



Bloombase Spitfire KeyCastle Payment Systems Security Server

Features

Rich Cryptographic Support for Payment Systems

Bloombase Spitfire KeyCastle Payment Systems Security Server provides unrivaled industry standard-based protection for payment system and various banking and financial service institution cryptographic keys, safeguarding valued electronic transactions.

Cryptographic Key Life-Cycle Management

Bloombase Spitfire KeyCastle Payment Systems Security Server supports key generation, storage and protection, and is equipped with rich cryptographic cipher algorithms for enterprises and organizations meeting stringent information security compliance standards.

Tamper-proof and Tamper-resistant

Bloombase Spitfire KeyCastle Payment Systems Security Server is built based on NIST FIPS 140-2 validated Bloombase Cryptographic Module and supports large variety of tamper-proof and tamper-resistant hardware security modules (optional).

High Performance

Cryptographic processing can further improve with optional PKCS#11 hardware cryptographic acceleration modules to minimize performance impact to your mission-critical systems.

Security

NIST FIPS 197 AES encryption and decryption (NIST certificate #1041)

RSA public key cryptography (NIST certificate #496)

SHA-1, SHA-256, SHA-384, SHA-512 hash generation (NIST certificate #991)

Proven keyed-hash message authentication code generation (NIST certificate #583)

Proven random number generator (NIST certificate #591)

Japan NTT/Mitsubishi 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

DSA public key cryptography

MD5 and Chinese National SCH(SM3) hash generation

Pluggable cipher architecture for future cipher upgrade or custom cipher support

Hardware ASIC cryptographic acceleration (optional)

Payment Systems Cryptographic Support

ANSI X3.92 and X3.106 DES, two-key and three-key Triple-DES
ISO 10126-2 Banking Procedures for Message Encipherment, General Principles
ANSI X9.8, ISO 9564-1 and ISO 9564-2 Pin Management and Security
ANSI X9.9, ISO 8730 and ISO 8731 DES-MAC Message Authentication
ANSI X9.19, ISO 9807 and ISO 9797 3DES-MAC Message Authentication
ANSI X.24 Unique Key Per Transaction
Visa 3-D Secure Cardholder Authentication Verification Value (CAVV)
Visa CVV (Card Verification Value)
MasterCard CVC (Card Validation Code) and CVC2
American Express CSC (Card Security Code)
EMV Authorization Request Cryptogram (ARQC) Verification
EMV Authorization Response Cryptogram (ARPC) Generation
EMV Transaction Certificate/Application Authorization Cryptogram TC/AAC Generation

Payment Systems Pin Verification

IBM 3624
Visa PVV (Pin Verification Value)
Diebold
NCR

Payment Systems Pin Block Formats

ANSI X9.8-1982
PIN Pad
Diebold
Visa Derived Unique Key Per Transaction

Payment Systems Key Management

ANSI X9.17 Financial Institution Key Management (Wholesale) Standard
ANSI X9.24 Retail Financial Services Symmetric Key Management
ANSI X9.28
ANSI X9.52

Key Management

Multiple certificate authority (CA) support

Hardware true random (optional) or software pseudo-random key generation, inquiry and deletion

No limitation on number of cryptographic keys managed or scales with system storage infrastructure

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) compliant

IEEE 1619.3 Enterprise Key Management Infrastructure standard

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

Client Accessibility

PKCS#11
OpenSSL
Java JCA/JCE
Web services
Plain socket
HTTP/HTTPS
Java HTTP tunneling
Java Remote Method Invocation (RMI)
Native language support: C, C++, Java
PKI-based client authentication and identity management
PKI-based channel encryption

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
Solaris
HP-UX
OpenVMS
IBM AIX
Linux
Microsoft Windows
Mac OS X

Hardware Support

i386-base architecture

AMD 32 and 64 architecture

Intel Itanium-2 architecture

IBM Power6 architecture

PA-RISC architecture

UltraSPARC architecture

System Requirements

System free memory 512MB

Free storage space 512MB

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