VSI SSL111 for OpenVMS

V1.1-1DA Release Notes

October 2019

Based on OpenSSL 1.1.1d

VSI SSL111 V1.1-1DA for OpenVMS Itanium

VSI-I64VMS-SSL111-V0101-1DA-1.PCSI

VMS Software, Inc. is pleased to provide you with the latest release of
VSI SSL111 for OpenVMS. VSI SSL111 (Secure Sockets Layer) is based on the
1.1.1d release from the OpenSSL Group.

The VSI SSL111 product is designed to co-exist with VSI SSL 1.4 and VSI SSL1
so that applications and components dependent on either version will
run on the same system.

Below is the snapshot of co-existing VSI SSL V1.4, SSL1, and VSI SSL111 V1.1:

```
$ product show product ssl*
---------------------------------- ----------- ---------
PRODUCT                            KIT TYPE    STATE
---------------------------------- ----------- ---------
VSI I64VMS SSL V1.4-503            Full LP     Installed
VSI I64VMS SSL1 V1.0-2RA           Full LP     Installed
VSI I64VMS SSL111 V1.1-1DA         Full LP     Installed
---------------------------------- ----------- ---------
3 items found
```

For more information related to coexistence in terms of using directory
structures, command procedure names, libraries, and logical names refer to
SSL111_I64_INSTALL_RELEASE_NOTES.TXT "Installation Guide and Release Notes"
found in the SYS$COMMON:[SSL111.DOC] directory.

See http://www.openssl.org for information about OpenSSL.

There are post installation activities that need to be performed. This includes
the following items that are described in detail:

- Ensuring SSL111 startup and logical name creation files are executed

- Updating or copying the necessary startup, shutdown, and configuration files
  from the installed template files

- Running the Installation Verification Program (IVP)

The SSL111 installation creates the following directory structure and files in
PCSI$DESTINATION, which defaults to SYS$SYSDEVICE:[VMS$COMMON]:

```
[SSL111]                -  Top-level SSL111 directory
[SSL111.IA64_EXE]       -  Contains the images for the Itanium platform*
[SSL111.COM]            -  Directory to hold the various command procedures
[SSL111.DEMOCA]         -  Directory structure to demo SSL111's CA features
[SSL111.DEMOCA.CERTS]   -  Directory to hold the certificates and keys
[SSL111.DEMOCA.CONF]    -  Contains the configuration files
[SSL111.DEMOCA.CRL]     -  Contains revoked certificates and CRLs
[SSL111.DEMOCA.PRIVATE] -  Directory for private keys and random data
[SSL111.DOC]            -  OpenSSL.org provided documentation and information
[SSL111.INCLUDE]        -  Contains the C Header (.H) files
[SSL111.TEST]           -  Contains the files used during the IVP
```

```
[SYS$STARTUP]            -  Startup and shutdown templates and files
[SYSHLP]                 -  Release notes
[SYSHLP.EXAMPLES.SSL111] -  SSL111 crypto and secure session examples
[SYSLIB]                 -  SSL111 shareable image files
[SYSTEST]                -  SSL111$IVP.COM test files

* Note: Each system will have only one xxx_EXE.DIR, depending on the
        architecture of the system.


SSL111 startup, shutdown, and logical names
-------------------------------------------
Add SSL111$STARTUP.COM to SYS$MANAGER:SYSTARTUP_VMS.COM to define SSL111$ logical
names and install shareable images. If there is already a SSL$STARTUP.COM and/or
SSL1$STARTUP.COM present in SYSTARTUP_VMS.COM you can either comment these out
or conditionalize the command procedure as appropriate.

For example:

   $ 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
   $ if f$search("sys$startup:ssl111$startup.com") .nes. ""
   $ then
   $    @sys$startup:ssl111$startup.com
   $ endif

The SSL111$STARTUP.COM, SSL1$STARTUP.COM and SSL$STARTUP.COM startup command
procedures in the above example will automatically define the SSL111$, SSL1,
and SSL$ executive-mode logical names in the SYSTEM logical name table and will
install into memory the SSL111, SSL1, and SSL 1.4 shareable images that
reside in the [SYSLIB] directory.

Ensure that the SSL111$STARTUP.COM command procedure is invoked after
invoking SSL$STARTUP.COM or SSL1$STARTUP.COM. The command procedures define
a common logical "OPENSSL" that points to the include (header) file directory
used when building applications using OpenSSL. Invoking SSL111$STARTUP.COM
last ensures that the logical is defined to correctly point to the latest
VSI SSL111 1.1 header files.

Also, add SSL111$SHUTDOWN.COM to SYS$MANAGER:SYSHUTDWN.COM to remove installed
images and deassign the SSL111$ logical names at system shutdown. If there is a
SSL$SHUTDOWN.COM and/or SSL1$SHUTDOWN.COM already present in
SYS$MANAGER:SYSHUTDWN.COM, conditionalize the script as appropriate.

For example:

   $ if f$search("sys$startup:ssl$shutdown.com") .nes. ""
   $ then
   $    @sys$startup:ssl$shutdown.com
   $ endif
   $ if f$search("sys$startup:ssl1$shutdown.com") .nes. ""
   $ then
   $    @sys$startup:ssl1$shutdown.com
   $ endif
   $ if f$search("sys$startup:ssl111$shutdown.com") .nes. ""
   $ then
   $    @sys$startup:ssl111$shutdown.com
```

```
   $ endif

Please refer to "Logical names" under section "Coexistence and major changes
between VSI SSL V1.4, VSI SSL1, and VSI SSL111 V1.1" in VSI SSL111 installation
guide.


Apply SSL specific changes to SSL111 files
------------------------------------------
If this is the first time using a system with VSI SSL111 V1.1 and there
exist site-specific changes to VSI SSL V1.4 or VSI SSL1 files then it may
be necessary to migrate those changes to the SSL111 environment.

Examples:

 - Copy any manual changes done to the site-specific startup command procedures
   SSL$COM:SSL$SYSTARTUP.COM or SSL1$COM:SSL1$SYSTARTUP.COM to
   SSL111$COM:SSL111$SYSTARTUP.COM.

 - If SYS$STARTUP:SSL$STARTUP.COM or SYS$STARTUP:SSL1$STARTUP.COM have any
   manual changes, ensure that these changes are copied to the site-specific
   startup command procedure SSL111$COM:SSL111$SYSTARTUP.COM. This command
   procedure will be invoked by SYS$STARTUP:SSL111$STARTUP.COM.

 - Copy any manual changes done to the site-specific shutdown command procedures
   SSL$COM:SSL$SYSHUTDOWN.COM or SSL1$COM:SSL1$SYSHUTDOWN.COM to
   SSL111$COM:SSL111$SYSHUTDOWN.COM.

 - If SYS$STARTUP:SSL$SHUTDOWN.COM or SYS$STARTUP:SSL1$SHUTDOWN.COM have any
   manual changes, ensure that these changes are copied to the site-specific
   shutdown command procedure SSL111$COM:SSL111$SYSHUTDOWN.COM. This command
   procedure will be invoked by SYS$STARTUP:SSL111$SHUTDOWN.COM.

 - Copy any manual changes done to the OpenSSL configuration files
   SSL$ROOT:[000000]OPENSSL.CNF or SSL1$ROOT:[000000]OPENSSL.CNF to
   SSL111$ROOT:[000000]OPENSSL.CNF.

 - Copy any manual changes done to the OpenSSL configuration files
   SSL$ROOT:[000000]OPENSSL-VMS.CNF or SSL1$ROOT:[000000]OPENSSL-VMS.CNF to
   SSL111$ROOT:[000000]OPENSSL-VMS.CNF.

 - Migrate any SSL certificates store content to VSI SSL111 V1.1 by following
   the steps highlighted under "Migrate certificate store from VSI SSL V1.4
   or VSI SSL1 to VSI SSL111 V1.1" to SSL111 V1.1".


SSL111 Symbols
--------------
SSL111 foreign symbols are defined with the SSL111 command procedure
SSL111$COM:SSL111$UTILS.COM as follows:

$ @SSL111$COM:SSL111$UTILS.COM


Installation Verification Procedure (IVP)
-----------------------------------------
Normally the Installation Verification Procedure (IVP) is executed when
SSL111 is installed. To run the SSL111 IVP manually, type the following
command:

$ @SYS$TEST:SSL111$IVP.COM

Note that the IVP would not be executed at installation time if the
PCSI qualifier /NOTEST was utilized.
```

Removing SSL111

To remove SSL111 from the system disk or destination directory, type
the following command:

$ PRODUCT REMOVE SSL111

Note that some files may remain and will not be removed when the VSI SSL111
product is removed. These are generated files such as SSL111$IVP.LOG that
gets created by running the IVP test program and other files such as
certificates that have been created in the SSL111$CERTS directory.

Migrate certificate store from VSI SSL V1.4 or VSI SSL1 to VSI SSL111 V1.1

 - The top level directory structure of VSI SSL111 V1.1 is modified to
   SYS$SYSDEVICE:[VMS$COMMON.SSL111] from SYS$SYSDEVICE:[VMS$COMMON.SSL] or
   SYS$SYSDEVICE:[VMS$COMMON.SSL1] (Which are the top level directorys for
   VSI SSL 1.4 and VSI SSL1 respectively).

   In case there is a certificate store manually created in
   SYS$SYSDEVICE:[VMS$COMMON.SSL.DEMOCA...] or SYS$SYSDEVICE:[VMS$COMMON.SSL1.DEMOCA...],
   copy the certificate store to SYS$SYSDEVICE:[VMS$COMMON.SSL111.DEMOCA...].

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

   From VSI SSL V1.4 or VSI SSL1 to VSI SSL111 V1.1, this hash is modified
   from the MD5 to the SHA-1 algorithm. Due to this modification, validation of
   certificates will fail with SSL111 if we use the same hash names.

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

   An example of moving a certificate from VSI SSL V1.4 to VSI SSL111 V1.1 is
   as follows:

        a) Assume we have VSI SSL V1.4 installed and had 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 VSI SSL111 V1.1, executing the
"openssl x509 -hash" command from SSL111 gives "37d8de08" which is
a SHA-1 hash of the certificate subject.

```
$ @SSL111$COM:SSL111$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 wish to use this certificate store with VSI SSL111 V1.1:

```
$ COPY SSL$ROOT:[DEMOCA.CERTS]438F16D6.0 -
       SSL111$ROOT:[DEMOCA.CERTS]37d8de08.0

 OR

$ openssl x509 -hash -in SSL$ROOT:[DEMOCA.CERTS]438F16D6.0 .out
SSL111$ROOT:[DEMOCA.CERTS]37d8de08.0
```

(Here we are assuming that SSL111$ROOT:[DEMOCA.CERTS] is the new
certificate store directory used with VSI SSL111 V1.1)

d) Repeat steps b) and c) for all certificates in the certificate store.

e) Certificate verification (using either the "openssl verify" command
or verifying the certificate using OpenSSL API's) will work with
VSI SSL111 V1.1, only if (for the above example) the certificate name
in the certificate store is "37d8de08.0"

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

- 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