



# SSH G3™ - Third Generation Secure Shell Implementation

*White Paper*

*August 2006*

*This document introduces the third generation, high-performance Secure Shell (SecSh) protocol implementation SSH G3™ designed to overcome the processing bottlenecks in securing throughput-intensive file transfers and large-scale business-application connectivity. The protocol architecture, its features, and encryption performance data are provided in the document.*

## BACKGROUND

### Three Generations of Secure Shell

Secure Shell is the standard protocol used by millions worldwide for remote login, remote command execution, and file transfer over TCP/IP networks. The Secure Shell protocol was originally developed in 1995 by Tatu Ylönen. To respond to the growing demand for protocol enhancements and new product features, Mr. Ylönen founded SSH Communications Security. The original protocol code also laid foundation on the later open-source development of OpenSSH by the OpenBSD community.

To overcome the limitations and security vulnerabilities of the original SSH1 protocol, SSH Communications Security decided to re-write the protocol specifications. The new, more functional and secure protocol version (SSH2) was also submitted to the IETF SecSh working group for standardization. Later in 1998, SSH Communications Security released products incorporating the new SSH2 protocol code. The second generation was born.

In 2005, 10 years since the invention of SSH1, SSH Communications Security continued to lead the development of the Secure Shell technology and introduced the third complete implementation of the Secure Shell protocol, the SSH G3™ architecture. SSH G3, based on and compatible with the standard SSH2, takes Secure Shell encryption performance to a new level, securing throughput-intensive file transfers and applications without causing processing bottlenecks.

The SSH Tectia™ client/server solution version 5 (and later) from SSH Communications Security incorporates the SSH G3 architecture.

### SSH Tectia Solution

SSH Tectia is the leading Secure-Shell-based end-to-end communications security solution for large enterprises, financial institutions, and government agencies. SSH Tectia provides secure system administration, secure file transfers

(SFTP and SCP), and secure application connectivity (Secure Shell tunneling).

The centralized management capabilities of SSH Tectia Manager support centralized deployment, maintenance, and monitoring of communications security, facilitating improved regulatory compliance and reduced total costs.

The SSH Tectia solution is available for a broad range of platforms including common Unix, Linux, Windows, and IBM mainframe operating systems. The FIPS 140-2 certification of the cryptographic libraries make SSH Tectia an ideal solution for even the most demanding government and enterprise environments.

For more information on SSH Tectia, please visit [www.tectia.com](http://www.tectia.com).



Figure 1 SSH Tectia has a modular product structure

## THE SSH G3™ ARCHITECTURE

### Introduction

The main driver for developing the SSH G3™ technology was to meet the growing requirements for encryption performance in throughput-intensive file transfers and large-scale use of application tunneling. The goal was to increase the protocol performance to a new level so that Secure Shell would not become a processing bottleneck even in the most demanding environments.

## SSH Communications Security

SSH G3 consists of a completely re-written Secure Shell protocol implementation with a new architecture and enhanced cryptographic algorithm support. It is important to note that only the implementation of the protocol is upgraded and the protocol itself is fully SSH2-compatible as defined by the SecSh working group of IETF.

The key performance improvements can be divided into:

- Improved protocol throughput enabled by a new optimized architecture
- Enhanced connection scalability with highly optimized memory consumption
- Improved encryption and data authentication performance with the use of the CryptiCore® algorithm (optional).

Other improvements include plugin support for easy integration of new encryption and authentication modules.

The new SSH G3 architecture is a part of the SSH Tectia client/server solution version 5 (and later) distributions.

### Connection Broker

One of the biggest architecture-level changes in SSH G3 is the introduction of a component called the *Connection Broker*. The Connection Broker is a common component for all client-side Secure Shell programs. Unlike in the second-generation Secure Shell implementations, the client-side Secure Shell programs based on SSH G3 do not incorporate the protocol code in them. Instead, they request channels from the Connection Broker, which implements the Secure Shell protocol functionality and all cryptographic operations.

The key feature of the new Connection-Broker-based architecture is the need to have only a single Connection Broker instance running per session. The main benefit of handling all client-side connections from a single point is to avoid replication of code and policies resulting in ease of use and reduced memory consumption. For example, all clients, including Windows clients with GUI (SSH Tectia Client and

Connector), and command-line tools can share the same configuration file and settings.

Security is also further improved by isolating all security-critical operations including authentication data handling in a single component. Additionally, the Connection Broker enables easy integration of Secure Shell functionality to client applications without the need to integrate the whole protocol stack to each application.

### Server-Side Throughput

As improved throughput is one of the main objectives for the new protocol implementation, special attention was given to code paths that involve processing the Secure Shell channel data and the actual payload. For example, the number of data copy operations in that code has been reduced to absolute minimum to minimize the throughput time.

The new Secure Shell server architecture in SSH G3 is also multi-threaded making it possible to fully leverage multi-processor servers for better performance.

### Server-Side Scalability

SSH G3 implements an *n x m server process architecture* for optimized server-side memory consumption and performance.

Most other Secure Shell server implementations always create a new server-side process when a new connection is established to the server. For example, in secure application connectivity (tunneling) this leads to a large number of server-processes, each used for running a single tunnel. As a consequence, the memory usage becomes inefficient.

In the new *n x m server process architecture* there are always  $n + 1$  server processes running: one *master server* distributes the connections to  $n$  *servant servers*. While each *servant server process* can handle a maximum of  $m$  concurrent connections, the maximum supported number of concurrent connections becomes  $n \times m$ . Depending on the environment and tunneled applications, this number can in practice be thousands.

## CryptiCore® Algorithm

SSH G3 architecture supports a broad range of encryption ciphers including 3DES and AES. Additionally, the algorithm support has now been expanded to include CryptiCore® encryption for an extra boost in encryption performance on Intel-based platforms. The CryptiCore encryption and data authentication technology, developed by a Danish data security company Cryptico, is software-based and fully processor optimized to offer a significantly higher speed than other encryption and data authentication software.

The CryptiCore encryption is based on the Rabbit stream cipher, which has been presented at leading international conferences and endorsed by experts in the field.

While all performance-specific Secure Shell protocol improvements can be experienced with all supported ciphers including the FIPS 140-2 crypto, using CryptiCore brings further throughput improvements and is well suited for data-intensive environments (see the next chapter for quantitative performance data).

For more information on CryptiCore, please visit the Cryptico website at [www.cryptico.com](http://www.cryptico.com).

## Plugin Support

To facilitate easier integration of proprietary or rarely used cryptographic methods, SSH G3 implements a plugin-based architecture on both client and server sides. For example, ciphers, MACs, compression algorithms, key exchange algorithms, and new authentication methods can be integrated in the products as plugins. In fact, the same plugin mechanism has also been used for implementing the supported built-in cryptographic algorithms in SSH G3. The new plugin-based architecture makes it also easier to add support for crypto accelerators and other third-party crypto modules.

## PERFORMANCE DATA

The following Secure Shell tests compare tunneling and secure file transfer performance between OpenSSH 4.1 and SSH Tectia™ client/server solution 5.0.

All the tests were performed in a 1Gb Ethernet Lab-Network on MS-Windows and Enterprise RedHat operating systems running on Intel Xeon x86 processor architecture. The hosts were loaded with 4 Gbyte of RAM memory and 3.0GHz Intel dual Xeon processors.

The tests have been run with similar hardware using AES128 cipher and MD5 HMAC.

In addition, performance tests have been run with the CryptiCore cipher and HMAC (based on the Rabbit stream cipher). Note that the CryptiCore cipher is currently optimized and available only for Intel x86 processor platforms.

### Linux to Linux Tunneling (AES128-MD5 vs. CRYPTICORE128-CRYPTICORE128)

Compared product	Throughput Mbit/s	Increase compared to slowest
OpenSSH 4.1	286	-
SSH Tectia client/server solution 5.0	<b>306</b>	<b>+ 7%</b>
SSH Tectia client/server solution 5.0 cc128-ccmac	<b>723</b>	<b>+ 153%</b>

## SSH Communications Security

### Linux to Linux File Transfer (AES128-MD5 vs. CRYPTICORE128-CRYPTICORE128)

Compared product	Throughput Mbit/s	Increase compared to slowest
OpenSSH 4.1	210	-
SSH Tectia client/server solution 5.0	<b>250</b>	<b>+ 19%</b>
SSH Tectia client/server solution 5.0 cc128-ccmac	<b>400</b>	<b>+ 90%</b>

### Windows to Windows Secure Shell File Transfer (AES128-MD5 vs. CRYPTICORE128-CRYPTICORE128)

Test results for OpenSSH on Windows to Windows data transfer cannot be provided here since there is no OpenSSH server available for MS Windows.

Compared product	Throughput Mbit/s	Increase compared to slowest
OpenSSH 4.1	N/A	-
SSH Tectia client/server solution 5.0	<b>220</b>	-
SSH Tectia client/server solution 5.0 cc128-ccmac	<b>300</b>	<b>+ 36%</b>

Designed to address the critical performance requirements of large file transfers, large-scale tunneling, and other throughput-intensive Secure Shell uses, the new SSH G3 architecture provides accelerated encryption throughput and scalability. SSH G3 is a completely new implementation of the standard Secure Shell (version 2) protocol as defined by the IETF.

SSH G3 introduces multiple new architecture-level changes and features including Connection Broker, n x m server architecture, optimized use of multi-processor capability, and optional CryptiCore algorithm support for extra encryption throughput. The whole new architecture combined with multiple smaller optimizations, make SSH Tectia an ideal communications security solution for even the largest and most demanding network environments.

Depending on the network set-up and ciphers in use, the throughput improvement in data transfer with SSH G3 compared to other implementations can reach even more than 150% in demanding tunneling applications.

## SUMMARY

SSH Communications Security, the original developer of Secure Shell and the leading provider of end-to-end communications security solutions, has introduced the next generation of Secure Shell implementations with its new SSH G3 technology.