VSI SSL1 for OpenVMS

V1.0-2UA Release Notes

January 2020

Based on OpenSSL 1.0.2u

VSI SSL1 V1.0-2UA for OpenVMS Alpha

VSI-AXPVMS-SSL1-V0100-2UA-1.PCSI

VMS Software, Inc. is pleased to provide you with the latest
release of VSI SSL1 for OpenVMS. VSI SSL1 (Secure Sockets Layer)
is based on the 1.0.2u release from the OpenSSL Group.

The VSI SSL1 product is designed to co-exist with VSI SSL 1.4 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 and VSI SSL1 V1.0 :

```
$ product show product ssl*
------------------------------------ ----------- ---------
PRODUCT                              KIT TYPE    STATE
------------------------------------ ----------- ---------
VSI AXPVMS SSL V1.4-503              Full LP     Installed
VSI AXPVMS SSL1 V1.0-2UA             Full LP     Installed
------------------------------------ ----------- ---------
2 items found
```

For more information related to coexistence in term of using directory
structures, command procedure names, libraries and logical names refer to
SSL1_AXP_INSTALL_RELEASE_NOTES.TXT "Installation Guide and Release Notes" found
in the SYS$COMMON:[SSL1.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 SSL1 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)

SSL1 has created the following directory structure and files in
PCSI$DESTINATION, which defaults to SYS$SYSDEVICE:[VMS$COMMON]

```
[SSL1]                 -  Top-level SSL1 directory
[SSL1.ALPHA_EXE]       -  Contains the images for the Alpha platform*
[SSL1.COM]             -  Directory to hold the various command procedures
[SSL1.DEMOCA]          -  Directory structure to demo SSL1's CA features
[SSL1.DEMOCA.CERTS]    -  Directory to hold the certificates and keys
[SSL1.DEMOCA.CONF]     -  Contains the configuration files
[SSL1.DEMOCA.CRL]      -  Contains revoked certificates and CRLs
[SSL1.DEMOCA.PRIVATE]  -  Directory for private keys and random data
[SSL1.DOC]             -  OpenSSL.org provided documentation and information
[SSL1.INCLUDE]         -  Contains the C Header (.H) files
[SSL1.TEST]            -  Contains the files used during the IVP
```

```
[SYS$STARTUP]         -  Startup and shutdown templates and files
[SYSHLP]              -  Release notes
[SYSHLP.EXAMPLES.SSL1] -  SSL1 crypto and secure session examples
[SYSLIB]              -  SSL1 shareable image files
[SYSTEST]             -  SSL1$IVP.COM test files

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

SSL1 Startup, Shutdown and Logicals

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

```
   $if f$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 define a common logical "OPENSSL" which points to the include (header) file directory. Invoking SSL1$STARTUP.COM last ensures that the logical is defined to the latest VSI 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$startup:ssl1$shutdown.com") .nes. ""
   $then
   $@sys$startup:ssl1$shutdown.com
   $endif
```

Please refer to "Logical names" under section "Coexistence and major changes between VSI SSL V1.4 and VSI SSL1 V1.0" in VSI SSL1 installation guide.

Apply SSL specific changes to SSL1 Files

If this is the first time using a system with VSI SSL1 V1.0 and there exist site specific changes to the VSI SSL V1.4 files, then it may be necessary to migrate those changes to the SSL1 files.

Examples:

 - 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

 - 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 SSL certificates store content to VSI SSL1 V1.0 by following
   the steps highlighted under "Migrate certificate store SSL 1.4 to
   SSL1 V1.0"

SSL1 Symbols

SSL1 foreign symbols are defined with the SSL1 command procedures:

SSL1$COM:SSL1$UTILS.COM

Installation Verification Procedure (IVP)

Normally the Installation Verification Procedure (IVP) is
executed when SSL1 is installed. To run the SSL1 IVP manually,
type one of the following commands:

$ @ SYS$TEST:SSL1$IVP.COM

The IVP test would not be executed at installation
time if, for example, the PCSI qualifier /NOTEST was utilized.

Removing SSL1

To remove SSL1 from the system disk or destination directory, type
the following command:

$ PRODUCT REMOVE SSL1

Note: some files may remain and will not be removed when the VSI SSL1 product
is removed. These are generated files like SSL1$IVP.LOG that gets created by
running the IVP test program, Other files may include certificates,
such as those created by the certificate tool in the SSL1$CERTS: directory.

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

 - The top level directory structure of VSI 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 is a certificate store manually created in the SYS$SYSDEVICE:[VMS$COMMON.SSL.DEMOCA...], copy the 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 VSI 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 VSI SSL1 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 VSI SSL1 V1.0 and executing the "openssl x509 -hash" command from VSI 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 VSI 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 used with VSI 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
       VSI 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.

- 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
```