Bloombase
Least Invasive Security

Achieving SOA Security with Bloombase Least Invasive Security Solution

WHITE PAPER

Service Oriented Architecture (SOA) is an architectural style whose goal is to achieve loose coupling among interacting software agents. A service is a unit of work done by a service provider to achieve desired end results for a service consumer. Providers and consumers are roles played by software agents on behalf of their owners.

A typical example of SOA service in real -world application is balance inquiry. Client application residing in an enterprise, for example, an enterprise resource and planning (ERP) system requesting account balance from a bank balance check service remotely in another continent.

In enterprise ERP system's point of view, obtaining a balance is simply issuing a request and consuming the response returned from a service offered by the bank. On receipt of a request from client, bank balance inquiry service will have to go through complicated authentication, authorization, database access and other business logic checking before a balance value is obtained and sent back to the client. The public service exposed by the bank shields their clients from knowing the every details of the inquiry process. Clients are only interested in the end results (balance value) rather than the sophisticated steps to achieve the results.

The whole design concept of SOA relies heavily on the use of decoupled technologies and public interface for heterogeneous systems to inter-communicate. With recent trends in the use of XML in describing complex business data, it opens up its use in service oriented Web Services technologies.

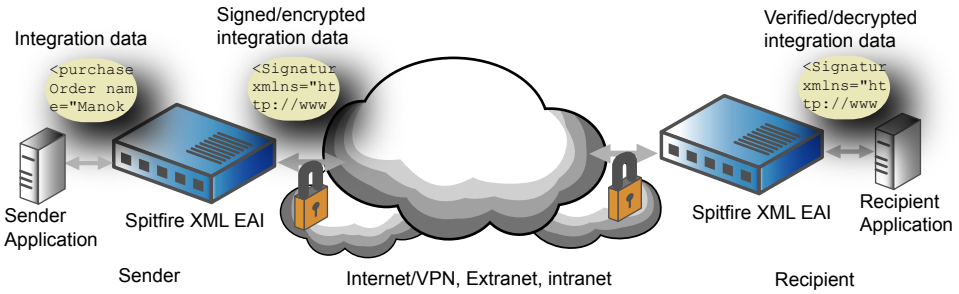
Web Services, as its name suggests, is built upon web/HTTP infrastructure in the entire request and response processes. To human beings, signing on an Internet banking website and clicking on the balance query button will retrieve the current bank balance from the bank's internal database. Similar to this, Web Services clients compose a remote procedural call (RPC) together with the parameters in form of an XML document, and submitted to the bank's service. Once bank's service interceptor receives the request, it goes through the detailed steps to obtain client's balance. The results, together with other check values are composed as an XML and returned to client.

Security Challenge

As depicted in example above, a bank inquiry service contains confidential and secret information which should not be made open to public and not to be altered during transmission

- User identity
- User credentials
- Bank account number
- Inquiry command
- Balance value
- Bank's remarks
- Return check value

W3C and Web Services Security defined standards to protect SOA data from prying eyes and unauthorized alteration. XML and web services security recommend the use of strong encryption and digital signature to achieve information confidentiality and integrity. However, to business systems including ERP, finance and banking, XML processing is too resource intensive and complicated to fit in immediately. The industry needs a standalone and high performance SOA security system to offload the security tasks and at the same time be able to deploy without affecting existing infrastructure.



Bloombase Solution

Bloombase created Spitfire XML EAI as a standalone hardware to address the emerging security needs of enterprises having SOA practice. Spitfire XML EAI is a network attached cryptographic box to secure SOA data by digital signature and strong encryption. Digital signature provides evidence on potential security threats including identity theft and unauthorized data alteration. Encryption bars hackers and crackers from obtaining the true contents of SOA information.

High Performance and Standards Compliance

Spitfire XML EAI is itself a hardware accelerated cryptographic appliance specifically designed for XML security processing. Spitfire XML EAI is built with concerns on processing large XML documents. Unlike other XML processing engines with maximum limit on XML document size, Spitfire XML EAI can process documents of any size.

Spitfire XML EAI is equipped with international cryptographic standards including PKCS#1, PKCS#5, PKCS#7, S/MIME, W3C enveloping XML, W3C enveloped XML and W3C detached XML, FIPS-197 AES, FIPS-46-3 3DES, DES, RC2, RC4, CAST, SHA-1, MD-5, RSA and DSA.

Hardened Architecture

Spitfire XML EAI appliance is built upon Bloombase's hardened SpitfireOS which is tamper -proof and purposely tuned for XML cryptographic use. The core Spitfire Security Platform is a highly flexable architecture that has prepared for future upgrades and customization. Customers can code their own cryptographic ciphers and load to Spitfire XML EAI via a user-friendly web-based administration interface to meet their inhouse security requirements.

Transparent Deployment and Operation

Spitfire XML EAI is a network-based appliance that gaurantees to get deployed within a day. Spitfire XML EAI offers industry standard interfaces including FTP, SMTP and HTTP for submission and reclamation of EAI messages which are readily supported by any messaging systems on any hardware /software platform.

Rich Connectivity

Spitfire XML EAI offers client connectivity package for customers with special need for more integrated connection to Spitfire XML EAI. Spitfire XML EAI client package supports languages including C, C++ and Java with broad OS platform support. For customers requiring integration in other languages, Spitfire XML EAI supports the lowest level plain socket communications for them to work directly with.

Bloombase
Least Invasive Security

Bloombase Technologies - Least Invasive Security **email** info@bloombase.com **web** bloombase.com