Trusted Key Entry (TKE) PTF Migration Documentation

Notice

The information in this document is applicable only if you have applied APAR PQ16805.

The TKE machine can be used to generate RSA keypairs for SET certificate requests using **eecertreq** SET defines the modulus of the generate keys as 1024 and the type of keys generated by TKE as signature only. Additional information about using TKE is found in *ICSF Trusted Key Entry*, SC23-3978.

The following information will be added to the:

- *IBM CommercePOINT Gateway for OS/390 System Administration Guide and Reference*, SC24-5873.
- *IBM CommercePOINT eTill for OS/390 Administrator's Guide*, SC24-5869.

After hardware crypto is enabled on your machine and selected by the application, an exception will occur if you have not migrated your databases using the migration utility. The exception is:

> "Hardware crypto is enabled but software generated keys are being used. You must use the migration utility to migrate your databases or disable hardware crypto."

Migration is a one-way process. You can move from using software encryption to hardware encryption, but not from hardware encryption to software encryption.

The Migrate Utility

The migrate utility converts a `key.db` and a `keypair.db` containing RSA keypairs to use hardware based labels for the same keypairs. The utility is part of the SET toolkit product tape.

There are three environment variables that can be set before the migration utility is run.

MIGSWHWDBPATH the path to the databases

MIGSWHWKEYDB the name of the `key.db` database.
The default database name `key.db` is assumed if the environment variable is not set.

MIGSWHWKEYPAIRDB the name of the `keypair.db` database.
The default database name `keypair.db` is assumed if the environment variable is not set.

The file `MIGRATE.p.o` becomes the executable MIGRATESWHWDBS. To execute the migrate utility, type `migrateswhwdbs` in the directory `usr/lpp/set/bin` and press Enter.

During execution the following questions are asked:

1. Is tracing desired?
   Answer: Y for yes and N for No
2. What is the path to the databases if MIGSWHWDBPATH was not set?
   Answer: Enter the path to the database files.

   During eTill migration, you will be asked:
3. What is the password for the databases?
   Answer: Enter the password.

After execution, two new files are added in the database path entered. The migrated database names have an extension of `.mig`; `key.db.mig` and `keypair.db.mig`. Migrate will fail if one or more of these files already exist in the specified database path. For example, if key.db is one of the databases and key.db.mig exists in the same directory, migrate will not execute. When migration is complete, rename the files to remove the `.mig` extension. For example, `key.db.mig` renames to `key.db`.

Migration Security Issues

The migrate utility eases moving from software to hardware encryption. If you prefer not to migrate your software based keys to hardware, you need to start with hardware based keys, turn encryption on, and request your certificates again.

Changes to Using the eecertreq Utility

The changes associated with the steps in both the *IBM CommercePOINT Gateway for OS/390 System Administration Guide and Reference*, SC24-5873-00, and the *IBM CommercePOINT eTill for OS/390 Administrator's Guide* are documented separately below. Please refer to the appropriate section.

Using the eecertreq Utility in Gateway

To use the **eecertreq** utility found in the `/usr/lpp/set/bin` directory, complete the following steps:

1. Before running the **eecertreq** utility, you must first stop the instance of the Payment Gateway for which you are obtaining new certificates. Failure to do so results in the loss of the new certificates.
2. Start **eecertreq** by issuing the **eecertreq.exe** command.
3. When the following message appears, reply Y if you have stopped the Payment Gateway instance; otherwise, reply N and go back to Step 1 in this scenario.

   ```
   WARNING WARNING WARNING WARNING WARNING!!

   Running this program will affect the Payment Gateway application.
   Please terminate the Payment Gateway before proceeding.  Otherwise
   Data files may be corrupted.

   Do you wish to continue (Y/N)?
   ```

4. Unless you have encountered problems and want additional information, reply to the following question with N.

   ```
   Do you want to turn tracing on (Y or N)?
   ```

   If you reply Y, you will be asked to enter the directory path where the trace file will be created.
5. Answer the following question with Y or N:
   Is OS/390 ICSF HardwareCrypto enabled on your machine and do you plan to use it?
6. Enter the directory path where your databases are located or are to be created. If the databases do not already exist, you will be asked to confirm that you want to create them.
7. Select **REQUEST NEW CERTIFICATES** from the main menu to request certificates for a Payment Gateway.
8. Enter **P** to indicate that you want Payment Gateway certificates.
9. Enter **B** to select both a signature and an encryption certificate.
10. Enter the Brand ID provided by your Certificate Authority (CA) vendor in the wakeup message. This ID is case sensitive.

11. Enter the Request URL provided by your CA vendor in the wakeup message in the X-SET-SET-REQUEST field. This information is case sensitive.
12. If a Signing certificate is being requested and you replied Y in Step 5, enter the RSA keypair label for Signing that you entered on the TKE box. If TKE is not being used to generate the RSA keypair, just press Enter.
13. If an encryption certificate is being requested and you replied Y in Step 5, enter the RSA keypair label for Encryption you entered on the TKE box. If TKE is not being used to generate the RSA keypair, just press Enter.
14. Enter the acquirer ID.
15. Enter the 6-digit acquirer BIN.
16. The following messages appear:

```
Composing the certificate initiation message
Connecting to the host
Sending
Receiving
Processing the message
```

17. If the certificate initiation is successful, you are prompted for registration information. This information varies and depends on the CA vendor with whom you are working.
18. If the certificate initiation is rejected, you will see the following messages:

```
CertTranaction Operation Failed, return code 1830
Program Ending
Enter to continue
```

Using the eecertreq Utility Supplied with SET in eTill

Complete the following steps using the **eecertreq** utility found in the `/usr/lpp/set/bin` directory:

__ 1. Start **eecertreq** by issuing the **eecertreq.exe** command.

__ 2. Unless you have encountered problems and want additional information, reply to the following question with N.

```
Do you want to turn tracing on (Y or N)?
```

If you reply Y, you will be asked to enter the directory path where the trace file will be created.

__ 3. Answer the following question with Y or N:
Is OS/390 ICSF HardwareCrypto enabled on your machine and do you plan to use it?

__ 4. Enter the key database password. If the database already exists, the password must be the one specified when it was created. If the key database does not exist, it will be created using this password.

__ 5. Enter the directory path where your databases are located or will be created. If the databases do not exist, you will be asked to confirm that you want to create the databases.

__ 6. Select **REQUEST NEW CERTIFICATES** from the main menu to request certificates for a Merchant or a Payment Gateway.

__ 7. Enter **M** for a Merchant Certificate.

__ 8. Enter **B** to select a signature and an encryption certificate.

__ 9. Enter the Brand ID provided by your Certificate Authority (CA) vendor in the wakeup message. This ID is case sensitive.

__ 10. Enter the Request URL provided by your CA vendor in the wakeup message in the X-SET-SET-REQUEST field. This information is case sensitive.

__ 11. If a Signing certificate is being requested and you replied Y in Step 3, enter the RSA keypair label for Signing that you entered on the TKE box. If TKE is not being used to generate the RSA keypair, just press Enter.

__ 12. If an encryption certificate is being requested and you replied Y in Step 3, enter the RSA keypair label for Encryption you entered on the TKE box. If TKE is not being used to generate the RSA keypair, just press Enter.

__ 13. Enter the merchant ID.

__ 14. Enter the 6-digit Merchant BIN.

__ 15. The following messages appear:

```
Composing the certificate initiation message
Connecting to the host
Sending
Receiving
Processing the message
```

__ 16. If the certificate initiation is successful, you are prompted for registration information. This information varies and depends on the CA vendor with whom you are working.

__ 17. If the certificate initiation is rejected, you will see the following messages:

```
CertTransaction Operation Failed, return code 1830
Program Ending
Enter to continue
```