

WHITE PAPER

Electronic data interchange (EDI) 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 EDI include ASC X12's CICA, FIN-XML for financial transactions, C-XML for diverse commercial transactions, and XML/EDIFACT all are defining the next generation document format. One thing in common is the use of extensible markup language (XML).

XML is an infinitely extensible tree-structured format to model any business document in real world. XML supports localized language in specified regional encoding at the same time ready for internationalization in unicode encodings.

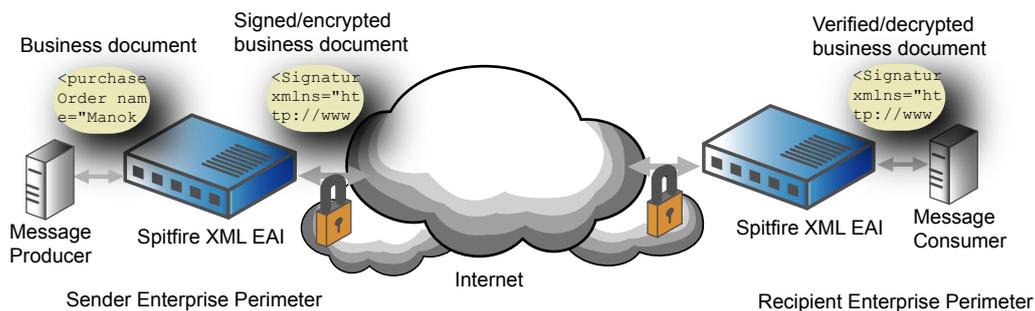
Security Challenge

Digital communications made over the Internet risk data privacy and authenticity. There is no exception to data carried by EDI messages. EDI messages contain sensitive and secret information including customer particulars and pricing information which should not be made to public and once the document is created, it should have legal binding and not be altered. Enterprises send or receive sensitive business data via EDI. Transient data in plain has to be protected from unauthorized tampering and ensure data integrity

EDI standard heavily relied on delimited plain texts to model business documents. Typical examples include X12 and EDIFACT. Protecting these plain texts from disclosure and alteration can be achieved by PKCS#1 standard which is of small footprint and normally is supported readily by EDI message exchange engines.

As EDI migrates to XML era, security becomes more technically difficult. XML follows a complex tree structure which require intensive resources to get processed. Adding digital signature and encryption to XML is a lot more than just processing a plain text message but parsing, well-form checking, validation, syntax verification, data extraction, hash generation and signature generation.

Latest XML-based EDI standards including ASC X12's CICA and XML/EDIFACT requires W3C and Oasis-Open standards for signature generation and encryption. Migrating a corporate EDI system to XML-based format is a costly and resource demanding task. Development of XML digital signature generation modules is not trivial and signature generation process itself is resource intensive that should not be embedded in business applications. How to control cost in EDI migration at the same time fulfilling security requirements is a challenge to all enterprises.



Bloombase Solution

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 flexible 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 guarantees to get deployed within a day. Spitfire XML EAI offers industry standard interfaces including FTP, SMTP and HTTP for submission and reclamation of EDI 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.