CUSTOMER SPOTLIGHT

A Global Top 10 Bank

Bloombase® Spitfire SOA™ Security Server

Bloombase® Spitfire StoreSafe™ Storage Security Server

Bloombase® Spitfire KeyCastle™ Key Management Server

Bloombase® Spitfire™ High Availability Module

A global top 10 bank operates more than 12,000 branches worldwide. Their core banking systems support a wide range of users including tellers and back office internal staff for mission critical services including fund transfer, bill settlement, inter-bank wire transfer, automatic payment, card payment, credit analysis, and customer services, etc. They successfully implemented Bloombase Spitfire security servers. The end result is the assurance of confidentiality, integrity and authenticity of message interchange, data warehouse and disaster recovery infrastructure meeting various stringent in-house, state and industry information security regulatory standards including Payment Card Industry Data Security Standard (PCI DSS).

AT A GLANCE

ABOUT THE CUSTOMER

- Global top 10 bank
- Number of branches: More than 12,000
- Employees: More than 250,000

SUMMARY

To protect intra-bank and payment card transactions in form of XML-based SOA data-in-flight from being tapped or tampered over the wire traversed through virtual private network via the Internet and to secure database and backup data-at-rest from unauthorized exposure as a result of hardware or media theft

KEY CHALLENGES

- A single and total solution for SOA information security, database encryption, backup protection, and full life cycle key management
- Immediate compliance to various information security regulatory standards especially Payment Card Industry Data Security Standard (PCI DSS)
- OASIS ebXML and W3C XML digital signature and cryptography compliant
- High throughput XML transaction security processing
- Gigabyte-XML transaction security batch processing
- Online database on-the-fly encryption and decryption
- Backup archives are protected from exposure and alteration
- No key exchange allowed and automatic key revocation is supported
- No change to end user, administrator and operator workflow
- Mission critical and fault-tolerant
- Interoperable with real-time data replication services for storage synchronization

OVERVIEW

A global bank operates its extensive network of over 12,000 branches all over the world in more than 20 countries, inter-connects distributed computing infrastructure in every single branch for electronic data exchange supporting their business operations including teller services, customer services, fund transfer, inter-bank transfer, merchant transaction settlement, automated payment, credit analysis, etc. The customer used to rely on proprietary value-added network (VAN), a high cost dedicated private communications network to enable transaction information exchange which contain vast amount of highly sensitive and confidential data that can never be known to outsiders or at worst, be altered. Each and individual branch office has its local database storing confidential customer data for uninterrupted operations and business continuity in event of network outage. There it also preserves a staging area for batch transactions containing highly sensitive monetary information that are yet to be settled and synchronized with headquarters' central clearing system after hours.

To cope with the growth of transactions, higher service availability requirements and lower total cost

PROJECT OBJECTIVES

- Secures confidentiality, authenticity and integrity of bank transactions in form of XML and/or proprietary flat file EDI-like data
- Protects privacy of confidential customer data stored in relational database systems
- Protects backup media and hardware from unauthorized exposure and alteration of sensitive archives
- Automated and full life cycle key management
- Achieves compliance to various information security regulatory standards including PCI DSS

SOLUTIONS AND SERVICES

- Spitfire SOA™ security server
- Spitfire StoreSafe™ enterprise storage security server
- Spitfire KeyCastle™ Payment Systems security server
- Spitfire KeyCastle™ key management server
- Spitfire High Availability Module

WHY BLOOMBASE SOLUTIONS

- Highly secure and industry standard based
- High performance, high throughput and low latency
- Capable of handling extremely large data payloads and huge volume of database data
- Proven and mission critical ready
- Hardware, platform and software interoperability and portability
- Able to scale with hardware and platform resources for future growth
- Transparent operation and administration
- Complete segregation of data ownership and operation
- Wire-speed automated encryption, decryption, signature generation and verification

of ownership (TCO), customer is planning for a change of network carrier from dedicated VAN to the Internet. However, multi-routing and cost saving as benefits of Internet bring in higher chance of attacks and thereby, vulnerabilities of information. Traditional link encryptors and virtual private network (VPN) have been put into consideration to enhance information privacy and integrity against outsider/ trespasser attacks, however, such measures are easily defeated by core attacks at network encryption end-points. As network-based protection is insufficient, customer turns to defense in-depth application layer data protection measures which can effectively secure confidentiality, authenticity and integrity of transaction information sent over the wire, plus persistent data protection securing sensitive database and backup information from unauthorized exposure and tamper.

On drawing up a total solution, customer's IT security team discovered a number of major design flaws that can hardly overcome with existing technologies and products they have in hand, if not properly addressed, it makes no difference than without a single protection at all. First major problem is the management, secure trusted exchange and revocation of large number of cryptographic keys on every branch nodes. Second, the proposed proprietary delimited flat-file data encryption format is hardly extensible for future expansion in data fields and message types. Third, available enterprise grade data cryptography libraries all made no success to process batch transactions of volume in order of hundreds of megabytes to gigabytes. Last but not least, database and backup encryption utilities all require significant change to platform, software and application which are not accepted.

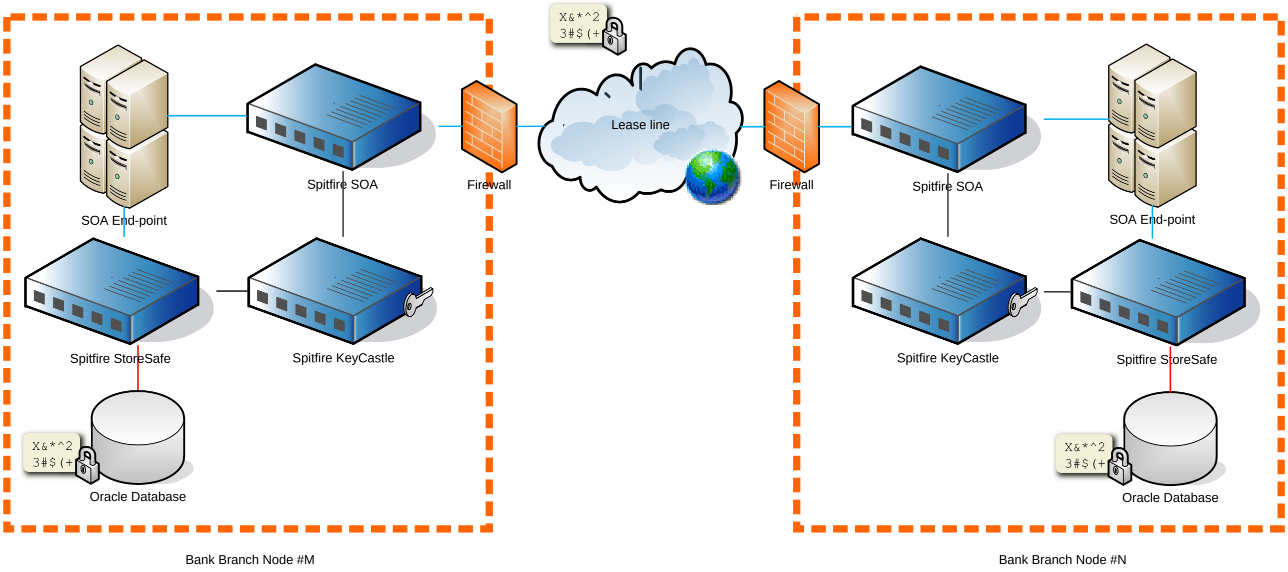
End customer eventually turned to Bloombase for their Spitfire information security server platform to achieve end-to-end data protection at full transparency and infinite scalability. Bloombase Spitfire SOA Security Server assures confidentiality, integrity and authenticity of transaction messages by state-of-the-art cryptography and digital signature technologies. Transparent encryption of database, files and backup media are achieved without application change by use of Bloombase Spitfire StoreSafe Storage Security Server. Spitfire KeyCastle Key Management Server protects encryption keys and offers centralized full life-cycle management.

HIGHLY SECURE INTRA-BANK AND INTER-BANK INFORMATION INTERCHANGE

To comply with end customer's information privacy requirements on data-in-flight protection, Bloombase Spitfire SOA Security Server protects XML and flat-file message payloads encapsulated in OASIS ebXML compliant message envelopes by encryption and digital signature. Bloombase Spitfire SOA Security Server supports operation in pass-through mode which appears as an SOA end-point proxy or look-aside mode for SOA end-point's remote invocation. Spitfire SOA Security Server secures SOA payloads transparently based on predefined rules configured in its rule-based security processing engine.

An outgoing bank transaction message produced at an SOA endpoint is intercepted at Spitfire SOA Security Server where confidential payload is first encrypted by recipients' keys, later signed by sender's private key. The secured ebXML envelope traverses through the VPN where sniffers have no way of obtaining the private information prior encrypted by Spitfire SOA Security Server. As the message enters recipient, Spitfire SOA Security Server acting as recipient end-point proxy to authenticate message sender identity and integrity by examining authenticity of its digital signature. Once it is verified valid, Spitfire SOA Security Server decrypts the ciphered payload contents automatically before plain original electronic transaction message is presented to the actual recipient SOA service end-point, follow by actual business application processing. Thus, message privacy, content integrity and source identity for data exchange among branches can well be guaranteed.

Unlike traditional data cryptographic libraries, Spitfire SOA Security Server is a purpose-built highly



threaded server capable of handling huge payload data of gigabyte sizes or above, and large amount of concurrent message requests at one time, enabling customer to support their real time online business operations and resource intensive offline batch processing needs.

With Bloombase Spitfire KeyCastle Key Management Server, customer enjoys centralized management of encryption keys. No more cumbersome insecure key exchange, Spitfire KeyCastle is designed and built using public key infrastructure (PKI) technology which requires no need of shared secrets providing true privacy of secret keys and establishing trust and key validity on individual nodes. The end result to customer is simplified management yet increased security on key management.

> **"Bloombase Spitfire™ enterprise security platform brings together data in-flight protection, data at-rest encryption and key management in a single solution at high return on investment**

PERSISTENT DATA — SECURE AND SAFE

Enter persistent data protection, customer deployed Bloombase Spitfire StoreSafe Storage Security Servers to secure their Oracle database, file system and backup archives. Bloombase Spitfire StoreSafe Storage Security Server features storage block device and disk proxy, which virtualizes actual database storage and backup tape devices for database servers and backup agents to access as if they are plain persistent data. Spitfire StoreSafe leverages cryptographic technologies on enterprise storage communication infrastructure providing virtual disks for encryption of confidential information on write operations, whereas automatic decryption of ciphered sensitive data on storage reads.

Confidential bank transactions and customer data are stored encrypted naturally on physical disks, tapes and virtual tape libraries (VTL), administrators, operators and intruders have no way of accessing the plain secret information persisted. Customer is assured in worst case scenario storage media are taken or if any occasion of hardware theft, confidential information remain secret and private meeting industry and their internal information security requirements.

Spitfire StoreSafe virtual storage enables ease of deployment and transparent operation requiring zero change to database system and backup infrastructure. No application change is needed, customer saves second development efforts and is assured minimum impact to existing computing services, the outcome is an efficient and more secure banking system.

All in all, information privacy and integrity is improved with higher level of trust to information in-flight and at-rest without deteriorating user satisfaction and operational efficiency, helping customer achieve goals of cost saving, service enhancement, client confidence, effective risk management and preparing for the next level of business development.

FOR MORE INFORMATION

To learn more about Bloombase information security solutions for banking and financial services institutions, contact your Bloombase sales representative, or visit:

www.bloombase.com

IMPLEMENTATION HIGHLIGHTS

A true end-to-end secure and super-scale message interchange and data warehouse system fully committed to Bloombase Spitfire security platform

KEY BENEFITS

- Fully transparent information privacy, integrity and authenticity for both data in-flight and at-rest
- Truly secure and total key management
- Highly available and fault-tolerant
- High encryption performance
- Immediate and risk-free information security standards compliance

HARDWARE

- IBM p-Series
- IBM z-Series
- IBM i-Series
- Egenera BladeFrame

OPERATING SYSTEM

- IBM AIX 5.3
- IBM z/OS
- IBM i5/OS
- Sun Solaris 10
- Red Hat Enterprise Linux
- Microsoft Windows Server 2003

SOFTWARE

- Oracle Database
- IBM DB2
- IBM WebSphere
- BEA WebLogic

The information contained herein is subject to change without notice. The only warranties for Bloombase products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Bloombase shall not be liable for technical or editorial errors or omissions contained herein.

12/2007