

SECURLIB/SSL

SecurLib/SSL – Easily integrate standard SSL cryptographic operations into your applications

Various security mandates like PCI-DSS, Sarbanes Oxley, and HIPAA enforce the encryption of data in transit. TLS is one of the standard protocols to do this and is available as the HPE NonStop SSL product for NonStop X and J-Series systems.

Standard communication protocols such as Telnet and FTP work well with a TLS proxy but many applications, such as line-handlers, require a tighter integration with the TCP/IP environment than a proxy can provide. In these environments the SecurLib/SSL range of products is often the solution.

Purpose

The SecurLib/SSL product family provides the power of comForte's proven SSL implementation to existing TCP/IP (socket) applications in two ways:

- ▶ If you have access to the source code of the application and if the application is implemented in native code, SecurLib/SSL-classic allows you to add SSL encryption capabilities with just a few lines of code.
- ▶ If you do not have the source code or do not want to change it, SecurLib/SSL-AT (Application Transparent) adds SSL encryption transparently, with no changes to the application or configuration. For example, SecurLib/SSL-AT can encrypt ATM traffic for existing BASE24™ installations.

In both instances, your application will now fully support the SSL encryption standard without requiring the configuration and performance overhead of a proxy-based solution.



System Requirements

NonStop System

- ▶ H06.15 or later
- ▶ J06.04 or later
- ▶ L16.05 or later

SecurLib can be called from C,C++, pTAL and COBOL. Native compilers are required.

Features & Benefits

Proven SSL technology.

- ▶ The SecurLib/SSL products share code with comforte's proven SSL products, which are now part of the HPE NonStop operating system as HPE NonStop SSL.
- ▶ SecurLib/SSL-classic is in use by HPE for the OSM product.
- ▶ comforte has delivered SSL solutions to the NonStop market since 2001.

Tight integration of SSL into the application - unlike a proxy-based solution, both SecurLib/SSL-classic and SecurLib/SSL-AT grant the application full access and control to the remote IP address and port number of the connection.

Performance improvement compared to a proxy-based solution. Tests by comforte have shown that response times can be twice as long using a proxy-based solution.

Plain data cannot be viewed through PTRACE - with a proxy-based approach, the plain data can be traced via PTRACE on the so-called loopback connection. While this can be avoided by properly securing the NonStop system, that remains a residual risk.

Requirements and architecture for SecurLib/SSL-classic

In order to use SecurLib/SSL-classic successfully, the following requirements apply:

- ▶ Full source code of the application must be available
- ▶ The application is written in C, C++, TAL or COBOL and uses native compilers
- ▶ SecurLib/SSL-classic is delivered as a static library which needs to be bound into your application with a header file.

Requirements and architecture for SecurLib/SSL-AT

SecurLib/SSL-AT will work with any object file. However, for non-native object files SecurLib/SSL-AT will need to use a proxy process so the performance improvement and protection against PTRACE will not be present.

comforte AG, Germany
phone +49 (0) 611 93199-00
sales@comforte.com

comforte, Inc., USA
phone +1 646 438 5716
ussales@comforte.com

comforte Asia Pte. Ltd., Singapore
phone +65 6808 5507
asiasales@comforte.com

comforte Pty Ltd, Australia
phone +61 2 8197 0272
aussales@comforte.com

www.comforte.com