BLOOMBASE®

BROCHURE

Bloombase Spitfire SOA

Enterprise SOA Security Server / Virtual Appliance

Electronic information exchange is everywhere in business world: bank transactions, brokerage clearance, customs declaration, purchasing, billing, workflow, and reporting, all relate to private and sensitive data that require high level of security handling. Latest proceedings in data interchange include ASC X12's CICA, FIN-XML for financial transactions, C-XML for diverse commercial transactions, UN-backed ebXML initiative, and XML/EDIFACT all are defining the next generation document format. One thing in common is extensible markup language (XML).

Web services is a next-wave enterprise-application-integration (EAI) technology for implementation of Service Oriented Architecture (SOA), again it is based on XML messaging. Digital communications made over the Internet risk data privacy and authenticity. There is no exception to XML data.

Bloombase Technologies develops and markets a complete basket of middleware solutions for corporations and governments. The flagship product Spitfire SOA Server is developed to tackle the security problem in data exchange. Imagine secret data are transmitted as plain over the insecure Internet, intruders tap important business data and alter contents, trespassers send transactional messages on behalf of another company, these lower confidence level of enterprises to e-commerce, introduce potential legal lawsuit and degrade corporate image. However, the biggest challenge to securing enterprise application integration is the requirement of application transparency and be least invasive to existing systems, at the same time not sacrificing performance and manageability.

Spitfire SOA Server speaks for itself to solve all above problems at low cost and high return-on-investment. Horizontally, the product has converging focus in XML, web services, enterprise application integration (EAI) and public key infrastructure (PKI) technologies including digital signing and verifying, encryption and decryption.

Vertically, it solves business document exchange security problems amongst government, financial institutions, logistics and e-commerce bodies. It is the fundamental and indispensable piece protecting e-commerce operations. Spitfire SOA Security Server plays key roles in enterprise message interchange/integration and value-added service for corporate and governmental applications which require bullet-proof security with concern at application transparency.

The industry started to have the initiatives to utilize XML as metadata storage and transmission standard years ago and only since recently specifications on e-commerce use were defined. XML and web services will rule enterprise message exchange in coming years if not now. While most people are concerning how enterprise applications can be integrated using XML/web services, platform neutrality, middleware connectivity, Bloombase Technologies already has the incentives to protect integration paths with state-of-the-art XML technologies and data cryptography.

Spitfire SOA Server is a secure electronic document platform built on public key infrastructure (PKI), extensible markup language (XML) and time-stamping technology . PKI can enhance level of assurance to user authentication, message authentication, data integrity and non-repudiation.

Spitfire SOA Server supports a large variety of document formats and international standards including

- PKCS#1
- PKCS#7
- Enveloping XML
- Enveloped XML
- Detached XML
- Secure MIME
- Adobe PDF

Plug-ins can easily be added to further enhance its document support.

Spitfire SOA Server is designed to be incorporated into core enterprise systems with concern at low cost, highly scalable, highly extensible and with rich features including digital signing services, signature verification services, key life cycle management services, certificate validation services, auditing services and time-stamping services. It is also equipped with logging and monitoring modules.

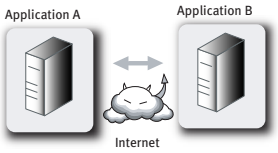
Spitfire SOA can be used in a broad range of real-world e-commerce applications such as

- Banking and securities trading systems
- Supply chain management systems
- Pharmaceutical and healthcare database protection
- Electronic contract and legal document management
- Online transaction and electronic data exchange
- Insurance systems

Risks with existing Enterprise Application Integration and Electronic Data Interchange

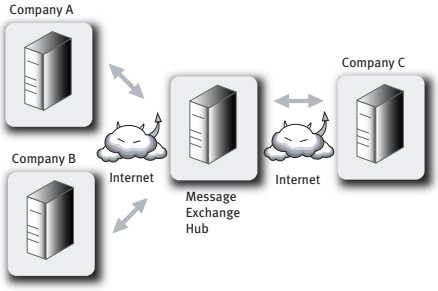
Enterprise Application Integration (EAI) nowadays faces a number of security threats

- EAI Remote Procedure Calls (RPC) sensitive contents are readable by Internet trespassers
- No way to identify if data transmitted are altered
- Lack of sender and recipient's proof of identity



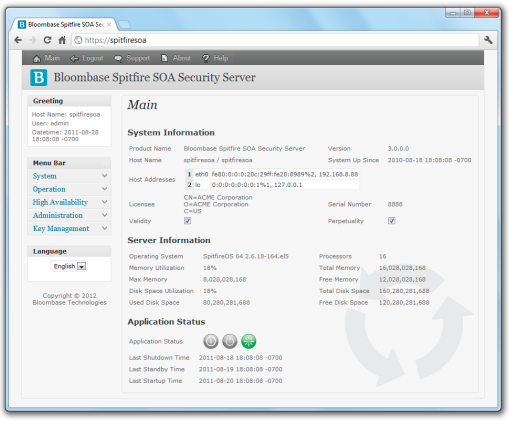
Electronic Data Interchange (EDI) nowadays faces a number of security threats

- EDI sensitive business data are in plain and readable by Internet trespassers
- Data transmitted are prone to unauthorized alterations
- Sender and recipient's identities are lack of legal support



Spitfire management console is a web-based application for administration, configuration and management of Spitfire modules as well as security data including keys and remote resource locations.

With simply a generic web browser with SSL support, administrators can configure resource location of key repository, cache profile and sizing, personalized look-and-feel, service registry and alter status of individual framework components.



Requiring no learning curve, Spitfire management console users can import X.509 digital certificates and PKCS#12 keystores, define revocation resource locations, specify certificate authority LDAP URLs, configure revocation preferences, inquire keys, examine logs, and generate reports.

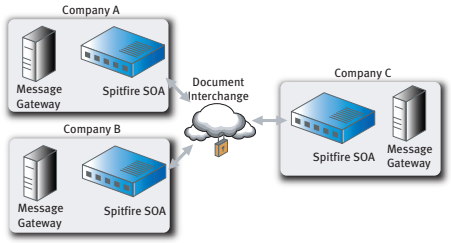
Spitfire SOA is built on Java technologies which is portable on virtually all enterprise platforms including Sun Solaris, HPUX, IBM AIX, Linux and Windows. Out-of-the-box client connectivity suite supports native languages including Java and C. Generic connectivity protocols including plain socket, HTTP and web services support heterogeneous language integration without sacrificing performance.

Spitfire SOA has well prepared for the most demanding application integration or messaging environments. It supports server cluster architecture. With optional Spitfire High-Availability (HA) component, it scales up easily and guarantees non-stop service for mission-critical applications.

Business Applications of Spitfire SOA Server

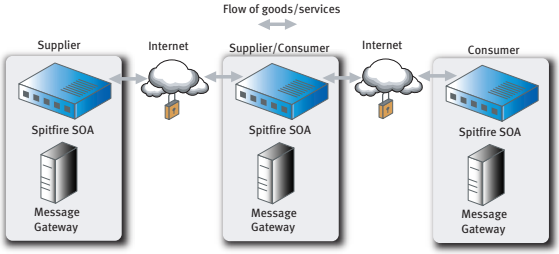
Interbank Transaction Clearing

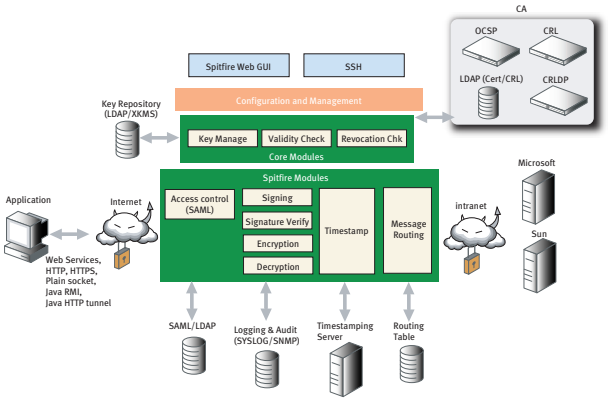
- Encryption protects sensitive financial data being exposed to general public, trespassers or hackers
- Digital signature on financial data ensuring data unaltered during transmission
- No two signatures are identical adding trust to sender identity



Supply Chain Management Data Exchange

- Hackers and trespassers see sensitive data as if garbage
- Recipients are confident received data are never tampered or altered
- Business partners have mutual trust on each other's identity and data sent or received





Technical Specifications Highlights

Feature Highlights

- XML Proxy - Firewall
- XML Parsing, Filtering and Schema Validation
- Encryption and Decryption
- Signature Generation and Verification
- Transforms
- Message Routing

Key Management

- X.509 and PKCS#12 DER and PEM Key Import and Export
- RDBMS and Generic LDAP Support and Integration
- Industry Standard PKCS#11 Support

Security Compliance

- NIST FIPS 140-2 validated
- Automatic Certificate Retrieval via HTTP and LDAP
- Certificate Validity Check
- Certificate Revocation Check via HTTP and LDAP - Certificate Revocation List (CRL), Certificate Revocation List Distribution Point (CRLDP), Online Certificate Status Protocal (OCSP)

XML Features

- Parsing and Well-form Validation
- Encryption and Decryption
- Signature Generation and Verification - Enveloping, Enveloped, and Detached
- Transforms and Canonicalization
- Web Services - SOAP, XML-RPC, XPath

Non-XML Features

- PKCS#1 Signature Support
- PKCS#7 Signature Support
- SMIME Signature Support
- PDF Signature Support

Management

- Web-based Central Management Console
- Serial Console
- SNMP (v1, v2, v3)
- syslog, audit trail and archive

Client Application Programming Interface (API)

- Web Services - SOAP, XML-RPC
- Plain Socket
- HTTP
- Java HTTP Tunneling
- Java Remote Method Invocation (RMI)
- Native Language Support - C/C++

Scalability and Extensibility

- J2EE Compliant Supporting Commercial Application Containers Including Sun Glassfish, Oracle WebLogic, Redhat JBoss, IBM WebSphere and Tomcat
- Broad Platform Support Including Sun Solaris, HPUX, IBM AIX, Linux and Windows
- Highly-Scalable
- Pluggable Framework
- High-Availability Support for Mission Critical Use

BLOOMBASE®