



Bloombase KeyCastle Life-Cycle Key Management Security Server

Features

Life-Cycle Cryptographic Key Management

Bloombase KeyCastle 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.

Standards-based Key Management

Bloombase KeyCastle Security Server supports tamper-proof and tamper-resistant PKCS#11 Hardware Security Modules and OASIS KMIP-compatible key managers for central key management.

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 cipher algorithm support (NIST certificate #1041)

RSA public key cryptography (NIST certificate #496)

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

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

Japan NTT/Mitsubishi Camellia cipher algorithm support

Korean SEED and ARIA cipher algorithm support

GOST, Kalyna and SM4 cipher algorithm support

NIST FIPS 46-3 3DES and DES cipher algorithm support

RC2, RC4, RC5 and RC6 cipher algorithm support

CAST5 cipher algorithm support

Twofish and Blowfish cipher algorithm support

IDEA cipher algorithm support

Serpent and Skipjack cipher algorithm support

DSA public key cryptography

Pluggable cipher architecture for future cipher upgrade or custom cipher support

Hardware ASIC cryptographic acceleration (optional)

Key Generation

Accredited random number generator (NIST certificate #591)

ID Quantique Quantis true random number generator support (optional)

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 Hardware Security 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

Cavium NITROX XL

IBM Security Key Lifecycle Manager (SKLM) (formerly Tivoli Key Lifecycle Manager TKLM)

Micro Focus Atalla Enterprise Secure Key Manager (ESKM)

Thales keyAuthority

Thales nShield

Thales payShield

Oracle Sun Crypto Accelerator

Utimaco CryptoServer

Ultra Electronics AEP Keyper

PKCS#11 compliant hardware security modules

OASIS KMIP compliant key managers

Hardware Cryptographic Acceleration Support

Intel AES-NI

UltraSPARC cryptographic accelerator

Exar/Hifn Express DS cards

Standard Support and Certification

OASIS Key Management Interoperability Protocol (KMIP) compliant (optional)

NIST FIPS 140-2 compliant Bloombase Cryptographic Module

RSA PKCS#11 Cryptographic Token Interface Standard

Management

Web based management console

Central administration and configuration

User security

Command line interface console

SNMP v1, v2c, v3

syslog, auto log rotation and auto archive

Heartbeat and keep alive

Client Accessibility

PKCS#11

OASIS KMIP

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

High Availability

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

Stateless active-standby failover

Interoperable with Bloombase Quorum Server to mitigate split-brain scenarios (optional)

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 Bloombase KeyCastle operation

Operating System Support

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

Virtual Platform Support

VMware ESX/ESXi
VMware Server
Oracle VirtualBox
Citrix XenServer
Microsoft Hyper-V
Red Hat KVM

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 1GB
Free storage space 1GB

Warranty and Maintenance

Software maintenance and support services are available.

BLOOMBASE®

Bloombase - Next Generation Data Security

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, Inc. in United States, 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 2017 Bloombase, Inc. All rights reserved.

Specification Sheet
H87998