Specification Sheet

BLOOMBASE®

Bloombase Spitfire Message Security Server

Features

Transparent SMIME Implementation

Spitfire Messaging can integrate with corporate messaging systems to achieve higher level of email security using SMIME industry standard. Outgoing emails are digitally signed and encrypted protecting email contents during transmission and as persisted in recipient end. As soon as user requests to read an SMIME protected email, Spitfire Messaging checks for data integrity and readily decrypts data to be viewed by user

Email repository storage protection

Incoming and out-going plain emails are encrypted before reaching corporate groupware. Emails get persisted in storage in their encrypted form

Hardware and Platform Independent

Spitfire Messaging Security Server supports all hardware and operating system platforms.

High Availability

Highly scalable and multiple Spitfire Messaging boxes running in cluster for failover in mission-critical systems and load-balancing for high-throughput enterprise messaging systems.

Security

Simple Mail Transfer Protocol (SMTP) over secure sockets layer (SSL) or transport layer security (TLS)

SMTP authentication (SMTP-AUTH)

Message sender identity validation

Network-based message relay restriction

S/MIME encryption and decryption

S/MIME digital signature and verification

Industry-proven cryptographic processing engine

NIST FIPS-197 AES encryption and decryption

Japan NTT/Mitsubishi Electric Camellia encryption and decryption

Korean SEED and ARIA encryption and decryption

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

NIST FIPS-46-3 3DES encryption and decryption

CAST5, RC2 encryption

512/1024/2048-bit long X.509 asymmetric key

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

Messaging

Acts transparently as email proxy server

Supports X.400 Simple Mail Transfer Protocol (SMTP)

Supports messaging servers including Microsoft Exchange, Sun JES, IBM Lotus Notes, Sendmail, etc

Intelligent criteria based message filtering engine

High performance message processing routing engine

Network based message relay enabling/disabling email dispatch via Spitfire Messaging

Message Filtering Criteria

Attachment existence check

Attachment filename pattern check

Header existence and numeric comparison

Mail attribute and value pattern check

Sender address pattern check

Recipient address pattern check

Host and remote address and network check

S/MIME encrypted and/or signed part check

X.509 certificate subject check

Subject pattern check

Spammer blacklist and spam filter

Message size check

Recipient mailbox quota full check

Message Processing and Routing

Message header processing

Message footer processing

Regular expression based message content alteration

Header logging

Message counter

Message bounce

Message forward

Message redirect

Message resend

Message stealth delivery

Sender, postmaster and recipient notification

Local and remote delivery

Mail attribute modification

S/MIME encryption and decryption

S/MIME digital signing and verification

Hierarchical and stacking message router

Delivery status notice (DSN) bounce

Key Management

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 Protocal (OCSP)

CRL scheduled download, caching and automatic retry

OCSP scheduled request, caching and automatic retry

Hardware Security Module Support

AEP Networks Keyper

Oracle Sun Crypto Accelerator

Sophos Utimaco SafeGuard CryptoServer

Thales nShield

HP Atalla

IBM 4758 Cryptographic CoProcessor

IBM eServer Cryptographic Accelerator

IBM Crypto Express2

IBM CP Assist for Cryptographic Function

Cavium NITROX XL

Other PKCS#11 compliant hardware security modules

Hardware Cryptographic Acceleration Support

UltraSPARC cryptographic accelerator

Intel AES-NI

Exar/Hifn Express DS cards

High Availability and Clustering

Stateless active-standby failover

Stateful active-standby failover

Stateless active-active round-robin load-balancing

Stateful active-active round-robin load-balancing

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

Solaris

HP-UX

OpenVMS

IBM AIX

z/OS

AS400

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®

Bloombase - Transparent Data Security

email info@bloombase.com
web http://www.bloombase.com

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.