NAME

SSL_CTX_use_serverinfo, SSL_CTX_use_serverinfo_file - use serverinfo extension

SYNOPSIS

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

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 ServerHello Extensions into the SSL_CTX. A ‘‘serverinfo’’ extension is returned in response to an empty ClientHello Extension.

SSL_CTX_use_serverinfo() loads one or more serverinfo extensions from a byte array into **ctx**. The extensions must be concatenated into a sequence of bytes. Each extension must consist of a 2-byte Extension Type, a 2-byte length, and then length bytes of extension_data.

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 consist of a 2-byte Extension Type, a 2-byte length, and then length bytes of extension_data. Each PEM extension name must begin with the phrase ‘‘BEGIN SERVERINFO FOR ’’.

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.

RETURN VALUES

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

COPYRIGHT