Rocky Enterprise Linux 9.2 Manual Pages on command 'SSL_CTX_use_serverinfo_file.3ossl'

$ man SSL_CTX_use_serverinfo_file.3ossl

SSL_CTX_USE_SERVERINFO(3ossl) OpenSSL SSL_CTX_USE_SERVERINFO(3ossl)

NAME

SSL_CTX_use_serverinfo_ex, SSL_CTX_use_serverinfo,

SSL_CTX_use_serverinfo_file - use serverinfo extension

SYNOPSIS

```
#include <openssl/ssl.h>

int SSL_CTX_use_serverinfo_ex(SSL_CTX *ctx, unsigned int version,
                              const unsigned char *serverinfo,
                              size_t serverinfo_length);

int SSL_CTX_use_serverinfo(SSL_CTX *ctx, const unsigned char *serverinfo,
                           size_t serverinfo_length);

int SSL_CTX_use_serverinfo_file(SSL_CTX *ctx, const char *file);
```

DESCRIPTION

These functions load "serverinfo" TLS extensions into the SSL_CTX. A "serverinfo" extension is returned in response to an empty ClientHello Extension.

SSL_CTX_use_serverinfo_ex() loads one or more serverinfo extensions from a byte array into ctx. The version parameter specifies the format of the byte array provided in *serverinfo which is of length serverinfo_length.

If version is SSL_SERVERINFOV2 then the extensions in the array must consist of a 4-byte context, a 2-byte Extension Type, a 2-byte length, and then length bytes of extension_data. The context and type values have the same meaning as for SSL_CTX_add_custom_ext(3). If serverinfo is being loaded for extensions to be added to a Certificate message, then the extension will only be added for the first certificate in the message (which is always the end-entity certificate).

If version is SSL_SERVERINFOV1 then the extensions in the array must consist of a 2-byte Extension Type, a 2-byte length, and then length bytes of extension_data. The type value has the same meaning as for SSL_CTX_add_custom_ext(3). The following default context value will be used in this case:

SSL_EXT_TLS1_2_AND_BELOW_ONLY | SSL_EXT_CLIENT_HELLO | SSL_EXT_TLS1_2_SERVER_HELLO | SSL_EXT_IGNORE_ON_RESUMPTION

SSL_CTX_use_serverinfo() does the same thing as SSL_CTX_use_serverinfo_ex() except that there is no version parameter so a default version of SSL_SERVERINFOV1 is used instead.

SSL_CTX_use_serverinfo_file() loads one or more serverinfo extensions from file into ctx. The extensions must be in PEM format. Each

extension must be in a format as described above for SSL_CTX_use_serverinfo_ex(). Each PEM extension name must begin with the phrase "BEGIN SERVERINFOV2 FOR " for SSL_SERVERINFOV2 data or "BEGIN SERVERINFO FOR " for SSL_SERVERINFOV1 data.

If more than one certificate (RSA/DSA) is installed using SSL_CTX_use_certificate(), the serverinfo extension will be loaded into the last certificate installed. If e.g. the last item was a RSA certificate, the loaded serverinfo extension data will be loaded for that certificate. To use the serverinfo extension for multiple certificates, SSL_CTX_use_serverinfo() needs to be called multiple times, once after each time a certificate is loaded via a call to SSL_CTX_use_certificate().

RETURN VALUES

On success, the functions return 1. On failure, the functions return 0. Check out the error stack to find out the reason.

SEE ALSO

ssl(7)

COPYRIGHT