BLOOMBASE®

BLOOMBASE KEYCASTLE TECHNICAL SPECIFICATIONS

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 algorithms support

GOST, Kalyna and SM4 cipher algorithms support

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

RC2, RC4, RC5 and RC6 cipher algorithms support

CAST5 cipher algorithm support

Twofish and Blowfish cipher algorithms support

IDEA cipher algorithm support

Serpent and Skipjack cipher algorithms support

DSA public key cryptography

CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon, Sphincs+, BIKE, Classic McEliece, HQC, SIKE Post-quantum cryptographic (PQC) cipher algorithms support

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

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 Revocation Check via HTTP or LDAP

Certificate Revocation List (CRL), Certificate Revocation List Distribution Point (CRLDP), and Online Certificate Status Protocol (OCSP) support

Hardware Security Module and Key Manager Support

Futurex/VirtuCrypt

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

Marvell Cavium LiquidSecurity/NITROX XL

nCipher nShield

Oracle Sun Crypto Accelerator

Thales payShield

Thales Gemalto SafeNet KeySecure

Thales Gemalto SafeNet Luna

Thales Vormetric DSM (formerly keyAuthority)

Ultra Electronics AEP Keyper

Utimaco CryptoServer

Utimaco Enterprise Secure Key Manager (ESKM) (formerly HP/HPE/Micro Focus Atalla)

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

Cloud Key Management Support

AWS CloudHSM

AWS Key Management Service (KMS)

Google Cloud HSM

Google Cloud Key Management Service (KMS)

IBM Cloud Key Protect

Microsoft Azure Key Vault

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 Access

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

Bloombase OS

Solaris

HP-UX

OpenVMS

IBM AIX

Linux

Red Hat Enterprise Linux (RHEL)

SUSE Linux Enterprise Server (SLES)

Microsoft Windows

Apple macOS

Server Processor Hardware Architecture Support

AMD64 architecture

Arm AArch32 and AArch64 architecture

Intel x86 and x86-64 architecture

Intel Itanium-2 architecture

IBM Power6 architecture

PA-RISC architecture

UltraSPARC architecture

Virtual Platform Support

VMware vSphere / ESX / ESXi

Oracle VirtualBox

Oracle VM Server

Citrix XenServer

Microsoft Hyper-V

Red Hat KVM

System Requirements

System free memory space 1GB

Free storage space 2GB

Warranty and Maintenance

Software maintenance and technical support services are available for subscription

Item No. BLBS-PROD-Bloombase-KeyCastle-Technical-Specifications-USLET-EN-R9