



Bloombase Spitfire StoreSafe for Storage Replication Security Server

Security

IETF IPSec

IPv4 and IPv6 support

Encapsulating security payload (ESP) support

Authentication header (AH) support

Internet key exchange (IKE) support

Industry-proven cryptographic processing engine

NIST FIPS-197 AES encryption and decryption

Japan NTT/Mitsubishi Electric Camellia encryption and decryption

Chinese National SCB2(SM1), SSF33, SSF28 encryption and decryption

NIST FIPS-46-3 3DES and DES encryption and decryption

RC2, RC4, RC5 and RC6 encryption and decryption

CAST5 encryption and decryption

Twofish and Blowfish encryption and decryption

IDEA encryption and decryption

Serpent and Skipjack encryption and decryption

Pluggable cipher architecture for future cipher upgrade or custom cipher support

128, 256, 512, 1024 and 2048 bit public key cryptography

RSA and DSA public key cryptography

SHA-1, MD5 and Chinese National SCH(SM3) hash generation

Shared secret authentication

RSA signature authentication

Hardware ASIC cryptographic acceleration (optional)

Key Management

Manual keying or automatic keying
Diffie-Hellman key negotiation
Multiple certificate authority (CA) support
Hardware true random (optional) or software pseudo-random key generation, inquiry and deletion
Built-in certificate request and revocation check (CRL/OCSP)
X.509 and PKCS#12 DER and PEM key import and export
Key Usage Profiling
RDBMS and Generic LDAP Support and Integration
Industry Standard PKCS#11
NIST FIPS-140-1 level 2 cryptographic module support (optional)
Automatic Certificate Retrieval via HTTP or LDAP
Certificate Validity Check
Certificate Revocation Check via HTTP or LDAP
Certificate Revocation List (CRL)
Certificate Revocation List Distribution Point (CRLDP)
Online Certificate Status Protocol (OCSP)
CRL scheduled download, caching and automatic retry
OCSP scheduled request, caching and automatic retry

Hardware Security Module Support

Gemalto/Schlumberger/Axalto Cryptoflex
Gemalto/Schlumberger/Axalto Cyberflex
Gemalto/Schlumberger/Axalto e-gate
Gemalto/Gemplus GPK
Aladdin eToken PRO
Hifn Express DS cards
Sun Microsystems Crypto Accelerator cards
Siemens CardOS M4
IBM JCOP
Micardo
Oberthur 64k Java-card
OpenPGP 1.0 card
Setcos 4.4.1 cards
RSA SecurID 3100 cards
Giesecke & Devrient Starcos
Eutrom Cryptodensity IT-SEC
Rainbow iKey 3000

Standard Support and Certification

OASIS Key Management Interoperability Protocol (KMIP) support

NIST FIPS 140-2 compliant Bloombase Cryptographic Module

Management

Web based management console

Central administration and configuration

User security

Serial console

SNMP v1, v2c, v3

syslog, auto log rotation and auto archive

Heartbeat and keep alive

Disaster Recovery

Configurations backup and restore

FIPS-140 hardware security module recovery key or software recovery key vault for settings restoration

Customer-defined recovery quorum (e.g. 2 of 5)

FIPS-140 hardware security module operator key or operator pin for daily Spitfire KeyCastle operation

High-availability option for active-active or active-standby operation

Stateless active-standby failover

Platform Support

Bloombase SpitfireOS

Hardware Support

i386-base architecture

AMD 32 and 64 architecture

Intel Itanium-2 architecture

IBM Power6 architecture

UltraSPARC architecture

StrongARM architecture

System Requirements

System free memory 1GB

Free storage space 1GB

Warranty and Maintenance

Software maintenance and support services are available.



Bloombase Technologies - Information Security Company

email info@bloombase.com

web <http://www.bloombase.com>

Bloombase, Spitfire, Keyparc, StoreSafe, and other Bloombase products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Bloombase Technologies Ltd in Hong Kong, China and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies.

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.

Copyright 2008 Bloombase Technologies. All rights reserved.

Specification Sheet
H87998

www.bloombase.com