Abstract

TietoEnator in Karlstad develops a protocol stack based on SS7 (Signaling System Nr 7). There is a desire to increase the security provided by SS7 when it is used in an IP network (Internet Protocol network). A possible solution is to use TLS (Transport Layer Security).

There is an existing implementation of TLS called openSSL. TietoEnator has decided to use openSSL in order to test how TLS functions with SS7. The openSSL code is designed to run on top of the transport layer protocol TCP (Transmission Control Protocol). However, SS7 uses SCTP (Stream Control Transmission Protocol) at the transport layer. To use openSSL with SS7 openSSL must be adapted to SCTP.

This document analyses parts of the existing SS7 environment, including SCTP, and the openSSL code. The openSSL code analysis concentrates on the parts of openSSL that communicate with TCP, because these are the parts that need to be adapted to SCTP. The analysis shows that there are at least three different design approaches to the adaptation of openSSL to SCTP. One approach involves translation of each TCP call into a SCTP call. However, this is not possible because of the differences between TCP and SCTP. Another approach involves creation of a translating software module between the TCP calls and SCTP. This demands too much time for a test implementation but is suitable for the production version. The last approach involves rewriting the parts of openSSL that communicate with TCP. This requires a lot of openSSL modifications but is adequate for a test implementation. An initial implementation according to the third approach is made as a part of this work.