Security concerns are receiving an unprecedented focus from IT organizations these days. While risks associated with security issues have been well understood, many companies are in dire need of a single integrated security solution for their connectivity environment.

**Key benefits**
The need for a safe and secure enterprise system is an important concern in today’s business computing world. Security breaches can cause serious harm to a company that does not have the proper safeguards in place. Administrators are realizing they cannot afford to take any chances with mission-critical enterprise information assets that affect the success of the organization.
Open Text Secure Shell is a full-featured security suite that provides support for the following security standard-based protocols:

- **Secure Shell** is a transport protocol that allows users to log on to other computers over a network, execute commands on remote machines, and securely move files from one machine to another. It provides powerful authentication and secure communications over insecure channels, and is intended as a replacement for rlogin, rsh, and rcp. By using Open Text Secure Shell, administrators can eliminate the act of eavesdropping on sensitive information such as user credentials.

- **SSL/TLS** consist in a set of cryptographic libraries which can be used by software applications to provide strong encryption and authentication for transmitting data over a network. SSL/TLS uses cipher suites that encrypt data in such a way that it becomes virtually impossible for any eavesdropper to decrypt the information. SSL/TLS also provides support for key exchange and X.509 certificates authentication.

- **Kerberos** is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. Kerberos was created by Massachusetts Institute of Technology as a solution to solve network security authentication problems.

Open Text Secure Shell allows organizations to secure their network by providing authentication and encryption capabilities to the following communication types:

- X11
- NFS
- FTP
- Telnet
- Any other type of TCP/IP protocol

Open Text Secure Shell is fully and transparently integrated with other Open Text Connectivity Solutions Group software such as:

- Open Text® Exceed®: the leading-edge X Window server for Windows desktops
- Open Text NFS Client™: the de facto NFS client for Windows® PCs
- Open Text® HostExplorer®: the integrated traditional and web-to-host terminal emulation solution
- HostExplorer FTP™: the Windows Explorer integrated FTP client

Open Text Secure Shell 14 can also successfully provide Secure Shell and Kerberos services to third-party applications.

### Key features

**Certification**
- Compatible with Windows 7
- FIPS 140-2 Validated
- Citrix Ready

**Supported protocols**
- Secure Shell 2
- SSL v2/3 & TLS
- LIPKEY
- Kerberos V4 & v5

### Secure Shell 2
- Secure terminal, SFTP, X11 forwarding, and generic port forwarding
- Authentication method: password, keyboard interactive, public/private key, Kerberos, X.509 certificates
- Support for SSH-Agent and passphrase caching
- Command line SSH and SCP utility with third-party compatibility mode
- Graphic monitoring of Secure Shell activity
- Integrated SOCKS support with dynamic port forwarding
- Seamless integration with other Open Text Connectivity Solutions Group software
- "Black-Box" secure shell tunnels with no user interface
- Public/Private key and X.509 certificate creation wizard
- Auto-upload and multiple import/export format for public/private keys

**SSL-LIPKEY**
- Support for Low Infrastructure Public Key (LIPKEY)
- SSL/TLS encryption
- Support for X.509 certificate
- SafeNet® iKey™ 2000 USB-based authentication token support
- Support for smart card authentication

**Kerberos**
- Support for Kerberos v4 & v5 (authentication and encryption)
- Integration with Microsoft Windows Kerberos ticket cache
- Advanced ticket management function
- Simplified configuration file creation
### System requirements

- **Web-to-Host:** Server—any Web server on any operating system. Browser—Internet Explorer®, Firefox, Opera and third-party java-enabled browser
- **Terminal Services:** Windows Server 2008/2003 Terminal Services and Citrix® XenApp™ for Windows platforms
- **Minimum CPU requirements:** Pentium 4

### Supported software

- Exceed PowerSuite 14, Exceed 14, Open Text NFS Client 14, HostExplorer 14, other Open Text Connectivity Solutions or third-party software (restrictions may apply)

### General Information

<table>
<thead>
<tr>
<th>SSL-LIPKEY</th>
<th>Kerberos</th>
<th>Secure Shell</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Function</td>
<td>SSL v2/v3 &amp; TLS client LIPKEY</td>
<td>Kerberos v4/v5 client</td>
</tr>
<tr>
<td>Applicable Technology</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X11</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>VT</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>TN3270</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>TN5250</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Applicable Product</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exceed PowerSuite™</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Exceed</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Open Text NFS Client</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>HostExplorer</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>