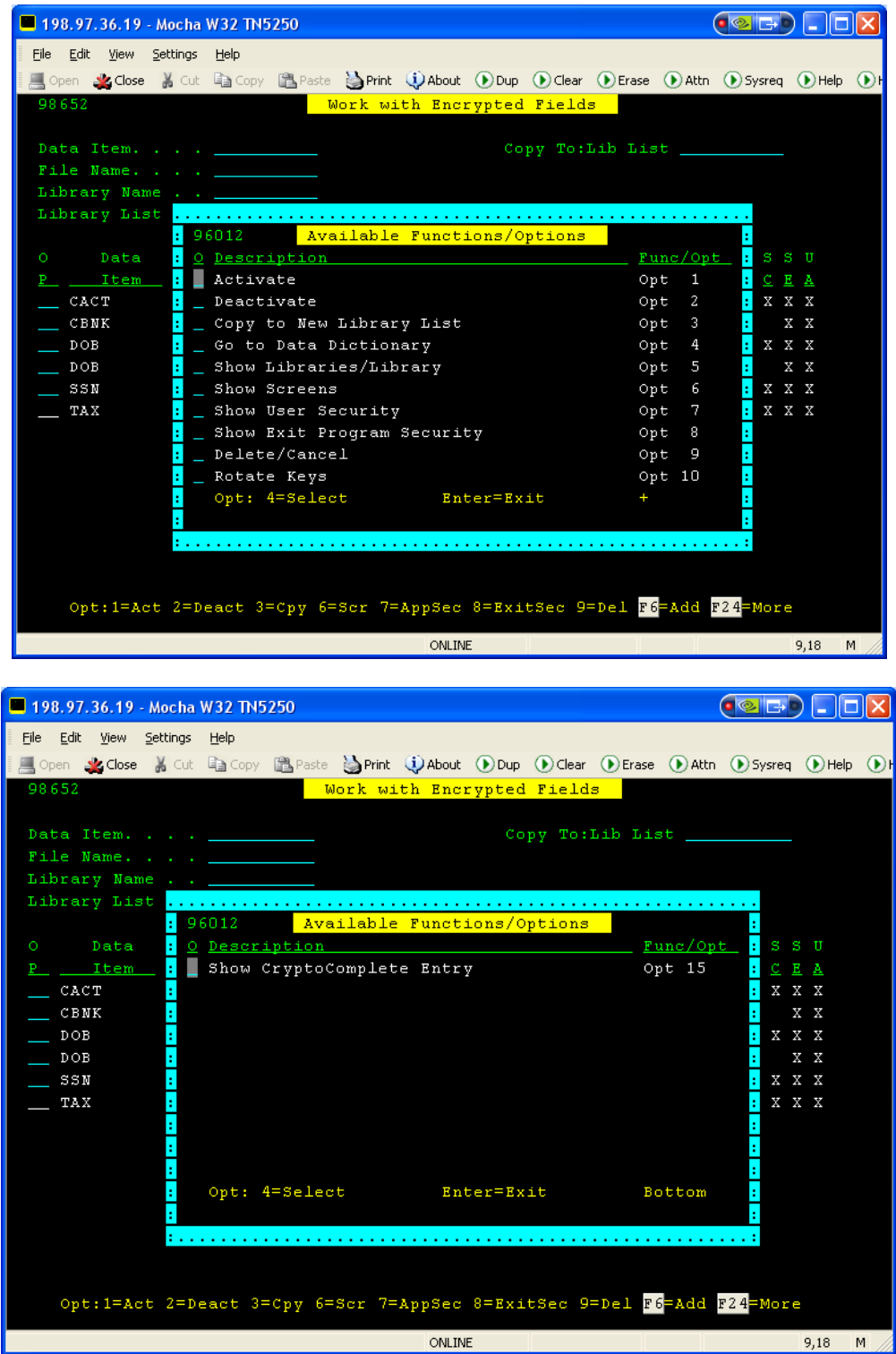
Entering 4 on the Option field next to the Field Name entry and pressing enter changes the Selection flag to X. This will add a registry entry for the field into the CryptoMondo registry and create default security for *PUBLIC in the security matrix screens.



Entering 9 on the Option field next to a selected Field Name entry and pressing enter changes the Selection flag to blank. This will remove a registry entry for the field from the CryptoComplete registry and remove default security records for *PUBLIC.

Press the F3 key 3 times or press F12 to return to the Work with Encrypted Fields screen. The new entry is now displayed.

Available Options

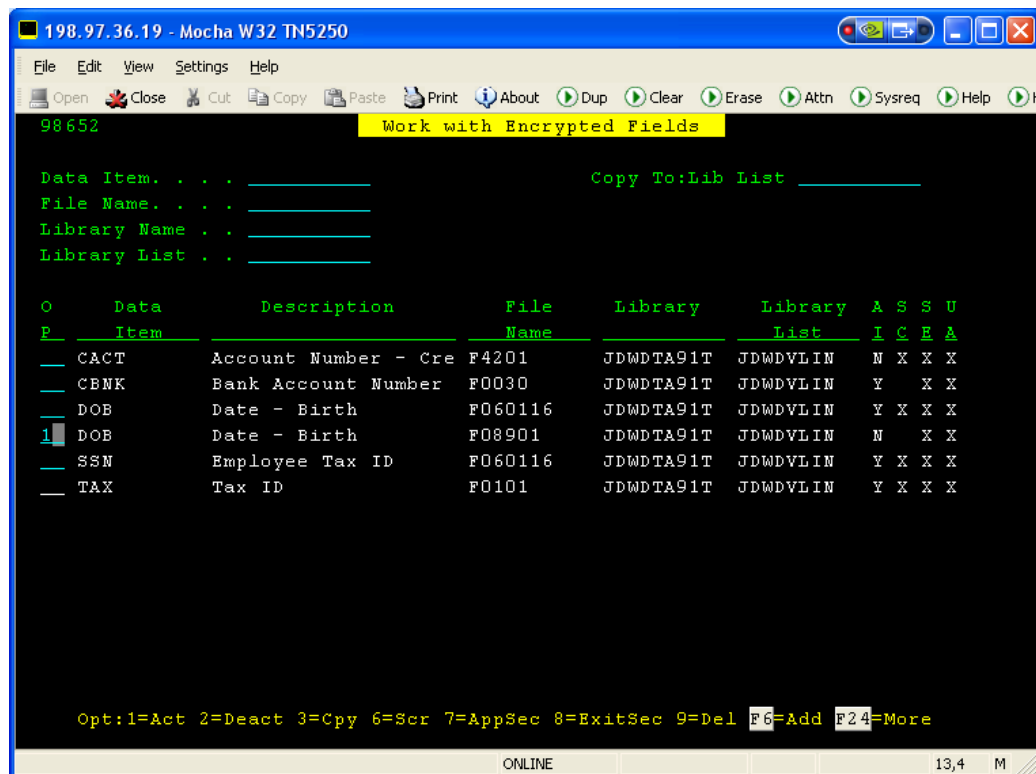


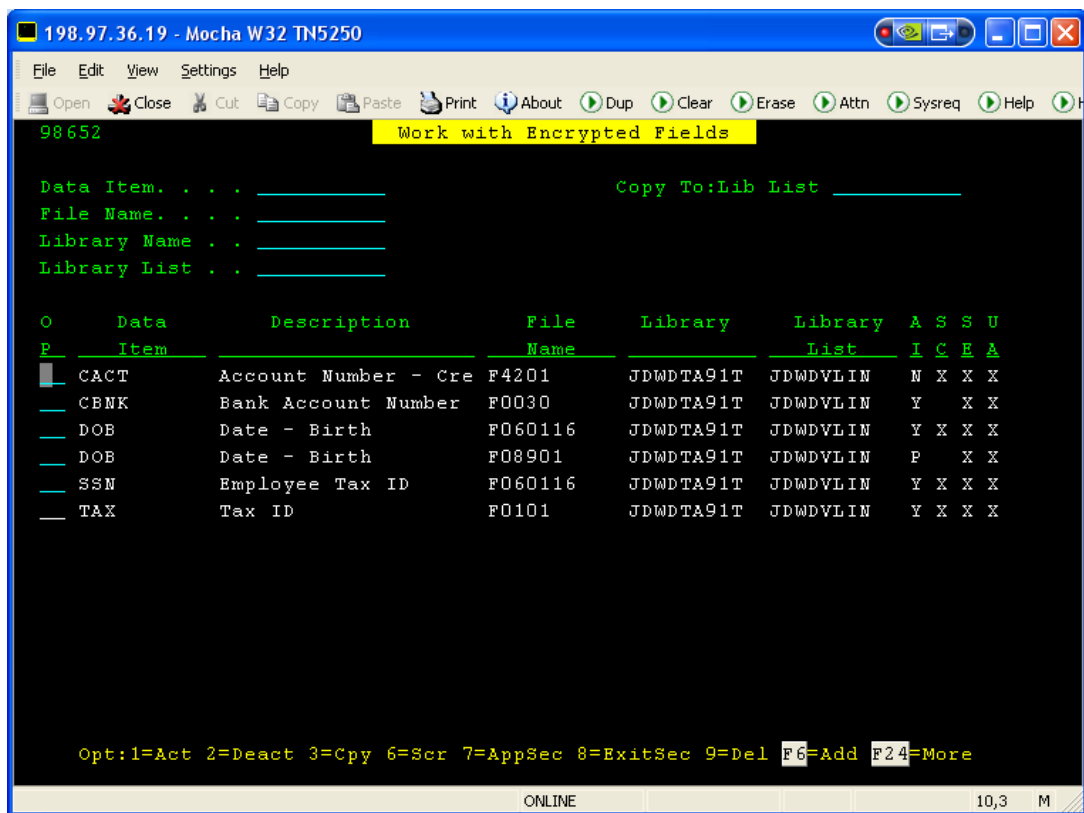
The Options available on the P98652 program include:

1. Activate
2. Deactivate
3. Copy to New Library List
4. Go to Data Dictionary
5. Show Libraries/Library
6. Show Screens
7. Show User Security
8. Show Exit Program Security
9. Delete/Cancel
10. Rotate Keys
12. Reset Entry
15. Show CryptoComplete Entry

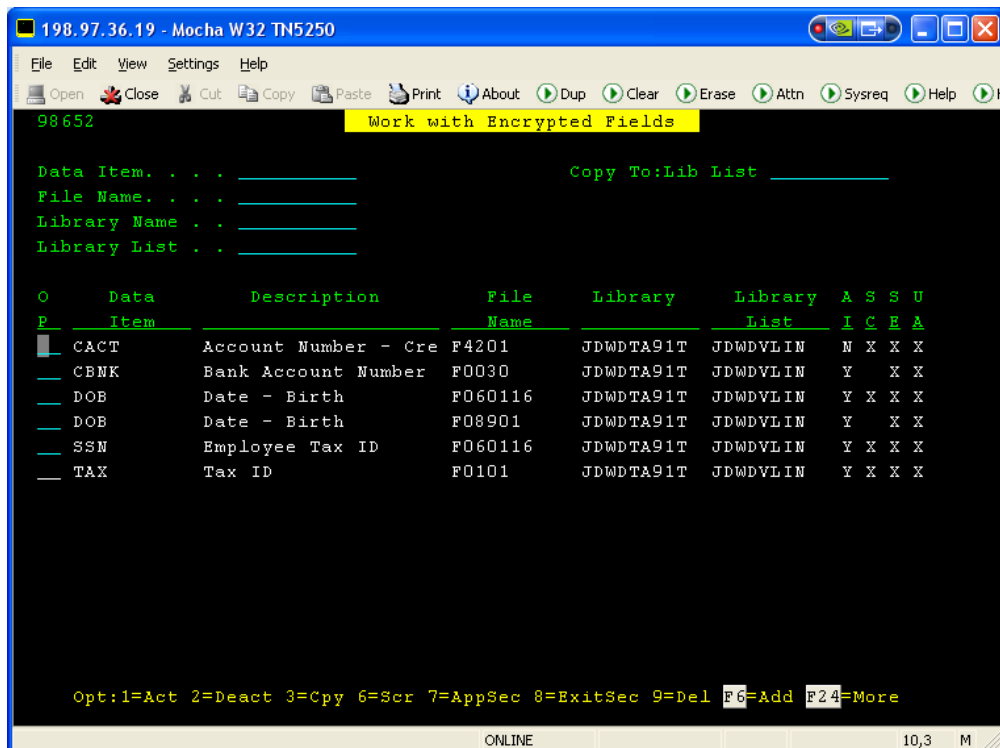
Activate

Once an Encrypted Field has been defined, it needs to be activated before either existing data or new entries are encrypted.





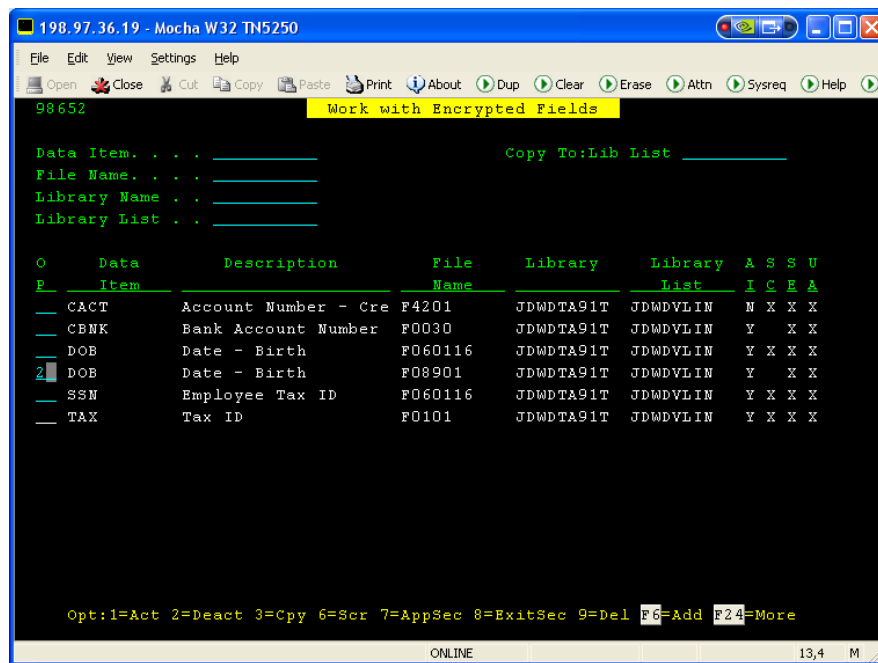
Entering 1 in the Option field next to an Encrypted Field entry that is inactive submits the encryption process to batch. The submitted job adds the triggers to the selected file and creates the external file that will contain the encrypted value. The "AI" will be set to 'P' after launching this command that tells you the entry is in queue. When processing is occurring, it will change to 'E' for Encrypting. When complete, it will change to 'Y'.

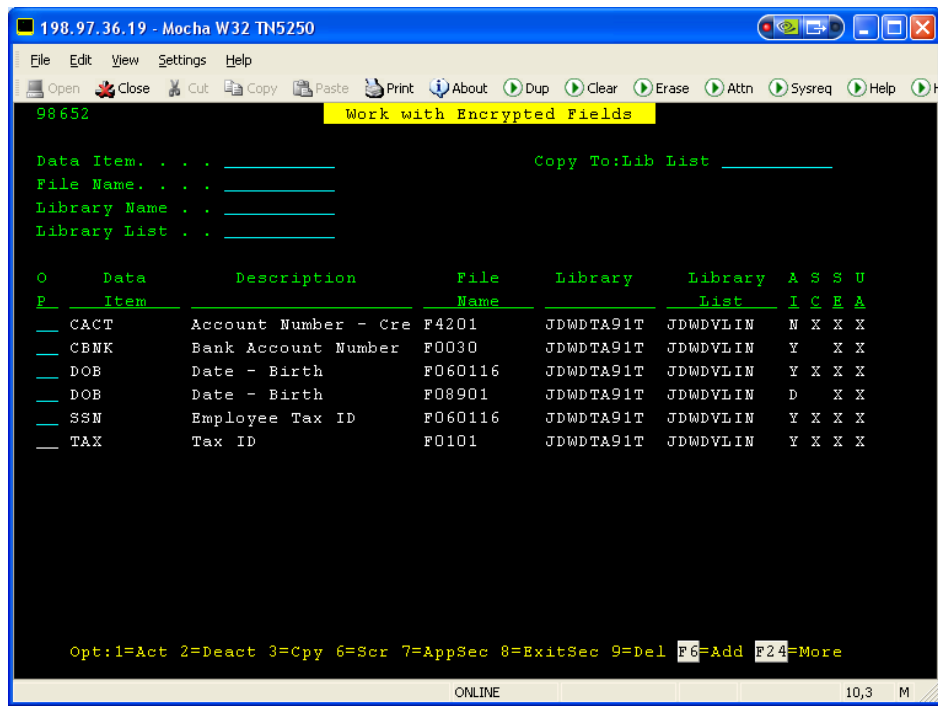
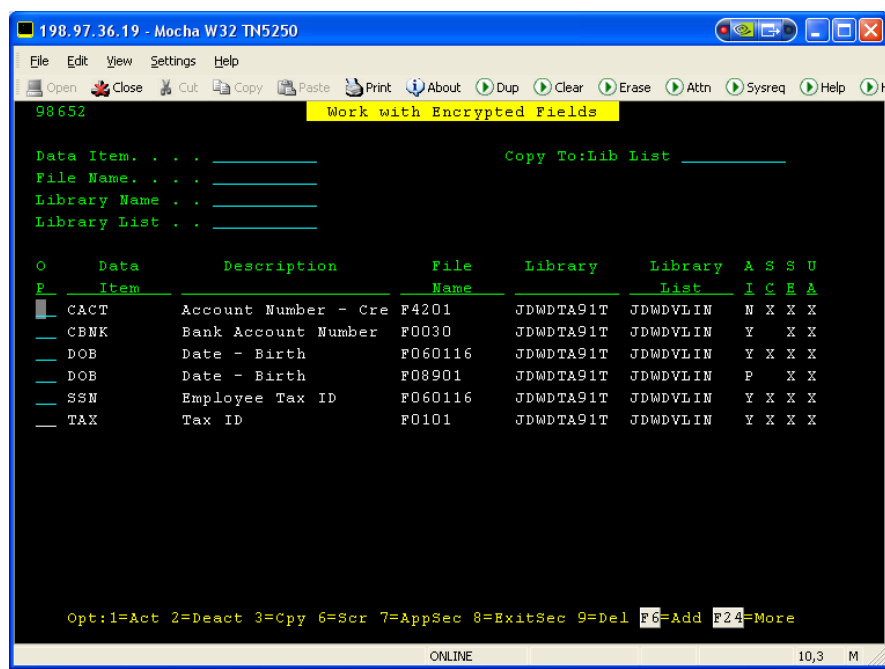


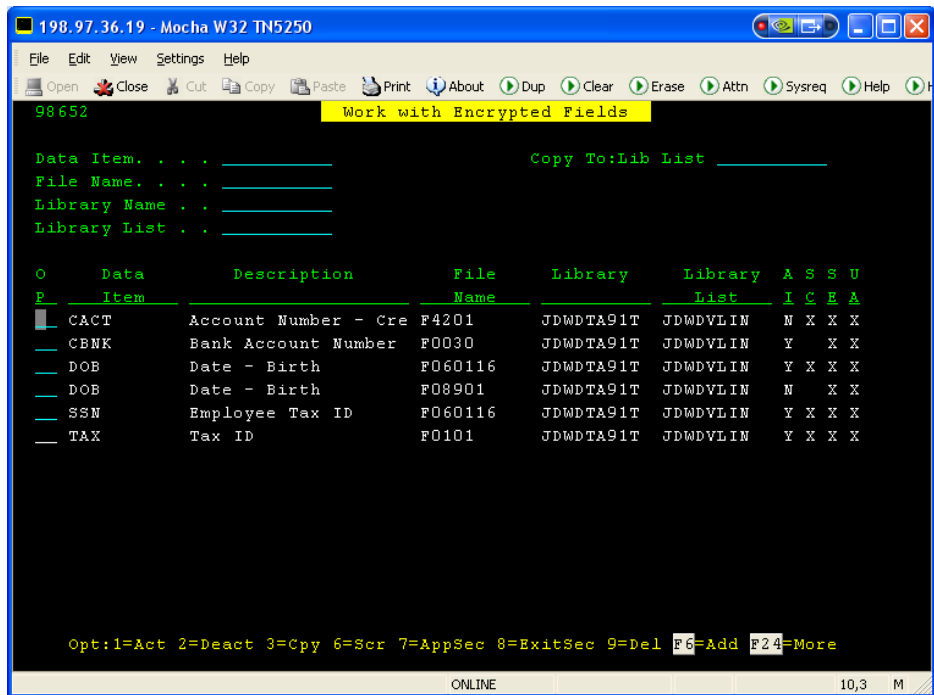
Deactivate

An encrypted field that has been activated can be deactivated thereby returning the encrypted values back to the decrypted values, removing the triggers from the affected file, and removing the external file containing the encrypted value.

The decryption process is submitted to batch and the Active/Inactive field is set to “P” for in Queue, ‘D’ when decrypting, and ‘N’ when decryption is complete.



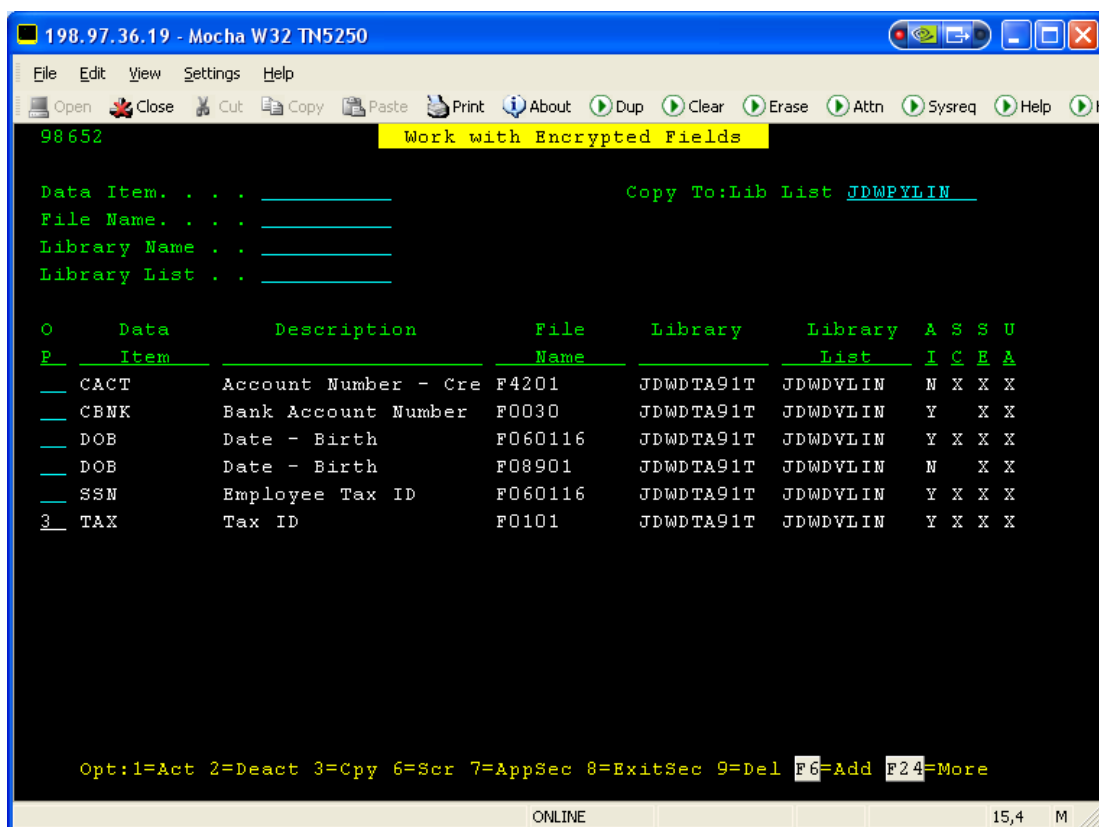




Copy to New Library List

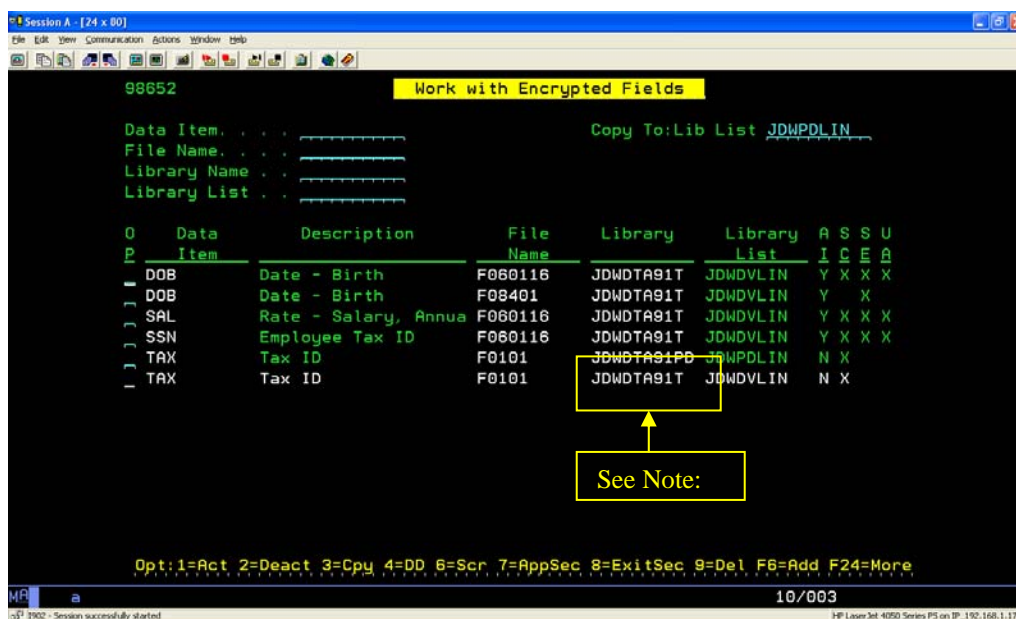
An encrypted field can be copied from one Library List to another so that once an encrypted field has been defined and tested in a development or prototype environment it can easily be copied into another environment. This would be for testing and then copying the entry to production. Copying also duplicates the security, generic exits, and screens for an entry.

For example, copying the TAX encryption from the JDWDVLIN Library List to the JDWPDLIN Library List requires that the User enter a 3 in the option field next to the TAX Data Item and entering JDWPDLIN in the Copy To Lib List field and pressing enter.



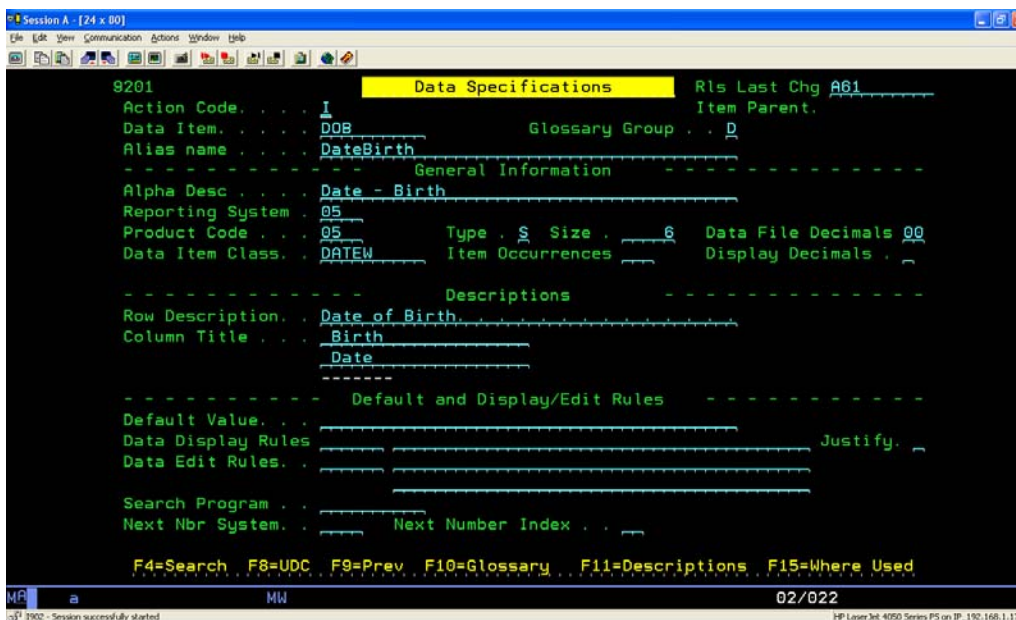
Once the field has been copied to the new Library List, it is displayed on the screen.

Note: Ensure that the “To Lib List” points to a different Library for the file as well as control files. You do not need to copy if it is in a different library list but the same library. The system will error if a different library is selected.



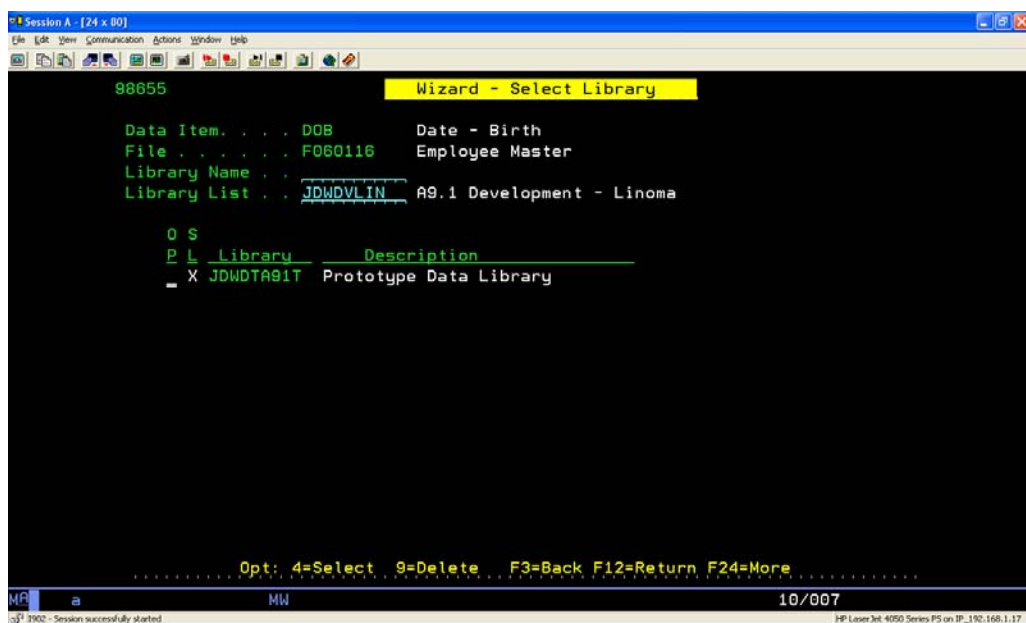
Go to Data Dictionary

Entering this option displays the JDE Data Dictionary definition for the data item.



Show Library/Libraries

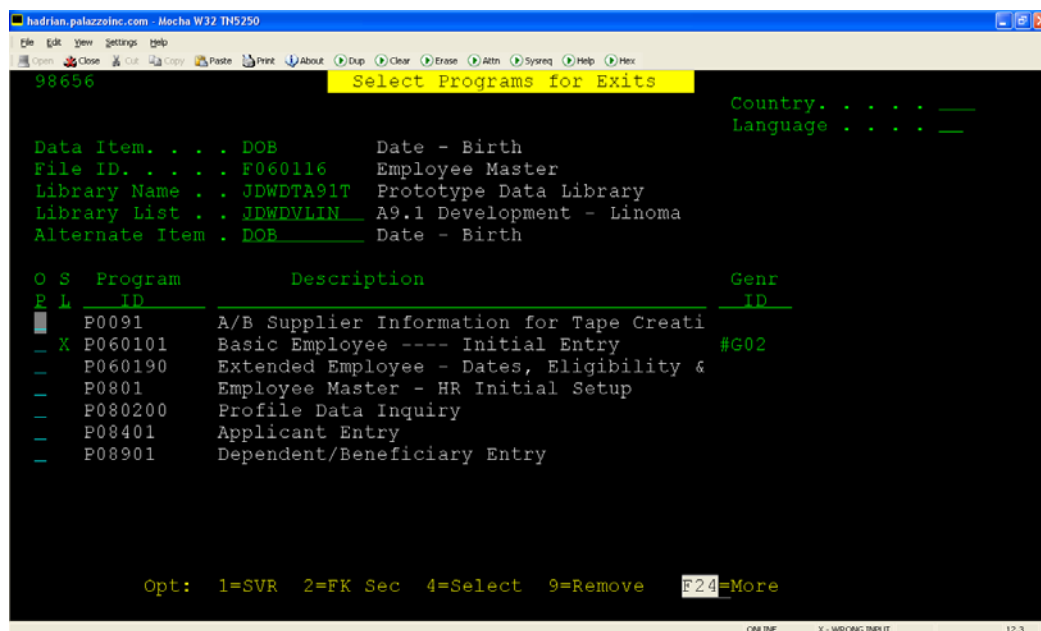
Entering this option executes the Wizard – Select Library (P98655) application displaying the library or libraries containing the file that is attached to this encrypted data item.



Show Screens

Entering this option executes the Select Programs for Exits (P98656) application used to enable the Generic Exit function for any application displaying the encrypted data item.

You may override the data item that is used for lookup using the “Alternate Item” field. This allows fields that are encrypted with one data item in the database file to have a generic exit created that uses the screen name of an object. For example, the tax id may be identified as TAX on the address book, but TX2 in another field.



The Options available on the P98656 program include:

1. Software Version Repository

9801 Software Versions Repository

Action Code . . . I
Member ID . . . P060101
Description . . . Basic Employee ---- Initial Entry
Function Code . . . RPG RPG Programs
Function Use . . . 111 File Maintenance
Product Code . . . 05 Time Accounting and HRM Base
Reporting System . . . 07 Payroll
Base Member Name . . . P060101 File Prefix . . .
Maint/RSTDSP . . . Omit Option . . . Generation Sev . . .
Copy Data (Y/N) . . . Optional File . . . Common File . . .

Precompiler Commands/Dream Writer Form

Source	Object	Source	SAR	Version	S	D	User	Date
P Library	Library	File	Number	ID	C	P	ID	Modified
JVDV0BJ	JVDV0BJ	JDESRC2	5		4		JVICUNA91	07/10/07
PSWSRC73T	PSWOB73T	JDESRC	5	A73PC00015	1		JDE	02/06/04
JDWSRC91T	JDWOB91T	JDESRC	5	A91	1		JDE	01/14/99

Opt: 1=Browse 2=Edit 3=Copy 5=SAR 8=Print 9=Dlt 10=Design 14=Crt

2. Function Key Security

9612 Function Key Security

Action Code . . . I
Video Screen . . . V060101 Basic Employee ---- Initial Se
-OR-
User ID . . .

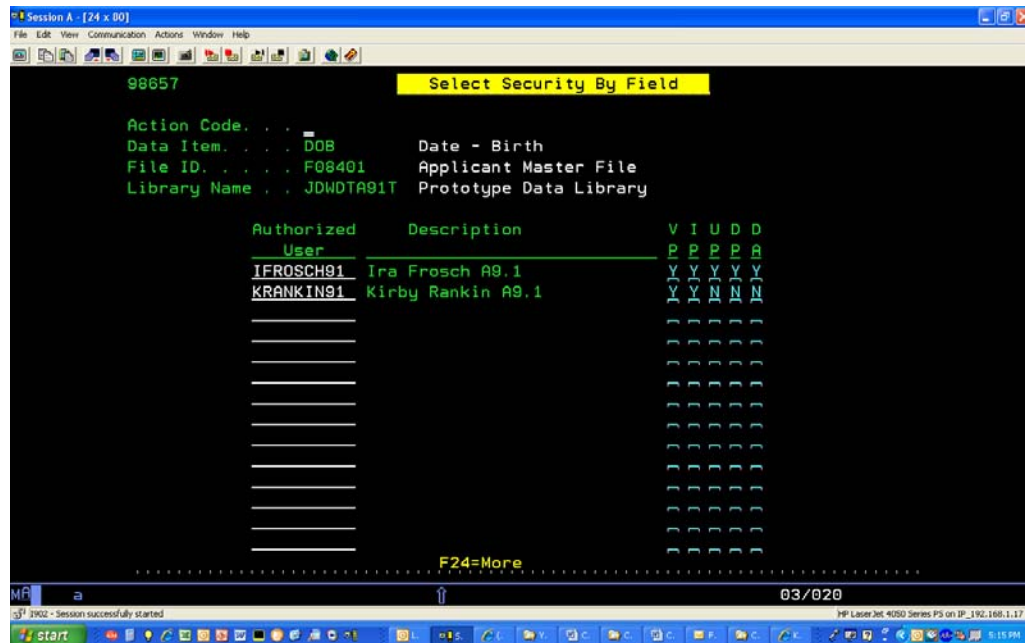
User	Description	Field	Description	A
*PUBLIC	All users	#G01		N
*PUBLIC	All users	#G02		N
*PUBLIC	All users	#G03		N
IFROSCH91	Ira Frosch A9.1	#G01		Y
IFROSCH91	Ira Frosch A9.1	#G02		Y

F3=Exit F24=More Keys

- 4. Select – this will add the next generic exit in sequence and add a default “*PUBLIC” function key security entry into the standard function key security table. The value comes from the constants.
- 9. Delete/Cancel - this will remove the generic exit entry as well as remove any Function Key Security overrides from the standard function key security table

Show User Security

Selecting the Show User Security option executes the “Select Security by Field” (P98657) application used to set the privileges for each user. Security can be set by user, group, or *PUBLIC. The *PUBLIC record comes in automatically when libraries are set from the constants.



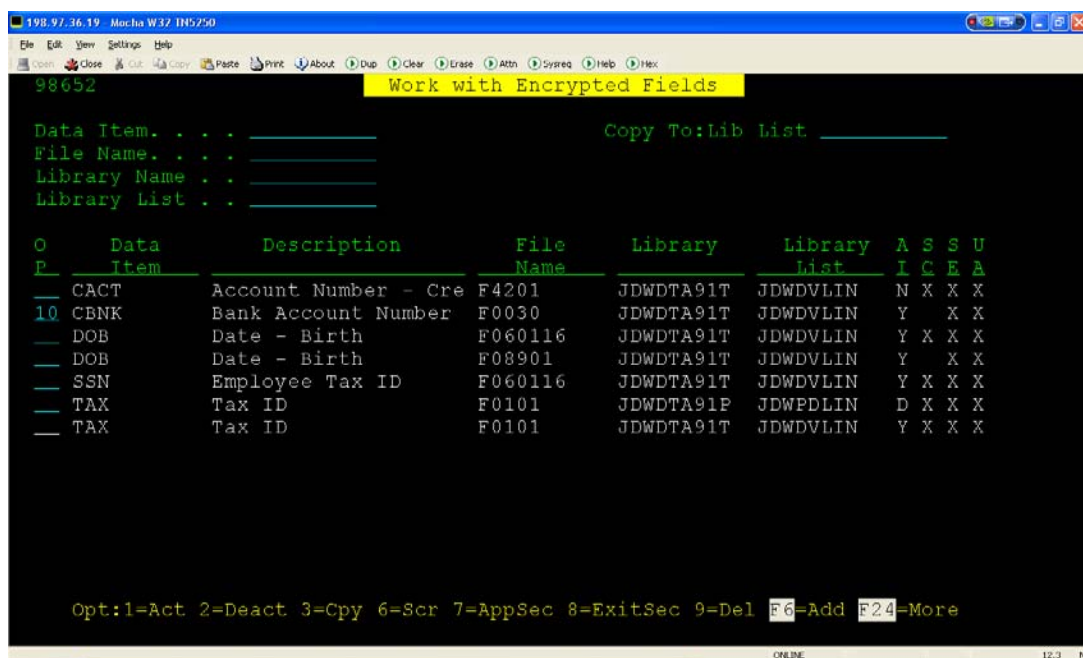
To add a new user or group, put a 'C' in the action code, put the user name in the Authorized user field and select the values for the different types of security. The five security types are:

- View (VP) – Ability to view the unencrypted value
- Insert (IP) – Ability to insert new values in an encrypted field
- Update (UP) – Ability to update values of an encrypted field
- Delete (DP) – Ability to delete values within an encrypted field
- Debug (DA) – Ability to use the debug feature in order to maintain encrypted fields

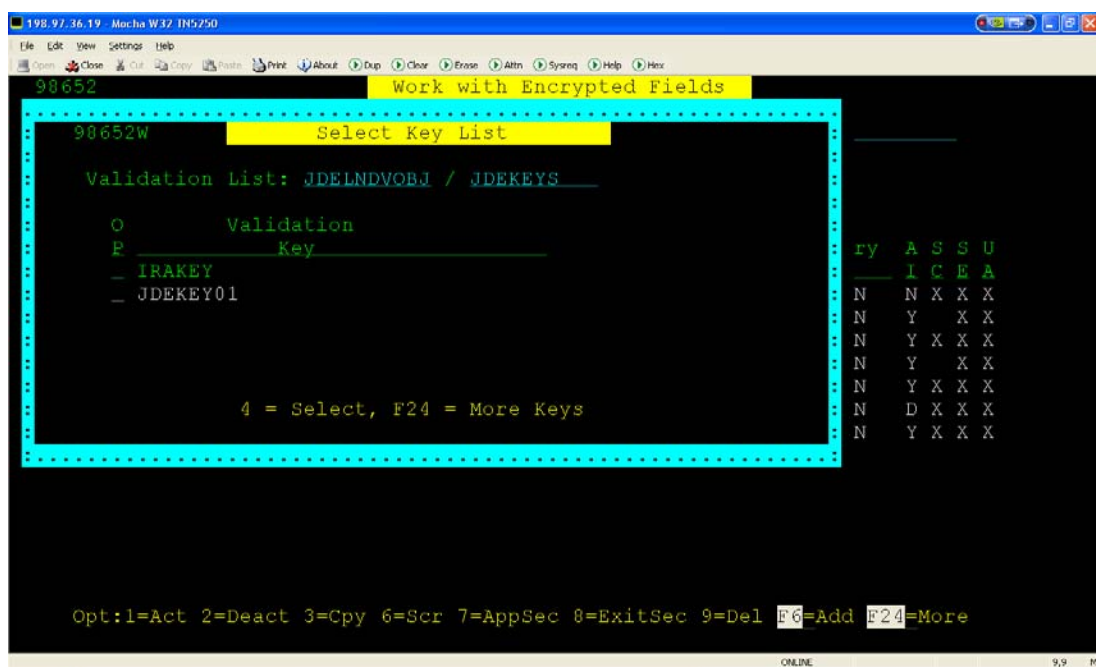
To remove users or groups, put a 'C' in the action code, blank out the user name, press enter, and the record will be deleted. To delete the entire listing, put a 'D' in the action code and press enter.

Show Exit Program Security

Selecting this option executes the “Security for Exit Program” (P98658) application used to identify which exit program applications are approved to update encrypted fields.



After selecting option 10, the select validation key window allows you to select the new key.



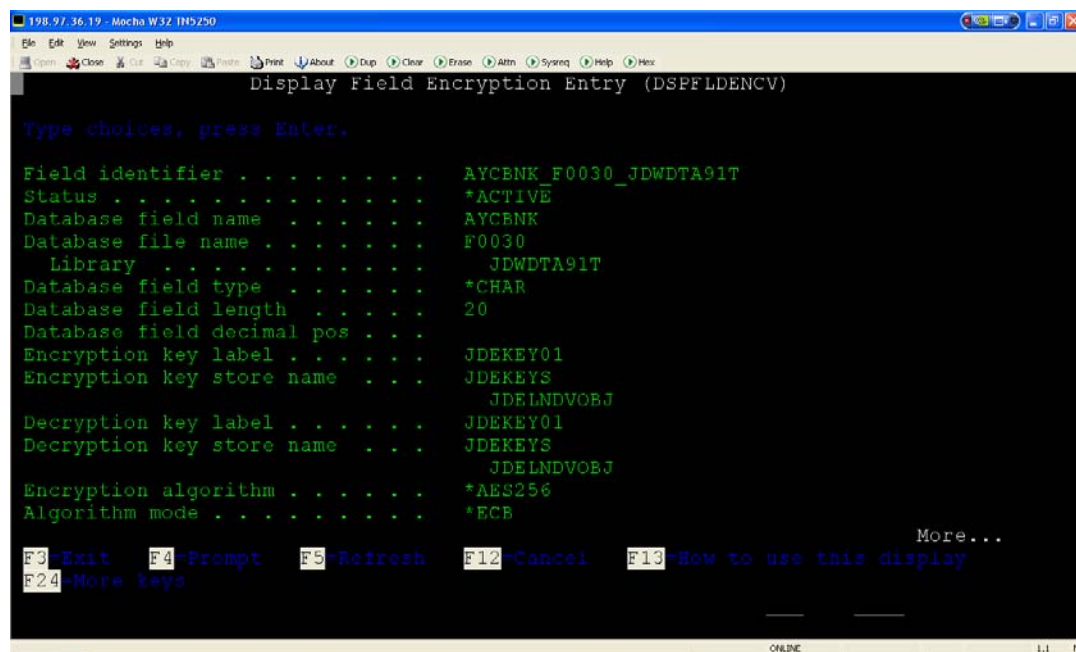
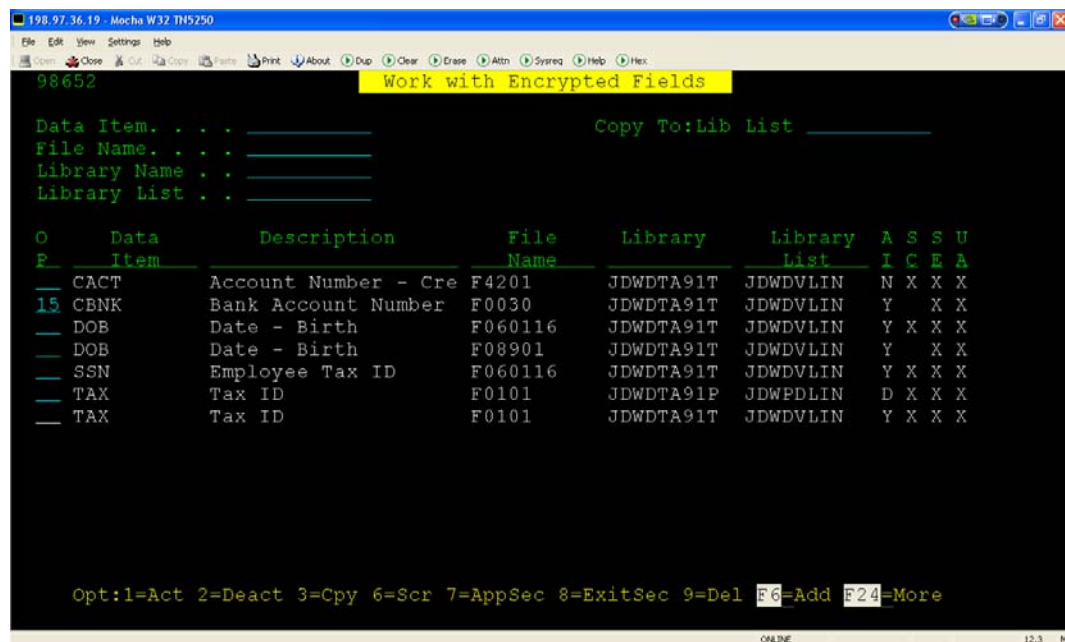
A batch job is launched to perform the rotation.

Reset Status

The encryption entry in CryptoMondo may become out of sync with the status of the CryptoComplete entry due to failure of the batch job to encrypt/decrypt. Option 12 will “reset” any statuses that are in encryption/decryption status without completion. Use this status only when a batch encryption/decryption job ends abnormally.

Show CryptoComplete entry

This option allows the user to see the entry in CryptoComplete.



```

198.97.36.19 - Mocha W32 TH5250
File Edit View Settings Help
Open Close Cut Copy Paste Print About Dup Clear Erase Altin Syntag Help Hex

Display Field Encryption Entry (DSPFLDENCV)

Type choices, press Enter.

Calculated cipher text length . 24
Calculated block length . . . . 24
Store values in external file . *YES
External file name . . . . . CRXX00003
                                JDWDTA91T
Store hash for security check . *YES
Store last retrieved user/time . *YES
Index number alignment . . . . . *LEFT      *LEFT, *RIGHT
Index number padding character '+'      Character value
Last index number issued . . . . 3
Use triggers to auto encrypt . . *YES
Trigger name for inserts . . . . F0030_AYCBNK_CRYPTINSERT
Library . . . . . JDWDTA91T
Trigger name for updates . . . . F0030_AYCBNK_CRYPTUPDATE
Library . . . . . JDWDTA91T

More...

F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys

ONLINE 1.1 M

```

```

198.97.36.19 - Mocha W32 TH5250
File Edit View Settings Help
Open Close Cut Copy Paste Print About Dup Clear Erase Altin Syntag Help Hex

Display Field Encryption Entry (DSPFLDENCV)

Type choices, press Enter.

Trigger name for deletes . . . . F0030_AYCBNK_CRYPTDELETE
Library . . . . . JDWDTA91T
Trigger exit program type . . . . *PGM      *NONE, *PGM, *SRVPGM
Trigger exit program . . . . . X98654      Name
Library . . . . . *LIBL      Name, *LIBL
Last modified by user . . . . . IFROSCH91
Last modified date/time . . . . . '2008-06-26-16.11.46.268000'

Bottom

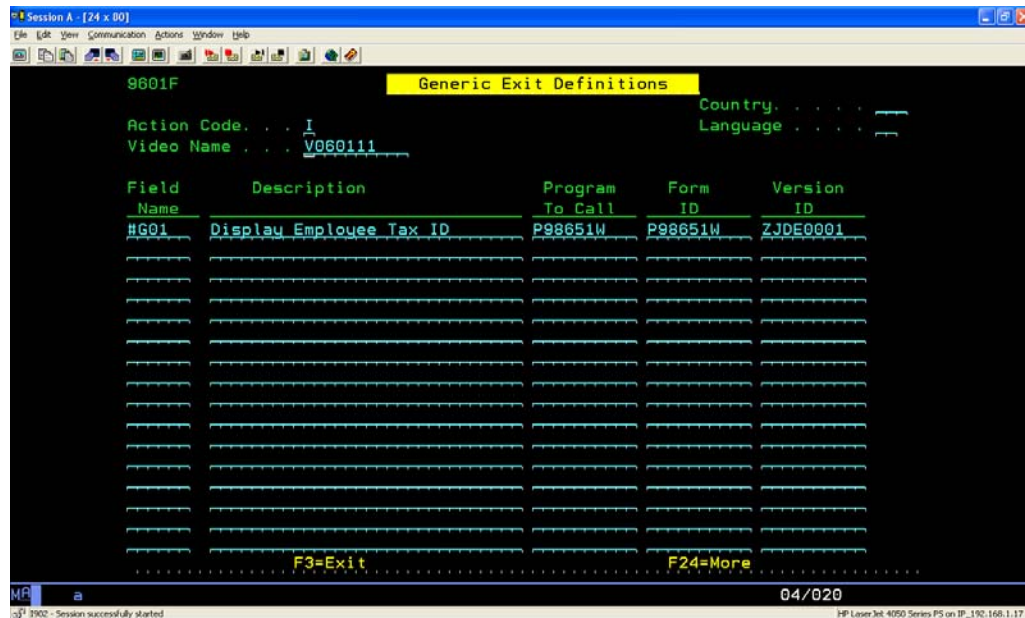
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys

ONLINE 1.1 M

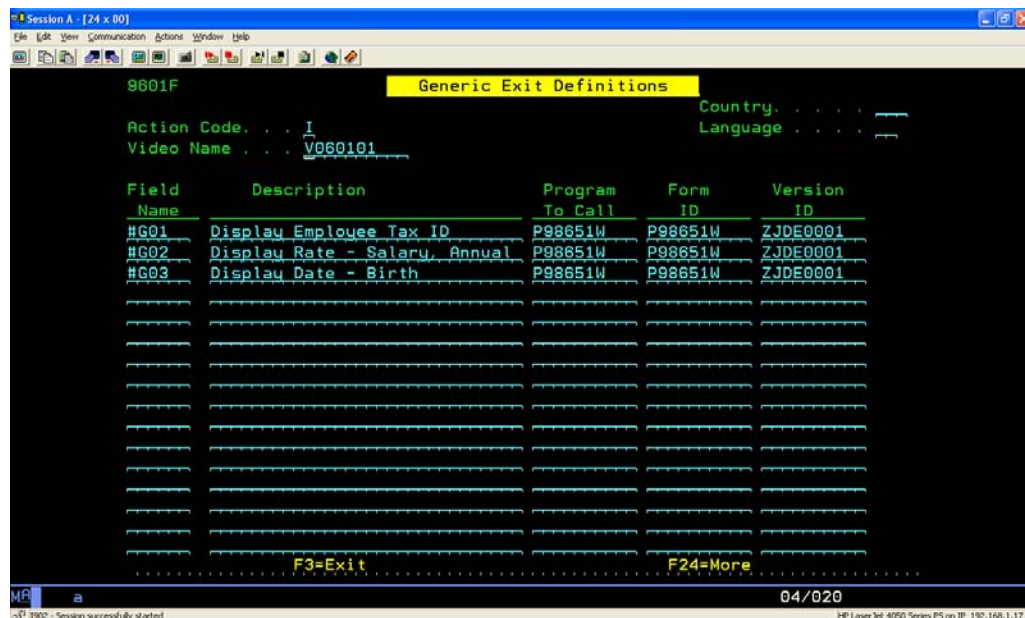
```

Generic Exit Definitions

Access the Generic Exit Definitions application by entering 16/ENCRYPT on the command line. CryptoMondo utilizes the Generic Exit Definitions to display encrypted information within a JD Edwards window. This application can be utilized to access the Generic Exits defined by the CryptoMondo system. The screen below shows the generic exits defined for a screen having 1 encrypted field.



The screen below shows the generic exits defined for a screen having 3 encrypted fields.



Inside the application, the screen looks as follows:

hadrian - Mocha W32 TN5250

060101 Employee Entry

Action Code. . . I

Employee No. . . 100009 Andretti, Mario L. Address Number . . 100009

Social Sec. No 3***** Home Company . . 00001

Add'l EE No. . . Home Business Unit . . W10

Name (F/M/L). M L Security Bus. Unit . . W10

Salary . . . 250,000.00 (A,M,S,B,W) A Date Started . . 01/04/2002

Hourly Rate. . 120.192 Pay Period Gross Orig. Hire Date. . 01/04/1900

Billing Rate . 125.000 10,416.67 Date Pay Starts. . 01/01/2002

Date of Birth. . .

Check Route Code . .

Department Code. .

Tax Area (Res.) . 06 Job Type/Step . /

Tax Area (Work). . 06 Pay Freq/Class S / S

Mart Stat(F/S/L) . S / S / S Pay Grade/Step /

Gender . . . M Workers Comp . 3365 / -

Category Cd 1 & 2. FLA Exmpt Y/N Y

Labor Load Method. 0 Benefit Group. .

Flat Bdn. Factor . 1.0000 Union Code . .

Std Hrs/Year . . 2080.00 EEO Job/Ethnic 007 / 03

F2=Taxes F5=Basic F6=Pay/Tax F15=Labor F16=DBA F21=Auto Dep F24=More

ONLINE 3,17 M

Notice the value of Social Security Number is 3***** - this means the field is encrypted. The Original Hire Date is also encrypted, as it is in the year 1900. Pressing F24 shows the generic exits.

hadrian - Mocha W32 TN5250

060101 Employee Entry

Action Code. . . I

Employee No. . . 100009 Andretti, Mario L. Address Number . . 100009

Social Sec. No 3***** Home Company . . 00001

Add'l EE No. . . W10

Name (F/M/L). 96012 Available Functions/Options W10

Salary . . . Q Description Func/Opt 4/2002

Hourly Rate. . _ Display Date - Birth *USR DFN* 4/1900

Billing Rate . _ Display Employee Tax ID *USR DFN* 1/2002

Check Route C . _ Field Sensitive Help F1

Department Co . _ Employee Tax Override Entry/Maintenance F2

Tax Area (Res . _ Exit Program F3

Tax Area (Wor . _ Contract/Calendar F4

Mart Stat(F/S . _ Basic Employee Revisions F5

Gender . . . _ Pay Rate & Tax Revisions F6

Category Cd 1 . _ Error Text F7

Labor Load Me . _ Profile Data Entry F8

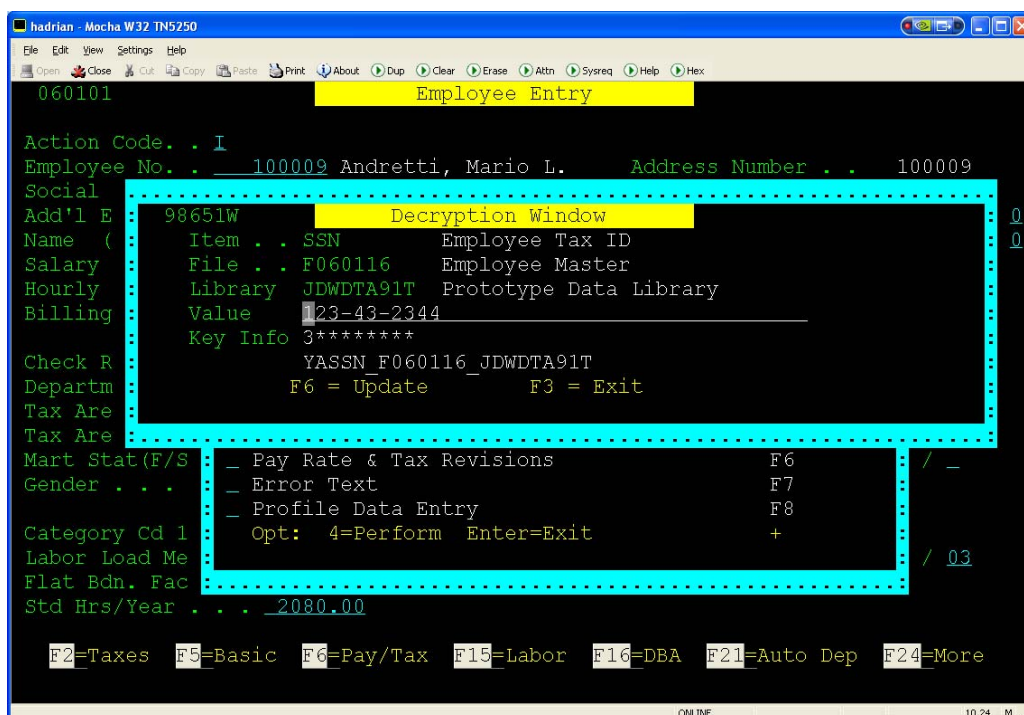
Flat Bdn. Fac . Opt: 4=Perform Enter=Exit +

Std Hrs/Year . . 2080.00 / 03

F2=Taxes F5=Basic F6=Pay/Tax F15=Labor F16=DBA F21=Auto Dep F24=More

ONLINE 10,18 M

The *USR DFN* shows that it is a “generic exit”. Putting a 4 next to the Employee Tax ID description results in the following:



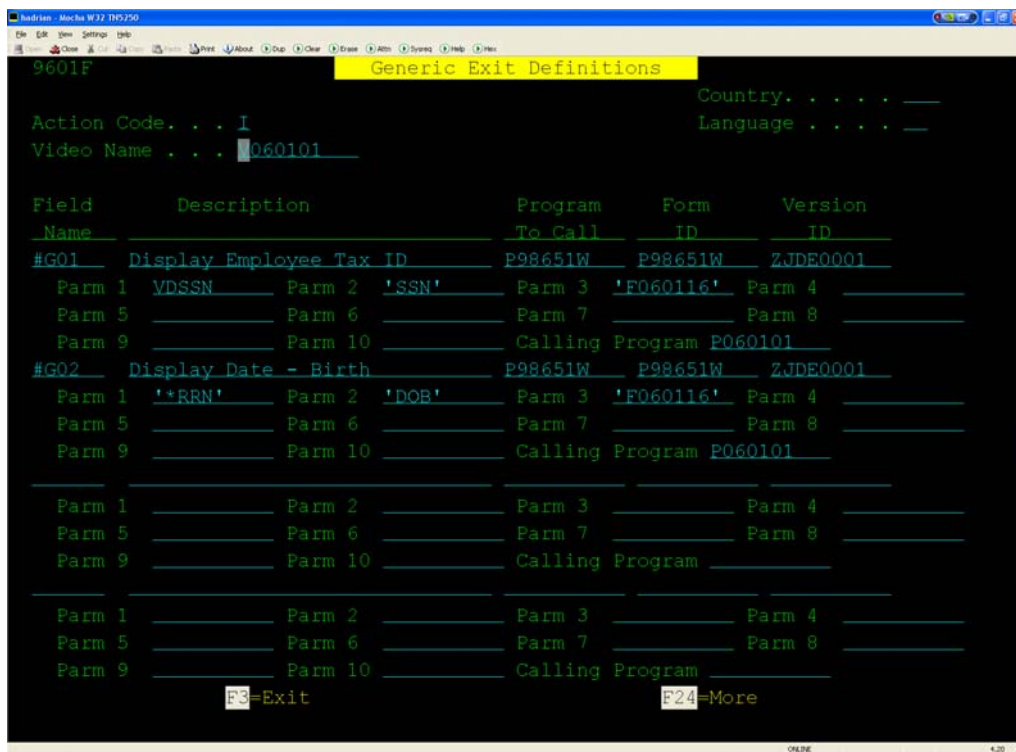
The original value is shown. If the field is underlined, that means the user has the rights to change the value. The Key Info shows based on the Debug security setting for the user.

Special Value Retrieval

In some situations, it is not possible to retrieve the value from the screen. An example is an encrypted date field in a file with more than 765 records. J.D.Edwards will display this value incorrectly in the screen as 1/1/1900, even though it could be record 800.

To handle this situation, CryptoMondo recognizes a value in the generic exits call '*RRN' in the first or fourth parameter. If the Exit Window sees this parameter, it will find the last file/logical for the selected field and determine the last read relative record number, and retrieve the value directly from the record, instead of using the value passed.

This should be used when the retrieval does not work from the main screen. Appendix B and the Palazzo website will be updated with those JDE programs that have been tested to work with this methodology. If this does not work, due to the wrong logical file being retrieved, you may need to add custom code. Sample code exists in the CryptoMondo library.



Reverse Lookup

In some situations, the user knows the hidden value, but needs to determine the encrypted key value. This would be most common for instances of knowing a Social Security Number, but not necessarily the associated Key value.

CryptoMondo provides a “reverse lookup” utility, P98653W. This must be manually entered as a generic exit for the screen that is desired, as such:

hadrian.palazzoinc.com - Mocha W32 TN5250

File Edit View Settings Help

Open Close Cut Copy Paste Print About Dup Clear Erase Attn Sysreq Help Hex

060101 Employee Entry

Action Code. . I

Employee No. . 100006 Marcia Caven Address Number . . 100006

Social

Add'l E : 98653W Value Lookup Window

Name (: Item . . SSN Employee Tax ID

Salary : File . . F060116 Employee Master

Hourly : Library JDWDTA91T Prototype Data Library

Billing : Lookup

Value. .

Check R

Departm : Enter = Lookup F3 = Exit

Tax Are

Tax Are

Mart Stat(F/S : _ Pay Rate & Tax Revisions F6 / _

Gender . . . : _ Error Text F7

Category Cd 1 : _ Profile Data Entry F8

Labor Load Me : Opt: 4=Perform Enter=Exit + / 03

Flat Bdn. Fac

Std Hrs/Year . . . 2080.00

F2=Taxes F5=Basic F6=Pay/Tax F15=Labor F16=DBA F21=Auto Dep F24=More

ONLINE 10,24

hadrian.palazzoinc.com - Mocha W32 TN5250

File Edit View Settings Help

Open Close Cut Copy Paste Print About Dup Clear Erase Attn Sysreq Help Hex

060101 Employee Entry

Action Code. . I

Employee No. . 100006 Marcia Caven Address Number . . 100006

Social

Add'l E : 98653W Value Lookup Window

Name (: Item . . SSN Employee Tax ID

Salary : File . . F060116 Employee Master

Hourly : Library JDWDTA91T Prototype Data Library

Billing : Lookup 77-67-4567

Value. . No matching index value

Check R

Departm : Enter = Lookup F3 = Exit

Tax Are

Tax Are

Mart Stat(F/S : _ Pay Rate & Tax Revisions F6 / _

Gender . . . : _ Error Text F7

Category Cd 1 : _ Profile Data Entry F8

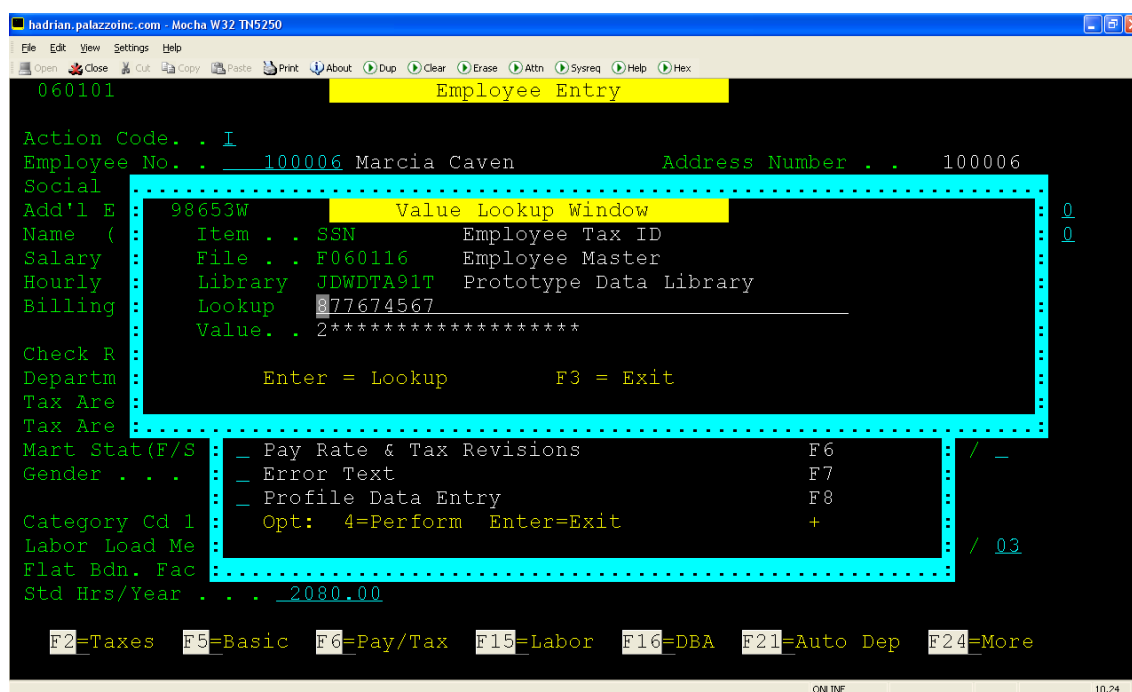
Labor Load Me : Opt: 4=Perform Enter=Exit + / 03

Flat Bdn. Fac

Std Hrs/Year . . . 2080.00

F2=Taxes F5=Basic F6=Pay/Tax F15=Labor F16=DBA F21=Auto Dep F24=More

Print Screen ONLINE 10,24



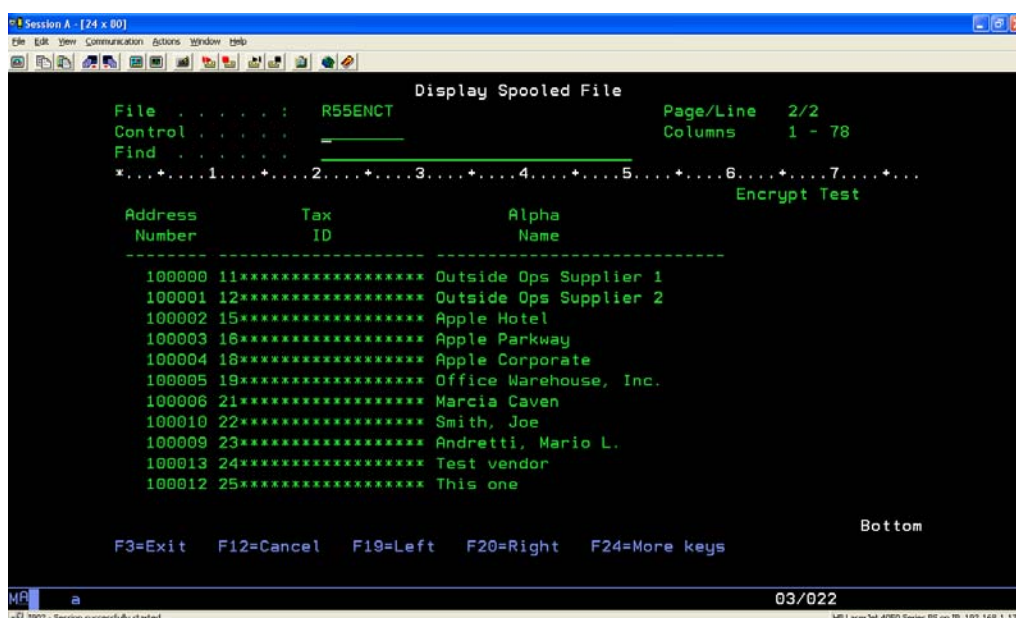
Batch Processing with Encrypted Fields

DREAM Writer

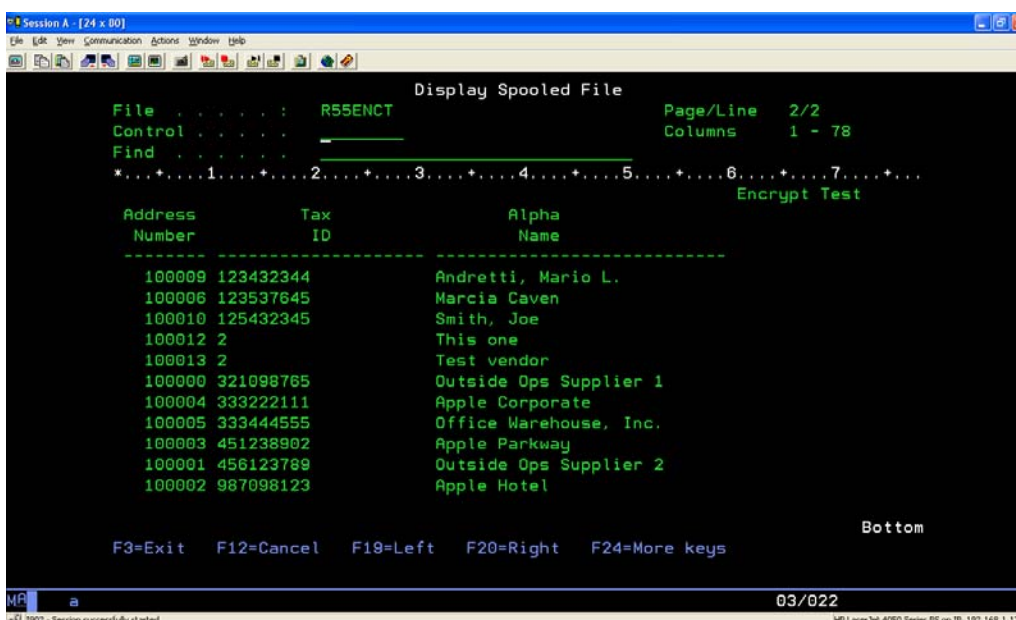
Using CryptoMondo, all of the reports that use encrypted fields will show the value in the field in the encrypted format mode. Data Sequencing with an encrypted field will also occur with the encrypted value, not the actual value.

To allow reports to display and query correctly, CryptoMondo adds an additional option to the DREAM Writer screens. The File Output Type can now be defined as '8' on the Additional Parameters screen of the DREAM Writer Menu. This instructs 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. Both Data Sequencing and Data Selection are enabled based on actual values when the '8' value is used.

This is a test report showing the encrypted Tax ID.



This is the same report showing the decrypted Tax ID.

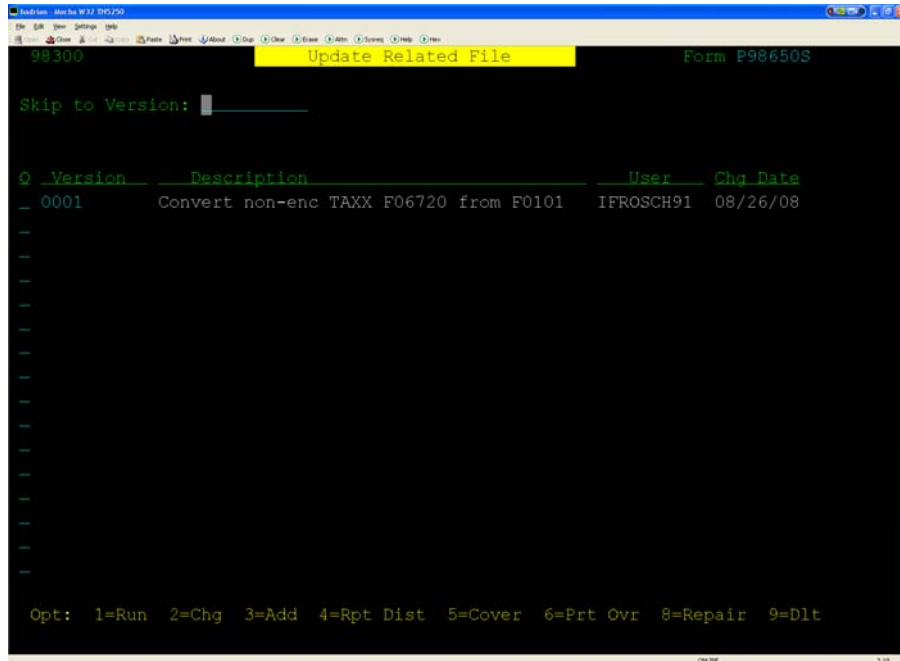


WorldWriter

Using CryptoMondo, all WorldWriter reports that use encrypted fields will show the actual value in the field if the user is authorized to the field. No extra processing or options are required by the user to set.

Updating Related Files

Many times, the encrypted value is moved to a different file. This file is not encrypted, but needs to have the actual value stored. Examples include the W2 workfile and 1099 files. This is different than the batch processing above, as this will handle situations where the based on file is not the encrypted file or it is a join logical.



The file to be unencrypted is selected from the Additional Parameters screen.



The Processing Options allow you to select which item is to be updated in the Based on file. You then select the encryption key that will be used to decrypt the value in the file.

You can run either in proof or final mode. The audit information does not get updated during this process.

98312 Processing Options Revisions Form ID. . . . P98650S
Version. . . . 0001
Convert non-enc TAXX F06720 from F0101 Display Level. 5

This job has various options described below. Enter the desired values and press ENTER to continue.

SELECTION

1. Data Item to Convert TAXX

SOURCE

2. Field Id

OR


3. Data Item TAX

4. File F0101

5. Library JEDWDTA91T

PROOF/FINAL

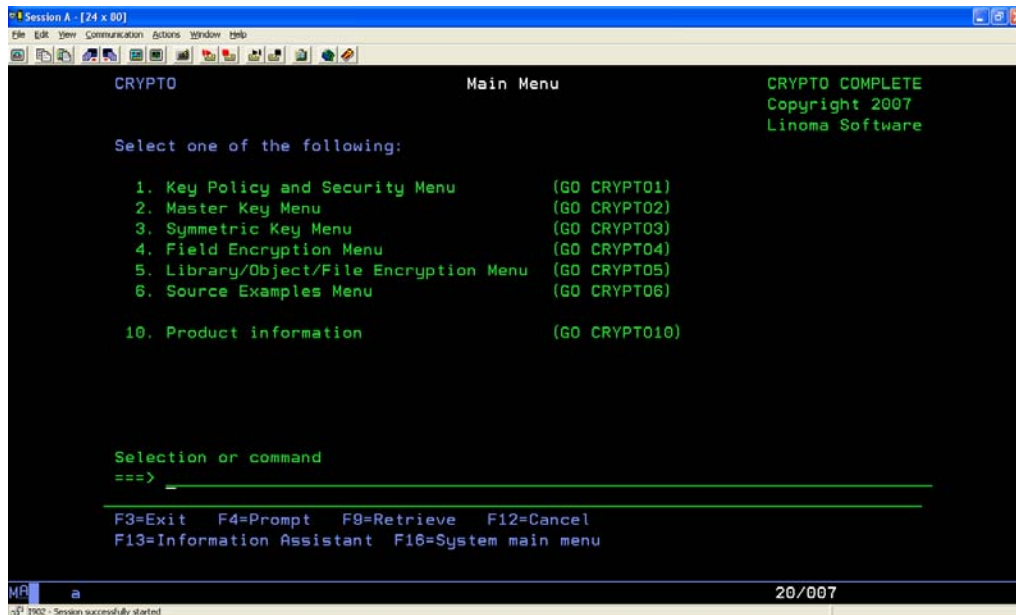
5. Enter a '1' for Final Mode 1

=Printer Overrides

Additional Encrypt Menu Features

Crypto Complete Main Menu

Access the Crypto Complete main menu by entering CRYPTO/CRYPTO or 2/ENCRYPT on the command line. The CRYPTO menu is where the initial setup is performed after installing Linoma's Crypto Complete software. See Linoma's documentation for installation and initial setup instructions.



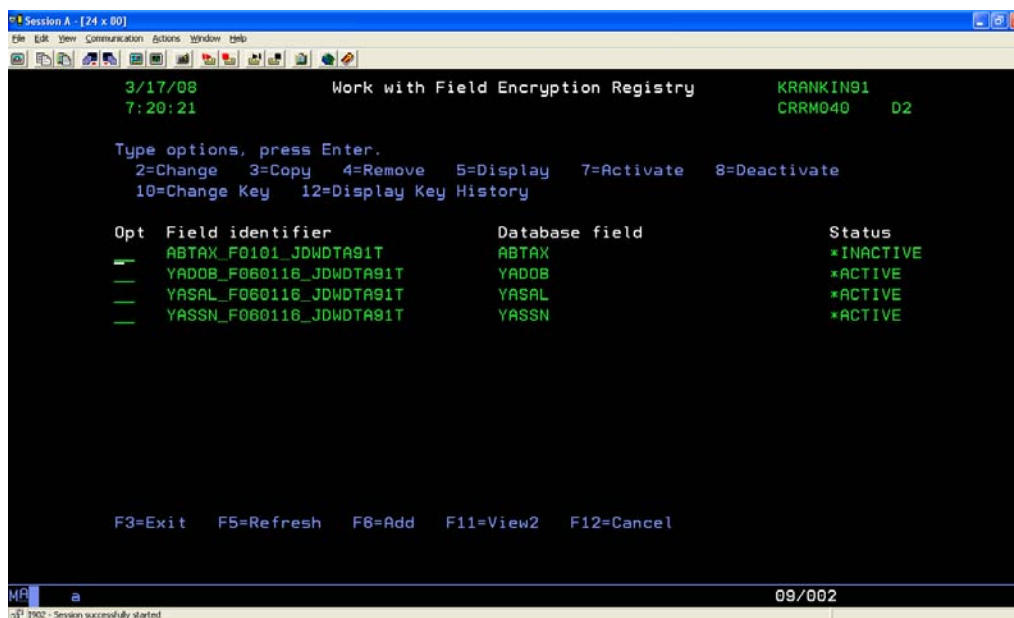
Work With Key Officers

Access the Key Officers application from the CRYPTO/CRYPTO menu by entering 1, then 10 or by entering 3/ENCRYPT on the command line. Key officers are fully explained in Linoma's Crypto Complete User Guide.



Work With Field Encryption

Access the Field Encryption application from the CRYPTO/CRYPTO menu by entering 4, then 1 or by entering 4/ENCRYPT on the command line. The Field Encryption Registry displays the various Field identifiers, Database fields encrypted, and the Status. Selecting option 5 displays the details of the encryption.



The following screens depict the information stored in the Field Encryption Registry.

```

Session A - [24 x 80]
File Edit View Communication Actions Window Help

Display Field Encryption Entry (DSPFLDENC)

Type choices, press Enter.

Field identifier . . . . . ABTAX_F0101_JDWDTA91T
Status . . . . . *INACTIVE
Database field name . . . . . ABTAX
Database file name . . . . . F0101
Library . . . . . JDWDTA91T
Database field type . . . . . *CHAR
Database field length . . . . . 20
Database field decimal pos . . . . .
Encryption key label . . . . . JDEKEY01
Encryption key store name . . . . . JDEKEYS
Decryption key label . . . . . JDEKEY01
Decryption key store name . . . . . JDEKEYS
Encryption algorithm . . . . . *AES256
Algorithm mode . . . . . *ECB

More...

F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys
Already at top of area.

01/001

```

```

Session A - [24 x 80]
File Edit View Communication Actions Window Help

Display Field Encryption Entry (DSPFLDENC)

Type choices, press Enter.

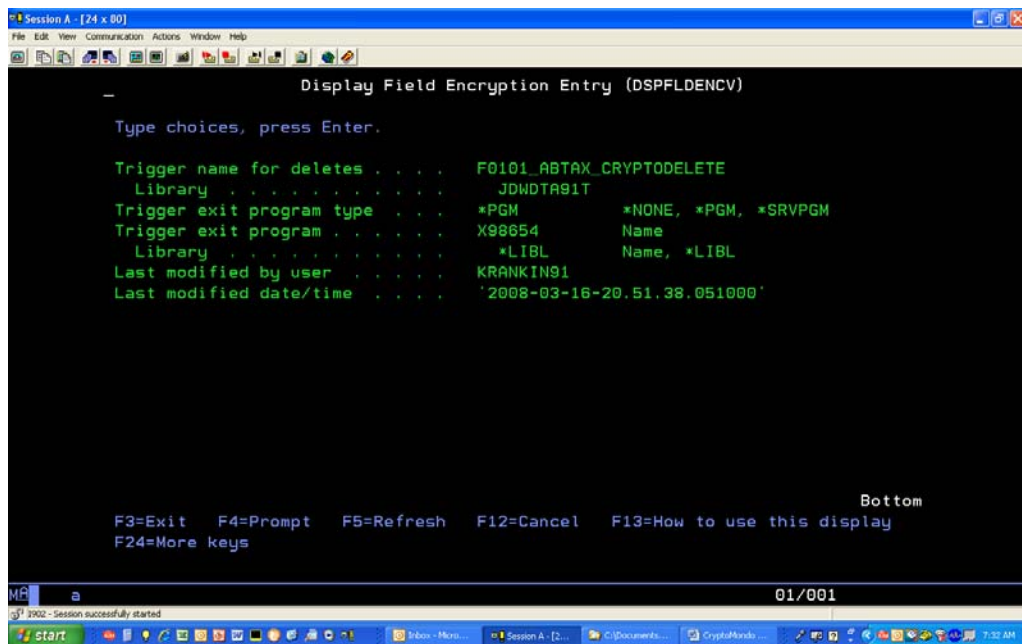
Calculated cipher text length . . . . . 24
Calculated block length . . . . . 24
Store values in external file . . . . . *YES
External file name . . . . . CRXX00003
Library . . . . . JDWDTA91T
Store hash for security check . . . . . *YES
Store last retrieved user/time . . . . . *YES
Index number alignment . . . . . *LEFT *LEFT, *RIGHT
Index number padding character . . . . . 'x' Character value
Last index number issued . . . . .
Use triggers to auto encrypt . . . . . *YES
Trigger name for inserts . . . . . F0101_ABTAX_CRYPTINSERT
Library . . . . . JDWDTA91T
Trigger name for updates . . . . . F0101_ABTAX_CRYPTUPDATE
Library . . . . . JDWDTA91T

More...

F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys

01/001

```

Installation Requirements

Prerequisites

JD Edwards World

Minimum: A7.3 (with generic exit enablement option)
Recommended: A9.1
Cross Reference (P980010) needs to be current

Crypto Complete

Version 1.52 or greater – Version 2.00 recommended for all features.

Install/Upgrade CryptoMondo

Please see *CryptoMondo Installation Guide*

Appendices

Appendix A – Restrictions

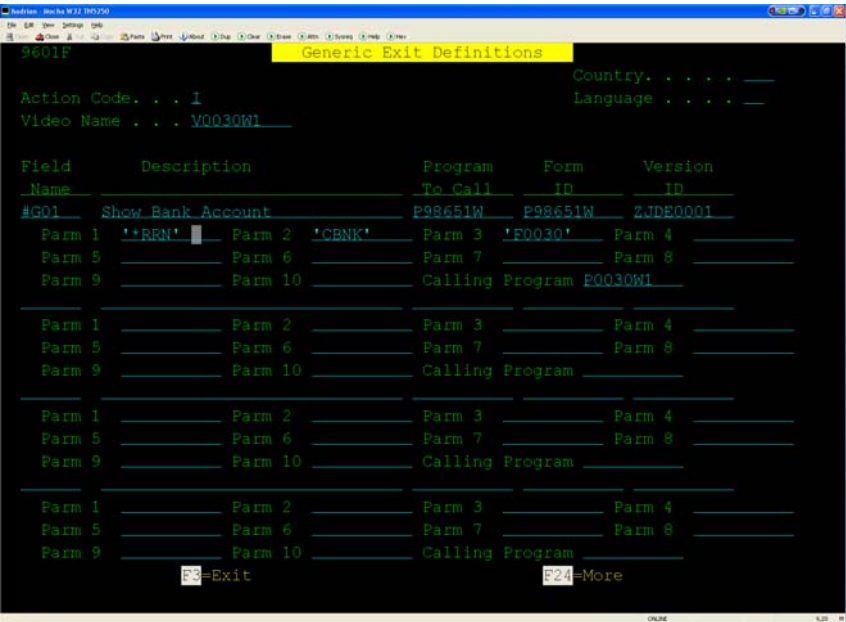
Cryptomondo currently cannot perform standard Generic Exit functionality in the following situations:

1. Subfiles
There is no Generic Exit functionality for subfiles in releases A8.1 or A9.1. These situations will require custom code as documented in Appendix C.
2. ILE
ILE programs do not work correctly with the Generic Exit debugging functionality, as retrieving debug values causes the P96012 program to crash. ‘*RRN’ functionality may work in certain circumstances. If this does not work, then custom code may be required.

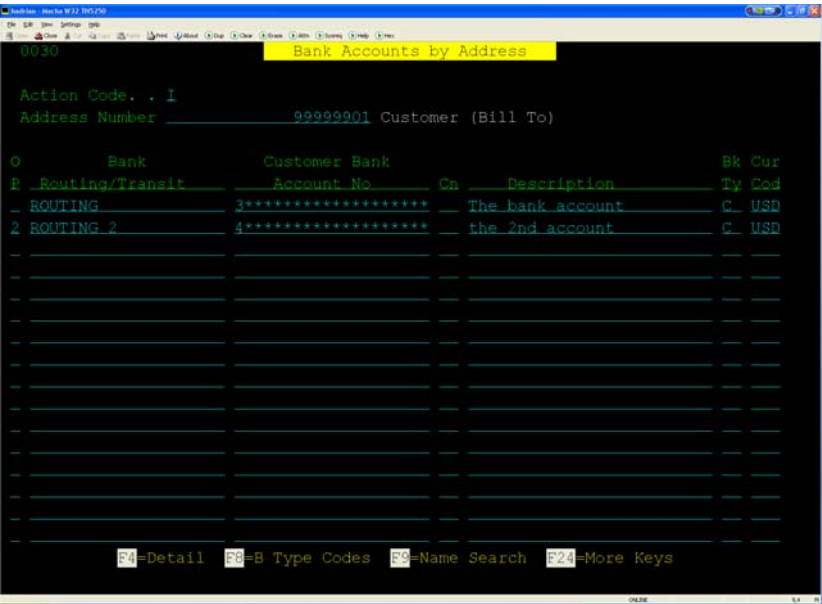
Appendix B – ‘*RRN’ working programs

At the current time, *RRN has been tested works with the generic exit functionality in the following programs:

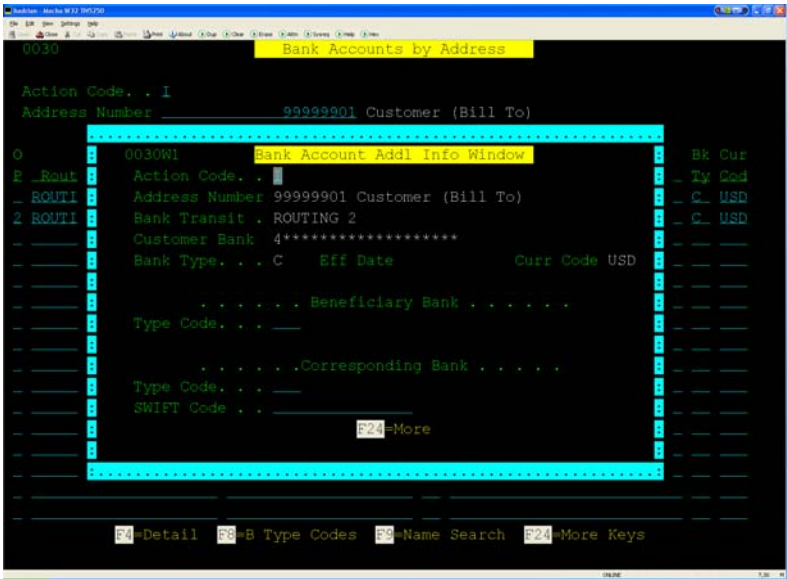
Data Item	File/Table	Video Program	Special Instructions
SSN	F060116	V060101	Use normal setup, but replace first parameter with ‘*RRN’
DOB	F060116	V060101	Use normal setup, but replace first parameter with ‘*RRN’
CBNK	F0030	V0030W1	This must be entered manually, as CBNK is not the field used on the screen. See Below. Update security can still be set.



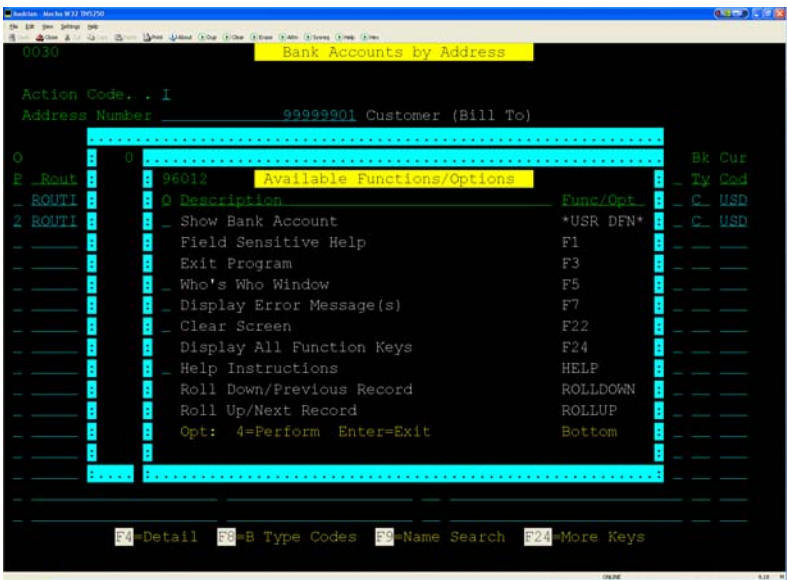
Setup for specific CBNK in Generic Exits



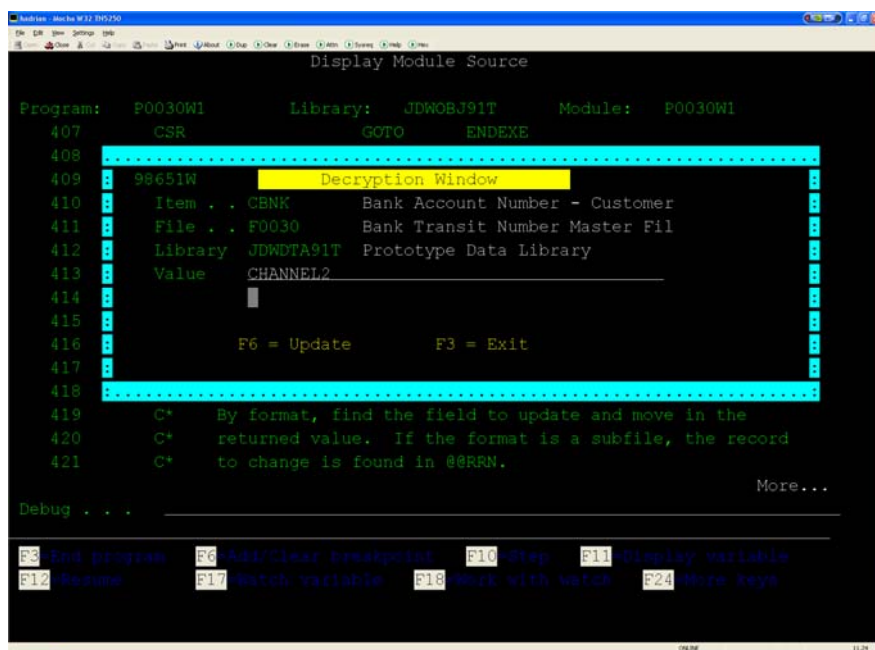
Select option 2 from Bank Accounts by Address



Press F24 for generic exits



Select Show Bank Account



The Decryption window appears with the correct value.

Appendix C – Code Examples for Customization

Palazzo has included two source files that will help you integrate your encryption needs if generic exits or ‘*RRN’ functionality will not work. These are:

- JDECPY
JDECPY includes copy modules that you can use for your own programming needs. Examples are in the JDEMOD source file.
- JDEMOD
JDEMOD includes program fixes from JDE as well as an example use for subfiles. P0030 is a good example of code that has been added that will properly interface with subfiles.