Rocky Enterprise Linux 9.2 Manual Pages on command 'sess_id.1ssl'

C:\>man sess_id.1ssl

SESS_ID(1SSL) OpenSSL SESS_ID(1SSL)

NAME

openssl-sess_id, sess_id - SSL/TLS session handling utility

SYNOPSIS

openssl sess_id [-help] [-inform PEM|DER] [-outform PEM|DER|NSS] [-in filename]
[-out filename] [-text] [-noout] [-context ID]

DESCRIPTION

The sess_id process the encoded version of the SSL session structure and optionally prints out SSL session details (for example the SSL session master key) in human readable format. Since this is a diagnostic tool that needs some knowledge of the SSL protocol to use properly, most users will not need to use it.

OPTIONS

-help

Print out a usage message.

-inform DER|PEM

This specifies the input format. The DER option uses an ASN1 DER encoded format containing session details. The precise format can vary from one version to the next. The PEM form is the default format: it consists of the DER format base64 encoded with additional header and footer lines.

-outform DER|PEM|NSS

This specifies the output format. The PEM and DER options have the same meaning and default as the -inform option. The NSS option outputs the session id and

the master key in NSS keylog format.

-in filename

This specifies the input filename to read session information from or standard input by default.

-out filename

This specifies the output filename to write session information to or standard output if this option is not specified.

-text

Prints out the various public or private key components in plain text in addition to the encoded version.

-cert

If a certificate is present in the session it will be output using this option, if the -text option is also present then it will be printed out in text form.

-noout

This option prevents output of the encoded version of the session.

-context ID

This option can set the session id so the output session information uses the supplied ID. The ID can be any string of characters. This option won't normally be used.

OUTPUT

Typical output:

SSL-Session:

Protocol : TLSv1

Cipher : 0016

Session-ID: 871E62626C554CE95488823752CBD5F3673A3EF3DCE9C67BD916C809914B40ED

Session-ID-ctx: 01000000

Master-Key: A7CEFC571974BE02CAC305269DC59F76EA9F0B180CB6642697A68251F2D2BB57E51DBBB4C7885573192AE9AEE220FACD

Key-Arg : None

Start Time: 948459261

Timeout : 300 (sec)

Verify return code 0 (ok)

These are described below in more detail.

Protocol

This is the protocol in use TLSv1.3, TLSv1.2, TLSv1.1, TLSv1 or SSLv3.

Cipher

The cipher used this is the actual raw SSL or TLS cipher code, see the SSL or TLS specifications for more information.

Session-ID

The SSL session ID in hex format.

Session-ID-ctx

The session ID context in hex format.

Master-Key

This is the SSL session master key.

Start Time

This is the session start time represented as an integer in standard Unix format.

Timeout

The timeout in seconds.

Verify return code

This is the return code when an SSL client certificate is verified.

NOTES

The PEM encoded session format uses the header and footer lines:

-----BEGIN SSL SESSION PARAMETERS-----

-----END SSL SESSION PARAMETERS-----

Since the SSL session output contains the master key it is possible to read the contents of an encrypted session using this information. Therefore appropriate security precautions should be taken if the information is being output by a "real" application. This is however strongly discouraged and should only be used for debugging purposes.

BUGS

The cipher and start time should be printed out in human readable form.

SEE ALSO

ciphers(1), s_server(1)

COPYRIGHT