Activating S/390 and zSeries Cryptographic Services for WebSphere

Overview
This paper provides instructions for activating the cryptographic coprocessors on your IBM 9672, 2064, 2066 or 7060 mainframe. References to the appropriate manuals are also included. WebSphere for OS/390 and z/OS uses the cryptographic coprocessors for Secure Sockets Layer (SSL) support as well as to encrypt and decrypt the security token used in form based authentication.

Caveat
Activating the cryptographic services is just scratching the surface of the wide-ranging and powerful capabilities of S/390 and zSeries crypto. This document will help you get crypto working, but does not take into account numerous policy, planning, performance, training and security factors associated with the management of cryptographic services.

The reader is strongly encouraged to attend the IBM Learning Services class, **S/390 & zSeries Crypto Hardware, ICSF, TKE Installation and Overview Workshop**. The course number is ES801 (ES800 in Canada). Please call (800) IBM-TEACH for more information or to register.

Scope
These instructions are for activating crypto in support of SSL and form-based authentication as used by the WebSphere Application Server, the HTTP Server for OS/390 and z/OS, the SSL-enabled TN3270 server, LDAP Server, FTP Server, etc. These instructions are not for enabling cryptography for Linux on S/390 or zSeries or for VM/ESA or zVM. Optional cryptographic features such as the Trusted Key Entry workstation, the PCI Cryptographic Coprocessor and the PCI Cryptographic Accelerator are not discussed.

While these instructions should be adequate for activating cryptographic services for proof-of-concept or testing, additional training is required on the management of cryptographic services in a production environment. See Caveat above.

Overview of Steps
The following basic steps are necessary to activate crypto on your 9672, 2064, 2066 or 7060:
1.) Verify your processor model has Cryptographic Coprocessor(s).
2.) Obtain the Configuration Enablement Diskette(s) for your processor.
3.) Load the Configuration Enablement Diskette(s).
4.) Assign Cryptographic Coprocessor(s) to LPARs.
5.) Install and Initialize ICSF, the Integrated Cryptographic Service Facility.
6.) Start ICSF.
7.) Initialize the CKDS and PKDS and load your master key.
8.) Configure your Applications to Use Crypto.

Each of the above steps will be described in detail in the following sections.

Activating S/390 and zSeries Cryptographic Services for WebSphere

1. Verify your processor model has Cryptographic Coprocessor(s).

The Cryptographic Coprocessor is a hardware feature available on current IBM S/390 and zSeries processors. It provides special purpose hardware for improved cryptographic performance and key storage.

This document refers to the processor families by their machine types. As a reminder:
The z900 is the 2064.
The z800 is the 2066.
The S/390 Parallel Enterprise Server is the 9672.
The Multiprise 3000 is the 7060.

Current 9672 models (G4 and above) and all 2064 models have one or two Cryptographic Coprocessor Features (CCF) standard. 7060 and 2066 models do not have CCFs standard, but they can be ordered as optional features. The presence of one or two CCFs is indicated by feature code 0800.

2. Obtain the correct Configuration Enablement Diskette(s) for your processor.

The Cryptographic Coprocessor Feature (CCF) is shipped disabled, to comply with U.S. Export Regulations. The CCFs are enabled by loading one or two Configuration Enablement Diskettes, which are not included with feature code 0800, but have an optional feature code of their own. They will have been shipped with your processor (if they were ordered) , or they can be ordered via a no-charge MES later.

Configuration Enablement Diskettes are unique; only the diskettes created for your machine/serial number will work in your processor. After you have confirmed your processor has cryptographic coprocessor(s), you will need to determine if your processor was ordered with Configuration Enablement Diskettes, if they were ever loaded, and where they are currently located.

Check the configuration data for your processor to see if the Configuration Enablement Diskettes were ordered. The feature code varies with processor family, but will be in the 081x or 082x range, and the description will probably be 'TDES with PKA' or 'TDES'. If your processor configuration includes the Trusted Key Entry workstation, make sure you have the Configuration Enablement Diskettes that indicate that (for example, the description will read 'TDES with PKA and TKE'). The sales manual (online at the IBMLink web site) will list the correct feature code for your machine/model. If the feature code was never ordered, place a no-charge MES for it as soon as possible.

If the Configuration Enablement Diskettes were ordered, you will need to locate them. To start, check with your IBM Customer Engineer (CE). The diskettes are sometimes stored in the processor cabinet or other storage area accessible by the CE. If they were originally ordered but are missing, the CE can obtain replacements by contacting the IBM Quality Hotline at 1 (800) IBM-LINE.

3. Loading the Configuration Enablement Diskette(s).

Loading the Configuration Enablement Diskettes requires that you have a userid and password, as well as physical access to the Hardware Management Console (HMC) or Support Element, so that you can insert the diskettes into the HMC or Support Element diskette drive. For processors with an integrated Support Element (e.g. 9672 G5 and G6) or any other processor where the Support Element is locked inside the processor cabinet, you should use the HMC. For safety reasons, only the Customer Engineer is authorized to open the processor cabinet. If you have not worked with the HMC or the Support Element, you should work with someone who has until you become familiar with it. After loading the Configuration Enablement Diskettes, a Power On Reset (POR) will be required on your processor

If the Configuration Enablement Diskettes were ordered with your processor, it's likely they were loaded by the CE when your processor was installed. If you order the Configuration Enablement Diskettes after the processor has been installed, you will need to schedule some time for a POR.

Reference information describing how to load the Configuration Enablement Diskettes can be found in the 'Support Element Operations Guide' for your processor. Accessing Support Element functions through the HMC is described in the 'Hardware Management Console Operations' guide for your processor. These books can be found at one of the following sites: Http://www-1.ibm.com/servers/s390/os390/bkserv/hw/disc1_srch.html#titles or Http://www-1.ibm.com/servers/s390/os390/bkserv/hwpdf/z900.html

Here are the instructions for loading the Configuration Enablement Diskettes, culled together from various sections of the Support Element and HMC guides.

1.) Sign on to the HMC using the system programmer or service rep id.

2.) Establish a Support Element session from the HMC, as follows:

A. Open the Task List from the Views area. (Note on terminology: the Views area is the colored area at the top half of the screen. The Work area is the area at the bottom half of the screen. The Tasks area is the vertical area on the right side of the screen.)

B. Open CPC Recovery from the Task List Work Area.

C. Open Groups from the Views area.

D. Open Defined CPCs from the Groups Work Area

E. Identify the CPC with the Support Element that you want to connect to.

F. Drag and drop (right mouse click and hold) the selected CPC to Single Object Operations in the CPC Recovery tasks area. The Single Object Operations Task Confirmation window is displayed. Click the yes button to continue establishing a session with the Support Element. The 'Support Element Workplace' session window opens, and your Support Element session has begun.

3.) Continuing in the Support Element Workplace window, open the Task List view.

4.) Open the CPC Configuration task in the Task List Work Area.

5.) Open the Groups view.

6.) Open the group containing the CPC.
7.) Drag and drop (right mouse click and hold) the CPC onto the Cryptographic Coprocessor Configuration under the CPC Configuration.
8.) On the Cryptographic Coprocessor Configuration screen, note the 'Current Configuration Description'. Use the slider bar to help.

If the 'Current Configuration Description' displays 'DES/TDES w/PKA', 'DES/TDES w/PKA & TKE' or something similar, the Cryptographic Enablement Diskettes have already been loaded. You may skip ahead to Step 4, **Assign Cryptographic Coprocessor(s) to LPARs**.

If the 'Current Configuration Description' displays 'No Configuration chosen', the Cryptographic Enablement Diskettes have not been loaded. Continue with the next item.

9.) If the Cryptographic Enablement Diskettes have not been loaded, click the line for coprocessor 0 to highlight it, then click the ‘Import’ button. A popup will request that you insert the correct Enablement Diskette into the diskette reader of the HMC. The diskettes are labeled by cryptographic coprocessor module identifier and the popup will indicate by identifier which diskette to insert. Insert the diskette and click the ‘Import’ button. You will receive a warning message that you are about to import the diskette. Click on the enter button to continue. A popup will indicate that the import was successful. Click OK to continue.
10.) Now, with coprocessor 0 highlighted on the Cryptographic Coprocessor Configuration screen, click the ‘Select for next activation’ button. On the Select Cryptographic Coprocessor for Next Activation screen, in the Next Configuration list box, highlight the description of the Cryptographic Enablement Diskette you just imported. Select the ‘Auto-initialize’ button (or would it be better to select the ‘Force cryptographic coprocessor zeroization and initialization on next activation’ button?) and click the ‘Save’ button. You will receive a warning message that the coprocessor will be initialized on the next activation. Click Enter to continue. You will receive a message to remove the enablement diskette. Remove the diskette and click OK.

11.) If your processor also has a coprocessor 1, complete steps 9 and 10 (above) to import the Cryptographic Enablement Diskette for coprocessor 1.
12.) A Power On Reset must occur for the cryptographic enablement to take effect. However, If you have not already done so, you should complete the next step, **Assign Cryptographic Coprocessor(s),** before you perform the POR. The POR will then activate the changes made in both steps.

4.) Assign Cryptographic Coprocessor(s).

Whether your processor is operating in basic mode or LPAR mode, the cryptographic coprocessors must be assigned so that they can be accessed. This is done by customizing either a reset profile or an image profile using the Hardware Management Console (HMC) to access the Support Element. If you have not worked with the HMC or the Support Element, you should work with someone who has until you become familiar with it.

Reference information on how to assign the cryptographic coprocessors can be found in the Support Element Operations Guide for your processor. Accessing Support Element functions through the HMC is described in the Hardware Management Console Operations Guide for your processor. These books can be found at one of the following sites:
Http://www-1.ibm.com/servers/s390/os390/bkserv/hw/disc1_srch.html#titles or
Http://www-1.ibm.com/servers/s390/os390/bkserv/hwpdf/z900.html

The instructions below assume you are assigning the cryptographic coprocessors to existing partitions on a central processor complex operating in LPAR mode. For each partition you wish to have access to the cryptographic coprocessors, you will customize that partition's image profile as follows:

1.) If you are continuing from step 3, **Loading the Configuration Enablement Diskette(s),** you will have already started a Support Element session on your HMC. If not, start a Support Element session on your HMC as follows:

A. Sign on to the HMC using the system programmer or service rep id.
B. Open the Task List from the Views area. (Note on terminology: the Views area is the colored area at the top half of the screen. The Work area is the area at the bottom half of the screen. The Tasks area is the vertical area on the right side of the screen.)
C. Open CPC Recovery from the Task List Work Area.
D. Open Groups from the Views area.
E. Open Defined CPCs from the Groups Work Area
F. Identify the CPC with the Support Element that you want to connect to.
G. Drag and drop (right mouse click and hold) the selected CPC to Single Object Operations in the CPC Recovery tasks area. The Single Object Operations Task Confirmation window is displayed. Click the yes button to continue establishing a session with the Support Element. The 'Support Element Workplace' session window opens, and your Support Element session has begun.

2.) From the Support Element Workplace window, open the Task List view.
3.) Open the CPC Operational Customization task in the Task List Work Area.
4.) Open Groups from the Views area.
5.) Open the Images group from the Groups Work Area.
6.) Locate the image with the same name as the logical partition.
7.) Drag and drop (right click and hold) the logical partition on the Customize/Delete Activation Profiles task to start it. This opens the image profile and the list of load profiles that you want to

customize. When the list is initially displayed, the highlighted profile is the currently assigned profile for the partition.

8.) Select from the list the name of the image profile you want to customize.

9.) Click the Customize button

10.) Click the Processor tab of your image profile. Highlight one or both cryptographic coprocessors to make them available to that partition. (Note that if central processors are dedicated to that partition, the cryptographic coprocessors you select will be dedicated as well, and they won't be available to any other partitions.) When you highlight one or both cryptographic coprocessors, a Crypto tab (as well as a PCI Crypto tab) is added at the bottom of your image profile.

11.) Click the Crypto tab of your image profile. Ensure a check mark is present in the following check boxes on the Crypto page:

- Enable public key algorithm (PKA) facility
- Enable cryptographic functions
- Enable special security mode
- Enable integrated cryptographic facility (ICRF) key entry
- Enable public key secure cable (PKSC) and integrated cryptographic service facility (ICSF)

The rest of the check boxes can be left blank.

For the Control domain index and the Usage domain index, highlight the value that corresponds with your lpar number, from 00 to 15. Write the lpar number down for use later.

12. When done updating the Crypto page, click the save button. You may have to use the scroll bar on the right side of your screen to scroll down to the Save button.

13. Complete steps 6 through 12 above for each partition you will be activating crypto on.

14. At this point each partition you modified will need to be deactivated and reactivated for the changes to take effect.

15. Log off of the Support Element session on your HMC by pressing and holding the alt key, and pressing F4.

16. Log off of the HMC by pressing and holding the alt key, and pressing F4.

5.) Install and Initialize ICSF, the Integrated Cryptographic Service Facility.

If you are running OS/390 V2R4 or above, or any release of z/OS, the Integrated Cryptographic Service Facility (ICSF) is included in your OS/390 or z/OS system. Chapter 2 of the 'ICSF System Programmer's Guide', has detailed instructions on the installation, initialization and customization of ICSF. The ICSF System Programmer's Guide and the other ICSF books can be found online at the following locations. Search on books with titles containing 'ICSF'.
Http://www-1.ibm.com/servers/s390/os390/bkserv/os390/bop10_srch.html#titles or
Http://www-1.ibm.com/servers/eserver/zseries/zos/bkserv/zos/zbop3_srch.html#titles

The following is a summary of the steps described in Chapter 2 of the ICSF System's Programmer Guide. You should perform all of these steps.

1. Customize SYS1.PARMLIB.
2. Create the Cryptographic Key Data Set (CKDS) and Public Key Data Set (PKDS).
3. Create the installation options data set.
4. Create the ICSF startup procedure.
5. Provide access to the ICSF panels.

Misc. Notes:

Each partition which requires cryptographic services must have ICSF running. Each ICSF must have it's own installation options data set.

The sample installation options values specified in the ICSF System Programmer's Guide will work, with the following comments/exceptions:

> The installation options data set value for SSM should be YES
>
> A PKDS data set is required as of OS/390 V2R9. It's a good idea to define it even if you are on an earlier release.
>
> The 'domain' value specified in the installation options data set must match the 'Usage Domain' you highlighted on the Crypto tab for the lpar in task 11 of step 4, Assign Cryptographic Coprocessor(s).
>
> Each partition must have a unique domain value. The hardware won't allow them to share. This is why means each partition which requires cryptographic services must have it's own installation options data set.
>
> Partitions can share CKDS and PKDS data sets, if the same master keys are loaded into each partition.

6.) Start ICSF.

ICSF runs as a started procedure, and each partition which requires cryptographic services must have ICSF running. Starting ICSF is described in Chapter of the 'ICSF System Programmer's Guide', referenced above.

7.) Initialize the CKDS and PKDS and load your master key

After ICSF is started, you should be able to access the ICSF administrative panels by entering ICSF from the ISPF main menu. At this point you must initialize the CKDS and PKDS and load your master keys, using the ICSF panels. You will do this once on each partition where cryptographic services are required.

The easiest way to do this is to use the Pass Phrase Initialization Utility, which is well documented in Chapter 4 of the 'ICSF Administrator's Guide'. This and the other ICSF books can be found online:
Http://www-1.ibm.com/servers/s390/os390/bkserv/os390/bop10_srch.html#titles or
Http://www-1.ibm.com/servers/eserver/zseries/zos/bkserv/zos/zbop3_srch.html#titles

Misc. Notes:

The following information is necessary on the Pass Phrase Initialization panel:

- Pass Phrase: A 16 to 64 character phrase that is the basis for your new Master Key
- CKDS : The dataset name of your VSAM Cryptographic Key Data Set
- Initialize the CKDS? (Y/N): **see note below.**
- Signature MK = Key Management MK?: **Specify Y**

Be sure to write down your Pass Phrase and store it in a safe place.

It is not necessary to enclose your Pass Phrase in quotes. If you do enclose your Pass Phrase in quotes, the quotes will be treated as part of the Pass Phrase.

You should enclose your CKDS data set name in quotes. Otherwise, TSO will prefix the name with your TSO userid and won't find the data set.

If you will not be sharing the CKDS and PKDS with another partition, specify 'Y' for the question 'Initialize the CKDS?'.

If you will be sharing the CKDS and PKDS with another partition, each partition must use the same Pass Phrase. On the first partition where you run Pass Phrase Initialization, specify 'Y' for the question 'Initialize the CKDS?'. On subsequent partitions which use the same CKDS and PKDS, use the same Pass Phrase but specify 'N' for the question 'Initialize the CKDS?'.

If the process is successful, you will receive a message that initialization has completed, and the system log will receive messages similar to the following:

IEE504I CRYPTO(0),ONLINE
IEE504I CRYPTO(1),ONLINE
CSFM400I CRYPTOGRAPHY - SERVICES ARE NOW AVAILABLE.

Resolving Problems with Pass Phrase Initialization.

There is a problem that can appear during Pass Phrase Initialization. It is usually the result of skipping steps in the installation instructions, or mistyping something along the way. The problem is indicated when the messages like 'Register not empty' or 'CKDS already initialized' appear in the upper right corner of the Pass Phrase Initialization panel. The problem occurs when Pass Phrase Initialization is started, but does not complete successfully for some reason. When this occurs the master key registers and CKDS/PKDS are left in a partly loaded state, which will then cause subsequent attempts at Pass Phrase Initialization to fail.

The solution is to fix the problem that caused Pass Phrase Initialization to fail in the first place, reset the master key registers, delete and reallocate the CKDS and PKDS, and try again. Steps are given below.

1. Identify the problem that caused Pass Phrase Initialization to fail. Console log messages will give clues as to what the problem is. One reason is forgetting to include CSFDAUTH as a value in the AUTHPGM list and AUTHTSF list (See 'Customize SYS1.PARMLIB' in the ICSF System Programmer's Guide). Another reason is failing to enclose the CKDS name in quotes on the Pass Phrase Initialization panel. Your TSO prefix is included and the data set is not found.

2. Reset the master key registers. To do this:

A. Disable PKA Services. From the ICSF main menu, enter option 7, User Control functions. At the User Control Functions menu, enter option 4, Disable PKA Callable Services.

B. Go to 'Clear Master Key Entry' (From the ICSF main menu, enter options 1, 1, 1).

C. Select your first KSU (0)

D. At the Clear Master Key Entry Panel, For Key Type, select 'KMMK'. For Part, select 'RESET'. Press enter. Ignore any messages about Restart Option Invalid or Ignored.

E. At the Clear Master Key Entry Panel, For Key Type, select 'SMK'. For Part, select 'RESET'. Press enter. Ignore any messages about Restart Option Invalid or Ignored.

F. At the Clear Master Key Entry Panel, For Key Type, select 'NMK'. For Part, select 'RESET'. Press enter. Ignore any messages about Restart Option Invalid or Ignored.

G. Select your second KSU (1), if you have two, and repeat steps 4, 5, and 6.

3. Stop ICSF. Using IDCAMS, delete your CKDS and PKDS, then allocate them again. Instructions can be found in the ICSF System Progammer's Guide.

4. Start ICSF. Skip back to the beginning of step 7, **'Initialize the CKDS and PKDS and load your master key**', and try again.

8.) Configure your Applications to Use Crypto.

At the completion of Pass Phrase Initialization, cryptographic services will be active and you may begin configuring your applications to use them.

In the case of SSL, there are no changes necessary to WebSphere or the HTTP Server for OS/390 and z/OS. If the cryptographic coprocessors are online and ICSF is configured correctly and running, the cryptographic hardware will be used for SSL public key operations and some symmetric operations (DES, Triple DES, but not RC4).

If you are using ICSF in support of Form Based Authentication in WebSphere for z/OS, follow the instructions in APAR # PQ54343 to create the cryptographic key used by WebSphere to encrypt the login token. The apar also describes changes required in the webcontainer.conf file. APAR # PQ54343 mentions the use of the Key Generator Utility Program (KGUP). KGUP is a utility which is accessed through the ICSF application in ISPF. Use of KGUP is described in the ICSF Administrator's Guide.

Remember to make a backup copy of your CKDS and PKDS.

Activating S/390 and zSeries Cryptographic Services for WebSphere

References and Resources:

The 'Support Element Operations Guide' and 'Hardware Management Console Operations' guide for your processor can be found at one of the following sites:
For the 9672:
http://www-1.ibm.com/servers/s390/os390/bkserv/hw/disc1_srch.html#titles
For the 2064:
http://www-1.ibm.com/servers/s390/os390/bkserv/hwpdf/z900.html

The ICSF System Programmer's Guide and the other ICSF books can be found online at one of the following locations. Search on books with titles containing 'ICSF'.
For OS/390:
http://www-1.ibm.com/servers/s390/os390/bkserv/os390/bop10_srch.html#titles
For z/OS:
http://www-1.ibm.com/servers/eserver/zseries/zos/bkserv/zos/zbop3_srch.html#titles

The Salesmanual is useful for identifying the feature codes available on a processor model. Search on your processor machine type (9672, 2064, 2066, 7060). The Salesmanual is available at the IBMLink website, online at:
http://www.ibmlink.ibm.com/

Two IBM Redbooks which describe the cryptographic capabilities on S/390 are available:
S/390 Crypto PCI Implementation Guide, SG24-5942-00
Exploiting S/390 Hardware Cryptography with Trusted Key Entry, SG24-5455-00
These books are available at the IBM Redbook site:
http://publib-b.boulder.ibm.com/cgi-bin/searchsite.cgi?query=sg24-5455

Comments, Questions, Problems?:

Your feedback on this document will be greatly appreciated. Please direct all comments, questions or problems to:
Mike Kearney, c/o
IBM Corp.
Room 2B141
800 North Frederick Ave.
Gaithersburg, MD 20879

Or via email to kearney@us.ibm.com

Or via phone: (301) 240-3760