Hints and Tips for the Installation of Open Cryptographic Services Facility

This document includes the steps necessary to install Open Cryptographic Services Facility (OCSF) and it is being provided to clarify some of the installation steps involved. This document should be used with the OCSF manuals and not as a stand alone document.

1. RACF FACILITY class profiles

OCSF services are controlled by RACF. Define the following data sets to RACF;

Example:

```
RDEF FACILITY CDS.CSSM UACC(NONE)
RDEF FACILITY CDS.CSSM.CRYPTO UACC(NONE)
RDEF FACILITY CDS.CSSM.DATALIB UACC(NONE)
```

These profiles must be defined before installing OCSF and the person performing the OCSF install must be granted READ access. Any OCSF application must also be given READ access in order for the application to process.

Example:

```
 PE CDS.CSSM CL(FACILITY) ID(ocsfinstaller) AC(READ)
SETR  RACLIST(FACILITY) REFRESH
```

2. Program Control

It is recommend that you turn on Program Control in RACF and use this additional security feature with OCSF.

SETR WHEN(PROGRAM) - activate program control

If you do active Program Control here are some data sets that must be defined.

a. C/C++ Runtime Libraries - xxxx.CPP.SCLBDLL
b. Language Environment Libraries - xxxx.LEMVS.SCEERUN
c. System data sets - xxxx.LINKLIB
d. OCSF data sets - xxxx.CRYPTO.SGSKLOAD

```
RDEF PROGRAM *  ADDMEM(SYS1.LINKLIB//NOPADCHK) UACC(READ)
RALT PROGRAM * ADDMEM(SYS1.CRYPTO.SGSKLOAD//NOPADCHK)
```

(* covers all modules in these dataset and places them under program control)

```
SETR WHEN(PROGRAM) REFRESH
```

If you are installing OCSF because of OS/390 Firewall Technologies 2.8, Virtual Private Network capability with dynamic tunnels, then you must have Program Control active and the above data sets defined. You must also activate the WHEN(PROGRAM) option in RACF SETROPTS. The Firewall SICALMOD dataset must also be programmed controlled.

3. HFS Program Control

HFS files in the UNIX file system can also be controlled by turning on the program-controlled extended attributed for the HFS file containing the program or the dynamically loaded libraries (DLL).

Before you can use the UNIX command to turn on this program-controlled extended attribute you must be authorized to issue the command. In RACF the profile BPX.FILEATTR.PROGCTL must be defined to the FACILITY class and your ID must be granted READ access.

Example:

```
REF FACILITY BPX.FILEATTR.PROGCTL   OW(SYS1)
PE BPX.FILEATTR.PROGCTL CL(FACILITY) ID(ocsfinstaller) AC(READ)
```

Set HFS program-controlled extended attributed for all members in all OCSF libraries. Libraries are;
/usr/lpp/ocsf/lib
/usr/lpp/ocsf/ivp
/usr/lpp/ocsf/bin
/usr/lpp/ocsf/addins

List these libraries and make sure the program control bit is set:

Example:

```
cd /usr/lpp/ocsf/lib
ls -E
   -rwxr-xr-x   ps-  2 OMVSKERN OMVSGRP   462848 Jul 16  2000 ibmcca.so
   -rwxr-xr-x   ps-  2 OMVSKERN OMVSGRP   598016 Jul 16  2000 ibmcl.so
```

p indicates the program control bit is set, if it is not listed you must turn it on.

```
cd /usr/lpp/ocsf/lib
extattr +p ibmcca.so
```

Enter this command for each member contained in the OCSF libraries if the bit is not already set.

4. **APF authorizations**

If using OCSF from APF-authorized applications, the extended attribute must be set for all members in the OCSF libraries.

Example:

```
cd /usr/lpp/ocsf/lib
ls -E
 -rwxr-xr-x  aps-  2 OMVSKERN OMVSGRP   462848 Jul 16  2000 ibmcca.so
-rwxr-xr-x  aps-  2 OMVSKERN OMVSGRP   598016 Jul 16  2000 ibmcl.so
-rwxr-xr-x  aps-  2 OMVSKERN OMVSGRP   724992 Jul 16  2000 ibmcl2.so
```

The **a** indicates the APF bit is turned on and the **p** indicates the program control bit is set. If the APF bit is not listed, you must active turn it on.

```
cd/usr/lpp/ocsf/lib
extattr +a ibmcca.so
```

Repeat this command for each member of the OCSF libraries if the APF bit is not already set.

5. **OCSF User Identities and Permission**

If you are using OS/390 UNIX security then BPX.SERVER must be defined in RACF. The user ID associated with an OCSF application must be granted READ access to this profile (this includes the ID used to install OCSF). This profile controls the use of the OS/390 services used by OCSF and what ID has access authority.

If UNIX security is being used on your system, the above file is not defined. Therefore, the OCSF application, (and person installing OCSF) must run with a UID of 0 (super user).

```
REF FACILITY BPX.SERVER OW(SYS1)
PE BPX.SERVER CL(FACILITY) ID(yourid) UACC(READ)
```

6. Running the Installation Scripts

For 2.8 users:

a. Serverpac customers running the OCSF IVP ocsf_baseivp receive missing symlink message for cssmmanp.dll and cssmusep.dll The APAR number is OW42870. This APAR describes how to create these links.

Example:

```
> enter UNIX environment
> change to OCSF directory: cd /usr/lpp/ocsf/lib
> generate links :  ln -s cssmmanp_sl3.dll /usr/lpp/ocsf/lib/cssmmanp.dll
                    ln -s cssmusep_sl3.dll /usr/lpp/ocsf/lib/cssmusep.dll
```

b. Before running the installation scripts check the $LIBPATH parameter in the UNIX .profile. For installation and OCSF applications the $LIBPATH should point to /usr/lib. /usr/lib contains links to /usr/lpp/ocsf/lib.

c. Change directory to /usr/lpp/ocsf/bin

Run **ocsf_install_basic_crypto** and **ocsf_install_strong_crypto** if Security Level 3 or Security Level 2 is installed on your system.

If Security Level 1 or the French feature is installed run **ocsf_install_basic_crypto** only.

Verify install runs correctly, compare to data in OCSF manual.

For 2.10 users:

a. The APAR mentioned above for 2.8 is already included in this release**.**

b. Before running the installation scripts check the $LIBPATH parameter in the UNIX .profile. For installation and OCSF applications the $LIBPATH should point to /usr/lib. /usr/lib contains links to /usr/lpp/ocsf/lib.

c. Change directory to /usr/lpp/ocsf/bin

Enter **ocsf_install_crypto**

Compare results from this script to those listed in the OCSF manual, if everything matches you can run the verification script. If problems exist, check error message and correct problem.

7. **Run the Installation Verification procedures**

For 2.8 users:.

a. Change the directory to **/usr/lpp/ocsf/ivp**

b. The README.IVP file instructs you how you can specify a different directory for the OCSF files.

If you are using the default directory specified in the OCSF manual you can

ignore the README files since you will not be required to make any changes.

The README.IVP file directs you to an “addins script” file. This script file is the file ocsf_install_basic_crypto located in /usr/lpp/ocsf/bin. If you changed the directory during the OCSF install you can enter the command EXPORT OCSFINSTALLDIR (followed by the correct directory). This must be done before running the verification procedures.

c. If Security Level 3 or 2 is installed run; **ocsf_baseivp** and **ocsf_scivp**. If Level 1 or the French feature is installed run **ocsf_baseivp**.

If you receive the message “CSSM_INIT 10305 error”, check the directory /usr/lpp/ocsf/bin and make sure the ivp script files have the HFS program control attribute turned on (ls -E filename). If the file displays a “p” after the read/write attributes then the file does have the program-controlled extended attribute turned on.

d. Read the Common Problems section in the OCSF manual for additional installation tips.

For 2.10 users:

a**.** The information related to README.ivp mentioned above for 2.8 applies to
2.10 as well.

b. change directory to **/usr/lpp/ocsf/ivp**

Compare results of verification script to results listed in the OCSF manual.
If everything matches OCSF installation is complete

C. Security Level 3 Feature

If the Security Level 3 Feature is installed, you should perform the additional step of verifying that the correct policy table files are being used.

The files **/usr/lpp/ocsf/lib/cssmmanp.dll** and **/usr/opp/ocsf/lib/cssmusep.dll** are actual links. When only the OCSF base is installed, these links should point to **cssmmanp_sl2** and **cssmusep_sl2.dll**. When Security Level 3 Feature is installed, they should point to **cssmmanp_sl3.dll** and **cssmusep_sl3.dll**