HPE SSL1 Version 1.0-2C for OpenVMS Installation Guide and Release Notes

November 2015

This document contains hardware and software prerequisites,
installation instructions, post-installation tasks,
instructions for building your application, the HPE SSL1 directory
structure, and release notes for HPE SSL1 Version 1.0-2C for OpenVMS.

For the latest information about HPE SSL1, see the HPE SSL1 for OpenVMS
website at

http://h71000.www7.hp.com/openvms/products/ssl/ssl.html

The information in this file applies to HPE SSL1 running on
OpenVMS Integrity servers and OpenVMS Alpha systems.

HPE SSL1 Version 1.0-2C for OpenVMS is based on OpenSource OpenSSL version
1.0.2C from OpenSSL.org.

Vulnerabilities CVE/CAN:

Please refer OpenSSL websites: https://www.openssl.org/news/vulnerabilities.html

---
Installation Requirements and Prerequisites

The following sections list hardware and disk space requirements, and
software prerequisites.

Hardware Prerequisites - Disk Space Requirements

The HPE SSL1 for OpenVMS kit requires approximately 200,000 blocks of
working disk space to install. Once installed, the software occupies
approximately 170,000 blocks of disk space.

Software Prerequisites

HPE SSL1 V1.0-2C for OpenVMS requires the following software.

- Operating System

HP OpenVMS Alpha Version 8.4 or
HP OpenVMS Integrity server Version 8.4

with patch kits:
VMS84A_MANAGE-V0200 or
VMS84I_MANAGE-V0200

- TCP/IP Transport

HP TCP/IP Services for OpenVMS Version 5.7

HPE SSL1 for OpenVMS has been tested and verified using HP TCP/IP Services for OpenVMS. Hewlett Packard Enterprise has not formally tested and verified HPE SSL1 for OpenVMS on TCPware and MultiNet from Process Software Corporation.

- Account Quotas and System Parameters

There are no specific requirements for account quotas and system parameters for installing or using HPE SSL1 for OpenVMS.

New Features in HPE SSL1 Version 1.0-2C for OpenVMS

HPE SSL1 Version 1.0-2C for OpenVMS is first release based on OpenSource OpenSSL version 1.0.2 stream.

Co-existance and major changes between HP SSL V1.4 and HPE SSL V1.0

To make SSL product version aligned with OpenSSL version and to allow the co-existence of HP SSL V1.4 (based on OpenSSL 0.9.8 stream) and HPE SSL1 V1.0 (based on OpenSSL 1.0.2 stream) the SSL product name is modified to SSL1.

HPE recommends that both the HPE SSL1 V1.0 and HP SSL V1.4 products are installed till all the dependent products or components are compatible with the HPE SSL1 V1.0.
Once all the dependent products or components are successfully migrated to HPE SSL1 V1.0, the earlier HP SSL V1.4 kit can be removed.

Following is a snapshot of co-existence :

```
$ PROD SHOW PROD SSL*
---------------------------------- ----------- ---------
PRODUCT                            KIT TYPE    STATE
---------------------------------- ----------- ---------
HP I64VMS SSL V1.4-502             Full LP     Installed
HP I64VMS SSL1 V1.0-2C             Full LP     Installed
---------------------------------- ----------- ---------
2 items found
```

Logical names:
^^^^^^^^^^^^^^
All the HPE SSL1 V1.0 logical names are prefixed with SSL1$ and following is the snapshot of logical names that are defined in "HP SSL V1.4" and "HPE SSL1 V1.0":

HP SSL V1.4-502 Logicals	HPE SSL1 V1.0-2C Logicals
"OPENSSL" = "SSL$INCLUDE:"	"OPENSSL" = "SSL1$INCLUDE:"
"SSL$CERT" = "SSL$ROOT:[DEMOCA.CERTS]"	"SSL1$CERT" = "SSL1$ROOT:[DEMOCA.CERTS]"
"SSL$CERTS" = "SSL$ROOT:[DEMOCA.CERTS]"	"SSL1$CERTS" = "SSL1$ROOT:[DEMOCA.CERTS]"
"SSL$COM" = "SSL$ROOT:[COM]"	"SSL1$COM" = "SSL1$ROOT:[COM]"
"SSL$CONF" = "SSL$ROOT:[DEMOCA.CONF]"	"SSL1$CONF" = "SSL1$ROOT:[DEMOCA.CONF]"

"SSL$CRL" = "SSL$ROOT:[DEMOCA.CRL]" "SSL1$CRL" = "SSL1$ROOT:[DEMOCA.CRL]"
"SSL$EXAMPLES" = "SYS$COMMON:[SYSHLP.EXAMPLES.SSL]" "SSL1$EXAMPLES" =
"SYS$COMMON:[SYSHLP.EXAMPLES.SSL1]"
"SSL$EXE" = "SSL$ROOT:[IA64_EXE]" "SSL1$EXE" = "SSL1$ROOT:[IA64_EXE]"
"SSL$INCLUDE" = "SSL$ROOT:[INCLUDE]" "SSL1$INCLUDE" = "SSL1$ROOT:[INCLUDE]"
"SSL$KEY" = "SSL$ROOT:[DEMOCA.CERTS]" "SSL1$KEY" = "SSL1$ROOT:[DEMOCA.CERTS]"
"SSL$KEYS" = "SSL$ROOT:[DEMOCA.CERTS]" "SSL1$KEYS" = "SSL1$ROOT:
[DEMOCA.CERTS]"
"SSL$PRIVATE" = "SSL$ROOT:[DEMOCA.PRIVATE]" "SSL1$PRIVATE" = "SSL1$ROOT:
[DEMOCA.PRIVATE]"
"SSL$ROOT" = "SYS$SYSDEVICE:[VMS$COMMON.SSL.]" "SSL1$ROOT" = "SYS$SYSDEVICE:
[VMS$COMMON.SSL1.]"

These logicals gets defined by invoking SYS$STARTUP:SSL$STARTUP.COM and
SYS$STARTUP:SSL1$STARTUP.COM startup command procedures respectively.

The logical "OPENSSL" is mainly used to identify the OpenSSL header file
location for building a product against OpenSSL. When both HP SSL V1.4 and
HPE SSL1 V1.0 versions are co-existing, the "OPENSSL" logical will be pointed
to the version of product that was started later. The new manage patch kit -
VMS84I_MANAGE-V0200 / VMS84A_MANAGE-V0200 supplies a modified
VMS$LPBEGIN-050_STARTUP.COM command procedure, which ensure that HPE SSL V1.0
startup procedure is invoked later than HP SSL V1.4 startup procedure.

If there are any custom command procedures on your system using
"SSL$..." logicals, ensure that they are modified to use
"SSL1$..." logicals, while migrating from HP SSL V1.4 to HPE SSL1 V1.0.

Directory names:
^^^^^^^^^^^^^^^^
The top level directory structure for HPE SSL1 V1.0 is
SYS$SYSDEVICE:[VMS$COMMON.SSL1]. The top level directory structure for
HP SSL V1.4 product continues as is i.e. top level directory is
SYS$SYSDEVICE:[VMS$COMMON.SSL].

HPE SSL1 V1.0 example programs are located in
SYS$COMMON:[SYSHLP.EXAMPLES.SSL1] directory.

If there are any custom command procedures on your system using
"[SSL]" directory, ensure that they are modified to use
"[SSL1]" directory, while migrating from HP SSL V1.4 to HPE SSL1 V1.0.

Command procedure names:
^^^^^^^^^^^^^^^^^^^^^^^^
The relevant command procedure names are prefixed with "SSL1" for
HPE SSL1 V1.0 product
e.g.
SYS$STARTUP:SSL1$STARTUP.COM
SSL1$COM:SSL1$CERT_TOOL.COM

Earlier command procedure in HP SSL V1.4 were prefixed with "SSL"
e.g.
SYS$STARTUP:SSL$STARTUP.COM
SSL$COM:SSL$CERT_TOOL.COM

If there are any custom command procedures on your system invoking

"SSL$..." command procedures, ensure that they are modified to invoke
"SSL1$..." command procedures, while migrating from
HP SSL V1.4 to HPE SSL1 V1.0.

Library names:
^^^^^^^^^^^^^^
library names for HPE SSL1 V1.0 is prefixed with SSL1$ as follows:

SYS$SHARE:SSL1$LIBSSL_SHR.EXE
SYS$SHARE:SSL1$LIBCRYPTO_SHR.EXE
SYS$SHARE:SSL1$LIBSSL_SHR32.EXE
SYS$SHARE:SSL1$LIBCRYPTO_SHR32.EXE

library names for HP SSL V1.4 are retained as is:
SYS$SHARE:SSL$LIBSSL_SHR.EXE
SYS$SHARE:SSL$LIBCRYPTO_SHR.EXE
SYS$SHARE:SSL$LIBSSL_SHR32.EXE
SYS$SHARE:SSL$LIBCRYPTO_SHR32.EXE

Applications that are linked with HP SSL V1.4 product will continue using HP SSL V1.4 libraries and applications that are linked with HPE SSL1 V1.0 product will use the new libraries shipped with HPE SSL1 product.

The logical "OPENSSL" is used commonly by both HPE SSL1 V1.0 and HP SSL V1.4 products. Care should be taken to identify that this logical is defined to the appropriate path (either SSL1$INCLUDE: or SSL$INCLUDE:) before rebuilding the application with the correct libraries and header files.

Migrate certificate store from HP SSL V1.4 (or HP SSL V1.3) to HPE SSL1 V1.0:
^^

- The top level directory structure of HPE SSL1 V1.0 is modified to SYS$SYSDEVICE:[VMS$COMMON.SSL1] from SYS$SYSDEVICE:[VMS$COMMON.SSL] (Which is the top level directory structure of HP SSL V1.4 and HP SSL V1.3 product).

  In case there are certificate store manually created in the SYS$SYSDEVICE:[VMS$COMMON.SSL.DEMOCA...], copy this certificate store to SYS$SYSDEVICE:[VMS$COMMON.SSL1.DEMOCA...].

- In a certificate store, the certificate file will have names of the form: hash.0 or have symbolic links to them of this form ("hash" is the hashed certificate subject name: see the -hash option of the openssl x509 utility).

  From HP SSL V1.4 (or HP SSL V1.3) to HPE SSL1 V1.0, this hash is modified from MD5 to SHA-1 algorithm. Due to this, validation of certificates will fail, if we use the same hash names for certificate.

  Manually rename the certificate file name to use the new hash.

  An example of moving a certificate from HP SSL V1.4 to HPE SSL V1.0 is as follows:

  a) Assume, we have HP SSL V1.4 installed and created a certificate store
     in SSL$ROOT:[DEMOCA.CERTS].

b) Assume we have a certificate file 438F16D6.0 in
SSL$ROOT:[DEMOCA.CERTS]. The name "438F16D6" of this certificate
file is the MD5 hash of the certificate subject.

```
$ @SSL$COM:SSL$UTILS
$ openssl x509 -hash -in SSL$ROOT:[DEMOCA.CERTS]438F16D6.0
438F16D6
-----BEGIN CERTIFICATE-----
MIIB9zCCAWACCQC1TifkDidaxTANBgkqhkiG9w0BAQUFADBAMQswCQYDVQQGEwJV
UzELMAkGA1UECgwCSFAxDTALBgNVBAsMBFNUU0QxFTATBgNVBAMMDENBIEF1dGhv
cml0eTAeFw0xNTExMjYyMTI3NThaFw0yMDExMjQyMTI3NThaMEAxCzAJBgNVBAYT
AlVTMQswCQYDVQQKDAJIUDENMAsGA1UECwwEU1RTRDEVMBMGA1UEAwwMQ0EgQXV0
aG9yaXR5MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC3v+0ecrW2nbQ7ASwe
6hNeCPyixt6FdqnADVTVAws7TG70JFtVPK6pbc81grwJZPbJn1oAxTGMLLiANr/Y
XPlU73OUG+rrSiirq5fhWjVrD6M+yK9XHo6qnjMVUuwXITc8Sxr1xzDb/nOBX1+L
qkzGIX/4hvc4ko4OZ8mhKkEauwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAJetkXxW
YSi/crNHg+vSPiK1QA/KwLKDSNFDNazyvM9toswa9yA6U6ZBal0WCTj9efOi8Rbd
l1AH7HEUXUTccIrjlzOVsO4safWGt/wpyHNMZGAxA25Dd8fQbf9GpAvooaSPrdJU
u23fgeoXF3GcLYd/hog/yhpOq1w+BsA+nVi+
-----END CERTIFICATE-----
$
```

b) Now after installing HPE SSL1 V1.0 and executing the
"openssl x509 -hash" command from HPE SSL1 V1.0 kit, gives
"37d8de08" which is a SHA-1 hash of the certificate subject.

```
$ @SSL1$COM:SSL1$UTILS
$ openssl x509 -hash -in SSL$ROOT:[DEMOCA.CERTS]438F16D6.0
37d8de08
-----BEGIN CERTIFICATE-----
MIIB9zCCAWACCQC1TifkDidaxTANBgkqhkiG9w0BAQUFADBAMQswCQYDVQQGEwJV
UzELMAkGA1UECgwCSFAxDTALBgNVBAsMBFNUU0QxFTATBgNVBAMMDENBIEF1dGhv
cml0eTAeFw0xNTExMjYyMTI3NThaFw0yMDExMjQyMTI3NThaMEAxCzAJBgNVBAYT
AlVTMQswCQYDVQQKDAJIUDENMAsGA1UECwwEU1RTRDEVMBMGA1UEAwwMQ0EgQXV0
aG9yaXR5MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC3v+0ecrW2nbQ7ASwe
6hNeCPyixt6FdqnADVTVAws7TG70JFtVPK6pbc81grwJZPbJn1oAxTGMLLiANr/Y
XPlU73OUG+rrSiirq5fhWjVrD6M+yK9XHo6qnjMVUuwXITc8Sxr1xzDb/nOBX1+L
qkzGIX/4hvc4ko4OZ8mhKkEauwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAJetkXxW
YSi/crNHg+vSPiK1QA/KwLKDSNFDNazyvM9toswa9yA6U6ZBal0WCTj9efOi8Rbd
l1AH7HEUXUTccIrjlzOVsO4safWGt/wpyHNMZGAxA25Dd8fQbf9GpAvooaSPrdJU
u23fgeoXF3GcLYd/hog/yhpOq1w+BsA+nVi+
-----END CERTIFICATE-----
$
```

c) You will have to use a certificate file name having "37d8de08" if
you have to use this certificate store with HPE SSL1 V1.0:

```
$ COPY SSL$ROOT:[DEMOCA.CERTS]438F16D6.0 -
     SSL1$ROOT:[DEMOCA.CERTS]37d8de08.0
```

OR

```
$ openssl x509 -hash -in SSL$ROOT:[DEMOCA.CERTS]438F16D6.0 -out SSL1$ROOT:
[DEMOCA.CERTS]37d8de08.0
```

(Here, we are assuming that SSL1$ROOT:[DEMOCA.CERTS] is the new
certificate store directory usied with HPE SSL1 V1.0)

d) Follow step b) to c) for copying/renaming all the certificates in
the certificate store.

e) The certificate verification (using either openssl verify command,
or verifying the certificate using OpenSSL API's), will work with
HPE SSL1 V1.0, only if the certificate name in the certificate store
is "37d8de08.0"

f) Once you have stopped using HP SSL V1.4 certificate store, you can
delete the older certificate file having MD-5 hash file names.

g) While copying certificate store from SYS$SYSDEVICE:[VMS$COMMON.SSL.DEMOCA...]
to SYS$SYSDEVICE:[VMS$COMMON.SSL1.DEMOCA...], file DELETE_HASH_FILES.COM
will be having command to delete hashes as :
" $ DELETE SSL$ROOT:[DEMOCA.CERTS]438F16D6.0;* "
Please modify the DELETE_HASH_FILES.COM. to reflect the changes in file specification.

e.g. Change DELETE SSL$ROOT:[DEMOCA.CERTS]438F16D6.0;* to
"DELETE SSL1$ROOT:[DEMOCA.CERTS]37d8de08.0;*"

- For more information, see help on

openssl x509 -hash, -subject, -subject_hash_old, -issuer, -issuer_hash_old
option - https://www.openssl.org/docs/man1.0.2/apps/x509.html

openssl verify -CApath option -
https://www.openssl.org/docs/man1.0.2/apps/verify.html

OpenSSL Documentation from The Open Group

Documentation about the OpenSSL project and The Open Group is
available at the following URL:

http://www.openssl.org

The OpenSSL documentation was written for UNIX users. When reading
UNIX-style OpenSSL documentation, note the following differences
between UNIX and OpenVMS:

- File specification format

The OpenSSL documentation shows example file specifications in UNIX
format. For example, the UNIX file specification
/dka100/foo/bar/file.dat is equivalent to DKA100:[FOO.BAR]FILE.DAT on
OpenVMS.

- Directory format

Directories (pathnames) that begin with a period (.) on UNIX begin
with an underscore (_) on OpenVMS. In addition, on UNIX, the tilde (~)
is an abbreviation for SYS$LOGIN. For example, the UNIX pathname
~/.openssl/profile/prefs.js is equivalent to the OpenVMS directory
[._OPENSSL.PROFILE]PREFS.JS.

Downloading and Installing HPE SSL1 for OpenVMS from Website

A PCSI kit of HPE SSL1 for OpenVMS is available for download from
the HPE SSL1 website at

http://h71000.www7.hp.com/openvms/products/ssl/

Installation Procedure:
^^^^^^^^^^^^^^^^^^^^^^^
Install the HPE SSL1 V1.0 for OpenVMS kit by entering the following command:

$ PRODUCT INSTALL SSL1

HPE SSL1 V1.0 is always installed into SYS$SYSDEVICE:[VMS$COMMON].
The /DESTINATION qualifier is no longer supported.

A sample installation procedure is as follows:

Specifying the /HELP qualifier on the PRODUCT INSTALL command line
displays additional information about HPE SSL1.

$ PROD INSTAL SSL1

Performing product kit validation of signed kits ...
%PCSI-I-HPCVALPASSED, validation of 5DKA0:[SYS0.][SYSMGR]HP-I64VMS-SSL1-V0100-2C-1.PCSI$COMPRESSED;1 succeeded

The following product has been selected:
    HP I64VMS SSL1 V1.0-2C   Layered Product

Do you want to continue? [YES]

Configuration phase starting ...

You will be asked to choose options, if any, for each selected product and for
any products that may be installed to satisfy software dependency requirements.

Configuring HP I64VMS SSL1 V1.0-2C: SSL1 for OpenVMS I64 V1.0-2C (Based on OpenSSL 1.0.2C)

    ¦ Copyright 2015 Hewlett Packard Enterprise Development LP.

Do you want the defaults for all options? [YES]

    HPE SSL1 is not Backward Compatible!

        The HPE SSL1 Version 1.0-2C for OpenVMS is based on the 1.0.2C baselevel of
        OpenSSL. Some of the OpenSSL API, data structure and command are changed
        from the previous HP SSL version 1.4 (Based on OpenSSL 0.9.8 versions) and
        HP SSL version 1.3 (Based on OpenSSL 0.9.7 versions).

        If your application is dependent on the HP SSL 1.4 or 1.3 version of
        product, you must recompile and relink your code with the latest SSL1
        header files and shareable images after you upgrade to HPE SSL1
        version 1.0-2C, to use the HPE SSL1 product libraries.

HPE SSL1 and HP SSL product libraries (shareable image) have different name
and located in different directories. Hence both the product can co-exist
on the same system. Applications that are linked with HP SSL product will
continue using HP SSL libraries and Applications that are linked with
HPE SSL1 product will use the new libraries shipped with HPE SSL1 product.

The logical "OPENSSL" is used commonly by both HPE SSL1 and HP SSL product.
Care should be taken to identify that this logical is defined to the
appropriate path before rebuilding the application with the correct libraries
and header files of HPE SSL1. See the HPE SSL1 "Installation Guide and
Release Notes" for more information on migrating applications to HPE SSL1.

Following list of HPE products/components that are dependent on HPE SSL1.
Look at the product website for these products that is compatible with
HPE SSL1 Version 1.0-2C

LDAP
ENCRYPT
Stunnel
HPE System Management Homepage (HPE SMH) for OpenVMS
HPE WBEM Services for OpenVMS Integrity servers
HPE OpenView Operations Agent for OpenVMS
OpenView Performance Agent (OVPA) for OpenVMS
Secure Web Server
ABS
HPE Enterprise Directory

If any of the product dependent upon the above list of products, also
will not work.

For example:
- iCAp/nPar depends upon HP WBEMServices also will not work
- "$ backup/encrypt command which is in turn dependent on
  Encrypt will not work

Links to the above products are available in the HPE SSL1 home page.
http://h71000.www7.hp.com/openvms/products/ssl/ssl.html

Do you want to continue? [YES]

Do you want to review the options? [NO]

Execution phase starting ...

The following product will be installed to destination:
HP I64VMS SSL1 V1.0-2C DISK$SENT25_VMS84:[VMS$COMMON.]

Portion done: 0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%

The following product has been installed:
HP I64VMS SSL1 V1.0-2C Layered Product

%PCSI-I-IVPEXECUTE, executing test procedure for HP I64VMS SSL1 V1.0-2C ...
%PCSI-I-IVPSUCCESS, test procedure completed successfully

HP I64VMS SSL1 V1.0-2C: SSL1 for OpenVMS I64 V1.0-2C (Based on OpenSSL 1.0.2C)

There are post-installation tasks that you must complete

after upgrading from previous SSL1 versions

including verifying startup command procedures and logical names.

Refer to SYS$HELP:SSL100-2C.RELEASE_NOTES for more information.
$

Stopping and Restarting the Installation:
^^^

Use the following procedure to stop and restart the installation:

To stop the procedure at any time, press Ctrl/Y.

Enter the DCL command PRODUCT REMOVE SSL1 to reverse any changes to the system that occurred during the partial installation. This deletes all files created up to that point and causes the installation procedure to exit.

To restart the installation, go back to the beginning of the installation procedure.

Post-installation Tasks

After the installation is complete, perform the steps in one of the following sections:

- Ensuring SSL1 startup and logical name creation files are executed

HPE SSL1 V1.0 product is dependent on the VMS84I_MANAGE-V0200 or VMS84A_MANAGE-V0200 patch kit, which provides a modified SYS$STARTUP:VMS$LPBEGIN-050_STARTUP.COM command procedure. This command procedures automatically starts the HP SSL V1.4 and HPE SSL1 V1.0 version of the product (if they are installed on the system) respectively at system startup.

If the OpenVMS startup procedure SYS$MANAGER:SYSTARTUP_VMS.COM, also has an entry to start the HPE SSL1 V1.0 or HP SSL V1.4 (by invoking @SYS$STARTUP:SSL1$STARTUP.COM and @SYS$STARTUP:SSL$STARTUP.COM respectively), you can either comment out invoking these command procedure or replace it with the below set of commands:

```
$if f$search("sys$startup:ssl$startup.com") .nes. ""
$then
$@sys$startup:ssl$startup.com
$endif
$if f$search("sys$startup:ssl1$startup.com") .nes. ""
$then
$@sys$startup:ssl1$startup.com
$endif
```

The SSL1$STARTUP.COM and SSL$STARTUP.COM startup command procedures will

automatically define the SSL1$, SSL$ executive mode logical names in the SYSTEM logical name table, and install the SSL1, SSL shareable images that reside in the [SYSLIB] directory to memory.

Ensure that the SSL1$STARTUP.COM command procedure is invoked after invoking SSL$STARTUP.COM. Both command procedures defines a common logical "OPENSSL" which points to the include (header) file directory. Invoking SSL1$STARTUP.COM, ensure that the logical is defined to the latest HPE SSL1 1.0 header files.

Also, add SSL1$SHUTDOWN.COM to the SYS$MANAGER:SYSHUTDWN.COM file to remove the installed images and deassign the SSL1$ logical name definitions. If there is a SSL$SHUTDOWN.COM already present in SYS$MANAGER:SYSHUTDWN.COM, conditionalize it in a if statement:

```
$if f$search("sys$startup:ssl$shutdown.com") .nes. ""
$then
$@sys$startup:ssl$shutdown.com
$endif
$if f$search("sys$startup:ssl$shutdown.com") .nes. ""
$then
$@sys$startup:ssl$shutdown.com
$endif
```

Please refer "Logical names" under section "Co-existance and major changes between HP SSL V1.4 and HPE SSL V1.0" of this document for additional information.

- Define the foreign commands that use the OpenSSL utility OPENSSL.EXE, such as openssl, ca, enc, req, and X509, by entering the following command:

```
 $ @SSL1$COM:SSL1$UTILS
```

- Updated HPE SSL1 Files requiring attention

If this is the first time HPE SSL1 V1.0 is installed on the system and earlier, the system had HP SSL V1.4 (or HP SSL V1.3) only, perform the following actions:

- Copy any manual changes done from site specific startup command procedure SSL$COM:SSL$SYSTARTUP.COM to SSL1$COM:SSL1$SYSTARTUP.COM

- If SYS$STARTUP:SSL$STARTUP.COM, had any manual changes done earlier, ensure that these changes are moved to site specific startup command procedure SSL1$COM:SSL1$SYSTARTUP.COM. This command procedure will be invoked by SYS$STARTUP:SSL1$STARTUP.COM.

- Copy any manual changes done from site specific shutdown command procedure SSL$COM:SSL$SYSHUTDOWN.COM to SSL1$COM:SSL1$SYSHUTDOWN.COM.COM

- If SYS$STARTUP:SSL$SHUTDOWN.COM, had any manual changes done earlier, ensure that these changes are moved to site specific shutdown command procedure SSL1$COM:SSL1$SYSHUTDOWN.COM. This command procedure will be invoked by SYS$STARTUP:SSL1$SHUTDOWN.COM.

- Copy any manual changes done from OpenSSL configuration file

SSL$ROOT:[000000]OPENSSL.CNF to SSL1$ROOT:[000000]OPENSSL.CNF

- Copy any manual changes done from OpenSSL configuration file SSL$ROOT:[000000]OPENSSL-VMS.CNF to SSL1$ROOT:[000000]OPENSSL-VMS.CNF

- Migrate any application built with HP SSL V1.4 to HPE SSL1 V1.0, by rebuilding and relinking the application with the HPE SSL1 V1.0 header files and libraries. See "Library names" and "Logical names" under section "Co-existance and major changes between HP SSL V1.4 and HPE SSL V1.0" of this document for information on library names and header file locations.

- Migrate any command procedure using HP SSL V1.4 directories, command procedures or logicals to point to HPE SSL1 V1.0 directories, command procedures or logicals. See "Co-existance and major changes between HP SSL V1.4 and HPE SSL V1.0" section of this document for more information.

- Migrate any certificates store created from HP SSL V1.4 (or HP SSL V1.3) version of product to HPE SSL1 V1.0, by following the steps highlighted under "Migrate certificate store from HP SSL V1.4 (or HP SSL V1.3) to HPE SSL1 V1.0" under section "Co-existance and major changes between HP SSL V1.4 and HPE SSL V1.0" of this document.

- Optionally, run the Installation Verification Program (IVP) test by entering the following command:

```
$ @ SYS$TEST:SSL1$IVP.COM
```

Normally the Installation Verification Program (IVP) test is executed when HPE SSL1 V1.0 is installed. (The IVP test would not be executed at installation time if, for example, the PCSI qualifier /NOTEST was utilized)

- Optionally, start the Certificate Tool by entering the following command:

```
$ @SSL1$COM:SSL1$CERT_TOOL
```

This menu-driven tool allows you to create and view certificates and certificate requests and to sign certificate requests.

HPE SSL1 Directory Structure

After the installation is complete, the HPE SSL1 directory structure is as follows:

[SSL1] - Top-level directory created by default in SYS$SYSDEVICE:[VMS$COMMON].

One of the following two directories:
[SSL1.ALPHA_EXE] - Contains images for the Alpha platform.
[SSL1.IA64_EXE] - Contains images for the Integrity server platform.

[SSL1.COM] - Contains command procedures.
[SSL1.DEMOCA] - Contains demos for SSL's CA features
[SSL1.DEMOCA.CERTS] - Contains certificates and keys.
[SSL1.DEMOCA.CONF] - Contains configuration files.
[SSL1.DEMOCA.CRL] - Contains revoked certificates and CRLs.

[SSL1.DEMOCA.PRIVATE] - Contains private keys and random data.
[SSL1.DOC] - OpenSSL Group-provided documentation and information.
[SSL1.INCLUDE] - Contains C header (.H) files.
[SSL1.TEST] - Contains files used during the Installation Verification
Procedure (IVP).
[SYS$STARTUP] - Contains startup and shutdown templates and files.
[SYSHLP] - Contains release notes.
[SYSHLP.EXAMPLES.SSL1] - Contains SSL crypto and secure session examples.
[SYSLIB] - Contains SSL shareable image files.
[SYSTEST] - Contains SSL1$IVP.COM test files.

Note that the HPE SSL1 example programs are located in
SYS$COMMON:[SYSHLP.EXAMPLES.SSL1]. (The logical name SSL1$EXAMPLES
points to this directory.)

Building an HPE SSL1 Application

HPE SSL1 for OpenVMS provides shareable images that contain 64-bit APIs
and shareable images that contain 32-bit APIs. You can choose which
APIs to use when you compile your application.

The file names for these shareable images are as follows:

SYS$SHARE:SSL1$LIBSSL_SHR.EXE - 64-bit SSL APIs
SYS$SHARE:SSL1$LIBCRYPTO_SHR.EXE - 64-bit Crypto APIs
SYS$SHARE:SSL1$LIBSSL_SHR32.EXE - 32-bit SSL APIs
SYS$SHARE:SSL1$LIBCRYPTO_SHR32.EXE - 32-bit Crypto APIs

When you compile your application using HP C, use the /POINTER_SIZE=64
qualifier to take advantage of the 64-bit APIs. The default value for
the /POINTER_SIZE qualifier is 32.

Linking your application is the same for either 64-bit or 32-bit APIs.
The options file used contains either the 64-bit or 32-bit references
to the appropriate shareable image.

Building an Application Using 64-Bit APIs

To build (compile and link) an example program using the 64-bit APIs,
enter the following commands:

```
$ CC/POINTER_SIZE=64/PREFIX=ALL SAMPLE.C
$ LINK/MAP SAMPLE,LINKER_OPT/OPTIONS
```

In these commands, LINKER_OPT.OPT is a simple text file that contains
the following lines:

```
SYS$SHARE:SSL1$LIBSSL_SHR/SHARE
SYS$SHARE:SSL1$LIBCRYPTO_SHR/SHARE
```

Building an Application Using 32-Bit APIs

To build (compile and link) an example program using the 32-bit APIs,
enter the following commands:

```
$ CC/PREFIX=ALL SAMPLE.C
$ LINK/MAP SAMPLE,LINKER_OPT/OPTIONS
```

In these commands, LINKER_OPT.OPT is a simple text file that contains
the following lines:

```
SYS$SHARE:SSL1$LIBSSL_SHR32/SHARE
SYS$SHARE:SSL1$LIBCRYPTO_SHR32/SHARE
```

Release Notes

This section contains notes on the current release of HPE SSL1 for
OpenVMS.

The TLS1_ALLOW_EXPERIMENTAL_CIPHERSUITES experimental ciphers which were
part of HP SSL V1.3 and HP SSL V1.4 release are enabled in HPE SSL1 V1.0
release as well.This change is to address the backward compatibility
issues in the cipher suites that were enabled in HP SSL V1.3 and HP SSL V1.4.

Legal Caution

SSL data transport requires encryption. Many governments, including
the United States, have restrictions on the import and export of
cryptographic algorithms. Please ensure that your use of HPE SSL1 is in
compliance with all national and international laws that apply to you.

HPE SSL1 APIs Not Backward Compatible

The HPE SSL1 V1.0 for OpenVMS is based on the 1.0.2C baselevel of OpenSSL.
Few of the OpenSSL API, data structure, and commands are changed from the
previous HP SSL V1.3 (based on OpenSSL 0.9.7) and HP SSL V1.4 (based on
OpenSSL 0.9.8).

Hewlett Packard Enterprise cannot guarantee the backward compatibility of
HPE SSL1 V1.0 with HP SSL V1.3 and HP SSL V1.4.

Applications will have to rebuild and relink the images that is using
HP SSL V1.3 and HP SSL V1.4 shareable images Of the library with the latest
HPE SSL1 V1.0 header files and shareable images. Do note that
the HPE SSL1 shareable images names have changed. Refer to the
"Co-existance and major changes between HP SSL V1.4 and HPE SSL V1.0" for
details.

Preserve Configuration Files Before Manually Uninstalling HPE SSL1

Preserving configuration files is not necessary when you perform a

regular upgrade or reinstallation of HPE SSL1 using the PRODUCT INSTALL command.

Using the PRODUCT REMOVE command to manually uninstall HPE SSL1 is not recommended (see the following note). However, if you made any modifications to the HPE SSL1 configuration files, preserve the files by backing up these files to a different disk and directory before you enter the PRODUCT REMOVE command that removes the HPE SSL1 kit. Otherwise, any changes you made to OPENSSL-VMS.CNF and OPENSSL.CNF will be lost. When you have completed the Version HPE SSL1 1.0 installation, move the saved items back into the HPE SSL1 directory structure.

Warning Against Uninstalling HPE SSL1 from OpenVMS Version 8.3 or Higher Using the PRODUCT REMOVE Command
---

The POLYCENTER Software Installation utility command PRODUCT REMOVE is not supported for HPE SSL1 on OpenVMS Version 8.3 or higher, even though there is an apparent option to remove HPE SSL1. HPE SSL1 is installed together with the operating system and is tightly bound with it. An attempt to remove it from Version 8.3 or higher would not work cleanly and could create other undesirable side effects.

If you ignore the warning and continue to remove HPE SSL1, HP strongly recommends that you use PRODUCT INSTALL to install the HPE SSL1 Version 1.3 PCSI kit as soon as possible. An attempt to remove HPE SSL1 results in the following message:
%PCSI-E-HRDREF, product HP AXPVMS SSL V1.3-xxx is referenced by DEC AXPVMS OPENVMS V8.3-xxx

The two products listed above are tightly bound by a software dependency.

If you override the recommendation to terminate the operation, the referenced product will be removed, but the referencing product will have an unsatisfied software dependency and may no longer function correctly.

Please review the referencing product?s documentation on requirements.

Answer YES to the following question to terminate the PRODUCT command. However, if you are sure you want to remove the referenced product then answer NO to continue the operation.

Terminating is strongly recommended. Do you want to terminate? [YES]

Configuration Command Procedure Template Files

The configuration files included in the HPE SSL1 kit are named OPENSSL.CNF_TEMPLATE and OPENSSL-VMS.CNF_TEMPLATE. This prevents PCSI from overwriting the .CNF files, and allows you to preserve any modifications you made to OPENSSL.CNF and OPENSSL-VMS.CNF if you installed a previous release of HPE SSL1 for OpenVMS.

If you are upgrading from a previous version of HPE SSL1, after you install the HPE SSL1 kit, compare the new .CNF_TEMPLATE files with your existing .CNF files and add any new information as required.

If you did not previously install an HPE SSL1 for OpenVMS kit, both the .CNF_TEMPLATE and .CNF files are provided.

HPE SSL1 Requirement to Install on System Disk

The option to install to a location other than the system disk is no longer available beginning in HPE SSL1 V1.0 and later. If you download HPE SSL1 V1.0 and later from the website and install it as a layered product, it must be installed on the system disk.

Shut Down HPE SSL1 Before Installing on Common System Disk

Before installing HPE SSL1 to a common system disk in a cluster, you must first shut down HPE SSL1 by entering the following command on each node in the cluster:

```
$ @SYS$STARTUP:SSL1$SHUTDOWN
```

Shutting down HPE SSL1 deassigns logical names and removes installed shareable images that may interfere with the installation.
After the installation is complete, start HPE SSL1 by entering the following command on each node in the cluster:

```
$ @SYS$STARTUP:SSL1$STARTUP
```

Note: If you are installing on a common cluster disk and not a common system disk, omit the SYS$STARTUP logical and specify the specific startup directory in the shutdown and startup commands. For example:

```
$ @device:[directory.SYS$STARTUP]SSL1$SHUTDOWN
$ @device:[directory.SYS$STARTUP]SSL1$STARTUP
```

OpenSSL Version Command Displays HPE SSL1 for OpenVMS Version

Starting with HPE SSL1 Version 1.0, the OpenSSL command line utility command VERSION now includes the HPE SSL1 for OpenVMS version. The OpenSSL VERSION command displays output similar to the following:

```
OpenSSL> version
OpenSSL 1.0.2c 12 Jun 2015
SSL1 for OpenVMS V1.0  Nov 20 2015
```

Certificate Tool Cannot Have Simultaneous Users

Only one user/process should use the Certificate Tool at a time. The tool does not have a locking mechanism to prevent unsynchronized

accesses of the database and serial file, which could cause database corruption.

Protect Certificates and Keys

When you create certificates and keys with the Certificate Tool, take care to ensure that the keys are properly protected to allow only the owner of the keys to use them. A private key should be treated like a password. You can use OpenVMS file protections to protect the key file, or you can use ACLs to protect individual key files within a common directory.

Environment Variables

OpenSSL environmental variables have two formats, as follows:

$var
${var}

In order for these variables to be parsed properly and not be confused with logical names, HPE SSL1 for OpenVMS only accepts the ${var} format.

IDEA, RC5 and MDC2 Symmetric Cipher Algorithms Not Supported

The IDEA, RC5 and MDC2 symmetric cipher algorithms are not available in HPE SSL1 V1.0 for OpenVMS. These algorithms are under copyright protection, and Hewlett Packard Enterprise does not have the right to use these algorithms.

APIs RAND_egd, RAND_egd_bytes, and RAND_query_egd_bytes Not Supported

The RAND_egd(), RAND_egd_bytes(), and RAND_query_egd_bytes() APIs are not available on OpenVMS.
To obtain a secure random seed on OpenVMS, use the RAND_poll() API.

Documentation from the OpenSSL Website

The documentation on the OpenSSL website is located at https://www.openssl.org/docs/.It is likely that the API and command line documentation shipped with this kit will differ from the documentation on the OpenSSL website at some point. If such a situation arises, you should consider the API documentation on the OpenSSL website to have precedence over the documentation included in this kit.

Extra Certificate Files ? *PEM

When you sign a certificate request using either the Certificate Tool or the OpenSSL utility, you may notice that an extra certificate is produced with a name similar to SSL$CRT01.PEM. This certificate is the same as the certificate that you produced with the name you chose. These extra files are the result of the OpenSSL demonstration Certificate Authority (CA) capability, and are used as a CA accounting function. These extra files are kept by the CA and can be used to generate Certificate Revocation Lists (CRLs) if the certificate becomes compromised.

-- end of file --