

## Bloombase Spitfire SOA Security Server



---

### Features

#### Rich XML and SOA Capabilities

XML proxy and firewall, XML parsing and filtering, secures EDI, EAI, SOA and Web Services (WS) data, schema validation, transforms and message routing

#### XML and WS Security

Rich and standard-based XML and WS security features including encryption, decryption, signature generation and verification

#### Hardware and Platform Independent

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

#### High Availability

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

---

### Applications

OASIS Security Assertion Markup Language (SAML)

Web Services Security (WSS)

Electronic Data Interchange (EDI) security

Enterprise Application Integration (EAI) security

Service Oriented Architecture (SOA) security

Visa 3-D Secure

Verified by Visa

MasterCard SecureCode

JCB International I/Secure

American Express SafeKey

Health Level Seven (HL7)

RosettaNet

---

## Security

W3C compliant enveloping, enveloped and detached XML signature generation and verification  
W3C compliant XML encryption and decryption  
PKCS#1 signature generation and verification  
PKCS#5 password-based encryption and decryption  
PKCS#7 signature generation and verification  
S/MIME encryption/decryption and signature generation  
PKCS#5 encryption/decryption  
Adobe Portable Document Format (PDF) signature generation and verification, encryption and decryption  
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  
DES, RC4, RC2, CAST5 encryption and decryption  
512, 1024 and 2048 bit public key cryptography  
RSA and DSA public key cryptography  
SHA-1, MD5 and Chinese National SCH(SM3) hash generation

---

## 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 Protocol (OCSP)  
CRL scheduled download, caching and automatic retry  
OCSP scheduled request, caching and automatic retry

---

## XML Features

Encryption

Decryption

Enveloping, enveloped and detached XML signature generation and verification

Transforms

Canonicalization

Web Services

SOAP

XML-RPC

XSLT/XML processing

XML schema validation

XPath

---

## Non-XML Features

PKCS#1 cryptography and digital signature

PKCS#7 cryptography and digital signature

Adobe PDF digital signature

---

## 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

---

## Accessibility

Web services  
Plain socket  
HTTP  
Java HTTP tunneling  
Java Remote Method Invocation (RMI)  
Native language support: C, C++, Java

---

## Portability, Scalability and Extensibility

Pluggable framework  
Configurable business logic and workflow  
User programmable

---

## 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 Technologies - Information Security Company

email [info@bloombase.com](mailto: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](http://www.bloombase.com)