Laborator 13 - OpenSSL

Realizarea unei conexiuni securizate

1. Initializare biblioteca
2. Initializare context
    a. `SSL_CTX * ctx = SSL_CTX_new(SSLv23_client_method());`
3. Incarcare trust store
    a. `if (!SSL_CTX_load_verify_locations(ctx,"TrustStore.pem",NULL)) {}`
4. Stabilire conexiune criptata
    a. creare de obiect BIO
        i. `BIO * bio = BIO_new_ssl_connect(ctx);`
    b. setare de hostname si port
        i. `BIO_set_conn_hostname(bio, "google.com:443");`
    c. conectare
        i. `if (BIO_do_connect(bio) <= 0) {}`
5. Verificare certificat
    a. `BIO_get_ssl(bio, & ssl);`
    b. `if (SSL_get_verify_result(ssl) != X509_V_OK) {}`

Comunicarea prin intermediul unei conexiuni securizate

1. Trimitere de request-uri
    a. `int w = BIO_write(bio, buffer, BUFSIZE);`
2. Primire de reply-uri
    a. `int r = BIO_read(bio, buffer, BUFSIZE);`
3. Inchidere conexiune
    a. `BIO_free_all(bio);`

https://www.cloudflare.com/learning/ssl/how-does-ssl-work/
https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/