



Banking & Finance Institute
**Secures Mainframe
Communications**

Customer's info

Industry: Financial Services

Size: 10,000+ employees

Region: Australia

Number of LPARs: 15+

Many banks are using IBM's Mainframe as their core operating system to retain control over security, transaction efficiency and data transmission. Though the emerge of new technologies like big data and faster networks are attempting to be the game changer, re-platforming would be a costly, disruptive and risky path, and the reliability and security nature of Mainframe, have kept itself as the best system for routine time-critical operations

Hence, an important Australian Bank and financial services provider decided to upgrade its solution and render its File Transfer Protocol (FTP) thus c-ached and become SFTP (Secure File Transfer) to send sensitive financial information, within the Mainframe architecture



Security Comes First

Security is a non-negotiable issue for the Bank. While the IBM Mainframe hosts multiple z/OS systems, it needs to keep its data-in-transit during credit card usage, management of investment capital as well as ATM functions, encrypted and secure. And more, the new server must be capable of daily and automatic transmission of huge amount of files and cannot afford any system downtime: a customer unable to check a balance or withdraw money from the ATM will, potentially, change banks

Tectia® SSH Server for IBM z/OS

The Bank decided to choose Tectia® SSH Server for IBM z/OS solution for securing file transfers, for several various reasons. The feature of complying with FIPS-certified cryptography regulations and PKI support with X.509 certificates, has enabled Tectia z/OS to automatically encrypt any transparent data-in-transit, including user ID and password. Further, there was no downtime during installation, providing a reliable and simple solution to encrypt FTP to the required SFTP, under Mainframe.

If IBM Crypto Express Card (CEX) is installed, the Tectia z/OS can direct or offload cipher functions to the co-processors in CEX via ICSF, helping to reduce CPU usage, accelerating of cryptographic operations within the hardware environment, and in turn, increase energy efficiencies. It also meets any internal and external compliance requirements including PCI DSS, SOX, HIPAA, FIPS, FISMA, and many others, thus suitable for organizations of all types and sizes.



The firewall-friendly architecture in Tectia z/OS takes a further step to empower the server. Whereas FTP requires two firewall ports, the SFTP feature in Tectia/OS needs only one, offering a cost-saving infrastructure in long run.

When it comes to business continuity and maintenance, Tectia/SSH offers platform support and updates for all its servers running on Unix, Linux or Windows. That's why it is trusted by 4/5 of the world's banks and 40% of Fortune 500 companies

The whole deployment of Tectia z/OS took only 18 weeks, and it works perfectly and seamlessly with Mainframe without the need of a system shutdown or start-up. As the customer commented:

“We have looked at different solutions on the market, but we found Tectia z/OS remains the simplest and most direct answer to our problems.”



Finland

SSH Communication Security Oyj
Karvaamokuja 2 B 00380 Helsinki
www.ssh.com
+358 20 500 7000
info.fi@ssh.com

USA

SSH Communication Security, INC.
434 W 33rd Street, Suite 842
New York, NY, 10001, USA
www.ssh.com
+1 781 247 2100
info.fi@ssh.com

Hong Kong

SSH Communication Security LTD.
35/F Central Plaza, 18 Harbour Road
Wan Chai
Hong Kong
www.ssh.com
+852 2593 1182
info.fi@ssh.com