Defense DB Setup Guide

Step-by-Step Instructions for Configuring and Activating Your New Database Encryption Tools

INTRODUCTION

This guide provides step-by-step instructions for configuring and activating your Crypto Complete software so that your credit union can begin reaping the benefits from your investment in database encryption tools for your CU*BASE member data.

While most of the information in this booklet represents a one-time-only setup process, you will also find some useful tips on setting up your ongoing policies and procedures so that you continue to get the most out of your investment. It even contains a handy decision matrix to record critical decisions you will make about how your system will be protected.

CONTENTS

Revision date: July 18, 2014

For an updated copy of this booklet, check out the Reference Materials page of our website:
http://www.cuanswers.com/client_reference.php

DECISIONS TO MAKE FIRST

Use this handy chart to discuss and record key decisions that will need to be made before you can proceed with your setup steps. (**See the Glossary** in Appendix A if you need an explanation of any of these terms.)

Decision to Make	*Considerations*	*Record Your Choices Here*
Who will be in charge of your Master Encryption Keys? *See Appendix B for a list of responsibilities*	▪ Must select 2 people. ▪ Each must have Security Administrator (*SECADM) authority on ALL of your IBM i systems. HINT: You could even set up new, separate user profiles just for key management tasks, if you wish. See Page Appendix B for more details.	Person #1 Name: ____________________ Person #1 User ID: ____________________
		Person #2 Name: ____________________ Person #2 User ID: ____________________
How often will you change keys?	▪ We recommend this be done at least once annually. ▪ It should be done following any test or event where passphrases are used (such as a Disaster Recovery test where backup files are loaded onto a different system). ▪ It should also be done whenever a person designated as Key Officer leaves your employ.	
What is your procedure when one of your Key Officers leaves the organization?	▪ Keys should be changed when a new Key Officer is designated. The timeframe and procedure should be part of your policy. ▪ The details will also depend on whether you set up unique user profiles just for key management tasks, or whether your Key Officers use their own profiles. See Appendix B for more tips.	
Where will the passphrases be stored securely?	▪ It is not adequate to rely on a person's memory for the passphrases necessary to access the keys. We recommend hard copies of the passphrases be retained in more than one secure off-site location. See Appendix C for sample archive procedures.	
Who will be responsible for keeping your policy	▪ Your policy should be established before doing your setup. See Appendix C	

Decision to Make	*Considerations*	*Record Your Choices Here*
and procedures up to date, and how often will they be reviewed?	for a sample policy you can adapt. ▪ It’s a good idea to review these documents regularly, at the same time you update your keys.	
Where will your procedures and policy be stored?	▪ Make sure your document(s) are readily available in the event of a disaster, as well as for periodic review by auditors.	

BEFORE YOU BEGIN

WHO SHOULD BE DOING THESE STEPS

Step 2 of the process (see Page 8) must be completed by both of your Key Officers. The remaining steps can be handled by just one of your Key Officers. This user must be able to log in all of the IBM i systems that will house encrypted data, including HA backup and development systems, if you have them. This user must have security administrator-level (*SECADM) authority on all systems.

> ***It is critical that the configuration be exactly the same across all your systems.*** *Therefore, we recommend that a single person completes the steps on all machines.*

WHAT TO EXPECT

Based on our experience one person will need to set aside about **2 hours of dedicated time** to complete all of the steps for initial setup. A second person will also be needed for a few minutes to complete Step 2.

After the steps in this Guide are complete, encryption will be activated and your data secured.

WHAT MUST ALREADY BE DONE

The instructions assume the following work has already been done. This will generally have been completed by a CU*Answers representative as part of your purchase of the software:

- Crypto Complete software has been installed on every one of your IBM i systems that will store encrypted data.
- Each system has a permanent Crypto Complete software license key. (There is such a thing as a temporary key, but it automatically becomes unusable after a certain number of days. Useful in an emergency but not for the long term.)

WHAT YOU WILL NEED AT HAND

1. The names and user IDs of two different individuals who will be in charge of your encryption keys (see the “Decisions” section on the previous page).
2. Your policies and procedures for managing encryption keys.
3. This booklet.
4. Ability to log on to all of your IBM i systems, including HA backup and development systems as applicable.

GETTING SUPPORT

Just as no one can set up your network password for you, CU*Answers support teams cannot complete the configuration steps to set up your encryption keys. However, we are available while you are working through the steps to answer questions that may arise.

After you've recorded all your decisions using the matrix on Page 3, and completed all of the preparation tasks on the previous page, contact Darrell Stickler (dstickler@cuanswers.com) or a member of the Production Team and make arrangements for us to be available during the block of time you've set aside to complete the remaining steps. We're happy to help!

Support is also available directly from Linoma Software.

Step-By-Step: Setting Up Crypto Complete

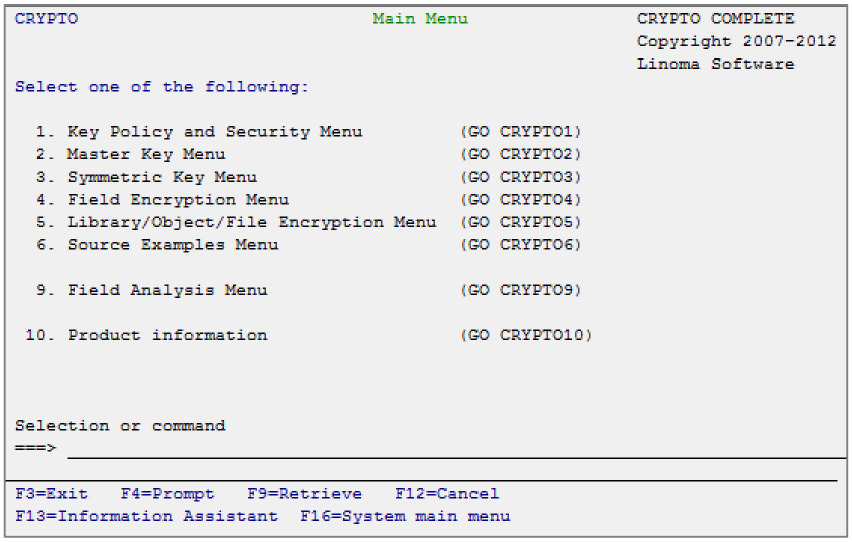
Step 1: Set Up the Key Officers

Follow the steps below to set up your two designated Key Officers in Crypto Complete. These Key Officers are the ones who load passphrases used to change MEKs.

For illustration purposes, we'll use "ABC" as the User ID for one and "XYZ" for the other one. Substitute your Key Officers' actual User IDs, of course.

1. From a command line, "**GO CRYPTO/CRYPTO**" to bring up the Main Menu.

Figure 1: Main Menu



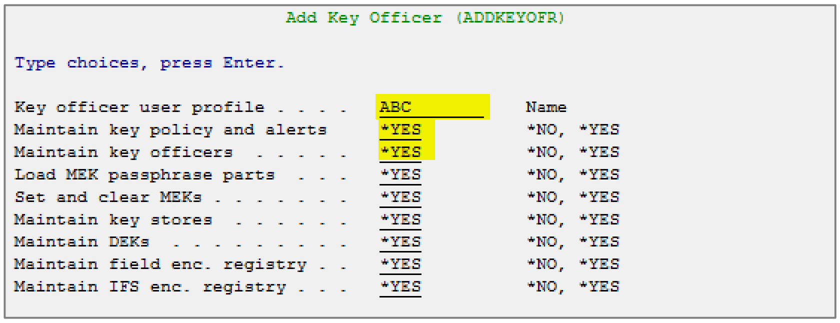
```
CRYPTO                          Main Menu                   CRYPTO COMPLETE
                                                            Copyright 2007-2012
                                                            Linoma Software

Select one of the following:

  1. Key Policy and Security Menu          (GO CRYPTO1)
  2. Master Key Menu                       (GO CRYPTO2)
  3. Symmetric Key Menu                    (GO CRYPTO3)
  4. Field Encryption Menu                 (GO CRYPTO4)
  5. Library/Object/File Encryption Menu   (GO CRYPTO5)
  6. Source Examples Menu                  (GO CRYPTO6)

  9. Field Analysis Menu                   (GO CRYPTO9)

 10. Product information                   (GO CRYPTO10)



Selection or command
===>

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=System main menu
```

2. Select **option 1** *Key Policy and Security Menu.*

3. Select **option 10** *Work with Key Officers.*

4. Press **F6=Add** to display the screen shown below. Fill in the following values (highlighted values are those that need to be changed; substitute the appropriate User ID for ABC):

Figure 2: New Values to Enter



```
                             Add Key Officer (ADDKEYOFR)

Type choices, press Enter.

Key officer user profile . . . .   ABC           Name
Maintain key policy and alerts     *YES          *NO, *YES
Maintain key officers  . . . . .   *YES          *NO, *YES
Load MEK passphrase parts  . . .   *YES          *NO, *YES
Set and clear MEKs . . . . . . .   *YES          *NO, *YES
Maintain key stores  . . . . . .   *YES          *NO, *YES
Maintain DEKs  . . . . . . . . .   *YES          *NO, *YES
Maintain field enc. registry . .   *YES          *NO, *YES
Maintain IFS enc. registry . . .   *YES          *NO, *YES
```

5. Press Enter to complete the addition of the Key Officer and return to the *Work with Key Officers* screen.

6. Repeat these steps using the user ID for your second Key Officer's user ID, with all other settings the same.

> *HINT: Other Key Officers can be set up besides these two people, with different settings in their profile if you wish. This Guide specifically refers only to the two Key Officers with the permissions settings shown above. Refer to the Crypto Complete Users Guide for more details about other functions available within the Linoma software.*

Step 2: Set Up the Master Encryption Key (MEK)

NOTE: This is the only step that must be completed separately by BOTH of your Key Officers.

> ***IMPORTANT NOTE:*** *The MEK passphrase needs to be entered* ***exactly the same on every IBM i*** *that will use CU*BASE applications with Crypto Complete. If it is not entered* ***exactly*** *the same the encrypted data will* ***not be accessible****.* ***Please be very careful during this step!***

This will require the two Key Officers that were created in Step 1 to perform the same task, independent of each other. The order in which the Key Officers enter their passphrase is not important, but both must be completed before the MEK can be activated in Step 3.

1. IMPORTANT: **Each Key Officer must first log in to the IBM i as usual** (either using their own personal User ID or the one you've designated for key management tasks) before proceeding through the remaining steps to set up their part of the passphrase.

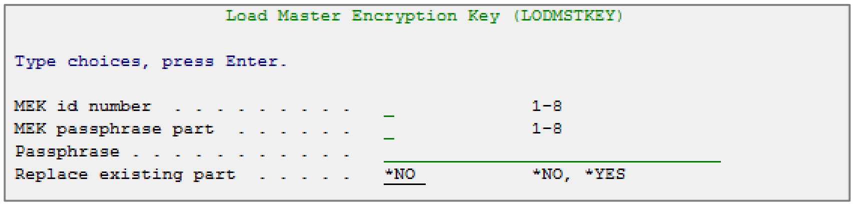
2. Navigate to the Crypto Complete Main Menu.

3. Select **option 2** *Master Key Menu.*

4. Select **option 1** *Load Master Encryption Key*.

5. The following screen will appear:

Figure 3: Load Master Encryption Key



```
                     Load Master Encryption Key (LODMSTKEY)

Type choices, press Enter.

MEK id number  . . . . . . . . .   _              1-8
MEK passphrase part  . . . . . .   _              1-8
Passphrase . . . . . . . . . . .
Replace existing part  . . . . .   *NO            *NO, *YES
```

6. Enter the following values (**in bold**):

Choice	*Value that should be entered*
MEK id number	**1**
MEK passphrase part	For user "ABC" enter **1** here For user "XYZ" enter **2** here

Choice	*Value that should be entered*
Passphrase	Each Key Officer must enter a *unique* passphrase here. Can be a maximum of 32 characters long, contain spaces, and **is case-sensitive**. Spaces and special characters are allowed, but can be more difficult to see when you print a screenshot, so be careful.
Replace existing part	Enter ***NO** here if creating a brand-new passphrase. If a passphrase was already entered incorrectly and saved, you can change this to *YES in order to overwrite the existing passphrase. See "If You Make a Mistake" below.

7. Print a screenshot showing the passphrase that was entered.

> *IMPORTANT: Make sure the passphrase displays clearly as you typed it and that you secure this document properly according to your key management policy.*

8. Press **Enter** to save the settings and return to the menu.

If You Make a Mistake

The MEK passphrase needs to be entered **exactly the same on every IBM i** that will use CU*BASE applications with Crypto Complete, or your data will be rendered unusable. If you typed your passphrase incorrectly while working through this step, you can go back into the *Load Master Encryption Key* screen and retype the passphrase correctly then change "Replace existing part" setting from ***NO** to ***YES**.

This must be done prior to setting the MEK in the next step.

STEP 3: SET / ACTIVATE THE LOADED MEK

Once both passphrases have been entered correctly, you will need to "set" or activate the MEK using the steps below. (This only needs to be done by one of the Key Officers, remember.)

1. Navigate to the Crypto Complete Main Menu.
2. Select **option 2** *Master Key Menu.*
3. Select **option 2** *Set Master Encryption Key*.
4. Enter **1** for the MEK id number and press **Enter**.
5. Press **F3** to return to the Crypto Complete Main Menu.

STEP 4: SET UP THE KEY STORE

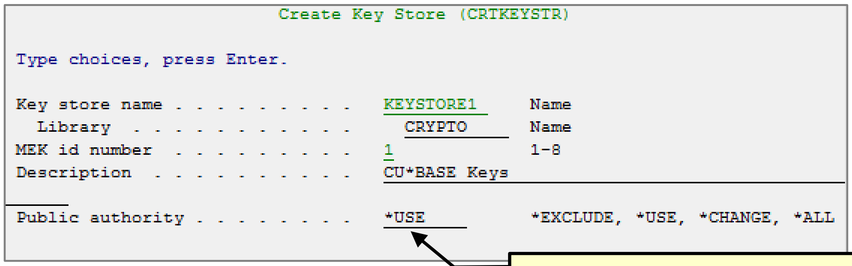
The next step is to create the default key store for the DEKs to be used for encryption of CU*BASE data:

1. Navigate to the Crypto Complete Main Menu.
2. Select **option 3** *Symmetric Key Menu.*

3. Select **option 1** *Create Key Store.*

4. Fill in the screen *exactly* as shown below:

Figure 4: Create Key Store



```
                         Create Key Store (CRTKEYSTR)

Type choices, press Enter.

Key store name . . . . . . . . . .   KEYSTORE1     Name
  Library  . . . . . . . . . . . .     CRYPTO      Name
MEK id number  . . . . . . . . . .   1             1-8
Description  . . . . . . . . . . .   CU*BASE Keys

Public authority . . . . . . . . .   *USE          *EXCLUDE, *USE, *CHANGE, *ALL
```

IMPORTANT: Don't forget to change the *Public authority* setting to ***USE** as shown!

5. Press **Enter** to create the key store. You are now ready to set up DEKs.

Step 5: Set Up the Key Policy

The key policy is where the environment settings for Crypto Complete are done. This needs to be completed by one of the Key Officers that were created in the previous steps, and as directed by your encryption key policy.

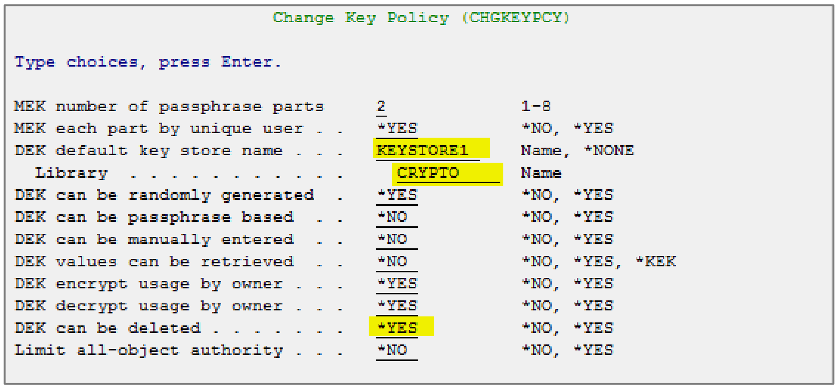
1. Navigate to the Crypto Complete Main Menu.

2. Select **option 1** *Key Policy and Security Menu*

3. Select **option 1** *Change Key Policy*.

4. Fill in the following values (highlighted values are those that need to be changed):

Figure 5: Change Key Policy



```
                         Change Key Policy (CHGKEYPCY)

Type choices, press Enter.

MEK number of passphrase parts     2             1-8
MEK each part by unique user . .   *YES          *NO, *YES
DEK default key store name . . .   KEYSTORE1     Name, *NONE
  Library  . . . . . . . . . . .     CRYPTO      Name
DEK can be randomly generated  .   *YES          *NO, *YES
DEK can be passphrase based  . .   *NO           *NO, *YES
DEK can be manually entered  . .   *NO           *NO, *YES
DEK values can be retrieved  . .   *NO           *NO, *YES, *KEK
DEK encrypt usage by owner . . .   *YES          *NO, *YES
DEK decrypt usage by owner . . .   *YES          *NO, *YES
DEK can be deleted . . . . . . .   *YES          *NO, *YES
Limit all-object authority . . .   *NO           *NO, *YES
```

5. Values that should be changed from the defaults:
   - The *DEK default key store name* needs to be **KEYSTORE1** and the library needs to be **CRYPTO**.
   - The *DEK can be deleted* setting needs to be ***YES**.

6. Press **Enter** to save the changes.

Step 6: Set Up the Data Encryption Keys (DEKs)

Next the DEKs need to be set up. The following steps will set up a DEK for the credit card number in CU*BASE.

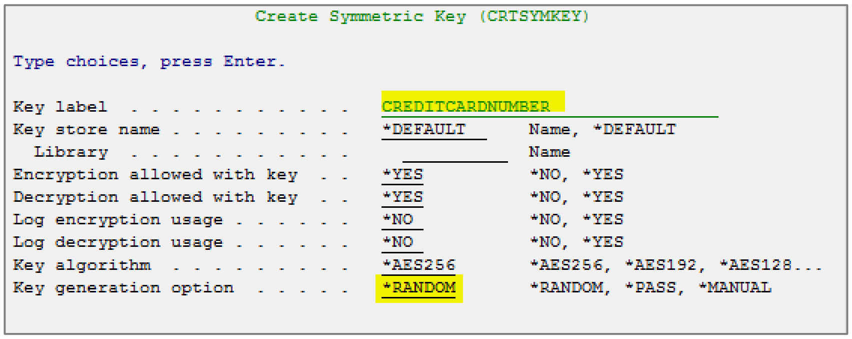
1. Navigate to the Crypto Complete Main Menu.

2. Select **option 3** *Symmetric Key Menu.*

3. Select **option 11** *Create Symmetric Key.*

4. The following screen appears:

Figure 6: Create Symmetric Key



```
                      Create Symmetric Key (CRTSYMKEY)

Type choices, press Enter.

Key label  . . . . . . . . . . .   CREDITCARDNUMBER
Key store name . . . . . . . . .   *DEFAULT      Name, *DEFAULT
  Library  . . . . . . . . . . .                 Name
Encryption allowed with key  . .   *YES          *NO, *YES
Decryption allowed with key  . .   *YES          *NO, *YES
Log encryption usage . . . . . .   *NO           *NO, *YES
Log decryption usage . . . . . .   *NO           *NO, *YES
Key algorithm  . . . . . . . . .   *AES256       *AES256, *AES192, *AES128...
Key generation option  . . . . .   *RANDOM       *RANDOM, *PASS, *MANUAL
```

5. Type **CREDITCARDNUMBER** for the *key label.*

> *It is **very important** that this key label be entered correctly. This will be used to encrypt and decrypt the credit card number in CU*BASE.*

6. Leave everything the same as shown above. Make sure that the *Key generation option* is set to ***RANDOM** as this gives the highest level of security.

7. Press **Enter** to generate the DEK.

This completes the Crypto Complete setup for use with CU*BASE.

Step 7: Repeat on All Systems

Repeat Steps 1 through 6 on your HA backup system, as well as on any development systems you may have.

> ***BE VERY CAREFUL:*** *The MEK needs to be entered **exactly the same on every IBM i** that will use CU*BASE applications with Crypto Complete. If it is not entered **exactly** the same the encrypted data will **not be accessible**. For obvious reasons there is no "back door" method for accessing encrypted data, so **be very careful** to be consistent on all your systems!*

STEP 8: CONTACT CU*ANSWERS TO ENCRYPT YOUR DATA

The final step, once your keys are set up, is for our programming team to encrypt the data in your CU*BASE database. This involves a couple of steps:

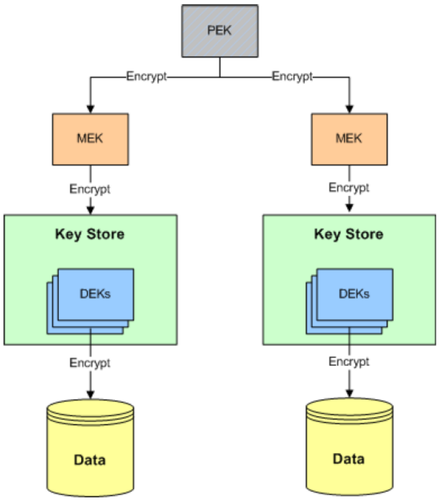
1. First we will save a copy of your FILExx library as a backup.
2. Next we will run a routine that encrypts the data in your CU*BASE files.

   > *At this time, only your online credit cards numbers will be encrypted. Future encryption projects, such as ATM/Debit card numbers, will be handled separately as they come up.*

3. We will then verify that the process worked by accessing an account via ***Update/Order Online Credit Cards*** on the Online ATM/Debit/Credit Card Processing menu (MNATMD). If the screen can be accessed and a credit card number decrypted and displayed on the screen, then the encryption process is complete.

APPENDICES

APPENDIX A: GLOSSARY OF TERMS



Source: Linoma Group, Inc.

It can be helpful to think of keys in terms of a hierarchy, as shown in the illustration to the right. Each key is protected (encrypted) by the key above it in the hierarchy.

This hierarchy is part of the IBM i architecture; Crypto Complete simply provides tools to help you navigate and configure these mechanisms more easily and consistently. *(NOTE: CU*BASE makes use of only one of the MEKs shown in this illustration.)*

Following is a brief description of some of the special terms used in this booklet.

Term	*Description*
Crypto Complete™	A software tool for the IBM i, sold and serviced by Linoma Group, Inc. (www.linomasoftware.com).
Data Encryption Policy	A document that outlines your decisions about how encryption keys will be handled, how often keys will be changed, where passphrases will be securely stored, and so on.
DEKs	Data Encryption Keys. Each DEK can encrypt/decrypt an individual file or field in your CU*BASE database. For example, CU*BASE would use one DEK to encrypt/decrypt credit card numbers, another to encrypt/decrypt ATM/Debit card numbers.
Key	The information needed to control the mathematical algorithms that encrypt and decrypt data. Compared to human-generated passwords, keys are more secure since they are computer-generated, represented as an obscure series of bits (1001110…).
Key Officers	The users designated as being responsible for managing the MEKs.
Key store	A group of Data Encryption Keys controlled by a single Master Encryption Key. Key stores allow you to group DEKs so that you do not have to use a separate MEK for each individual piece of data you need to encrypt.
MEK	Master Encryption Key, which encrypts and protects the Data Encryption Keys. There are 8 of these available on every IBM i; you will make use of only one ("MEK 1") for encrypting your CU*BASE data.
Passphrase	Another name for a password. A string of characters (which will be entered by each of your Key Officers), used to create a key. In this case, the passphrase actually has two parts, each entered by one of the Key Officers.
PEK	Product Encryption Key. Each IBM i has one PEK, unique to that machine. The PEK encrypts up to 8 Master Encryption Keys on that machine.

APPENDIX B: KEY OFFICER RESPONSIBILITIES

You will need to identify **two** separate individuals to serve as Key Officers, both with *SECADM authority as part of their user profiles.

These two employees will be responsible for:

- Setting up Master Encryption Keys.
- Changing keys on a periodic basis or as needed after an event when the passphrases are used (such as when you perform a DR test that requires encrypted data to be copied to another machine).

  > *CU*Answers recommends changing keys annually as a best practice.*

- Entering passphrases should your files need to be loaded onto a different IBM i (since MEKs are unique by box).
- Ensuring your key management policy and procedures are reviewed regularly and kept up to date.

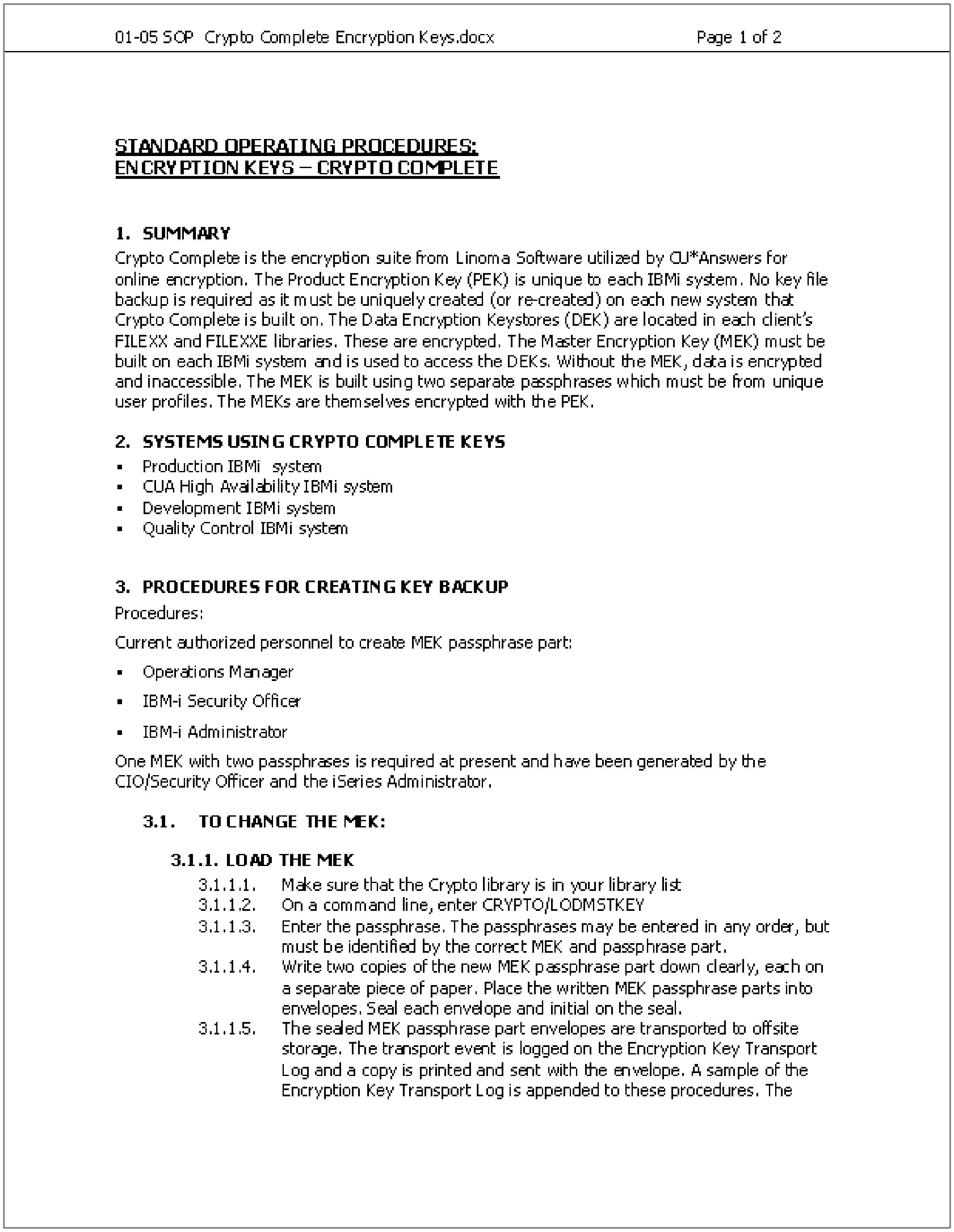
The Crypto Complete software requires that you enter a User Profile (the ID used to log in to the IBM i) for two separate individuals. These profiles can be two of your employees who have security administrator-level (*SECADM) authority on all of your systems. Or you can create two unique User Profiles to be used only for key management tasks.

The advantage of using existing profiles is that since the users will be using those profiles daily, they will be able to log on easily if they need to. Just remember that if one of those people leaves your employ, you will need to set up a new Key Officer to replace them and then also change your Master Encryption Key.

If you set up unique Key Officer profiles just for key management duties, make sure to use them occasionally so passwords are fresh and the profiles can be used easily when needed. The advantage there is that the profile can be passed along to someone new in the event the original employee's job situation changes, and the unique profile ID allows you to more closely control and log what that user does on your system.

APPENDIX C: SAMPLE POLICIES

The following policy documents are samples taken from the CU*Answers policies. Contact us if you would like editable versions of these so you can modify them for yourself!



01-05 SOP Crypto Complete Encryption Keys.docx Page 1 of 2

STANDARD OPERATING PROCEDURES:
ENCRYPTION KEYS – CRYPTO COMPLETE

1. SUMMARY

Crypto Complete is the encryption suite from Linoma Software utilized by CU*Answers for online encryption. The Product Encryption Key (PEK) is unique to each IBMi system. No key file backup is required as it must be uniquely created (or re-created) on each new system that Crypto Complete is built on. The Data Encryption Keystores (DEK) are located in each client's FILEXX and FILEXXE libraries. These are encrypted. The Master Encryption Key (MEK) must be built on each IBMi system and is used to access the DEKs. Without the MEK, data is encrypted and inaccessible. The MEK is built using two separate passphrases which must be from unique user profiles. The MEKs are themselves encrypted with the PEK.

2. SYSTEMS USING CRYPTO COMPLETE KEYS

- Production IBMi system
- CUA High Availability IBMi system
- Development IBMi system
- Quality Control IBMi system

3. PROCEDURES FOR CREATING KEY BACKUP

Procedures:

Current authorized personnel to create MEK passphrase part:

- Operations Manager
- IBM-i Security Officer
- IBM-i Administrator

One MEK with two passphrases is required at present and have been generated by the CIO/Security Officer and the iSeries Administrator.

3.1. TO CHANGE THE MEK:

3.1.1. LOAD THE MEK

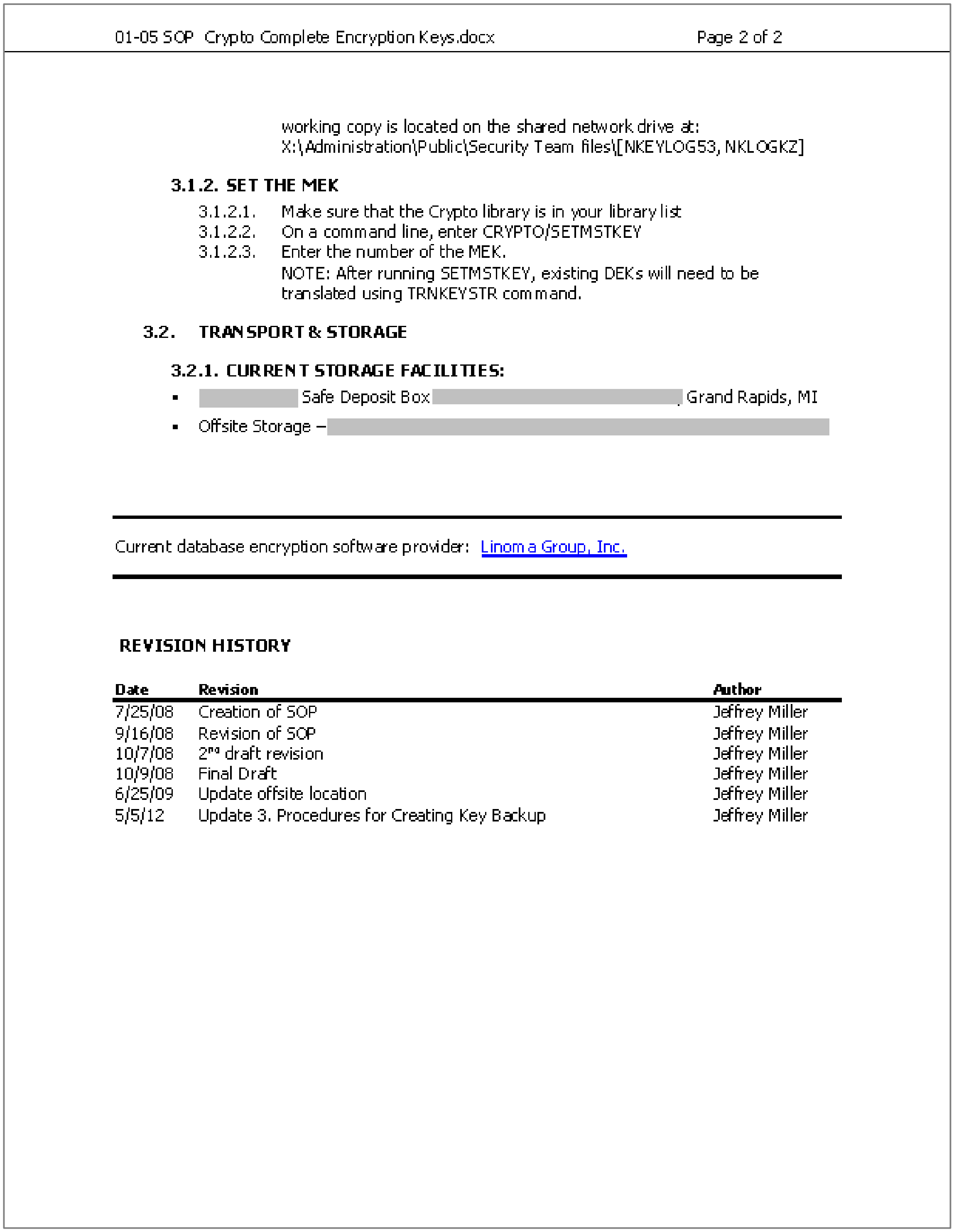
3.1.1.1. Make sure that the Crypto library is in your library list

3.1.1.2. On a command line, enter CRYPTO/LODMSTKEY

3.1.1.3. Enter the passphrase. The passphrases may be entered in any order, but must be identified by the correct MEK and passphrase part.

3.1.1.4. Write two copies of the new MEK passphrase part down clearly, each on a separate piece of paper. Place the written MEK passphrase parts into envelopes. Seal each envelope and initial on the seal.

3.1.1.5. The sealed MEK passphrase part envelopes are transported to offsite storage. The transport event is logged on the Encryption Key Transport Log and a copy is printed and sent with the envelope. A sample of the Encryption Key Transport Log is appended to these procedures. The



01-05 SOP Crypto Complete Encryption Keys.docx Page 2 of 2

working copy is located on the shared network drive at:
X:\Administration\Public\Security Team files\[NKEYLOG53, NKLOGKZ]

3.1.2. SET THE MEK

3.1.2.1. Make sure that the Crypto library is in your library list
3.1.2.2. On a command line, enter CRYPTO/SETMSTKEY
3.1.2.3. Enter the number of the MEK.
NOTE: After running SETMSTKEY, existing DEKs will need to be translated using TRNKEYSTR command.

3.2. TRANSPORT & STORAGE

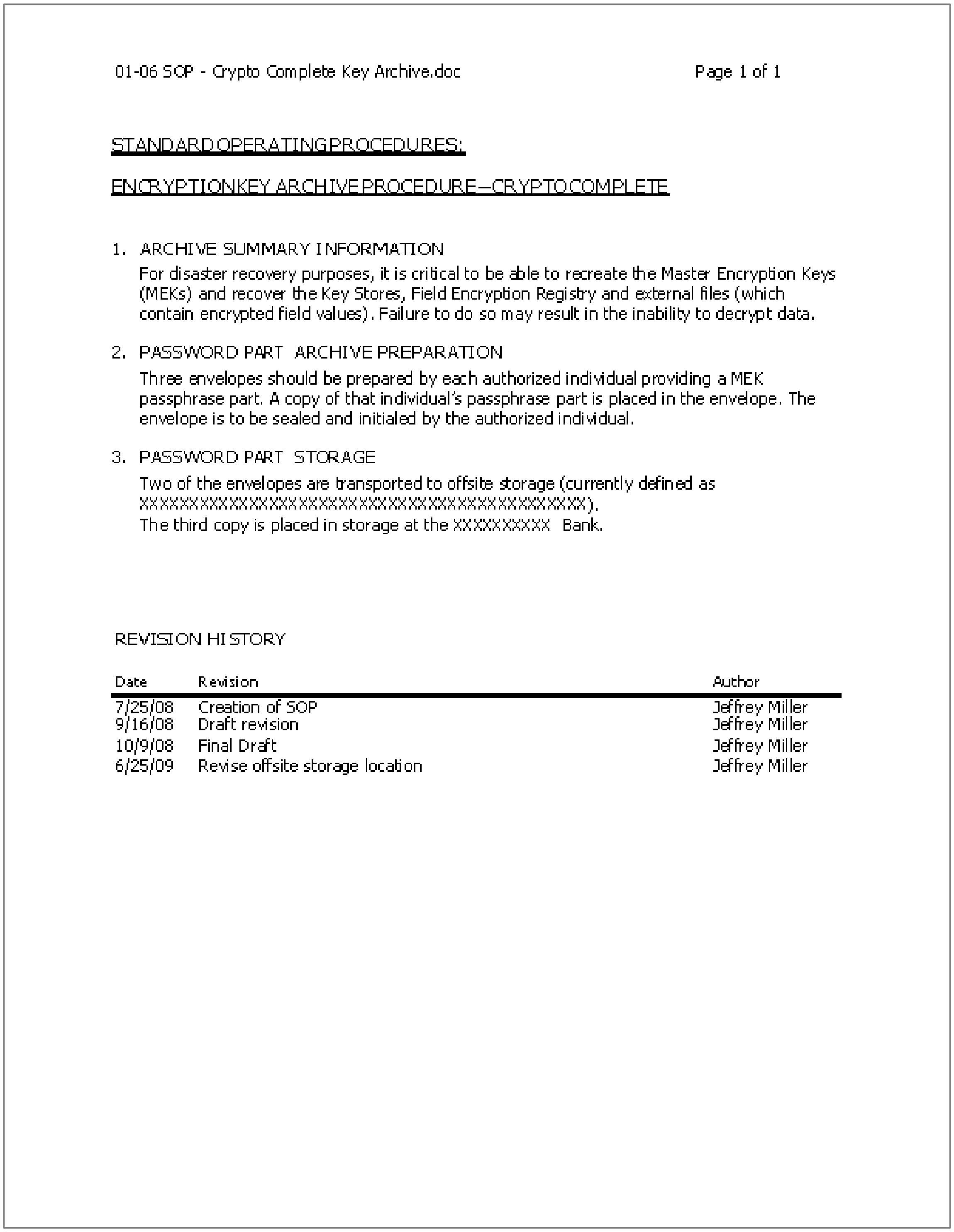
3.2.1. CURRENT STORAGE FACILITIES:

- [redacted] Safe Deposit Box [redacted], Grand Rapids, MI
- Offsite Storage – [redacted]

Current database encryption software provider: Linoma Group, Inc.

REVISION HISTORY

Date	Revision	Author
7/25/08	Creation of SOP	Jeffrey Miller
9/16/08	Revision of SOP	Jeffrey Miller
10/7/08	2nd draft revision	Jeffrey Miller
10/9/08	Final Draft	Jeffrey Miller
6/25/09	Update offsite location	Jeffrey Miller
5/5/12	Update 3. Procedures for Creating Key Backup	Jeffrey Miller



01-06 SOP - Crypto Complete Key Archive.doc Page 1 of 1

STANDARD OPERATING PROCEDURES:

ENCRYPTION KEY ARCHIVE PROCEDURE – CRYPTO COMPLETE

1. ARCHIVE SUMMARY INFORMATION

   For disaster recovery purposes, it is critical to be able to recreate the Master Encryption Keys (MEKs) and recover the Key Stores, Field Encryption Registry and external files (which contain encrypted field values). Failure to do so may result in the inability to decrypt data.

2. PASSWORD PART ARCHIVE PREPARATION

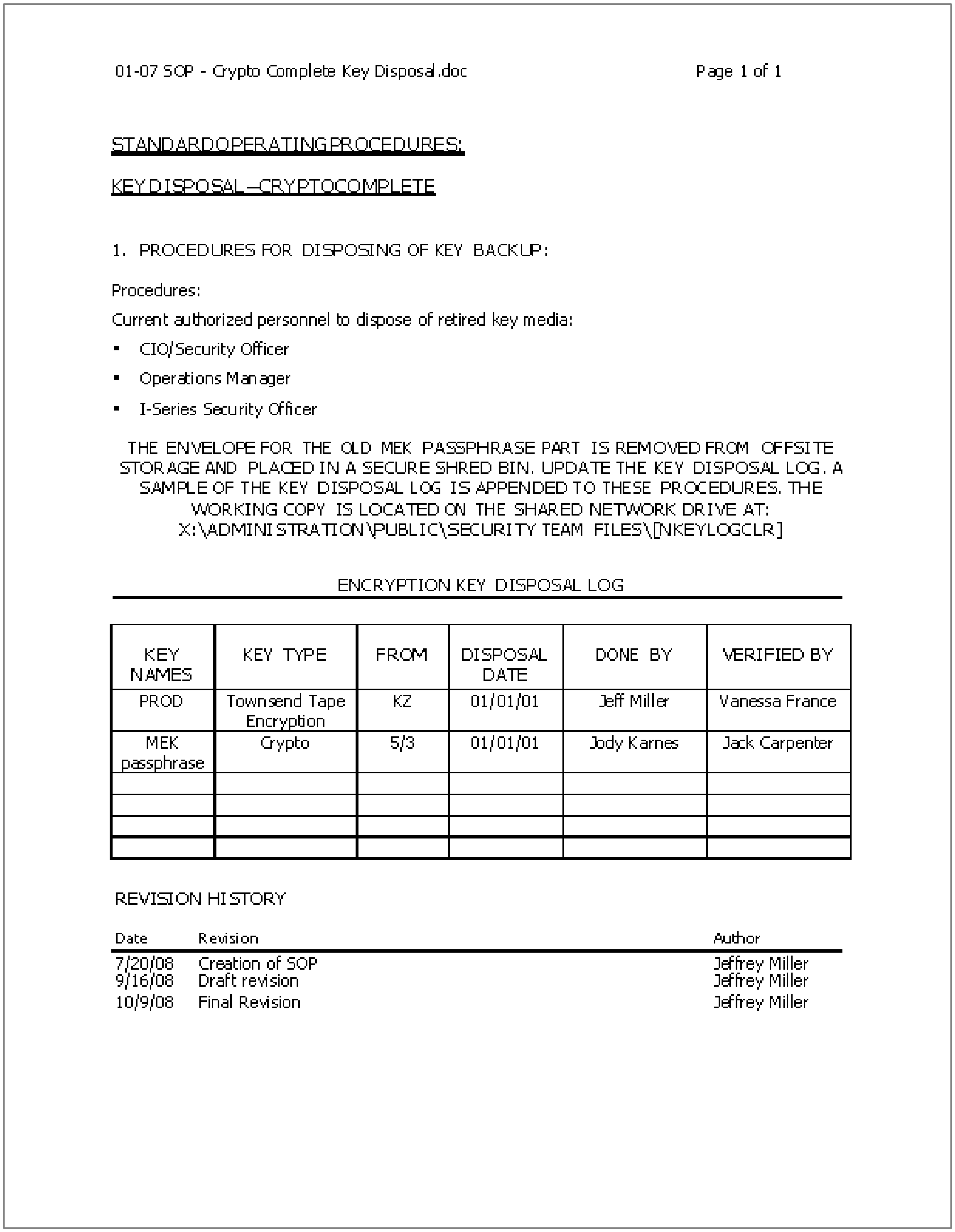
   Three envelopes should be prepared by each authorized individual providing a MEK passphrase part. A copy of that individual's passphrase part is placed in the envelope. The envelope is to be sealed and initialed by the authorized individual.

3. PASSWORD PART STORAGE

   Two of the envelopes are transported to offsite storage (currently defined as XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX).
   The third copy is placed in storage at the XXXXXXXXXX Bank.

REVISION HISTORY

Date	Revision	Author
7/25/08	Creation of SOP	Jeffrey Miller
9/16/08	Draft revision	Jeffrey Miller
10/9/08	Final Draft	Jeffrey Miller
6/25/09	Revise offsite storage location	Jeffrey Miller



01-07 SOP - Crypto Complete Key Disposal.doc Page 1 of 1

STANDARDOPERATINGPROCEDURES:

KEYDISPOSAL –CRYPTOCOMPLETE

1. PROCEDURES FOR DISPOSING OF KEY BACKUP:

Procedures:

Current authorized personnel to dispose of retired key media:

- CIO/Security Officer
- Operations Manager
- I-Series Security Officer

THE ENVELOPE FOR THE OLD MEK PASSPHRASE PART IS REMOVED FROM OFFSITE STORAGE AND PLACED IN A SECURE SHRED BIN. UPDATE THE KEY DISPOSAL LOG. A SAMPLE OF THE KEY DISPOSAL LOG IS APPENDED TO THESE PROCEDURES. THE WORKING COPY IS LOCATED ON THE SHARED NETWORK DRIVE AT: X:\ADMINISTRATION\PUBLIC\SECURITY TEAM FILES\[NKEYLOGCLR]

ENCRYPTION KEY DISPOSAL LOG

KEY NAMES	KEY TYPE	FROM	DISPOSAL DATE	DONE BY	VERIFIED BY
PROD	Townsend Tape Encryption	KZ	01/01/01	Jeff Miller	Vanessa France
MEK passphrase	Crypto	5/3	01/01/01	Jody Karnes	Jack Carpenter

REVISION HISTORY

Date	Revision	Author
7/20/08	Creation of SOP	Jeffrey Miller
9/16/08	Draft revision	Jeffrey Miller
10/9/08	Final Revision	Jeffrey Miller