CUSTOMER SPOTLIGHT

A Tokyo Stock Exchange Listed Financial Institution

Bloombase® Spitfire StoreSafe™ Storage Security Server

Bloombase® Spitfire KeyCastle™ Key Management Server

Bloombase® Spitfire™ High Availability Module

Japan Personal Information Protection Act (PIPA) came into effect on 1 April 2005 and imposes very strict regulations on Japanese companies. A Japanese financial institution managed to overcome the pressures in getting their distributed storage sub-systems protected by using Bloombase® Spitfire StoreSafe™ storage encryption solution achieving highly available fault-tolerant data services at low costs and most importantly, customer information remain secret and safe.

AT A GLANCE

ABOUT THE CUSTOMER

- Financial institution listed on Tokyo Stock Exchange
- Employees: More than 6,000

SUMMARY

To protect customer personal information as mandated by Japan Personal Information Protection Act (PIPA) in production and disaster recovery (DR) storage sub-systems in Tokyo and Osaka respectively

KEY CHALLENGES

- No change to end user, administrator and operator workflow
- Support Microsoft Active Directory
- Sensitive information are physically stored encrypted at all times and no physical plain originals and copies are allowed
- Operators at disaster recovery (DR) data center have no way of obtaining the stored data
- Backup archives are to be encrypted also
- Support transparent data service failover
- Interoperable with real-time data replication services for storage synchronization
- High performance encryption and decryption

OVERVIEW

A Tokyo Stock Exchange listed financial institution hosted a primary core business data center at Tokyo and a disaster recovery (DR) center at Osaka privately connected via a wide area lease line, supporting over 6,000 employees in various cities in Japan. The core system supporting their daily business operation includes a customer record and inquiry sub-system in which customer name, social identity, bank account information, transaction history, credit information are stored.

The primary customer database system, housing over 1 million customer records of total volume exceeding 1 terabyte, located at Tokyo is configured to replicate to their DR center at real time, such that in worst case scenario when primary data center is unavailable, DR system takes over and fulfills business continuity requirements.

According to Japan Personal Information Protection Act (PIPA) came into effect on 1 April 2005, any company, referred as Personal Information Handlers (PIH) which utilizes a database of more than 5,000 individuals' personal information for conducting business which personal information or personal data means any information regarding an individual, have to be protected and kept secret.

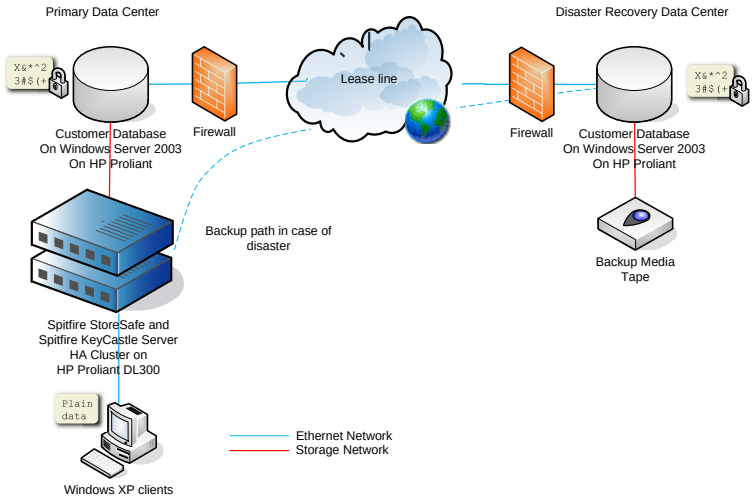
A PIH must comply with a number of restrictions on how to handle personal data including limitation of provision of personal data to third parties, disclosure, correction and suspension of usage of retained personal data, etc. If ever an information leak found and not properly reported, the responsible officer of PIH may be subject to a maximum penalty of up to six months imprisonment or fine up to JPY

BLOOMBASE®

300,000.

In addition to PIPA, customer faced one more challenge in customer data privacy enforced by Financial Services Agency (FSA). The FSA guideline requires any financial institution to report any personal information leak and suggest measures to prevent recurrence of such incident.

The financial institution needs to secure itself, in the worst, customer information are lost, the embarrassing public announcements would affect their reputation, customer confidence and most important of all, stock prices, at the very least. Their DR data center is outsourced to third party facilities. How to protect private customer information from being seen by third party operators without limiting their access to system nursing and daily backup operations together add up to a challenging core data security project.



OPEN ACCESS, HIGH SECURITY

End customer longed for a backup data center out of Tokyo to ensure uninterrupted business operations in case of power, hardware failure or even attack, however, potential risks of customer data leak kept frustrating them. Customer required customer data to be synchronized at real time to DR site, not only information were encrypted in the network channel, but also on Microsoft Windows storage sub-systems on both centers. To aim high at information privacy and integrity, the solution still, had to enable operators at third party DR data center to execute daily backup, restore and storage allocation tasks transparently, as if no encryption had ever been in place.

Enter Bloombase Spitfire StoreSafe enterprise storage encryption solution, customer deployed Spitfire StoreSafe in a two-node cluster running with Spitfire High Availability (HA) option to guarantee fault tolerant real-time wire-line storage data encryption and decryption. Under normal scenario, Spitfire StoreSafe cluster acts as a storage proxy on customer database located at primary site at Tokyo, automating data cryptographic requests on demand, whereas updates on customer information traversed over a lease line applied on a backup storage sub-system at DR site located at Osaka. If ever there is data service failure at primary site, backup storage takes over to be accessed by Spitfire StoreSafe storage encryptors, enabling highly available data services.

FLEXIBILITY TO MEET USER NEEDS

As confidential customer data are stored encrypted naturally on physical disks, administrators and operators have no way of opening up the secrets without breaking the encryption, which is considered technically impossible. Spitfire StoreSafe encrypted customer data remain discrete files stored on Windows NTFS formatted disks supported by previously invested data replication and backup/restore utilities. No costly extra software investment, training and operation procedures needed.

End users access customer database as if no storage protection had ever been in place. Customer benefits from simplified user workflow during disaster recovery and they managed to minimize the down time from an hour to within 5 minutes.

FOR MORE INFORMATION

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

bloombase.com

PROJECT OBJECTIVES

- Protects privacy of confidential customer data stored in Windows file servers from prying eyes
- Encrypts backup archives to keep information secret and safe
- Encrypted storage data get replicated as of today

SOLUTIONS AND SERVICES

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

WHY BLOOMBASE SOLUTIONS

- Native support on Microsoft Windows 2003 Server platform
- Success cases in protection real time mission critical data storage systems in banking, financial and public sectors
- Ease of deployment
- Perfect segregation of data ownership and operation
- Wirespeed automatic encryption and decryption

IMPLEMENTATION HIGHLIGHTS

First customer to deploy Spitfire StoreSafe in high availability mode on a remote Windows file server over a wide area network (WAN) link

KEY BENEFITS

- Immediate compliance to PIPA
- Increases data availability and security
- No client user training required for third party data providers
- Highly available and fault-tolerant
- High encryption performance
- Transparent failover

HARDWARE

- HP Proliant DL320 series servers
- HP Proliant DL380 series servers

OPERATING SYSTEM

- Microsoft Windows Server 2003

4AA0-0838AAA 09/2007